IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

MICROSOFT CORPORATION, a Washington corporation, Plaintiff, v. JOHN DOES 1-2, CONTROLLING A COMPUTER NETWORK AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS, Defendants.	 Civil Action No: 1:21-CV-1346 LMB/TCB **FILED UNDER SEAL PURSUANT TO LOCAL CIVIL RULE 5**

DECLARATION OF CHRISTOPHER COY IN SUPPORT OF MICROSOFT'S 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 Senior Investigator in the Digital Crimes Unit (DCU) of Microsoft Corporation's Corporate, External, and Legal Affairs Group. I make this declaration in support of Microsoft's application for an Emergency Ex Parte Temporary Restraining Order And Order To Show Cause Re Preliminary Injunction. I make this declaration of my own personal knowledge and, 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 technical security threats to Microsoft and the impact of such threats on Microsoft's business and customers, and I manage DCU's Cyber Threat Intelligence Program which includes cyber threat intelligence development and assessment, global partner management, and intelligence data sharing platforms. Prior to this role, I was a Senior Engineer, responsible for assessing quality and value of patents across a diverse set of technology areas in Microsoft's patent portfolio, and analyzing patent portfolios for acquisition, licensing, or litigation. Prior to that, while also employed by Microsoft, I worked as a Senior

Program Manager responsible for development of the corporate Security Development Lifecycle (SDL) security policy; and as a Software Design Engineer, I lead 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 Corp. 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 20 years as an Intelligence Officer and qualified Information Warfare Officer, attaining the rank of Commander. I am a graduate of the University of Kansas, Lawrence. I have been employed by Microsoft since March 1998.

I. OVERVIEW OF INVESTIGATION INTO NICKEL AND CONCLUSIONS

3. My declaration concerns an organization that is engaged in systematic criminal activity on the Internet. Because the identities of the individuals behind the activity addressed in this declaration are unknown, I therefore refer to them collectively by the codename that Microsoft has assigned to this group: "Nickel." Others in the security community who have researched this group of actors refer to the group by other names, including "KE3CHANG," "APT15," "Vixen Panda," "Royal APT," and "Playful Dragon." I have investigated the infrastructure described in this declaration and have determined that the defendants have registered Internet domains that are purportedly located in multiple cities and countries. Defendants have registered domains using functioning email addresses by which they communicated with domain registrars in order to complete the registration process.

4. Microsoft investigators have been monitoring and gathering information on the Nickel defendants. In the course of such investigation, I have been working with and directing a team that (1) engaged in the reverse engineering, analysis and creation of "signatures" (which can be thought of as digital fingerprints) for the infrastructure used by the Nickel defendants, (2) discovered unauthorized logins targeting Microsoft customers' accounts from Nickel-controlled infrastructure on the Internet, (3) observed sophisticated techniques to evade computer network defenses, (4) matched reported Nickel malware activities enabling further malicious campaigns to

registered domains, (5) monitored infrastructure frequently utilized by the Nickel defendants in order to identify domains being registered by the Nickel defendants, (6) monitored Nickel defendants activities in Microsoft 365 environments, and (7) reviewed peer findings and public reporting on the Nickel defendants.

5. As described in paragraph 4 (1), the investigative team has developed methods to help us identify new domains registered by the Nickel actors. Our investigation has determined that Nickel domains contain technical features used exclusively and specifically associated with the Nickel defendants. These features described more fully below, when identified in the aggregate, provide a high level of confidence that a given domain is a Nickel domain. Each such domain is manually reviewed in detail by one or more subject matter experts as necessary to ascertain whether it is, in fact, a Nickel domain. Based on this analysis, we have identified characteristics of the registration and maintenance of certain domains which, when coupled with the nature of the activities observed being carried out through the domains, are a reliable method to correlate such domains to actions undertaken by the defendants.

6. Based on our investigation and analysis, Microsoft has determined that Nickel specializes in targeting, penetration, and stealing sensitive information from high-value computer networks connected to the Internet. Nickel targets Microsoft customers in both the private and public sectors, including diplomatic organizations and missions in North America, Central America, South America, the Caribbean, Europe and Africa. For example, such organizations associated with the following countries have been targeted:

Region	**Countries**
Caribbean	Barbados, Jamaica, Trinidad and Tobago, Dominican Republic
Central and South America	Mexico, Panama, Guatemala, Honduras, El Salvador, Colombia, Brazil, Peru, Chile, Venezuela
Europe	United Kingdom, France, Italy, Switzerland, Montenegro, Portugal, Bosnia and Herzegovina, Croatia, Hungary, Bulgaria, Czech Republic
Africa	Mali

7. Nickel has targeted government employees, organizations and individuals working on a myriad of foreign diplomacy issues, think tanks, members of organizations that attempt to

maintain world peace, human rights organizations, as well as many other organizations and individuals. For example, attached as **Exhibit 1** is a true and correct copy of a research report by security research firm ESET regarding the Nickel group (which that firm refers to as "KE3CHANG").

8. The Nickel defendants' objective appears to be obtaining account credentials to later retrieve sensitive communications within the accounts. We believe that the Nickel defendants continue to pose a threat today and into the future.

II. NICKEL'S METHOD OF COMPROMISING AND STEALING INFORMATION FROM VICTIMS

9. The Nickel defendants are a sophisticated team of cybercriminals that employ a variety of techniques to compromise victim computers for the purpose of installing malware. The Nickel defendants have compromised third-party remote access solutions in order to further compromise Windows devices. For example, the defendants compromise third-party virtual private network ("VPN") appliances. Defendants also likely use spear phishing techniques to install malware on such victim computers. Through these and other means defendants establish backdoor capabilities to then surreptitiously gain control over a victim's infected computer. These backdoors, as described more thoroughly below, enable the Nickel defendants to connect that infected device to a command and control (C2) infrastructure and run commands manually to conduct further operations.[1]

10. The command and control computers send the most fundamental instructions, updates, and commands, and overall control of the Nickel defendants is carried out from these computers. Command and control computers include the servers at various domain names listed in **Exhibit 2** to this declaration (also attached as Appendix A to the complaint), which are described more fully below.

---

[1] Microsoft has already initiated the distribution of signatures to remediate the defendants' backdoor functionality on computers running the Windows operating system. But this legal action and the relief sought in this motion is necessary to cut off defendants' access to computers that remain compromised by the defendants

11. Each instance of malware disseminated by the Nickel defendants infecting a user's computing device is preprogrammed to connect and communicate with several of these 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. To create the command and control computers, the Nickel defendants set up accounts with web-hosting providers—i.e., companies, usually legitimate, that provide facilities where computers can be connected through connections to the Internet and locate their servers in those facilities.

12. In the course of our investigation, Microsoft has observed Nickel using exploits to gain access to internet networks to perpetuate their malicious scheme. For example, Nickel has used exploits to gain access to Microsoft Sharepoint and Microsoft Exchange. Specifically, the Nickel defendants have exploited several Microsoft Exchange vulnerabilities that enable the Nickel defendants to bypass the authentication, impersonate an arbitrary user, and write an arbitrary file to achieve remote code execution. Doing so enables the Nickel defendants to run arbitrary code to steal the full contents of several user mailboxes.

13. In addition, we and others in the security community have seen evidence of Nickel defendants attacking remote access solutions like Fortinet and Pulse Secure VPN devices, as reflected in a CISA advisory and reports by other security researchers.[2] This level of access furthers the Nickel defendants' infiltration within the victim device's network. In particular, we have seen evidence that the Nickel defendants are capable of moving laterally on the network. Lateral movement is a technique whereby threat actors systematically move through a network in search of data or assets to exfiltrate. After entering the network, the attacker maintains ongoing access by moving through the compromised environment and obtaining increased privileges using various tools.

14. Our investigation has further uncovered that, and as explained later in this

[2] *See* https://us-cert.cisa.gov/ncas/current-activity/2021/04/02/fbi-cisa-joint-advisory-exploitation-fortinet-fortios ; https://www.zdnet.com/article/many-organisations-dont-know-how-to-manage-vpn-security-properly-and-cyber-criminals-are-taking-advantage/ ; https://www.mandiant.com/resources/updates-on-chinese-apt-compromising-pulse-secure-vpn-devices

declaration, the Nickel defendants' malware is used to harvest credentials information. The Nickel defendants, after compromising an Exchange or SharePoint server using harvested credentials, are stealing the MachineKeys used by ASP[.]NET applications from the targeted system. ASP[.]NET is a developer platform made up of tools, programming languages, and libraries for building many different types of applications. ASP[.]NET extends the .NET developer platform with tools and libraries specifically for building web apps. The MachineKeys are used for encryption and authentication purposes and Microsoft understands that the Nickel defendants' exploitation of MachineKeys enables them to attempt to regain access to victim computers and networks even after the victim has remediated the prior malware instances.

15. Our investigation has led to additional evidence that identify the Nickel defendants' signature on a victim device. For example, the Nickel defendants' malware regularly deploys Nete[.]exe which is used for Microsoft Windows network reconnaissance. In addition, the Nickel defendants use NTDSDump[.]exe to exfiltrate information and passwords from the Windows Active Directory. The Nickel defendants also infiltrate a victim device and exfiltrate the victim's passwords to enable greater access to the victim's systems. Collectively, the activities we have observed are designed to enable the Nickel defendants to gain greater control of the victim device and avoid detection.

16. The Nickel defendants have been associated with several forms of backdoor malware to perpetuate their crime, including "Ketrican" and "Okrum." Once they have gained access to the victim device, Nickel defendants are able to distribute additional malware to continue their unlawful conduct, including Metushy, Mimikatz, MirageFox, Royal DNS, RoyalCli, and TidePool. In addition to public names Microsoft has seen Nickel malware under the following family names: Lesson, Neoichor, NullItch, NightImp, and Rokum. Critically, however, these malware executables are not readily visible to the victim computer. Instead, they execute code in Microsoft's Windows Registries to gain control of the victim device and exfiltrate information. But to the customer, Windows is operating normally.

17. After compromise, the Nickel defendants' initial conduct is to infiltrate the victim

system – at the registry level[3] – and collect information about the system, including the software and hardware data. This information enables the Nickel actors to strategically deploy custom malware and ultimately continue the operation. For example, once the Nickel defendants have infiltrated the victim system, our investigation has shown that the Nickel defendants exfiltrate spreadsheets, documents, local network data information, and harvest credentials. The Nickel defendants place this information into a password protected RAR archive folder for exfiltration. In addition, the Nickel defendants routinely search across the victim system and network to locate new files that may have been created since the previous exfiltration.

18. Nickel has been associated with a malware known as Okrum. Okrum features capabilities that enable it to impersonate the victim and gain administrator privileges. The malware contains commands allowing the Nickel defendants to download and upload files, execute binaries, or run shell commands.

19. Okrum malware creates a highly effective backdoor that negates normal authentication procedures to access a system and avoid normal security measures. As a result, malicious actors gain high lever user access (i.e., root access) on a computer system to resources within an application, such as databases and file servers, giving perpetrators the ability to remotely issue system commands and update malware.

20. The Okrum backdoor is a dynamic-link library that is installed and loaded by two earlier-stage components. These components include an optional "stage 0 loader," a "Stage 1 loader," and an "installer component."

21. The Stage 1 loader is designed to ensure that the infection process is not being emulated or executed within a sandbox. A sandbox is an isolated computing environment that provides a safe environment for researchers and investigators to analyze and debug malware as

[3] A registry is a database of information, settings, options, and other values for software and hardware installed on the Microsoft Windows Operating system. When a program is installed, a new subkey is created in the registry. This subkey contains settings specific to that program, such as its location, version, and primary executable.

part of a technical investigation into a malware's functionality. The Okrum's Stage 1 loader, as identified in **Exhibit 1**, is capable of testing for an emulation environment (a sandbox) before completing the infection process in one of four ways:

a. Two calls to GetTickCount function separated by a 20-second sleep. If the GetTickCount value hasn't changed (i.e., the time has been accelerated), the malware terminates itself.
b. Two subsequent calls to GetCursorPos function. If the position of the cursor on the x-axis has changed (i.e., the cursor positions were randomly generated), the malware terminates itself.
c. GetGlobalMemoryStatusEx is called. If the amount of actual physical memory is less than 15 Gigabytes, the malware terminates itself.
d. The payload starts only after the left (physical) mouse button has been pressed at least three times (GetAsyncKeyState is queried in an infinite loop).

22. In essence, what the Okrum Stage 1 loader is analyzing is whether the malware has infected an actual victim computer/device or is being observed within a controlled environment such as a sandbox. If all the checks pass, the Stage 1 loader decrypts the backdoor and loads it within its process. Next, we understand that the malware's backdoor is installed into the victim device through a method known as steganography. This technique is an attempt by the malicious actors to stay unnoticed and evade detection and involves injecting the malware's compromised script into a specifically tailored "Portable Graphics Format" ("PNG") file. A PNG file is the most frequently used uncompressed raster image format on the Internet. Researchers in the security community have uncovered one method by which the Nickel defendants infiltrate victim systems. According to security researchers at ESET, when the Okrum PNG file is viewed in an image viewer, in this case the familiar image of Microsoft's Internet Explorer trademark is displayed (as seen in **Figure 1**) but there is an extra encrypted file that the user cannot see.

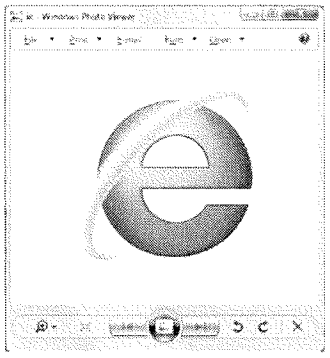


Figure 1

23. Once the backdoor is executed, Okrum is designed to evade detection and log into the victim's system by using a computer call named "ImpersonateLoggedOnUser." Once deployed, Okrum will automatically collect the following information about the infected device:

a. Computer Name
b. User Name
c. Host IP Address
d. Primary DNS suffix value
e. OS version, build number
f. Architecture
g. User agent string
h. Locale info (language name, country name)

24. In addition to collecting valuable system information, Okrum will communicate with the command and control infrastructure over HTTP protocols using GET, POST, and HEAD requests in the following ways:

a. HTTP HEAD request to negotiate AES key
b. HTTP GET request to get a command or download a file
c. HTTP POST request to upload a file

25. If any proxy servers are configured on the compromised system, Okrum is able to identify them and use them to make HTTP requests. When communicating with the command and control infrastructure, the Nickel defendants always send communications that contain the campaign name or contain foreign languages depending on which country they've infiltrated. Per our investigation, this process enables the Nickel defendants to keep track of the operation. In addition, the Nickel defendants always encrypt their communications to the command and control infrastructure.

26. During the infection process, the Nickel defendants will push malware to the user's computer. Depending on the malware being pushed from the command and control infrastructure, the malware file will be installed in any one of a number of possible locations. For example, Microsoft has observed certain malware making changes to settings on the user's Windows Registry, for example, we have observed certain malware executing cmd.exe process for powershell commands that affirmatively modify basic settings for Internet Explorer designed to be configurable by the authorized user. Modifying these settings enables the Nickel defendants to

establish persistence on the victim computers.

27. Below is one example of a powershell command executed by the Nickel defendants:

cmd.exe /C powershell -command "&{New-ItemProperty 'HKCU:\Software\Microsoft\Windows\CurrentVersion\Internet Settings' **-Property DWORD -name IEHardenIENoWarn -value 0 -Force***}"*

This powershell command is designed to modify the Internet Explorer registry and disable Internet Explorer's Enhanced Security Configuration. That setting establishes security parameters that define how users browse the Internet and intranet websites. The Nickel defendants execute this code in the following manner: the italicized portion shows the powershell command being executed in command prompt (cmd.exe); the underlined portion identifies the Windows registry path; the bolded portion is the command that is being introduced to the underlying Windows Registry. The command is designed to set the value of the Enhanced Security Configuration to "0", which disables that setting on Internet Explorer.

28. Microsoft has observed the following artifacts of the Nickel defendants modifying additional Windows Registries, all designed to disable critical features in Internet Explorer (modifications identified in bold):

a. *cmd.exe /C powershell -command "&{New-ItemProperty* 'HKCU:\Software\Microsoft\Internet Explorer\PhishingFilter' **-Property DWORD -name Enabled -value 1 -Force***}"*
b. *cmd.exe /C powershell -command "&{New-ItemProperty* 'HKCU:\Software\Microsoft\Internet Explorer\PhishingFilter' **-Property DWORD -name ShownVerifyBalloon -value 3 -Force***}"*
c. *cmd.exe /C powershell -command "&{New-ItemProperty* 'HKCU:\Software\Microsoft\Internet Explorer\Main' **-Property String -name Check_Associations -value 'no' -Force***}"*
d. *cmd.exe /C powershell -command "&{New-ItemProperty* 'HKCU:\Software\Microsoft\Internet Explorer\Main' **-Property DWORD -name DisableFirstRunCustomize -value 2 -Force***}"*
e. *cmd.exe /C powershell -command "&{New-ItemProperty* 'HKCU:\Software\Microsoft\Internet Explorer\Main' **-Property DWORD -name DEPOff -value 1 -Force***}"*
f. *cmd.exe /C powershell -command "&{New-ItemProperty* 'HKCU:\Software\Microsoft\Internet Explorer\Recovery' **-Property DWORD -name AutoRecover -value 2 -Force***}"*
g. *cmd.exe /C powershell -command "&{New-ItemProperty* 'HKCU:\Software\Microsoft\Windows\CurrentVersion\Internet Settings' **-Property DWORD -name WarnonZoneCrossing -value 0 -Force***}"*

h. *cmd.exe /C powershell -command "&{New-ItemProperty 'HKCU:\Software\Microsoft\Windows\CurrentVersion\Internet Settings' -* **Property DWORD -name WarnOnPostRedirect -value 0 -Force***}"*

Collectively, these powershell commands significantly alter Microsoft Windows and Internet Explorer, but these are subtle changes that the victim would not readily experience. Instead, the victim believes Internet Explorer is operating as if the application was unaltered and the authentic Microsoft product.

29. We have also observed NICKEL using cmd.exe through their malware to query for the settings of the WDigest registry key then making changes to the key to allow the capture of user credentials in memory of the computer.

a. reg query HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest
b. reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1 /f

30. Upon successful compromise of a victim account, the Nickel defendants will not only be able to log into the account and review the victim's emails, as discussed more thoroughly below, but may also exfiltrate information and disseminate additional malware to perpetuate their unlawful activity. Specifically, and as identified in **Exhibit 1**, through Okrum, Nickel defendants are able to deploy the following attack techniques:

Tactic	ID	Name	Description
Execution	T1059	Command-Line Interface	Okrum's backdoor uses `cmd.exe` to execute arbitrary commands.
	T1064	Scripting	The backdoor uses batch scripts to update itself to a newer version.
	T1035	Service Execution	The Stage 1 loader creates a new service named `RtmaSvc` to execute the payload.
Persistence	T1050	New Service	To establish persistence, Okrum installs itself as a new service named `RtmSevc`.
	T1060	Registry Run Keys / Startup Folder	Okrum establishes persistence by creating a .lnk shortcut to itself in the `Startup` folder.
	T1053	Scheduled Task	The installer component tries to achieve persistence by creating a scheduled task.
	T1023	Shortcut Modification	Okrum establishes persistence by creating a .lnk shortcut to itself in the `Startup` folder.

Privilege Escalation	T1134	Access Token Manipulation	Okrum can impersonate a logged on user's security context using a call to the `ImpersonateLoggedOnUser` API.
Defense Evasion	T1140	Deobfuscate/Decode Files or Information	The Stage I loader decrypts the backdoor code, embedded within the loader or within a legitimate PNG file. A custom XOR cipher or RC4 is used for decryption.
	T1107	File Deletion	Okrum's backdoor deletes files after they have been successfully uploaded to C&C servers.
	T1158	Hidden Files and Directories	Before exfiltration, Okrum's backdoor uses hidden files to store logs and outputs from backdoor commands.
	T1066	Indicator Removal from Tools	Okrum underwent regular technical improvements to evade antivirus detection.
	T1036	Masquerading	Okrum establishes persistence by adding a new service `RemSvc` with the display name `Removable Storage` in an attempt to masquerade as a legitimate Removable Storage Manager.
	T1027	Obfuscated Files or Information	Okrum's payload is encrypted and embedded within the Stage I loader, or within a legitimate PNG file.
	T1497	Virtualization/Sandbox Evasion	The Stage I loader performs several checks on the victim's machine to avoid being emulated or executed in a sandbox.
Credential Access	T1003	Credential Dumping	Okrum was seen using *Mimikatz Lite* and modified *Quarks PwDump* to perform credential dumping.
Discovery	T1083	File and Directory Discovery	Okrum was seen using *DriveLetterView* to enumerate drive information.
	T1082	System Information Discovery	Okrum collects computer name, locale information, and information about the OS and architecture.
	T1016	System Network Configuration Discovery	Okrum collects network information, including host IP address, DNS and proxy information.
	T1049	System Network Connections Discovery	Okrum used *NetSess* to discover NetBIOS sessions.
	T1033	System Owner/User Discovery	Okrum collects the victim user name.
	T1124	System Time Discovery	Okrum can obtain the date and time of the compromised system.
Collection	T1056	Input Capture	Okrum was seen using a keylogger tool to capture keystrokes.
Exfiltration	T1002	Data Compressed	Okrum was seen using a RAR archiver tool to compress data.
	T1022	Data Encrypted	Okrum uses AES encryption and base64 encoding of files before exfiltration.
	T1041	Exfiltration Over Command and Control Channel	Data exfiltration is done using the already opened channel with the C&C server.
Command And Control	T1043	Commonly Used Port	Okrum uses port 80 for C&C.
	T1090	Connection Proxy	Okrum identifies a proxy server if it exists and uses it to make HTTP requests.
	T1132	Data Encoding	The communication with the C&C server is base64 encoded.
	T1001	Data Obfuscation	The communication with the C&C server is hidden in the `Cookie` and `Set-Cookie` headers of HTTP requests.
	T1071	Standard Application Layer Protocol	Okrum uses HTTP for communication with its C&C.
	T1032	Standard Cryptographic Protocol	Okrum uses AES to encrypt network traffic. The key can be hardcoded or negotiated with the C&C server in the registration phase.

31. Through various investigative techniques, including those summarized above, Microsoft recently uncovered the Nickel defendants' scheme to gain unauthorized access and compromise of Microsoft 365 accounts and use this malicious infrastructure and surveillance efforts to target compromised account victim's wider network. For example, Microsoft has observed the Nickel defendants using malware known as KeyLoggers and Mimikatz to harvest user credentials to gain access to a victim's Microsoft 365 account without authorization. I participated in the investigation of Defendants' conduct and am personally familiar with the details of Microsoft's investigation in this case. Microsoft 365 is an online service that provides, among other things, access to Microsoft's Office software on a subscription basis. Customers purchase a subscription to Microsoft 365 that may provide access to both cloud and locally stored versions of the Office software. Use of Microsoft 365 requires an online account.

32. Microsoft goes to great lengths to protect customer accounts. In particular, Microsoft engineered Microsoft 365 with the intent to eliminate threats before reaching Microsoft 365 users. Microsoft uses real-time anti-spam and multiple anti-malware engines to prevent threats from reaching customer inboxes. Microsoft also offers Microsoft Defender for Microsoft 365,[4] which helps protect customers against new, sophisticated attacks in real time. In addition to incorporating tools to stop phishing emails before they reach users, Microsoft also investigates the underlying phishing attacks to identify and prevent malicious attacks. Microsoft also updates and patches all known vulnerabilities.

33. After the Nickel defendants gained unauthorized access to the Microsoft 365 accounts, Microsoft has observed the Nickel defendants accessing victim mailboxes and reading victim emails. To do so, the Nickel defendants are abusing software code underlying Microsoft's Exchange Web Services for an unintended purpose – i.e., they are using authentic Microsoft code but for an unauthorized malicious purpose via the use of compromised credentials. For example,

[4] *See generally* https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-advanced-threat-protection-service-description.

we understand from researchers in the security community that the Nickel defendants are abusing Microsoft Exchange Web Services APIs to enable access to the victim's mailbox and read the victim's emails. While we have not observed the Nickel defendants sending emails from a victim's Microsoft 365 environment, the malware and deceptive activities enable the Nickel defendants with the opportunity and level of access to disseminate emails from the victim's mailbox.

34. The installation of this malicious software damages the victim's computer and the Windows operating system on the victim's computer. During the infection of a victim's computer, the Nickel defendants deploy malware designed to makes changes at the deepest and most sensitive levels of the computer's Windows operating system. The consequences of these changes are that the user's version of Windows is essentially adulterated, and unknown to the user, has been converted into a tool to steal credentials and sensitive information from the user. This inherently involves abuse of Microsoft's trademarks and brands, and deceives users by presenting an unauthorized, modified version of Windows to those users. For example, the defendants create registry key paths bearing the Microsoft "Windows" trademark, within the Microsoft operating system, including, among others.

35. Through research and investigation, Microsoft has determined that the Nickel defendants currently uses the domains identified in **Appendix A** of the complaint, also attached as **Exhibit 2** to this declaration, in its command and control infrastructure. As part of my investigation, I performed lookups of these domains in a publicly accessible "Whois" database, which contains contact information regarding the registrants of these domains and technical details about the domains. Information in **Exhibit 2** is generated from the publicly available Whois registration data.

III. NICKEL HAS ATTACKED MANY MICROSOFT CUSTOMERS IN THE EASTERN DISTRICT OF VIRGINIA AND AROUND THE WORLD

36. Through its investigation, Microsoft has determined that the Nickel defendants have directed their malicious activities to the Eastern District of Virginia in order to harm Microsoft customers and partners. In particular, Microsoft has determined that the Nickel

defendants are using domains identified **Exhibit 2** to this declaration in order to establish and maintain its malicious activities. Specifically, Microsoft understands that the Nickel defendants use the domains identified in **Exhibit 2** to transmit the malware to the victim devices. The domains identified in **Exhibit 2** have a top-level domain ("TLD" either as [.]com or [.]org.

37. The domain .com is a generic TLD in the domain name system ("DNS") of the Internet and is operated by Verisign Inc., which is an American company based in the Eastern District of Virginia.

38. The domain .org is a generic TLD in the DNS and is operated by Public Interest Registry, which is an American company based in the Eastern District of Virginia.

39. In addition, the Nickel defendants are targeting Microsoft's customers and partners, including those in the public sector, in the Eastern District of Virginia and across the globe. At least one of Microsoft's customers or partners targeted by the Nickel defendants, the sovereign nation of El Salvador, has its consulate in the Eastern District of Virginia.

IV. HARM TO MICROSOFT AND MICROSOFT CUSTOMERS

40. Nickel irreparably harms Microsoft by damaging its reputation, brands, and customer goodwill. Microsoft is the provider of the Windows operating system, Internet Explorer, and Microsoft 365 cloud-based business and productivity suite of services, as well as a variety of other software and services. Microsoft is the owner of the "Microsoft," "Windows," "Internet Explorer," "and "Microsoft 365" trademarks. Trademark registrations for marks infringed by the Nickel defendants are attached to Microsoft's complaint as **Appendix B** to the complaint. 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 expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, has established a strong brand, and 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 service and its brand, including the

trademarks listed above.

41. Microsoft's customers whose email accounts are compromised through the defendants' credential theft are damaged by these activities. Similarly, Microsoft's customers whose computers are infected with malware deployed by the Nickel defendants are damaged by changes to Windows, which alter the normal and approved settings and functions of the user's operating system, destabilize it, and enable unauthorized monitoring of the user and theft of user data.

42. In effect, once infected, altered and controlled by the Nickel defendants, the Windows operating system ceases to operate normally and is now a tool of deception and theft aimed at the owner of the infected computer. Yet they still bear the Microsoft Windows trademark. This is obviously meant to mislead Microsoft's customers, and it causes extreme damage to Microsoft's brands and trademarks.

43. Customers are usually unaware of the fact that their email accounts are compromised, that their computers are infected, that they are being monitored by the defendants, or that sensitive information is being stolen from them. Even if aware of an account intrusion or an infection of their computer, users often lack the technical resources or skills to resolve the problem, allowing their accounts and computers to be misused indefinitely, as manual steps to change account credentials or remove the malicious software may be difficult for ordinary users. They may be futile to a degree too where the Nickel defendants have software installed to observe the victim's activities and attempts to remediate the intrusion. Even with professional assistance, cleaning an infected end-user computer can be exceedingly difficult, time-consuming, and frustrating. This demonstrates the extreme problems that the activities of the Nickel defendants cause for Microsoft's customers and the irreparable injury to both Microsoft and its customers. Microsoft and other members of the public must invest considerable time and resources investigating and remediating the defendants' intrusion into accounts and computers.

44. The activities of the Nickel defendants injure Microsoft and its reputation, brand, and goodwill. Users subject to the negative effects of the Nickel defendants' malicious activities

sometimes incorrectly believe that Microsoft is the source of the problem, and thus there is a significant risk that Microsoft customers will be confused in this way in the future. There is a great risk that Microsoft customers may incorrectly attribute these problems to Microsoft and associate these problems with Microsoft's products and services, thereby diluting and tarnishing the value of these trademarks and brands. Microsoft has invested substantial resources, well in excess of $5,000 in researching, investigating and working to remediate the activities of the Nickel actors.

V. DISRUPTING NICKEL'S ILLEGAL ACTIVITIES

45. Evidence indicates that the Nickel defendants are highly sophisticated, well-resourced, organized, and patient. The Nickel defendants specialize in targeting individuals in organizations holding sensitive data, by gathering extensive information about their employees through publicly available information and social media, using that information to fashion phishing attacks intended to trick those employees into compromising their credentials, and disguising its activities using the trademarks of Microsoft.

46. There is one vulnerable point in the Nickel defendants' command and control infrastructure. In particular, there are a number of Internet domains through which the Nickel defendants obtain victim credentials, log into compromised accounts, and review sensitive information from victim accounts. A core subset of these is listed in Appendix A to the Complaint. Granting Microsoft possession of these domains will enable Microsoft to cut off the means by which the Nickel defendants are able to gain access to victim accounts or devices. Specifically, the Nickel defendants' domains are used to receive information stolen from victim accounts or as a backdoor to the victim device. Therefore, transferring them to a controlled, secure server hosted by Microsoft would disrupt the Nickel defendants' operations. While it is not possible to rule out the possibility that the Nickel defendants could use additional fall back mechanisms to evade the requested relief, redirecting this core subset of Nickel domains will directly disrupt current Nickel infrastructure, mitigating risk and injury to Microsoft and its customers. The requested relief will also serve the public interest, in protecting customers of other web services companies who have

consented to the relief sought in this action.

47. I believe that the most effective 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 Nickel defendants' ability to compromise additional accounts and identify new potential victims to target. In the absence of such action, the Nickel defendants will be able to continue using this infrastructure to target new accounts, exposing potential new victims to the Nickel defendants' malicious activities.

48. The Nickel defendants' techniques are designed to resist technical mitigation efforts, eliminating easy technical means to curb the injury being caused. For example, once domains in the Nickel defendants' active infrastructure become known to the security community, the defendants abandon that infrastructure and move to new infrastructure that is used to continue the Nickel defendants' efforts to compromise accounts of new victims. For this reason, providing notice to the Nickel defendants in advance of redirection of the domains at issue would render attempts to disable the infrastructure futile. Further, when the Nickel defendants become aware of efforts to mitigate or investigate their activities, they take steps to conceal their activities and to conceal the injury that has been caused to victims, making it more difficult for victims to adequately assess the damage or take steps to mitigate that injury going forward. For this reason as well, providing notice to the Nickel defendants in advance of redirection of the domains at issue would render attempts to mitigate the harm futile, or at least much more difficult for Microsoft. Piecemeal requests to disable these domains, informal dispute resolution or notice to the defendants prior to redirecting the domains would be insufficient to curb the injury. Based on my experience observing the operation of numerous intrusions such as those carried out by the Nickel defendants, and prior investigations and legal actions involving such intrusions and actors, I believe that the Nickel defendants would take swift preemptive action to conceal the extent of the victimization of Microsoft and its customers and to defend their infrastructure, if they were to learn of Microsoft's impending action and request for relief.

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 29 day of November, 2021 in KIRKLAND, Washington.

Christopher T. Coy

TLP: WHITE

ENJOY SAFER TECHNOLOGY™

OKRUM AND KETRICAN: AN OVERVIEW OF RECENT KE3CHANG GROUP ACTIVITY

Author:
Zuzana Hromcová

CONTENTS

1 SUMMARY 2
2 INVESTIGATION TIMELINE. 2
3 OKRUM MALWARE 3
3.1 Technical analysis of Okrum 3
3.1.1 LOADERS 5
3.1.2 INSTALLERS 7
3.1.3 BACKDOOR 7
3.2 Auxiliary tools used by Okrum 10
4 KE3CHANG GROUP ACTIVITY IN 2015-2019 AND TIES TO OKRUM . . 11
4.1 Ke3chang activity in 2015 – Ketrican 11
4.1.1 WORKING DIRECTORY. 12
4.1.2 ANTI-EMULATION/ANTI-SANDBOX TRICK 12
4.1.3 NETWORK COMMUNICATION 13
4.1.4 DATA TRANSFORMATION 13
4.1.5 FURTHER ATTRIBUTION CONSIDERATIONS 14
4.2 Ke3chang activity in 2017 – Ketrican 14
4.3 Ke3chang activity in 2017 – RoyalDNS. 15
4.4 Ke3chang activity in 2018 – Ketrican 16
4.5 Ke3chang activity in 2019 – Ketrican 17
5 CONCLUSION 17
6 INDICATORS OF COMPROMISE 18
7 MITRE ATT&CK TECHNIQUES (OKRUM) 21

Author: Zuzana Hromcová

July 2019

1 SUMMARY

The *Ke3chang group*, also known as APT15, is a threat group believed to be operating out of China. Its attacks were first reported in 2012, when the group used a remote access trojan (RAT) known as *Mirage* to attack high-profile targets around the world. However, the group's activities were traced back to at least 2010 in FireEye's 2013 report on *operation Ke3chang* – a cyberespionage campaign directed at diplomatic organizations and missions in Europe. The attackers resurfaced with malware dubbed *TidePool*, documented as part of a campaign spanning from 2012 to 2015, and later with the *RoyalCLI and RoyalDNS backdoors*, which were used to target the UK government from 2016 to 2017. In 2018, the Ke3chang group was spotted using an apparently updated version of the Mirage RAT, dubbed *MirageFox*.

We have been tracking the malicious activities related to this threat actor and made several noteworthy discoveries.

First, from 2015 to 2019, we detected new versions of known malware families attributed to the Ke3chang group – BS2005 (operation Ke3chang malware) and the RoyalDNS malware.

Second, we identified a previously undocumented malware family with strong links to the Ke3chang group – a backdoor we named Okrum. We first detected Okrum, through ESET telemetry, in December 2016; it targeted diplomatic missions in Slovakia, Belgium, Chile, Guatemala and Brazil throughout 2017.

In this paper, we will take a deep technical look at this previously undocumented malware family and the other Ke3chang malware families detected from 2015 to 2019. We will provide evidence that the latter are evolved versions of known malware families attributed to Ke3chang group and explain how Okrum is linked to them – in terms of code, modus operandi and shared targets.

Note: *New versions of operation Ke3chang malware from 2015-2019 are detected by ESET systems as Win32/Ketrican, and collectively referred to across this paper as Ketrican backdoors/samples, marked with the relevant year.*

2 INVESTIGATION TIMELINE

2015: Ketrican

In 2015, we identified new suspicious activities in European countries. The group behind the attacks seemed to have a particular interest in Slovakia, where many of the discovered malware samples were detected; Croatia, the Czech Republic and other countries were also affected.

Our technical analysis of the malware used in these attacks showed close ties to BS2005 backdoors from *operation Ke3chang*, previously documented by FireEye in 2013, and to a related *TidePool malware family* discovered by Palo Alto Networks in 2016 that targeted Indian embassies across the globe.

2016-2017: Okrum

The story continued in late 2016, when we discovered a new, previously unknown backdoor that we named Okrum. The malicious actors behind the Okrum malware were focused on the same targets in Slovakia that were previously targeted by Ketrican 2015 backdoors.

2017: Ketrican and RoyalDNS

Red lights started flashing when we discovered that the Okrum backdoor was used to drop a Ketrican backdoor, freshly compiled in 2017.

In 2017, the same entities that were affected by the Okrum malware (and by the 2015 Ketrican backdoors) again became targets of the malicious actors. This time, the attackers used new versions of the RoyalDNS malware and a Ketrican 2017 backdoor.

2018: Ketrican

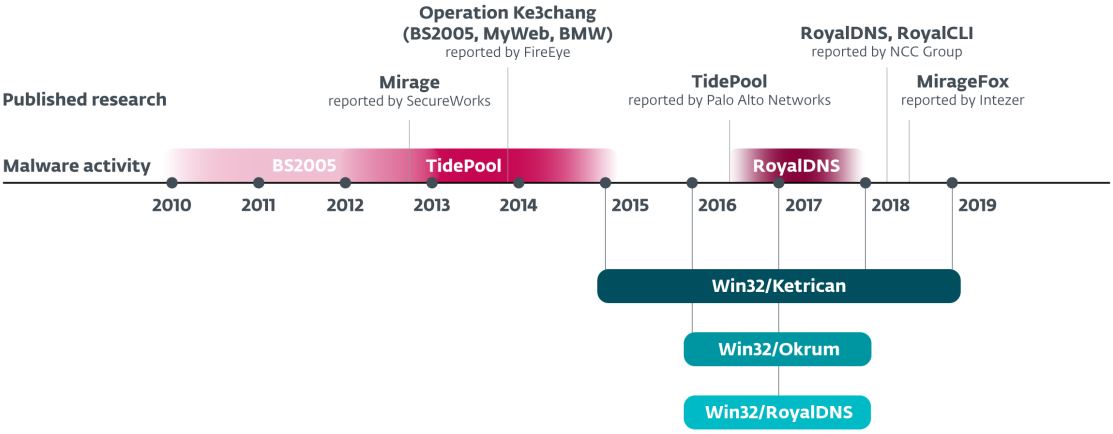
In 2018, we discovered a new version of the Ketrican backdoor that featured some code improvements.

2019: Ketrican

In March 2019, we detected a new Ketrican sample that has evolved from the 2018 Ketrican backdoor. It affected the same targets as the backdoor from 2018.

This timeline of events shows that the attackers were focused on the same type of targets but were using different malicious toolsets to compromise them – exposing their previously unknown project, Okrum, in the process.

Documented Ke3chang group activity



ESET investigation

Figure 1 // Timeline of previously documented Ke3chang group activity and detections related to our investigation

3 OKRUM MALWARE

In late 2016, we identified a previously unknown backdoor that we named Okrum. We discovered that the Okrum backdoor[1] was used to deliver a Ketrican sample[2]. This newly discovered Ketrican sample from 2017 has evolved from the Ke3chang group's BS2005 malware family and is described in section 4.2.

Moreover, the entities where we detected Okrum in 2017 were previously affected with backdoors known to be attributed to the Ke3chang group – another hint that Okrum is the work of the same threat actor.

The following sections provide a deep technical analysis of the Okrum backdoor.

3.1 Technical analysis of Okrum

The functionality of the Okrum backdoor is not unlike the other backdoors operated by the Ke3chang group. The commands allow the attackers to download and upload files, execute binaries or run shell commands. The backdoor can also update itself to a newer version and can adjust the time it sleeps after each backdoor command.

1 SHA-1: 1D271F22798313650C91C6FC34551CC8492A201
2 SHA-1: D3BFB10DB08C6828C3001C1F825ED6A6BF6F6E01

The backdoor itself is a dynamic-link library that is installed and loaded by two earlier-stage components. During our investigation, the implementation of these two components was changed frequently. Every few months, the authors actively changed implementation of the loader and installer components, to avoid detection. At the time of this publication, ESET systems have detected seven different versions of the loader component and two versions of the installer, although the functionality remained the same.

We have not been able to find the original attack vector and dropper of the malware, but we have identified several components used in the Okrum malware:

- An optional stage 0 loader
- Stage 1 loader
- An installer component
- A PNG file with an embedded backdoor

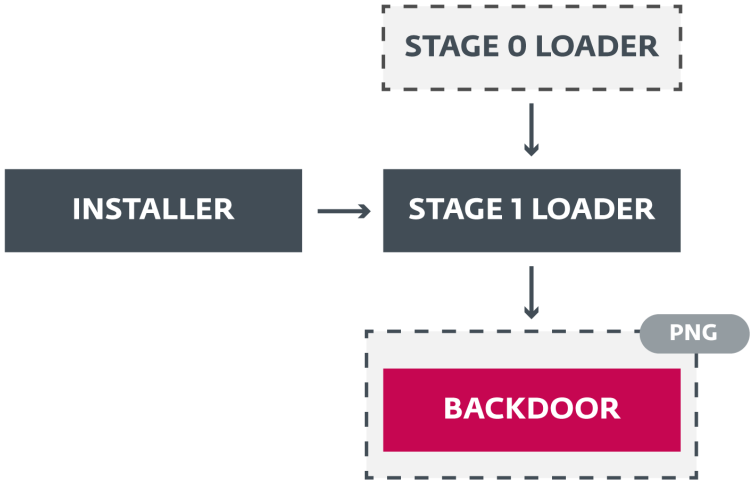


Figure 2 // Okrum architecture

Table 1 lists the analyzed Okrum backdoor components.

SHA-1	PE Timestamp	File extension	Comment
F42A9D85ABE04E721461FE2B52DDC9E0EA411D9E	-	PNG	PNG image with embedded backdoor
8D7E503D972C03C0F87F2D6F6EF65F1381D21BC6	2016-01-11	EXE	Stage 1 loader with embedded backdoor
AD740FD11688B2B39072C7024679CC22878E2619	2016-01-20	EXE	Stage 1 loader with embedded backdoor
1CDC632E0A26F39E527ACF7B1CDECD829A6A2B3D	2016-11-16	DLL	Stage 1 loader
A426BCC6317F0D49F0F0B68091E8161C512E22C3	2016-11-16	EXE	Installer
38299BCF0BA25E331939683597F161A3D7121A26	2016-12-19	EXE	Stage 1 loader
F0E2C3AF0297C80C0A14E95E151FC7DC319ACFC3	2016-12-19	EXE	Installer
371B14F8BFD9B5DB098139E7FE2EBD4381CB259C	2017-08-07	EXE	Stage 0 loader
1D271F22798313650C91C6FC34551CC8492A2019	2017-08-08	EXE	Stage 1 loader
48F8BAFB334C6980FB578C09D7297A4B7F5E09E2	2017-08-09	EXE	Stage 1 loader
5FBAFB71CFDF0C93E19882630D05F37C1F756CBF	2017-09-15	EXE	Stage 1 loader

Table 1 // Analyzed Okrum samples

3.1.1 LOADERS

Although the Stage 1 loaders have varied frequently, they are all responsible for loading the very same Okrum backdoor. The Stage 0 loader is an optional component that loads the Stage 1 loader into memory.

3.1.1.1 Early Stage 1 loaders

The Stage 1 loader samples[3] compiled in January 2016 are dynamic-link libraries with the backdoor bundled at the end of the file. The last four bytes of the file determine the size of the backdoor, which is encrypted using the RC4 algorithm and a hardcoded key.

The following RC4 keys were used in the analyzed samples:

- `0x4540DCA3FE052EBA0183D9FA36DA7F98`
- `0xCDABDCA3FE2934B10893DFA1FA7D3698`

The loader first checks to make sure the process is not being emulated or executed within a sandbox. Four tricks are employed, as Figure 3 illustrates:

- Two calls to `GetTickCount` function separated by a 20-second sleep. If the `GetTickCount` value hasn't changed (i.e. the time has been accelerated), the malware terminates itself.
- Two subsequent calls to `GetCursorPos` function. If the position of the cursor on the x-axis has changed (i.e. the cursor positions were randomly generated), the malware terminates itself.
- `GetGlobalMemoryStatusEx` is called. If the amount of actual physical memory is less than 1.5 Gigabytes, the malware terminates itself.
- The payload starts only after the left (physical) mouse button has been pressed at least three times (`GetAsyncKeyState` is queried in an infinite loop).

If all the checks pass, the loader decrypts the backdoor and loads it within its process, as described in the Backdoor section.

```
v0 = GetTickCount();
Sleep(20000u);
if ( v0 == GetTickCount() )
  goto emulatorDetected;
numberOfLeftButtonClicks = 0;
v3 = 8;
v4 = &position1;
do
{
  LOBYTE(v4->x) = 0;
  v4 = (struct tagPOINT *)((char *)v4 + 1);
  --v3;
}
while ( v3 );
v5 = 8;
v6 = &position2;
do
{
  LOBYTE(v6->x) = 0;
  v6 = (struct tagPOINT *)((char *)v6 + 1);
  --v5;
}
while ( v5 );
GetCursorPos(&position1);
v7 = 64;
v8 = &memoryStatusEx;
do
{
  LOBYTE(v8->dwLength) = 0;
  v8 = (struct _MEMORYSTATUSEX *)((char *)v8 + 1);
  --v7;
}
while ( v7 );
memoryStatusEx.dwLength = 64;
GlobalMemoryStatusEx(&memoryStatusEx);
if ( (double)(unsigned int)(memoryStatusEx.ullTotalPhys >> 20) < 1536.0
  || (GetCursorPos(&position2), position1.x != position2.x) )
{
emulatorDetected:
  isEmulatorDetected = 1;
}
else
{
  do
  {
    if ( GetAsyncKeyState(VK_LBUTTON) )
      ++numberOfLeftButtonClicks;
    Sleep(100u);
  }
  while ( numberOfLeftButtonClicks <= 3 );
  isEmulatorDetected = 0;
}
return isEmulatorDetected;
}
```

Figure 3 // Four anti-sandbox/anti-emulation tricks employed by the Okrum Stage 1 loader

3 SHA-1: 8D7E503D972C03C0F87F2D6F6EF65F1381D21BC6, AD740FD11688B2B39072C7024679CC22878E2619

3.1.1.2 Late Stage 1 loaders

The later Stage 1 loader samples[4] compiled at the end of 2016 and in 2017 take a different approach than the early samples. They no longer come bundled with the encrypted backdoor file; instead, the backdoor is embedded within a valid PNG file. When the file is viewed in an image viewer, a familiar image is displayed (as seen in Figure 4) but the loaders are able to locate an extra encrypted file that the user cannot see. This steganography technique is an attempt by the malicious actors to stay unnoticed and evade detection.

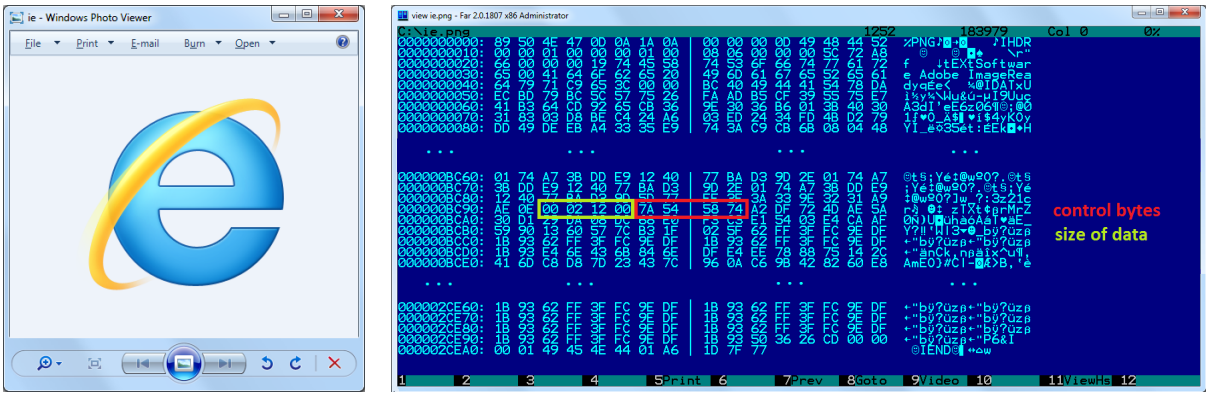


Figure 4 // An innocuous-looking PNG image with an encrypted, malicious DLL embedded within

All the loaders assume the PNG file is already dropped somewhere in this folder or its subfolders:

```
C:\program files
```

They search the folder recursively for a file (of any name and any extension) that has the following structure:

- PNG signature as the first 4 bytes:
  - `0x89504E47`
- PNG zTXt header present in the file:
  - `0x7A545874`
- PNG IEND header present in the file:
  - `0x49454E44`
- Byte 0x01 immediately following the IEND header

The encrypted payload is embedded in the zTXt chunk. According to the *PNG format specification*, this section should contain compressed text – such as licensing information – that would normally be displayed in the image properties. The zTXt chunk is, however, not critical for displaying the image correctly, and thus a PNG parser can ignore it if it is malformed (as in this case). Therefore, the image can be rendered correctly even when a broken zTXt section is present.

The payload is decrypted using *Tiny Encryption Algorithm (TEA)* with a hardcoded key, and loaded within the process of the loader. The same decryption key is hardcoded in all the loaders:

- `0x3E6A125F2387541296A3DC560C69AD1E`

The five loaders share exactly the same functionality (as described above) but the implementations are different.

4 SHA-1:38299BCF0BA25E331939683597F161A3D7121A26, 1D271F22798313650C91C6FC34551CC8492A2019, 48F8BAFB334C6980FB578C09D7297A4B7F5E09E2, 1CDC632E0A26F39E527ACF7B1CDECD829A6A2B3D, 5FBAFB71CFDF0C93E19882630D05F37C1F756CBF

While one of them is implemented as a service called `Ntmssvc` that needs a Service Installer, the others are standalone executables. Two of the loaders make use of forced exceptions and hide their payload in the exception handlers. All of the loaders are, however, responsible for locating, decrypting and loading the backdoor, as described above.

3.1.2 INSTALLERS

3.1.2.1 SHA-1: A426BCC6317F0D49F0F0B68091E8161C512E22C3

The first of the installers we detected is a Service Installer for the `Ntmssvc` service. Due to the same service name and matching PE Timestamps, we assume this component is to be used with the Stage 1 loader implemented as a service[5].

The component can be executed in two modes, determined by the command line argument (`install` or `uninstall`). It creates or removes a service called `Ntmssvc` that mimics the legitimate Removable Storage service but in fact, it loads one of the Okrum loaders on each system startup.

3.1.2.2 SHA-1: F0E2C3AF0297C80C0A14E95E151FC7DC319ACFC3

The second installer has the same PE Timestamp as one of the Stage 1 loaders[6], so it is reasonable to assume they are meant to be used together.

This component installs the specified file to be executed with each system start. Exactly three command line arguments are expected:

`md` – mode (1 = create a task, 2 = drop in a startup folder)
`tn` – name of the task or shortcut file
`fp` – binary file path

In mode 1, a new hidden task named `tn` is scheduled, that executes file `fp` with each user logon. In mode 2, a shortcut file named `tn` is created in a Startup folder that points to the specified file `fp`.

In both cases, COM interfaces are used (`IPersistFile`, `ITaskScheduler`, `ITaskService`).

3.1.3 BACKDOOR

The Okrum backdoor is a DLL with three exported functions:

- `DllEntryPoint`
- Reflective loader (`_xyz`/`_Rld`)
- Main payload (`_abc`/`_space`)

The Stage 1 loader decrypts and loads the backdoor, using an unusual execution method. The DOS header of the backdoor executable is valid, but can also be interpreted as shellcode. This allows the Stage 1 component to load the backdoor DLL into its address space, and execute a JMP or CALL instruction to offset 0x00 of the DLL, which passes control to the shellcode. The shellcode first calls the reflective loader export that applies relocations and resolves imports. Then it calls the export with the payload that executes the actual backdoor.

Interestingly, the PE header is valid, which also makes more common execution methods possible. If distributed in the original, unencrypted version, the backdoor could also be executed directly by having the DLL loaded by any executable. It would also be possible to inject it directly into another process using the reflective loader exported by the DLL. It is possible that these techniques were used by some older versions of the malware; however, we have only witnessed execution using the shellcode embedded in the DOS header, as illustrated in Figure 5.

5 SHA-1: 1CDC632E0A26F39E527ACF7B1CDECD829A6A2B3D
6 SHA-1: 38299BCF0BA25E331939683597F161A3D7121A26

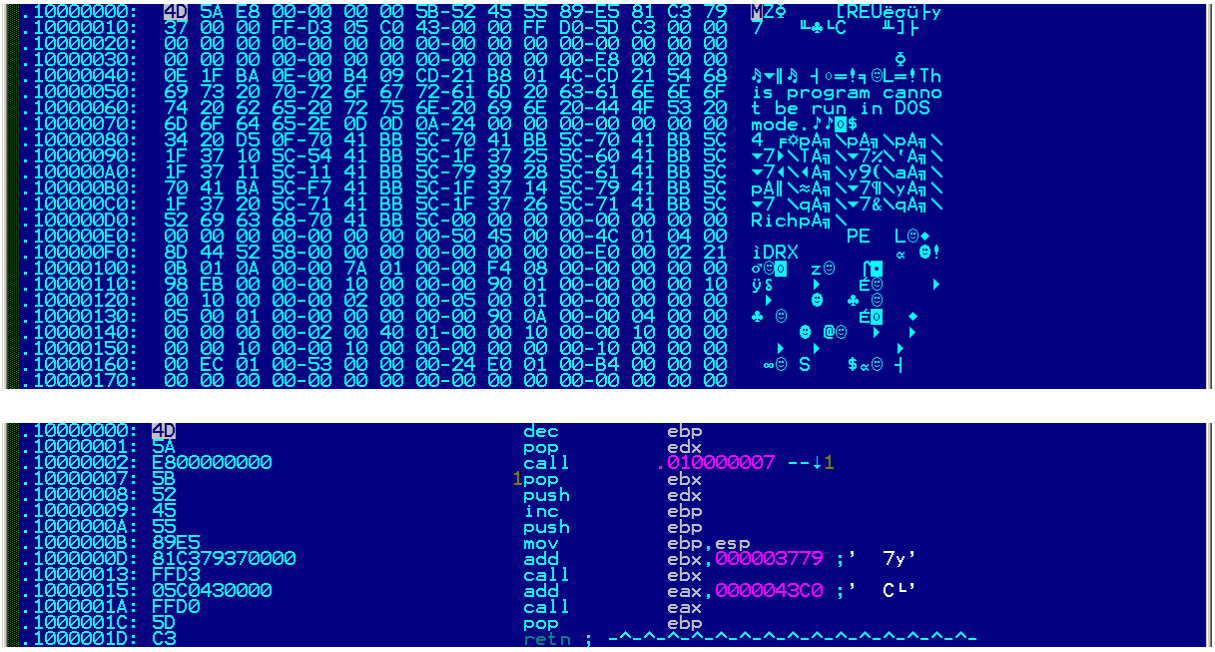


Figure 5 // The valid PE header of the Okrum backdoor can also be interpreted as shellcode

3.1.3.1 Overview

Okrum can impersonate a logged on user's security context using a call to the `ImpersonateLoggedOnUser` API, in order to gain administrator privileges.

It automatically collects the following information about the infected computer:

- computer name
- user name
- host IP address
- primary DNS suffix value
- OS version, build number
- architecture
- user agent string
- locale info (language name, country name)

It starts communication with the C&C server and negotiates an AES key used in further communication. If not successful, a hardcoded key is used. Then, it registers the victim with the server by sending the collected information. Finally, it starts a loop in which the compromised computer queries for a backdoor command and then interprets it locally.

3.1.3.2 Network communication

Okrum communicates with the remote server over the HTTP protocol using GET, POST and HEAD requests:

- HTTP HEAD request to negotiate AES key
- HTTP GET request to get a command or download a file
- HTTP POST request to upload a file

If any proxy servers are configured on the compromised system, Okrum is able to identify them and use them to make HTTP requests.

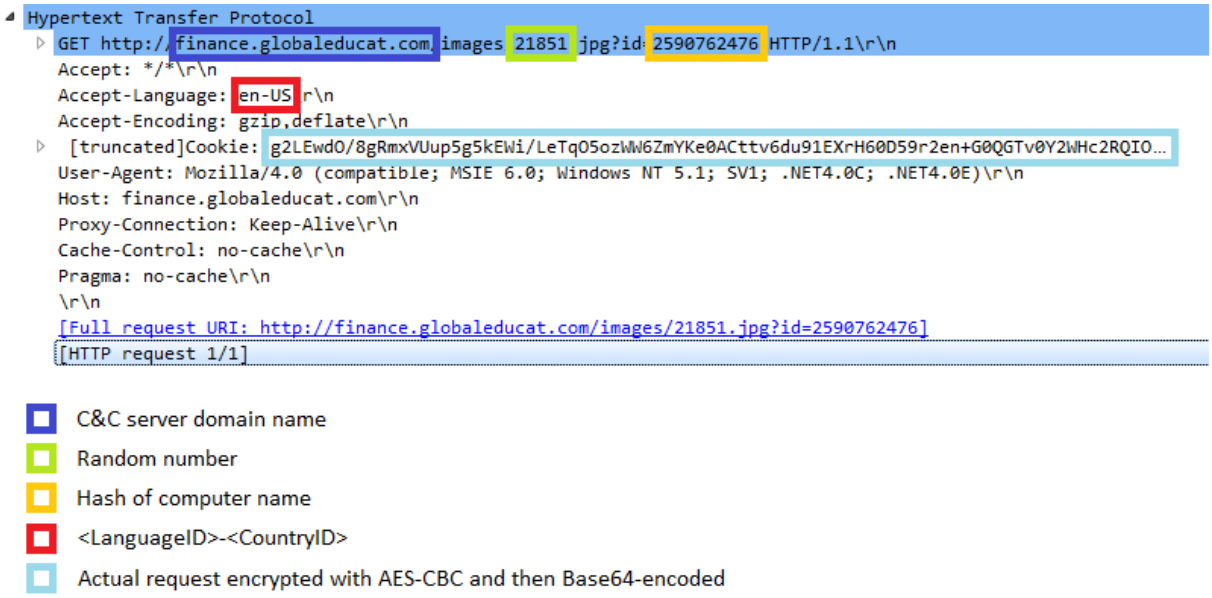


Figure 6 // Example of an HTTP GET request sent by Okrum to a remote server

In client->server direction of the communication, the data is transmitted in the **Cookie** header (additional data can be included in the HTTP Message Body if files are transmitted). In server->client direction, the data is embedded in the **Set-Cookie** header.

An example of a client->server HTTP request is illustrated in Figure 6. The URI is different for different types of requests, but the data is always transmitted within the Cookie header.

The data always consists of a series of parameters and values, separated by an ampersand, e.g.:

tm=01/09/2018 12:30:00**&hn**=My-Computer**&un**=JohnDoe**&dm**=my.dns.suffix**&ip**=127.0.0.1**&os**=Windows Server 2016**&fg**=finance

Several parameters are supported and which of them are used depends on the type of the request. In the client >server direction, the parameters identify the victim and the query made to the server; in the other direction, they determine the backdoor commands and arguments.

Just like in other backdoors attributed to the Ke3chang threat actor, a campaign name is always sent to the server as a part of the request, in order to help the operators keep track of the operation. In the Okrum samples we analyzed, we have encountered three campaign names:

- finance
- green[7]
- rehake

The data is always AES-CBC encrypted and base64 encoded. The AES key negotiated with the server is used in the communication.

Malware operators are trying to hide the malicious traffic with the C&C server within regular network traffic by registering seemingly legitimate domain names. For example, the samples that were used against Slovak targets communicated with a domain name mimicking a Slovak map portal:

- support.slovakmaps[.]com

Similarly, in a sample that was detected in a Spanish speaking country in South America, the operators used a domain name that translates as "missions support" in Spanish:

- misiones.soportesisco[.]com

7 Previous Ke3chang campaign names include "white" and "blue".

3.1.3.3 Backdoor commands

The backdoor commands are determined by the `ct` parameter embedded in the message from the remote server. A custom hash of this value is computed and compared with a hardcoded table. After interpreting a command, Okrum sleeps for a configurable amount of time.

The Okrum backdoor supports only basic commands, which indicates it is either a first-stage backdoor, or, more likely, the malware operators execute more complicated commands manually. The full list of backdoor commands can be found in Table 2.

Command ID	Command hash	Description
0	467BC6E8	Adjust sleep time
1	24196803	Execute a shell command
2	5F1C0F5B	Download a file
3	E16D3ACB	Execute a file / download a file / update itself
4	E008CB5C	Upload a file

Table 2 // Backdoor commands supported by Okrum malware

3.2 Auxiliary tools used by Okrum

Since the Okrum backdoor is not very technically complex, most of the malicious activity must be performed by manually typing shell commands, or by executing other available tools and software. This is a common practice of the Ke3chang group, as had also been pointed out previously in the *Intezer* and *NCC Group* reports monitoring Ke3chang group activity.

Not all of these tools are necessarily malicious – some of them are common utilities such as a RAR archiver; others are *potentially unsafe applications* that can be abused by the attackers. We have spotted tools for dumping passwords, enumerating network sessions and others. Information about all the utilities we have seen being used by the Okrum malware is listed in Table 3.

SHA-1	File name	Tool name / description / website
2D4713A598831E8F913857729CF4C193CA7B9B2E	csrss.exe	Keylogger
673F513186C5EFB465EBA1DFCEDE61979972F7FE	wnzip.exe	RAR archiver utility
3314780AB1C782D1B226BEAEE9DE16E9BEB00FD0	gp.exe	MimikatzLite
3FC6F7F66EEDA71B53C32B2086A4D737C94C4BCF	gpd.exe	MimikatzLite
E9D01DA30DA5FAE2EE333A8E446F0232E60AD8D9	Drives.exe	*DriveLetterView*
83A2F4F0E6DFFDFF5420048D9B37011FC50D45B4	nets.exe	*Netsess (RiskWare)*
858A9E32DBF619C68E1325590E87670E940B0E45	tif.exe	Modified *Quarks PwDump*

Table 3 // Tools (ab)used by the Okrum backdoor

Similar utilities were observed being used by other Ke3chang malware, which is described in the next section. For example, a Ketrican backdoor from 2017 used NetSess, NetE, ProcDump, PsExec, RAR archiver utility, and *Get-PassHashes*.

4 KE3CHANG GROUP ACTIVITY IN 2015-2019 AND TIES TO OKRUM

From 2015 to 2019, we detected malware that evolved from the BS2005 backdoors from *operation Ke3chang* – the Ketrican backdoors – and a new version of the RoyalDNS malware. In this section, we will go through these newly discovered samples, compare them to the malware families previously attributed to Ke3chang group, and explain how Okrum fits into the picture.

4.1 Ke3chang activity in 2015 – Ketrican

All of the analyzed Ketrican 2015 samples were backdoors supporting the same set of basic commands as malware used in operation Ke3chang, such as downloading and uploading files, executing files and shell commands, and sleeping for a configurable time. Likewise, each of the files has a hardcoded campaign name, the C&C server domain name and URI, as in the samples used in operation Ke3chang. The list of IoCs extracted from the Ketrican samples discovered in 2015 can be found in Table 4.

SHA-1	PE Timestamp	C&C server	URI	Campaign Name
2748A2928B6A4A528709ABA20AEF93D1EC9010F9	2014-03-12	dyname.europemis[.]com	twit4ter	name
94E6CB95585DBB59A61EC4029BC7EBB30BBA57E5	2014-03-17	dream.zepotac[.]com	whaced	water
D3A96C0FA84BFEE826E175D4664116A169D15D4E	2014-04-14	translate.europemis[.]com	twit4ter	baby
1C7559C57606B359EEB57F0416FE0B2784C01395	2014-09-04	view.beleimprensa[.]org	whaced	peach
233FF39DDE5A13CBF78EC1E9C020CF3CF18084E7	2015-01-28	store.ufmsecret[.]org	images	warm
A23EE1F17B746C1907293C7F8155E3E7DE135648	2015-06-18	daily.huntereim[.]com	whaced	pictu
10BD61F3FB03632E270FEF3AB6515677405A472F	2015-07-31	center.nmsvillage[.]com	content	video
809C53F71549D83ED8AB5BAB312249212F6F4149	2015-08-04	store.ufmsecret[.]org	images	warm
77369D3735B3B2C24CCAA93ECAA903D816EA9CD9	2015-09-15	control.mimepanel[.]org	whaced	panel
844E710D85DD63AA5BF245CEE94C1CC872429BD3	2015-11-06	rain.nmsvillage[.]com	twit4ter	snow
B49EDC05658907C888074905CE234BF3CF58D8A0	2015-11-18	wind.deltimesweb[.]com	whaced	cloud
4C1198F726ACAD7AF78B36F250A128D5E3C52D8C	2015-11-26	promise.miniaturizate[.]org	images	tree
1730D90FFB888877EA2F18198BCC592087218E9A	2015-09-29	item.amazonout[.]com	w4rmeg	fight

Table 4 // IoCs extracted from the analyzed Ketrican samples discovered by ESET in 2015

In the rest of this part of the paper, we will point out the major similarities between the coding style of the malware used in operation Ke3chang and the Ketrican backdoor samples discovered by ESET in 2015. These share the main features with the BS2005 malware family, but in some places, they have clearly evolved.

4.1.1 WORKING DIRECTORY

The first trait common to both BS2005 and some of the 2015 Ketrican samples is that they create a copy of the Windows Command Prompt (`cmd.exe`) in their working directories and then use it to interpret backdoor commands. Both BS2005 and Ketrican backdoors use similar command-line patterns to execute a file or shell command using their Command Prompt copy and redirect its output to a file, as seen in Figure 7.

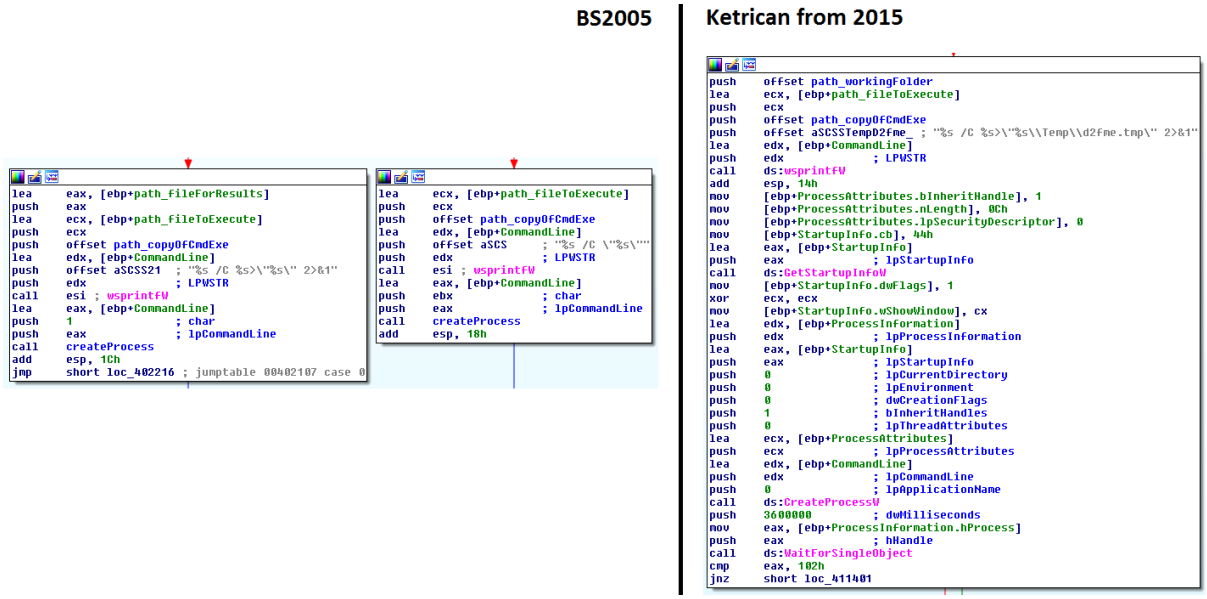


Figure 7 // Files and commands are executed using a copy of Command Prompt

The files created by the malware are stored in a working directory in one of Windows special folders (e.g. `Local Settings`). The special folder location is updated in different versions of the backdoors from operation Ke3chang but the path to the folder is always retrieved by accessing the following registry key, rather than using the `SHGetSpecialFolderLocation` API function:

`[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders]`

The `Shell Folders` registry key is only supported by Windows *for backwards compatibility* and is not the recommended way to access these folders. It is a rather unusual technique to use this key and that links the samples used in operation Ke3chang to the samples discovered in 2015.

4.1.2 ANTI-EMULATION/ANTI-SANDBOX TRICK

One of the artifacts shared among the analyzed samples is a heuristic to detect an emulated environment or a sandbox. The `GetTickCount` function is called before and after a loop with 999,999,990 iterations of incrementing a value. If the returned value doesn't change between calls, emulation or a sandbox is detected and the process terminates itself.

According to the *FireEye report*, at least one of the BS2005 samples from operation Ke3chang contained the very same heuristic. We were able to locate the same heuristic in all Ketrican backdoors discovered in 2015, as Figure 8 depicts.

BS2005

```
174     v6 = GetTickCount();
175     for ( j = 0; ; ++j )
176     {
177       v28 = j;
178       if ( j >= 999999990 )
179         break;
180     }
181     if ( v6 == GetTickCount() )
182       exit(0);
```

Ketrican from 2015

```
135   v36 = GetTickCount();
136   for ( i = 0; i < 999999990; ++i )
137     ;
138   if ( v36 == GetTickCount() )
139     exit(0);
```

Figure 8 // A trick to detect an emulated environment or a sandbox

4.1.3 NETWORK COMMUNICATION

Just like the BS2005 family, the 2015 Ketrican samples control the Internet Explorer browser process using the `IWebBrowser2` COM interface, to make their network communication look legitimate. Data is encrypted and encoded, and sent using the HTTP protocol.

The response from the server is an HTTP page with backdoor commands and arguments included in a hidden input field. This data is expected to have a specific format that varies across the samples, but the same pattern is used, as shown in Figure 9.

BS2005

```
push    edx             ; lpWideCharStr
call    sub_406960
mov     ebx, ds:strstr
mov     edi, eax
push    offset asc_40875C ; "((((((("
push    edi             ; Str
call    ebx ; strstr
push    offset asc_408764 ; "))))))))"
push    edi             ; Str
mov     [ebp+1150h+bstrString], eax
call    ebx ; strstr
push    offset asc_40876C ; "***"
push    edi             ; Str
mov     esi, eax
call    ebx ; strstr
push    offset asc_408770 ; "^^^^"
push    edi             ; Str
mov     [ebp+1150h+Str], eax
call    ebx ; strstr
push    offset asc_408774 ; "$$$"
push    edi             ; Str
mov     [ebp+1150h+var_1180], eax
call    ebx ; strstr
push    offset off_408778 ; SubStr
push    edi             ; Str
mov     ebx, eax
call    ds:strstr
push    offset asc_40877C ; "%%%"
push    edi             ; Str
mov     [ebp+1150h+var_1174], eax
call    ds:strstr
```

```
push    ecx             ; lpWideCharStr
call    sub_4042F0
mov     esi, eax
mov     [ebp+0C04h+var_C60], esi
push    offset asc_419D44 ; "(!("
push    esi             ; char *
call    _strstr
push    offset a?       ; "#?#"
push    esi             ; char *
call    _strstr
mov     edi, eax
mov     [ebp+0C04h+var_C44], edi
push    offset asc_419D4C ; "^^^*"
push    esi             ; char *
call    _strstr
mov     [ebp+0C04h+var_C1C], eax
push    offset asc_419D50 ; "$%$"
push    esi             ; char *
call    _strstr
mov     [ebp+0C04h+var_C30], eax
push    offset asc_419D54 ; ")!)"
push    esi             ; char *
call    _strstr
add     esp, 28h
mov     ebx, eax
mov     [ebp+0C04h+var_C48], ebx
mov     edx, [ebp+0C04h+bstrString]
push    edx             ; bstrString
call    ds:SysFreeString
mov     eax, [ebp+0C04h+IHtmlElement]
```

Ketrican from 2015

```
push    ecx             ; lpWideCharStr
call    sub_406470
mov     esi, eax
push    offset asc_41BBDC ; "(!("
push    esi             ; char *
call    _strstr
push    offset a?       ; "#?#"
push    esi             ; char *
call    _strstr
mov     [ebp+var_2D58], eax
call    _strstr
push    offset asc_41BBE4 ; "^^^*"
push    esi             ; char *
mov     edi, eax
call    _strstr
push    offset asc_41BBE8 ; "$%$"
push    esi             ; char *
mov     [ebp+var_2D40], eax
call    _strstr
push    offset asc_41BBEC ; ")!)"
push    esi             ; char *
mov     [ebp+var_2D4C], eax
call    _strstr
mov     edx, [ebp+responseBody]
add     esp, 28h
push    edx             ; bstrString
mov     ebx, eax
call    ds:SysFreeString
mov     eax, [ebp+IHTMLElement]
mov     ecx, [eax]
mov     edx, [ecx+IHTMLElementUtbl.Release]
push    eax
```

```
push    offset asc_417B2C ; "<<"
push    offset Buffer   ; char *
call    _strstr
push    offset asc_417B30 ; ">>"
push    offset Buffer   ; char *
mov     [ebp+var_A10], eax
call    _strstr
push    offset asc_417B34 ; "||"
push    offset Buffer   ; char *
mov     esi, eax
call    _strstr
push    offset asc_417B38 ; "^^"
push    offset Buffer   ; char *
mov     edi, eax
call    _strstr
push    offset asc_417B3C ; "(("
push    offset Buffer   ; char *
mov     ebx, eax
call    _strstr
add     esp, 28h
cmp     [ebp+var_A10], 0
mov     [ebp+var_A04], eax
jz      loc_414189
test    esi, esi
jz      loc_414189
test    edi, edi
jz      loc_414189
test    ebx, ebx
jz      loc_414189
test    eax, eax
jz      loc_414189
```

Figure 9 // Specific format of data received from the C&C server in samples from operation Ke3chang (left) and 2015 Ketrican samples

4.1.4 DATA TRANSFORMATION

In the BS2005 malware samples, a specific two-step transformation is used for the data before it is sent to a remote server. First, the data is encrypted with a custom algorithm and then it is URL-safe, base64 encoded, meaning that all "+" characters are replaced with "*" characters, which allows the data to be transmitted as a part of the URL.

In one of the samples, the following *encryption algorithm* is used:

- Each byte has 0x27 plus its positional index byte added to it
- The byte is then XORed with its positional index byte

The same transformation is used in other samples from operation Ke3chang, except that constants other than 0x27 are used. In the samples discovered in 2015, the malware authors continued with this practice, as shown in Figure 10. Ketrican 2015 backdoors also use the combination of encryption and this URL-safe, base64 encoding and similarly vary the encryption method.

In some of the samples, a similar weak-encryption algorithm is used except that the constant is subtracted instead of being added. In yet other samples, the encryption algorithm has been changed to AES.

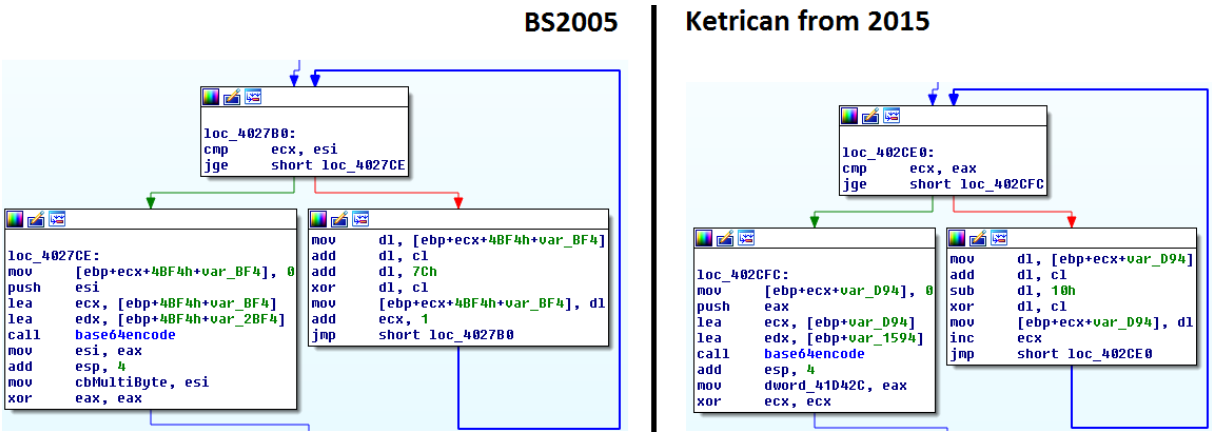


Figure 10 // Encryption algorithm used in a BS2005 sample and in a Ketrican backdoor discovered in 2015

4.1.5 FURTHER ATTRIBUTION CONSIDERATIONS

Our conclusions about the backdoors discovered in 2015 were also confirmed in a later Palo Alto Networks report about a malware family they call *TidePool*, which included two of the samples we analyzed[8]. The Palo Alto Network researchers claim the TidePool malware family is an evolution of BS2005 malware family, which is in accordance with our findings.

However, this fact alone would not be enough to attribute the malware samples detected in 2015 to the Ke3chang group, since we have to consider the possibility of malware reuse between different APT groups. As also stated in the *FireEye report*, the source code used in operation Ke3chang is likely shared among different developers or teams of developers. Thus, we cannot assume that anybody who uses this malware is automatically the Ke3chang group.

Nevertheless, we can confirm that the threat actor behind the samples discovered in 2015 had the same objectives and targeted the same type of organizations as the Ke3chang threat actor – diplomatic organizations and missions. This leads us to believe the group behind the Ketrican samples ESET discovered in 2015 is indeed the same actor that was behind operation Ke3chang.

4.2 Ke3chang activity in 2017 – Ketrican

The Ketrican samples from 2015 described in the previous section and Okrum samples from 2017 could easily look like being part of two independent operations targeted against the same organizations. However, we discovered a direct link between the two malware families - one of the Okrum backdoors[9] was used to drop a 2017 Ketrican sample[10].

This dropped backdoor had a PE Timestamp set to Aug 08 2017 that, according to our telemetry, appears to be valid. Our analysis showed it was – again – an evolution of backdoors used in operation Ke3chang, exhibiting the same coding style with several improvements. At some point, the attackers appear to have switched the Okrum backdoor to a freshly compiled Ketrican sample.

The samples detected in 2017 closely resemble BS2005 backdoors from operation Ke3chang. The same set of commands and methods of network communication are supported, and the main features remain unchanged.

8 SHA-1: 2748A2928B6A4A528709ABA20AEF93D1EC9010F9, 809C53F71549D83ED8AB5BAB312249212F6F4149
9 SHA-1: 1D271F22798313650C91C6FC34551CC8492A2019
10 SHA-1: D3BFB10DB08C6828C3001C1F825ED6A6BF6F6E01

Again, the authors continued to update the same parts of code as we have witnessed before. The special folder used as a working directory was updated to a new value (from `Local Appdata/Local Settings` to `Templates/AppData`).

Before the collected data is sent to a C&C server (using the very same technique as in the BS2005 malware), it undergoes the same transformation where encryption is combined with the same URL-safe base64 encoding. The encryption routine was updated to AES or RC4.

The authors also continue to use campaign names to keep track of the ongoing operations and to identify victims. Table 5 lists the IoCs extracted from the Ketrican samples detected in 2017.

SHA-1	PE Timestamp	C&C server	URI	Campaign Name
58DEA3A56DE1D95353230BE9BBBA582599AFE624	2009-01-14	forcan.hausblow[.]com	-	blue
FE2BF0A613482A40CCF84157361054EE77C07960	2016-12-19	login.allionhealth[.]com	-	login
D3BFB10DB08C6828C3001C1F825ED6A6BF6F6E01	2017-08-08	buy.babytoy-online[.]com	region	fvejautoexp
2C8B145EF5AC177C99DFCB8C0221E30B3A363A96	2017-08-08	newflow.babytoy-online[.]com	-	blue
D8AA9E4918E464D00BA95A3E28B8707A148EC4D7	2017-08-09	buy.babytoy-online[.]com	region	fvejautoexp
9D41B44AF5BAAF581C0D9D7BEF466213BD8BE01A	2017-08-10	press.premlist[.]com	-	press
F2BFDA51BDA3EE57878475817AF6E5F24FFBBB28	2017-08-23	items.babytoy-online[.]com	-	blue

Table 5 // IoCs extracted from the analyzed Ketrican samples discovered by ESET in 2017

4.3 Ke3chang activity in 2017 – RoyalDNS

In 2017, the entities affected by the Ketrican 2015 and Okrum backdoors were targeted with a variation of the RoyalDNS malware, which has already been attributed to the Ke3chang group. Its main characteristic is using the DNS protocol to communicate with the C&C server.

The RoyalDNS sample from the *NCC Group* report was compiled on June 3, 2017 while the data in the PE header of the newly discovered sample point to a more recent date, September 25, 2017. Both of the samples export the same functions, as seen in Figure 11, and use the very same rare type of communication with the C&C server.

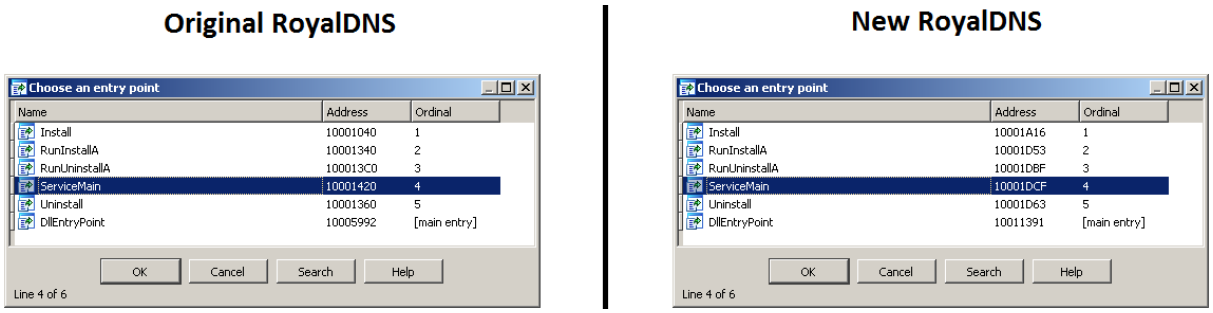


Figure 11 // The functions exported by the RoyalDNS backdoors

To communicate with the C&C server, a list of locally configured DNS servers is retrieved, and then the malware queries for specific TXT records of a C&C domain. The response from the DNS server encapsulates the backdoor commands. An example of such a DNS query packet is illustrated in Figure 12. The new RoyalDNS sample uses a different domain name than the original one:

- menorustru[.]com

Figure 12 // DNS query as a method to communicate with the C&C server

4.4 Ke3chang activity in 2018 – Ketrican

In 2018, we discovered new Ketrican samples. Among all the versions of the Ketrican backdoors we've found, these have evolved the most.

An option to load a DLL was added to the traditional set of supported commands. The encryption algorithm has been replaced with the XOR cipher (volume serial number of the C volume is used as the key).

The 2018 Ketrican backdoors use the same method of network communication as the samples from the BS2005 family – a combination of an HTTP request made via an instance of `IWebBrowser2` COM object and response HTML pages with hidden input fields. What is different is that instead of using the `CoCreateInstance` API function to create the COM object instance directly, a *registration-free COM* technique is used.

Finally, the 2018 Ketrican backdoors share another feature common for Ke3chang group backdoors. They are known to modify specific registry keys and values in order to weaken some security settings of the compromised machine, which can help them further extend their malicious capabilities to provide those not available via the backdoor itself.

For example, Internet Explorer Enhanced Security configuration can be disabled by setting the following registry value:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap]
    "IEHarden" = 0
```

By setting this value, prevention of script execution and other valuable protections are disabled.

This is not a new feature; the same set of registry keys is changed in *BS2005 and Tidepool malware families*, and in the Ketrican samples discovered in 2015, 2017 and 2018. The samples from 2018 are, however, the first ones to use PowerShell scripts to modify the keys. The older versions of the malware used registry API functions or the `reg.exe` utility for that.

SHA-1	PE Timestamp	C&C server	URI	Campaign Name
C1C89A1A1779515EC1DFD0EFFF293615D523279E	2018-02-01	dsmanfacture.privatedns[.]org	-	-
09B7999160C5D0DC9A7443F0FC248B6C23BC0724	2018-07-17	compatsec[.]com	-	-
6BF0923577FE5939DEA66F466B74683AE2EBBC3E	2018-07-17	compatsec[.]com	-	-

Table 6 // IoCs extracted from 2018 Ketrican samples

4.5 Ke3chang activity in 2019 – Ketrican

In March 2019, we detected two new Ketrican samples, one of which was similar to the 2018 Ketrican backdoor, and the other that has evolved from it. The previous Ketrican samples and the samples detected in 2019 largely overlap in commands, network communication, and obfuscation. The 2019 version also modifies the same rare combination of registry values as all earlier Ketrican samples, which is explained in the section above.

There is one noteworthy difference between the previous Ketrican samples and the 2019 ones: instead of executing a new `cmd.exe` process for each PowerShell command (i.e. to change every registry value), there is only one instance of the process, which communicates with the malware over anonymous pipes.

SHA-1	PE Timestamp	C&C server	URI	Campaign Name
D98D258C234F5CEAD43FD897613B2EA2669AA7C0	2019-01-28	chart.healthcare-internet[.]com	-	-
CE94EC2CFB23D8C662F558C69B64104C78B9D098	2019-04-25	inicializacion[.]com	-	cion

Table 7 // IoCs extracted from 2019 Ketrican samples

5 CONCLUSION

The Ke3chang APT group (a.k.a. APT15) has rightfully been on the radar of security researchers because of its decade-long operation, targeting high-value victims such as diplomatic entities, and other geopolitical aspects associated with them.

While ESET does not engage in attribution of these activities to a particular nation-state, we do attempt attribution of individual malware-driven cyberattacks to a particular APT group.

In this paper we have documented the previously unknown malware, Okrum, detected by ESET in Slovakia, Belgium, Chile, Guatemala and Brazil, documented other suspected Ke3chang activity (using the Ketrican and RoyalDNS malware families), and provided evidence that drives us to the conclusion that all of this is indeed the work of the Ke3chang threat actor.

Just like other known Ke3chang malware, Okrum is not technically complex, but we can certainly see that the malicious actors behind it were trying to remain undetected by using tactics such as embedding the malicious payload within a legitimate PNG image, employing several anti-emulation and anti-sandbox tricks, as well as making frequent changes in implementation. As for the analyzed Ketrican samples, these show visible evolution and code improvements from 2015 to 2019.

What remains to be answered is how the malware was distributed to the victim machines.

ESET will continue to track the malicious activities of the Ke3chang threat group.

6 INDICATORS OF COMPROMISE (IOCS)

6.1 Okrum

6.1.1 ESET DETECTION NAMES

- Win32/Okrum.A
- Win32/Okrum.B
- Win32/Okrum.C
- Win32/Okrum.D
- Win32/Okrum.E
- Win32/Okrum.F
- Win32/Okrum.G
- Win32/Okrum.H
- Win32/Okrum.I

6.1.2 SHA-1

- 1CDC632E0A26F39E527ACF7B1CDECD829A6A2B3D
- 1D271F22798313650C91C6FC34551CC8492A2019
- 371B14F8BFD9B5DB098139E7FE2EBD4381CB259C
- 38299BCF0BA25E331939683597F161A3D7121A26
- 48F8BAFB334C6980FB578C09D7297A4B7F5E09E2
- 5FBAFB71CFDF0C93E19882630D05F37C1F756CBF
- 8D7E503D972C03C0F87F2D6F6EF65F1381D21BC6
- A426BCC6317F0D49F0F0B68091E8161C512E22C3
- AD740FD11688B2B39072C7024679CC22878E2619
- F0E2C3AF0297C80C0A14E95E151FC7DC319ACFC3
- F42A9D85ABE04E721461FE2B52DDC9E0EA411D9E

6.1.3 C&C SERVERS

- finance.globaleducat[.]com
- support.slovakmaps[.]com
- misiones.soportesisco[.]com

6.1.4 MUTEX NAMES

- qDJsxrGpPacRndLdsdIoqesGBv
- SnpcnSHPPxsdfcwzEkmtdv
- zSpgnEHPPcvAltcFzlIscD

6.2 Ketrican

6.2.1 ESET DETECTION NAMES

- Win32/Ketrican.A
- Win32/Ketrican.B
- Win32/Ketrican.C
- Win32/Ketrican.D
- Win32/Ketrican.E
- Win32/Ketrican.F
- Win32/Ketrican.G
- Win32/Ketrican.H
- Win32/Ketrican.I
- Win32/Ketrican.J
- Win32/Ketrican.K
- Win32/Ketrican.L
- Win32/Ketrican.M
- Win32/Ketrican.N
- Win32/Ketrican.O
- Win32/Ketrican.P
- Win32/Ketrican.Q
- Win32/Ketrican.R
- Win32/Ketrican.S
- Win32/Ketrican.T

6.2.2 KETRICAN 2015

6.2.2.1 SHA-1

- 054EB61F2CE6DEB4FE011335CD88EBA530B8D09A
- 10BD61F3FB03632E270FEF3AB6515677405A472F
- 1730D90FFB888877EA2F18198BCC592087218E9A
- 1C7559C57606B359EEB57F0416FE0B2784C01395
- 233FF39DDE5A13CBF78EC1E9C020CF3CF18084E7
- 2748A2928B6A4A528709ABA20AEF93D1EC9010F9
- 43A4CC528134E218B9CEC2FF0C24B5912BF5C032
- 4636E5FB97AFA68F60BE9247F5EB9684CA9CDBA6
- 4C1198F726ACAD7AF78B36F250A128D5E3C52D8C
- 65E3947144F6A3C31BC88E445514A83FCB331AFD
- 7581337DB29E092101E4FD692D01AA26D65FA40A
- 77369D3735B3B2C24CCAA93ECAA903D816EA9CD9
- 809C53F71549D83ED8AB5BAB312249212F6F4149
- 844E710D85DD63AA5BF245CEE94C1CC872429BD3
- 86513FE43F2F2D2C486D6265C9098315E774F791
- 94E6CB95585DBB59A61EC4029BC7EBB30BBA57E5
- A23EE1F17B746C1907293C7F8155E3E7DE135648
- AB7F63649BBC53E45DEEB7269BEBD54815AE9E27
- B49EDC05658907C888074905CE234BF3CF58D8A0
- D3A96C0FA84BFEE826E175D4664116A169D15D4E

- D3D0DED17D0029DFD90DA2AE74ADA885779E8926
- D7DFB547033B82765F8B0A6B70A22A4EC204D7A8
- DD753FCBAD4BE31066F278585D14C411DB3D7795

6.2.2.2 C&C servers

- center.nmsvillage[.]com
- control.mimepanel[.]org
- daily.huntereim[.]com
- dream.zepotac[.]com
- dyname.europemis[.]com
- item.amazonout[.]com
- promise.miniaturizate[.]org
- rain.nmsvillage[.]com
- store.ufmsecret[.]org
- translate.europemis[.]com
- view.beleimprensa[.]org
- wind.deltimesweb[.]com

6.2.3 KETRICAN 2017

6.2.3.1 SHA-1

- 2C8B145EF5AC177C99DFCB8C0221E30B3A363A96
- 58DEA3A56DE1D95353230BE9BBBA582599AFE624
- 9D41B44AF5BAAF581C0D9D7BEF466213BD8BE01A
- D3BFB10DB08C6828C3001C1F825ED6A6BF6F6E01
- D8AA9E4918E464D00BA95A3E28B8707A148EC4D7
- F2BFDA51BDA3EE57878475817AF6E5F24FFBBB28
- FE2BF0A613482A40CCF84157361054EE77C07960

6.2.3.2 C&C servers

- buy.babytoy-online[.]com
- forcan.hausblow[.]com
- items.babytoy-online[.]com
- login.allionhealth[.]com
- newflow.babytoy-online[.]com
- press.premlist[.]com

Note: *We have not detected samples using the following C&C servers. We extracted them by observing the similarities in the C&C infrastructure used by the malware.*

- grek.freetaxbar[.]com
- items.burgermap[.]org
- upcv.inciohali[.]com
- www1.sanpaulostat[.]com
- cv.livehams[.]com
- info.audioexp[.]com

6.2.4 KETRICAN 2018

6.2.4.1 SHA-1

- 09B7999160C5D0DC9A7443F0FC248B6C23BC0724
- 6BF0923577FE5939DEA66F466B74683AE2EBBC3E
- C1C89A1A1779515EC1DFD0EFFF293615D523279E

6.2.4.2 C&C servers

- compatsec[.]com
- dsmanfacture.privatedns[.]org

6.2.5 KETRICAN 2019

6.2.5.1 SHA-1

- D98D258C234F5CEAD43FD897613B2EA2669AA7C0
- CE94EC2CFB23D8C662F558C69B64104C78B9D098

6.2.5.2 C&C servers

- chart.healthcare-internet[.]com
- inicializacion[.]com

6.3 RoyalDns

6.3.1 ESET DETECTION NAMES

- Win32/RoyalDNS.A
- Win32/RoyalDNS.B

6.3.2 SHA-1

- 23796442F7CE7288837536EBF4E8620DB55A0BC1

6.3.3 C&C SERVERS

- menorustru[.]com

7 MITRE ATT&CK TECHNIQUES (OKRUM)

Tactic	ID	Name	Description
Execution	T1059	Command-Line Interface	Okrum's backdoor uses `cmd.exe` to execute arbitrary commands.
	T1064	Scripting	The backdoor uses batch scripts to update itself to a newer version.
	T1035	Service Execution	The Stage 1 loader creates a new service named `NtmsSvc` to execute the payload.
Persistence	T1050	New Service	To establish persistence, Okrum installs itself as a new service named `NtmSsvc`.
	T1060	Registry Run Keys / Startup Folder	Okrum establishes persistence by creating a .lnk shortcut to itself in the `Startup` folder.
	T1053	Scheduled Task	The installer component tries to achieve persistence by creating a scheduled task.
	T1023	Shortcut Modification	Okrum establishes persistence by creating a .lnk shortcut to itself in the `Startup` folder.

Tactic	ID	Name	Description
Privilege Escalation	T1134	Access Token Manipulation	Okrum can impersonate a logged on user's security context using a call to the `ImpersonateLoggedOnUser` API.
Defense Evasion	T1140	Deobfuscate/Decode Files or Information	The Stage 1 loader decrypts the backdoor code, embedded within the loader or within a legitimate PNG file. A custom XOR cipher or RC4 is used for decryption.
	T1107	File Deletion	Okrum's backdoor deletes files after they have been successfully uploaded to C&C servers.
	T1158	Hidden Files and Directories	Before exfiltration, Okrum's backdoor uses hidden files to store logs and outputs from backdoor commands.
	T1066	Indicator Removal from Tools	Okrum underwent regular technical improvements to evade antivirus detection.
	T1036	Masquerading	Okrum establishes persistence by adding a new service `NtmsSvc` with the display name `Removable Storage` in an attempt to masquerade as a legitimate Removable Storage Manager.
	T1027	Obfuscated Files or Information	Okrum's payload is encrypted and embedded within the Stage 1 loader, or within a legitimate PNG file.
	T1497	Virtualization/Sandbox Evasion	The Stage 1 loader performs several checks on the victim's machine to avoid being emulated or executed in a sandbox.
Credential Access	T1003	Credential Dumping	Okrum was seen using *MimikatzLite* and modified *Quarks PwDump* to perform credential dumping.
Discovery	T1083	File and Directory Discovery	Okrum was seen using *DriveLetterView* to enumerate drive information.
	T1082	System Information Discovery	Okrum collects computer name, locale information, and information about the OS and architecture.
	T1016	System Network Configuration Discovery	Okrum collects network information, including host IP address, DNS and proxy information.
	T1049	System Network Connections Discovery	Okrum used *NetSess* to discover NetBIOS sessions.
	T1033	System Owner/User Discovery	Okrum collects the victim user name.
	T1124	System Time Discovery	Okrum can obtain the date and time of the compromised system.
Collection	T1056	Input Capture	Okrum was seen using a keylogger tool to capture keystrokes.
Exfiltration	T1002	Data Compressed	Okrum was seen using a RAR archiver tool to compress data.
	T1022	Data Encrypted	Okrum uses AES encryption and base64 encoding of files before exfiltration.
	T1041	Exfiltration Over Command and Control Channel	Data exfiltration is done using the already opened channel with the C&C server.
Command And Control	T1043	Commonly Used Port	Okrum uses port 80 for C&C.
	T1090	Connection Proxy	Okrum identifies a proxy server if it exists and uses it to make HTTP requests.
	T1132	Data Encoding	The communication with the C&C server is base64 encoded.
	T1001	Data Obfuscation	The communication with the C&C server is hidden in the `Cookie` and `Set-Cookie` headers of HTTP requests.
	T1071	Standard Application Layer Protocol	Okrum uses HTTP for communication with its C&C.
	T1032	Standard Cryptographic Protocol	Okrum uses AES to encrypt network traffic. The key can be hardcoded or negotiated with the C&C server in the registration phase.

ABOUT ESET

For 30 years, *ESET®* has been developing industry-leading IT security software and services for businesses and consumers worldwide. With solutions ranging from endpoint and mobile security, to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give consumers and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company. Backed by R&D centers worldwide, ESET becomes the first IT security company to earn *100 Virus Bulletin VB100* awards, identifying every single "in-the-wild" malware without interruption since 2003. For more information, visit www.eset.com or follow us on *LinkedIn*, *Facebook* and *Twitter*.

ENJOY SAFER TECHNOLOGY™

APPENDIX A

.COM, .NET DOMAINS

VeriSign, Inc.
VeriSign Information Services, Inc.
12061 Bluemont Way
Reston, Virginia 20190
United States

primenuesty.com	Domain Name: primenuesty.com Registry Domain ID: 2579399497_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2021-09-17T02:35:21Z Creation Date: 2020-12-18T02:27:04Z Registrar Registration Expiration Date: 2022-12-18T02:27:04Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Registrant Organization: Registrant State/Province: Registrant Country: PT Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=primenuesty.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=primenuesty.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=primenuesty.com Name Server: NS21.DOMAINCONTROL.COM Name Server: NS22.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

beesweiserdog.com	Domain Name: beesweiserdog.com Registry Domain ID: 2579399498_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2021-09-17T09:32:19Z Creation Date: 2020-12-18T02:27:04Z Registrar Registration Expiration Date: 2022-12-18T02:27:04Z 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 Registrant Organization: Registrant State/Province: Registrant Country: PT Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=beesweiserdog.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=beesweiserdog.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=beesweiserdog.com Name Server: NS21.DOMAINCONTROL.COM Name Server: NS22.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2021-10-27T20:30:48Z <<< For more information on Whois status codes, please visit https://icann.org/epp
bluehostfit.com	Domain Name: bluehostfit.com Registry Domain ID: 2578968116_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com

	Registrar URL: http://www.godaddy.com Updated Date: 2021-03-26T06:49:10Z Creation Date: 2020-12-15T22:20:50Z Registrar Registration Expiration Date: 2022-12-15T22:20:50Z 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 Registrant Organization: Registrant State/Province: Beijing Registrant Country: CN Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=blueheostfit.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=blueheostfit.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=blueheostfit.com Name Server: NS01.DOMAINCONTROL.COM Name Server: NS02.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
business-toys.com	Domain Name: business-toys.com Registry Domain ID: 2561049332_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2020-09-21T01:07:25Z Creation Date: 2020-09-20T19:54:28Z Registrar Registration Expiration Date: 2022-09-20T19:54:28Z 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 Registrant Organization: Registrant State/Province: Registrant Country: CN Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=business-toys.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=business-toys.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=business-toys.com Name Server: NS35.DOMAINCONTROL.COM Name Server: NS36.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
cleanskycloud.com	Domain Name: cleanskycloud.com Registry Domain ID: 2538226317_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2021-01-25T08:38:58Z Creation Date: 2020-06-15T02:21:36Z Registrar Registration Expiration Date: 2022-06-15T02:21:36Z 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 Registrant Organization: Registrant State/Province: Fujian Registrant Country: CN Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=cleanskycloud.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=cleanskycloud.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=cleanskycloud.com Name Server: NS67.DOMAINCONTROL.COM Name Server: NS68.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2021-10-27T20:32:07Z <<< For more information on Whois status codes, please visit https://icann.org/epp
czreadsecurity.com	Domain Name: czreadsecurity.com Registry Domain ID: 2565746605_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2020-10-14T08:55:33Z Creation Date: 2020-10-14T02:52:41Z Registrar Registration Expiration Date: 2021-10-14T02:52:41Z 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 Registrant Organization: Registrant State/Province: Guangxi Registrant Country: CN

	Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=czreadsecurity.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=czreadsecurity.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=czreadsecurity.com Name Server: NS17.DOMAINCONTROL.COM Name Server: NS18.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2021-10-27T20:32:48Z <<< For more information on Whois status codes, please visit https://icann.org/epp
elcolectador.com	omain Name: elcolectador.com Registry Domain ID: 2604797971_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2021-04-13T09:23:29Z Creation Date: 2021-04-13T04:11:47Z Registrar Registration Expiration Date: 2022-04-13T04:11:47Z 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 Registrant Organization: Registrant State/Province: Guangxi Registrant Country: CN Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=elcolectador.com Tech Email: Select Contact Domain Holder link at

	https://www.godaddy.com/whois/results.aspx?domain=elcolectador.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=elcolectador.com Name Server: NS27.DOMAINCONTROL.COM Name Server: NS28.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2021-10-27T20:33:38Z <<< For more information on Whois status codes, please visit https://icann.org/epp
fheacor.com	Domain Name: fheacor.com Registry Domain ID: 2443759095_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2021-09-17T07:12:49Z Creation Date: 2019-10-15T01:55:29Z Registrar Registration Expiration Date: 2022-10-15T01:55:29Z 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 Registrant Organization: Registrant State/Province: Fujian Registrant Country: CN Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=fheacor.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=fheacor.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=fheac

	or.com Name Server: NS53.DOMAINCONTROL.COM Name Server: NS54.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System : http://wdprs.internic.net/
francevrteepress.com	Domain Name: francevrteepress.com Registry Domain ID: 2514229656_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2021-01-25T07:38:24Z Creation Date: 2020-04-13T04:36:53Z Registrar Registration Expiration Date: 2022-04-13T04:36:53Z 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 Registrant Organization: Registrant State/Province: Beijing Registrant Country: CN Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=francevrteepress.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=francevrteepress.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=francevrteepress.com Name Server: NS35.DOMAINCONTROL.COM Name Server: NS36.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System : http://wdprs.internic.net/ >>> Last update of WHOIS database: 2021-10-27T20:34:32Z <<<

	For more information on Whois status codes, please visit https://icann.org/epp
gardienweb.com	Domain Name: gardienweb.com Registry Domain ID: 2455044810_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2019-11-14T03:33:07Z Creation Date: 2019-11-13T22:33:10Z Registrar Registration Expiration Date: 2021-11-13T22:33:10Z 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 Registrant Organization: Registrant State/Province: Shanghai Registrant Country: CN Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=gardienweb.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=gardienweb.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=gardienweb.com Name Server: NS31.DOMAINCONTROL.COM Name Server: NS32.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
heimflugaustr.com	Domain Name: heimflugaustr.com Registry Domain ID: 2538226316_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2021-01-25T08:40:53Z Creation Date: 2020-06-15T02:21:35Z

	Registrar Registration Expiration Date: 2022-06-15T02:21:35Z 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 Registrant Organization: Registrant State/Province: Fujian Registrant Country: CN Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=heimflugaustr.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=heimflugaustr.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=heimflugaustr.com Name Server: NS67.DOMAINCONTROL.COM Name Server: NS68.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
ivpsers.com	Domain Name: ivpsers.com Registry Domain ID: 2437342802_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2021-09-17T07:12:49Z Creation Date: 2019-09-26T01:57:33Z Registrar Registration Expiration Date: 2022-09-26T01:57:33Z 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 Registrant Organization: Registrant State/Province: Fujian Registrant Country: CN Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=ivpsers.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=ivpsers.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=ivpsers.com Name Server: NS13.DOMAINCONTROL.COM Name Server: NS14.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
micrlmb.com	Domain Name: micrlmb.com Registry Domain ID: 2014506531_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2021-01-19T09:44:02Z Creation Date: 2016-03-22T02:57:44Z Registrar Registration Expiration Date: 2022-03-22T02:57:44Z 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 Registrant Organization: Registrant State/Province: Beijing

	Registrant Country: CN Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=micrlmb.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=micrlmb.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=micrlmb.com Name Server: NS03.DOMAINCONTROL.COM Name Server: NS04.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System : http://wdprs.internic.net/
muthesck.com	Domain Name: muthesck.com Registry Domain ID: 2494791616_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2021-09-22T02:00:15Z Creation Date: 2020-02-20T04:17:56Z Registrar Registration Expiration Date: 2022-02-20T04:17:56Z 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 Registrant Organization: Registrant State/Province: Brussels Registrant Country: BE Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=muthesck.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=muthesck.com Admin Email: Select Contact Domain Holder link at

	https://www.godaddy.com/whois/results.aspx?domain=muthesck.com Name Server: NS09.DOMAINCONTROL.COM Name Server: NS10.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
netscalertech.com	Domain Name: netscalertech.com Registry Domain ID: 2482815370_DOMAIN_COM-VRSN Registrar WHOIS Server: WHOIS.ENOM.COM Registrar URL: WWW.ENOM.COM Updated Date: 2020-12-24T12:01:25.00Z Creation Date: 2020-01-21T07:53:00.00Z Registrar Registration Expiration Date: 2022-01-21T07:53:00.00Z Registrar: ENOM, INC. Registrar IANA ID: 48 Domain Status: ok https://www.icann.org/epp#ok Registrant Name: REDACTED FOR PRIVACY Registrant Organization: REDACTED FOR PRIVACY Registrant Street: REDACTED FOR PRIVACY Registrant Street: 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: Registrant Fax: REDACTED FOR PRIVACY Registrant Email: https://tieredaccess.com/contact/36c7166e-a01d-4a90-bf26-4b20a8f93d0a Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin Street: 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 Email: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY

	Tech Street: REDACTED FOR PRIVACY Tech Street: 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 Email: REDACTED FOR PRIVACY Name Server: DNS1.NAME-SERVICES.COM Name Server: DNS2.NAME-SERVICES.COM Name Server: DNS3.NAME-SERVICES.COM Name Server: DNS4.NAME-SERVICES.COM Name Server: DNS5.NAME-SERVICES.COM DNSSEC: unsigned Registrar Abuse Contact Email: abuse@enom.com Registrar Abuse Contact Phone: +1.4259744689 URL of the ICANN WHOIS Data Problem Reporting System : HTTP://WDPRS.INTERNIC.NET/
newgoldbalmap.com	Domain Name: newgoldbalmap.com Registry Domain ID: 2552476561_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2021-07-06T08:02:26Z Creation Date: 2020-08-12T03:34:33Z Registrar Registration Expiration Date: 2022-08-12T03:34:33Z 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 Registrant Organization: Registrant State/Province: Guangxi Registrant Country: CN Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=newg

	oldbalmap.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=newgoldbalmap.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=newgoldbalmap.com Name Server: NS21.DOMAINCONTROL.COM Name Server: NS22.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2021-10-27T20:37:04Z <<< For more information on Whois status codes, please visit https://icann.org/epp
news-laestrella.com	Domain Name: news-laestrella.com Registry Domain ID: 2497431532_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2020-12-25T00:56:25Z Creation Date: 2020-02-26T21:54:49Z Registrar Registration Expiration Date: 2022-02-26T21:54:49Z 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 Registrant Organization: Registrant State/Province: Gansu Registrant Country: CN Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=news-laestrella.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=news-laestrella.com

	Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=news-laestrella.com Name Server: NS11.DOMAINCONTROL.COM Name Server: NS12.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System : http://wdprs.internic.net/ >>> Last update of WHOIS database: 2021-10-27T20:37:16Z <<< For more information on Whois status codes, please visit https://icann.org/epp
opentanzanfoundation.com	Domain Name: opentanzanfoundation.com Registry Domain ID: 2642968289_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2021-09-23T03:40:31Z Creation Date: 2021-09-22T22:21:17Z Registrar Registration Expiration Date: 2022-09-22T22:21:17Z 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 Registrant Organization: Registrant State/Province: Jiangxi Registrant Country: CN Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=opentanzanfoundation.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=opentanzanfoundation.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=opentanzanfoundation.com Name Server: NS41.DOMAINCONTROL.COM

	Name Server: NS42.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System : http://wdprs.internic.net/ >>> Last update of WHOIS database: 2021-10-29T21:52:25Z <<< For more information on Whois status codes, please visit https://icann.org/epp
optonlinepress.com	Domain Name: opentanzanfoundation.com Registry Domain ID: 2642968289_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2021-09-23T03:40:31Z Creation Date: 2021-09-22T22:21:17Z Registrar Registration Expiration Date: 2022-09-22T22:21:17Z 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 Registrant Organization: Registrant State/Province: Jiangxi Registrant Country: CN Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=opentanzanfoundation.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=opentanzanfoundation.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=opentanzanfoundation.com Name Server: NS41.DOMAINCONTROL.COM Name Server: NS42.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System : http://wdprs.internic.net/

palazzochigi.com	Domain Name: palazzochigi.com Registry Domain ID: 2556091097_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2020-08-28T06:42:10Z Creation Date: 2020-08-27T22:29:52Z Registrar Registration Expiration Date: 2022-08-27T22:29:52Z 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 Registrant Organization: Registrant State/Province: Registrant Country: CN Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=palazzochigi.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=palazzochigi.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=palazzochigi.com Name Server: NS39.DOMAINCONTROL.COM Name Server: NS40.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
pandemicacre.com	Domain Name: pandemicacre.com Registry Domain ID: 2565746617_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2021-08-17T09:41:13Z Creation Date: 2020-10-14T02:52:45Z Registrar Registration Expiration Date: 2022-10-14T02:52:45Z

	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 Registrant Organization: Registrant State/Province: Guangxi Registrant Country: CN Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=pandemicacre.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=pandemicacre.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=pandemicacre.com Name Server: NS17.DOMAINCONTROL.COM Name Server: NS18.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
papa-ser.com	Domain Name: papa-ser.com Registry Domain ID: 2496683457_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2020-12-25T01:39:10Z Creation Date: 2020-02-25T03:49:12Z Registrar Registration Expiration Date: 2022-02-25T03:49:12Z 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 Registrant Organization: Registrant State/Province: Guangdong Registrant Country: CN Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=papa-ser.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=papa-ser.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=papa-ser.com Name Server: NS41.DOMAINCONTROL.COM Name Server: NS42.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
pekematclouds.com	Domain Name: pekematclouds.com Registry Domain ID: 2514229655_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2021-01-25T07:43:42Z Creation Date: 2020-04-13T04:36:53Z Registrar Registration Expiration Date: 2022-04-13T04:36:53Z 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 Registrant Organization: Registrant State/Province: Beijing Registrant Country: CN Registrant Email: Select Contact Domain Holder link at

	https://www.godaddy.com/whois/results.aspx?domain=pekematclouds.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=pekematclouds.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=pekematclouds.com Name Server: NS35.DOMAINCONTROL.COM Name Server: NS36.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System : http://wdprs.internic.net/
pipcake.com	Domain Name: pipcake.com Registry Domain ID: 2339451081_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2021-09-17T09:16:13Z Creation Date: 2018-12-03T08:14:20Z Registrar Registration Expiration Date: 2022-12-03T08:14:20Z 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 Registrant Organization: Registrant State/Province: Registrant Country: PT Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=pipcake.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=pipcake.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=pipcake.com

	Name Server: NS53.DOMAINCONTROL.COM Name Server: NS54.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
popularservicenter.com	Domain Name: popularservicenter.com Registry Domain ID: 2565746608_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2021-07-06T08:02:54Z Creation Date: 2020-10-14T02:52:42Z Registrar Registration Expiration Date: 2022-10-14T02:52:42Z 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 Registrant Organization: Registrant State/Province: Guangxi Registrant Country: CN Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=popularservicenter.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=popularservicenter.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=popularservicenter.com Name Server: NS17.DOMAINCONTROL.COM Name Server: NS18.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2021-10-27T20:39:15Z <<<

	For more information on Whois status codes, please visit https://icann.org/epp
projectsyndic.com	Domain Name: projectsyndic.com Registry Domain ID: 2538227371_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2021-01-25T08:37:00Z Creation Date: 2020-06-15T02:33:49Z Registrar Registration Expiration Date: 2022-06-15T02:33:49Z 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 Registrant Organization: Registrant State/Province: Fujian Registrant Country: CN Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=projectsyndic.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=projectsyndic.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=projectsyndic.com Name Server: NS67.DOMAINCONTROL.COM Name Server: NS68.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2021-10-27T20:39:52Z <<< For more information on Whois status codes, please visit https://icann.org/epp
qsadtv.com	Domain Name: qsadtv.com Registry Domain ID: 1839567499_domain_com-vrsn

	Registrar WHOIS Server: whois.paycenter.com.cn Registrar URL: http://www.xinnet.com Updated Date: 2020-11-30T08:34:16Z Creation Date: 2013-12-18T08:42:20Z Registrar Registration Expiration Date: 2021-12-18T08:42:20Z Registrar: Xin Net Technology Corporation Registrar IANA ID: 120 Registrar Abuse Contact Email: supervision@xinnet.com Registrar Abuse Contact Phone: +86.4008182233 Reseller: Domain Status: ok https://www.icann.org/epp#ok Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: REDACTED FOR PRIVACY Registrant Street: REDACTED FOR PRIVACY Registrant State/Province: AH Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: CN Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: link at http://whois.xinnet.com/sendemail/qsadtv.com 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 PostalCode: 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: link at http://whois.xinnet.com/sendemail/qsadtv.com 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 PostalCode: 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: link at http://whois.xinnet.com/sendemail/qsadtv.com Name Server: ns1.gnway.com Name Server: ns1.gnway.cn DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
scielope.com	Domain Name: scielope.com Registry Domain ID: 2451635946_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2021-09-29T07:28:57Z Creation Date: 2019-11-05T00:11:16Z Registrar Registration Expiration Date: 2022-11-05T00:11:16Z 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 Registrant Organization: Registrant State/Province: rehab Registrant Country: BO Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=scielope.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=scielope.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=scielope.com

	Name Server: NS65.DOMAINCONTROL.COM Name Server: NS66.DOMAINCONTROL.COM DNSSEC: unsignedURL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
seoamdcopywriting.com	Domain Name: seoamdcopywriting.com Registry Domain ID: 2550718929_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2021-03-26T00:14:59Z Creation Date: 2020-08-04T02:20:44Z Registrar Registration Expiration Date: 2022-08-04T02:20:44Z 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 Registrant Organization: Registrant State/Province: jiulong Registrant Country: HK Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=seoamdcopywriting.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=seoamdcopywriting.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=seoamdcopywriting.com Name Server: NS49.DOMAINCONTROL.COM Name Server: NS50.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2021-10-27T20:40:52Z <<<

	For more information on Whois status codes, please visit https://icann.org/epp
slidenshare.com	Domain Name: slidenshare.com Registry Domain ID: 2550718928_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2021-03-26T00:10:06Z Creation Date: 2020-08-04T02:20:44Z Registrar Registration Expiration Date: 2022-08-04T02:20:44Z 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 Registrant Organization: Registrant State/Province: jiulong Registrant Country: HK Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=slidenshare.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=slidenshare.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=slidenshare.com Name Server: NS21.DOMAINCONTROL.COM Name Server: NS22.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
somoswake.com	Domain Name: somoswake.com Registry Domain ID: 2550718924_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2021-03-25T09:13:58Z Creation Date: 2020-08-04T02:20:43Z

	Registrar Registration Expiration Date: 2022-08-04T02:20:43Z 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 Registrant Organization: Registrant State/Province: jiulong Registrant Country: HK Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=somoswake.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=somoswake.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=somoswake.com Name Server: NS11.DOMAINCONTROL.COM Name Server: NS12.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
squarespacenow.com	Domain Name: squarespacenow.com Registry Domain ID: 2578968112_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2021-03-26T00:04:43Z Creation Date: 2020-12-15T22:20:47Z Registrar Registration Expiration Date: 2022-12-15T22:20:47Z 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 Registrant Organization: Registrant State/Province: Beijing Registrant Country: CN Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=squarespacenow.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=squarespacenow.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=squarespacenow.com Name Server: NS31.DOMAINCONTROL.COM Name Server: NS32.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
subapostilla.com	Domain Name: subapostilla.com Registry Domain ID: 2592130574_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2021-02-18T01:29:35Z Creation Date: 2021-02-17T20:21:35Z Registrar Registration Expiration Date: 2022-02-17T20:21:35Z 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 Registrant Organization: Registrant State/Province: Beijing

	Registrant Country: CN Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=subaposTilla.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=subaposTilla.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=subaposTilla.com Name Server: NS77.DOMAINCONTROL.COM Name Server: NS78.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2021-10-27T20:42:06Z <<< For more information on Whois status codes, please visit https://icann.org/epp
suzukicycles.net	Domain Name: suzukicycles.net Registry Domain ID: 2451284254_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2021-01-20T09:03:41Z Creation Date: 2019-11-04T08:13:36Z Registrar Registration Expiration Date: 2021-11-04T08:13:36Z 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 Registrant Organization: Registrant State/Province: Kentucky Registrant Country: US Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=suzukicycles.net

	Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=suzukicycles.net Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=suzukicycles.net Name Server: NS25.DOMAINCONTROL.COM Name Server: NS26.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System : http://wdprs.internic.net/
tatanotakeeps.com	Domain Name: tatanotakeeps.com Registry Domain ID: 2384156074_DOMAIN_COM-VRSN Registrar WHOIS Server: WHOIS.ENOM.COM Registrar URL: WWW.ENOM.COM Updated Date: 2021-04-25T01:00:11.00Z Creation Date: 2019-04-25T07:52:00.00Z Registrar Registration Expiration Date: 2022-04-25T07:52:52.00Z Registrar: ENOM, INC. Registrar IANA ID: 48 Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited Registrant Name: REDACTED FOR PRIVACY Registrant Organization: REDACTED FOR PRIVACY Registrant Street: REDACTED FOR PRIVACY Registrant Street: Registrant City: REDACTED FOR PRIVACY Registrant State/Province: WI Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: Registrant Fax: REDACTED FOR PRIVACY Registrant Email: https://tieredaccess.com/contact/0cda1b74-a013-4048-8ae5-37fc47270e85 Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin Street: 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 Email: REDACTED FOR PRIVACY Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech Street: 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 Email: REDACTED FOR PRIVACY Name Server: DNS1.NAME-SERVICES.COM Name Server: DNS2.NAME-SERVICES.COM Name Server: DNS3.NAME-SERVICES.COM Name Server: DNS4.NAME-SERVICES.COM Name Server: DNS5.NAME-SERVICES.COM DNSSEC: unsigned Registrar Abuse Contact Email: abuse@enom.com Registrar Abuse Contact Phone: +1.4259744689 URL of the ICANN WHOIS Data Problem Reporting System : HTTP://WDPRS.INTERNIC.NET/
transactioninfo.net	Domain Name: transactioninfo.net Registry Domain ID: 2607722833_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2021-04-26T03:34:31Z Creation Date: 2021-04-25T22:32:23Z Registrar Registration Expiration Date: 2022-04-25T22:32:23Z 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

	Registrant Organization: Registrant State/Province: Guangxi Registrant Country: CN Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=transactioninfo.net Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=transactioninfo.net Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=transactioninfo.net Name Server: NS63.DOMAINCONTROL.COM Name Server: NS64.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
headhunterblue.com	Domain Name: headhunterblue.com Registry Domain ID: 2587613225_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2021-01-28T09:09:44Z Creation Date: 2021-01-28T02:28:33Z Registrar Registration Expiration Date: 2022-01-28T02:28:33Z 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 Registrant Organization: Registrant State/Province: Beijing Registrant Country: CN Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=headhunterblue.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=headh

	unterblue.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=headhunterblue.com Name Server: NS75.DOMAINCONTROL.COM Name Server: NS76.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System : http://wdprs.internic.net/ >>> Last update of WHOIS database: 2021-10-29T17:51:28Z <<< For more information on Whois status codes, please visit https://icann.org/epp
adelluminate.com	Domain Name: adelluminate.com Registry Domain ID: 2624694390_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2021-07-06T07:27:26Z Creation Date: 2021-07-06T02:02:56Z Registrar Registration Expiration Date: 2022-07-06T02:02:56Z 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 Registrant Organization: Registrant State/Province: Jiangsu Registrant Country: CN Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=adelluminate.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=adelluminate.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=adelluminate.com

	Name Server: NS11.DOMAINCONTROL.COM Name Server: NS12.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System : http://wdprs.internic.net/
eurolabspro.com	Domain Name: eurolabspro.com Registry Domain ID: 2567431353_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2021-03-26T06:59:41Z Creation Date: 2020-10-21T21:02:11Z Registrar Registration Expiration Date: 2022-10-21T21:02:11Z 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 Registrant Organization: Registrant State/Province: Registrant Country: VI Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=eurolabspro.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=eurolabspro.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=eurolabspro.com Name Server: NS75.DOMAINCONTROL.COM Name Server: NS76.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System : http://wdprs.internic.net/
tijuanazxc.com	Domain Name: tijuanazxc.com Registry Domain ID: 1905508291_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com

	Registrar URL: http://www.godaddy.com Updated Date: 2021-01-19T09:41:26Z Creation Date: 2015-02-26T03:23:57Z Registrar Registration Expiration Date: 2022-02-26T03:23:57Z 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 Registrant Organization: Registrant State/Province: Fujian Registrant Country: CN Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=tijuanazxc.com Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=tijuanazxc.com Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=tijuanazxc.com Name Server: NS65.DOMAINCONTROL.COM Name Server: NS66.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

.ORG DOMAINS

Registry
Public Interest Registry (PIR)
1775 Wiehle Avenue
Suite 200
Reston, Virginia 20190
United States

elperuanos.org	Domain Name: ELPERUANOS.ORG Registry Domain ID: D402200000014972892-LROR Registrar WHOIS Server: whois.godaddy Registrar URL: http://www.whois.godaddy.com Updated Date: 2021-03-26T00:22:52Z Creation Date: 2020-10-22T01:55:16Z Registry Expiry Date: 2022-10-22T01:55:16Z Registrar Registration Expiration Date: Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Reseller: 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 Registrant Organization: Registrant State/Province: Registrant Country: AR Name Server: NS33.DOMAINCONTROL.COM Name Server: NS34.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form https://www.icann.org/wicf/)
jkeducation.org	Domain Name: JKEDUCATION.ORG Registry Domain ID: D402200000015213414-LROR Registrar WHOIS Server: whois.godaddy Registrar URL: http://www.whois.godaddy.com Updated Date: 2021-09-17T09:10:08Z Creation Date: 2020-11-19T08:18:46Z Registry Expiry Date: 2022-11-19T08:18:46Z Registrar Registration Expiration Date: Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Reseller: Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clie

	ntRenewProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Registrant Organization: Registrant State/Province: Jiangsu Registrant Country: CN Name Server: NS53.DOMAINCONTROL.COM Name Server: NS54.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form https://www.icann.org/wicf/) >>> Last update of WHOIS database: 2021-10-29T23:30:30Z <<<