IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

MICROSOFT CORPORATION **Plaintiff,** **v.** **JOHN DOES 1-51, CONTROLLING MULTIPLE COMPUTER BOTNETS THEREBY INJURING MICROSOFT AND ITS CUSTOMERS** **Defendants.**	**CASE NO. 1:17-CV-4566**

DECLARATION OF MICHAEL ZWEIBACK IN SUPPORT OF NOTICE OF SERVICE

I, Michael Zweiback, declare as follows:

1. I am an attorney admitted to practice in the State of California and the District of Columbia. I am a partner at the law firm of Alston & Bird LLP ("Alston"), and was admitted to the Northern District of Georgia to appear in this matter pro hac vice. I am counsel of record in this matter for plaintiff, Microsoft Corporation ("Microsoft"). I make this declaration to advise the Court as to the steps Microsoft has under taken in support of its obligations to provide Notice of Service.

I have personal knowledge of the facts set forth in this declaration and, if called to testify as a witness, could and would testify to the following under oath.

Execution of Coordinated Takedown

2. On November 29, 2017, Microsoft and the third-party registries identified in Appendix A to this Court's Emergency *Ex Parte* Temporary Restraining Order And Order To Show Cause Re: Preliminary Injunction ("TRO") executed the TRO. As described in the Press Release[1] issued by Europol's European Cybercrime Centre, a true and correct copy of which is attached hereto as **Exhibit 1**, this joint effort "dismantled one of the longest running malware families in existence called Andromeda (also known as Gamarue)." (*Id.*)

3. The effectiveness of the coordinated botnet takedowns has been widely reported, and ESET and Microsoft have also provided technical descriptions (true and correct copies of which are attached hereto as **Exhibit 2** and **Exhibit 3**, respectively) of the botnet takedown and the related malware threats[2] that were

---

[1] Press Release, Europol European Cybercrime Centre (EC3), Andromeda Botnet Dismantled In International Cyber Operation (Dec. 4, 2017), *available at* https://www.europol.europa.eu/newsroom/news/andromeda-botnet-dismantled-in-international-cyber-operation.

[2] Microsoft Digital Crimes Unit, Microsoft Teams Up with Law Enforcement and Other Partners to Disrupt Gamarue (Andromeda), Windows Security Blog (Dec. 4, 2017), https://blogs.technet.microsoft.com/mmpc/2017/12/04/microsoft-teams-up-with-law-enforcement-and-other-partners-to-disrupt-gamarue-andromeda/; Jean-Ian Boutin, ESET Takes Part in Global Operation to Disrupt Gamarue,

disrupted by the joint efforts of the Federal Bureau of Investigation (FBI), the Luneburg Central Criminal Investigation Inspectorate in Germany, Europol's European Cybercrime Centre (EC3), the Joint Cybercrime Action Task Force (J-CAT), Eurojust, and the private-sector partners (including Microsoft and ESET).

Service

4. John Doe Defendants 1-51 ("Defendants") have been properly served with the Complaint, summons, and all orders, pleadings and submissions in this action pursuant to the means authorized by the Court in the TRO.

5. I submit that it is most reasonable to conclude that Defendants are aware of this proceeding given the significant impact of the TRO on their operations, in combination with the steps Microsoft took to serve process via e-mail and Internet publication which are discussed in detail below.

6. Following execution of the TRO, traffic from the subject Internet domains that comprised the Defendants' command and control infrastructure to infected victim operating systems and devices was redirected to Microsoft's secure servers. I believe that this effectively interrupted Defendants' attacks by severing communications between the infected operating systems and devices.

---

welivesecurity (Dec. 4, 2017), https://www.welivesecurity.com/2017/12/04/eset-takes-part-global-operation-disrupt-gamarue/.

Service By Internet Publication

7. Microsoft has served process by Internet publication as authorized by the TRO. The Court has authorized service by Internet publication, as follows: "the Complaint may be served by any means authorized by law, including . . . publishing notice on a publicly available Internet website. . . ." (Dkt. 19 at p. 12-13.)

8. I oversaw service of process by publication, including each of the following actions, on behalf of Microsoft.

9. On or before December 6, 2017, Microsoft published the Complaint, summons, TRO and all associated pleadings, declaration and evidence on the publicly available website www.noticeofpleadings.net/gamarue. Thereafter, we published all other pleadings, declarations, evidence, orders, and other submissions filed with the Court in this action to date on the publicly available website www.noticeofpleadings.net/gamarue.

10. The following text was made prominently at the top of the website:

> "Plaintiff Microsoft Corporation ("Microsoft") has sued Defendants John Does 1-51 associated with the Internet domains listed below. Microsoft alleges that Defendants have violated various Federal and state laws by hosting a cybercriminal operation through these Internet domains, causing unlawful intrusion into Microsoft and Microsoft's customers' computers and computing devices; and intellectual property violations to the injury of Microsoft and Microsoft's customers. Microsoft seeks a preliminary injunction directing the registry associated with these Internet domains to take all steps necessary to disable access to and operation of these Internet domains to ensure that changes or access to the Internet domains cannot be made absent

> a court order and that all content and material associated with these Internet domains are to be isolated and preserved pending resolution of the dispute. Microsoft seeks a permanent injunction, other equitable relief and damages. Full copies of the pleading documents are available at www.noticeofpleadings.net/gamarue.
>
> NOTICE TO DEFENDANT: READ THESE PAPERS CAREFULLY! You must "appear" in this case or the other side will win automatically. To "appear" you must file with the court a legal document called a "motion" or "answer." The "motion" or "answer" must be given to the court clerk or administrator within 21 days of the date of first publication specified herein. It must be in proper form and have proof of service on Microsoft's attorneys, Michael Zweiback at Alston & Bird LLP, 333 South Hope Street, 16th Floor, Los Angeles, CA 90071. If you have questions, you should consult with your own attorney immediately."

11. A link to the foregoing website was included in each service of process e-mail sent to Defendants at the e-mail addresses determined to be associated with the Defendants' domains used in the Gamarue operations. Attached hereto as **Exhibit 4** is a true and correct copy of a screenshot of the publicly available website www.noticeofpleadings.net/gamarue.

Service By E-mail

12. Microsoft has served process via e-mail as authorized by the TRO. The Court has authorized service by e-mail, as follows: "the Complaint may be served by any means authorized by law, including . . . transmission by e-mail . . . to the contact information provided by Defendants to Defendants in their domain registration and/or hosting agreements . . . ." (Dkt. 19 at p. 12-13.)

13. Through Microsoft's pre-filing investigation, Microsoft gathered contact information, particularly e-mail addresses, associated with the Defendants' domains. Defendants had provided these e-mail addresses to domain registrars when completing the registration process for the domains used in Defendants' command and control infrastructure. This contact information was used to serve the Defendants by e-mail.

14. In this case, the e-mail addresses provided by Defendants to the domain registrars are the most accurate and viable contact information and means of notice and service. For example, as set forth in my declaration in support of the TRO Application (Dkt. 7), ICANN domain registration polices require registrants to provide accurate e-mail contact information to registrars, and the registrars use such information to provide notice of complaints and to send other account-related communications about the domain, including communications which result in suspension or cancellation of the domain registration.

15. I oversaw the process of sending copies of the Complaint, summons, TRO, and all other pleadings, declarations, evidence, orders, and other submissions in this action, by attaching those documents as PDF files to e-mails sent to the e-mail addresses associated with the domains used by Defendants. The following e-mail addresses used by the Defendants are:

E-mail Address	**Domain(s)**
ishad2022222@gmail.com	cabinme24hrs.com

	produkktc.com
jad.dodo1@gmail.com	starmanspo.com
contact@whoissecret.org	joojlee.com
dertyert.info@regprivate.ru	dertyert.info
the-schwarz@linuxmail.org	windowsupdate-microsoft.com
bydevilz@gmail.com	windowsupdate-microsoft.com

16. With the exception of bydevilz@gmail.com, each of the e-mail addresses identified above was provided to the domain registrar as the contact e-mail address for the registrant. After the execution of the takedown (as described above), an individual claiming to be the registrant of windowsupdate-microsoft.com contacted me and other attorneys at my law firm using the e-mail address bydevilz@gmail.com. I have described this correspondence below. (See ¶¶ 23-24, below.)

17. In each e-mail to Defendants, a link to the website www.noticeofpleadings.net/gamarue was included, and the pleadings, declarations, evidence, and orders filed in this action have been made available and could be accessed at such website.

18. In particular, on December 6, 2017, I oversaw the service on Defendants by e-mail attaching the Complaint, summons, TRO, and the foregoing link to all other pleadings, documents, and orders in the case. In these e-mails attaching the documents, I included the following text:

> "Plaintiff Microsoft Corporation ("Microsoft") has sued Defendants John Does 1-51 associated with the Internet domains listed below. Microsoft alleges that Defendants have violated

> various Federal and state laws by hosting a cybercriminal operation through these Internet domains, causing unlawful intrusion into Microsoft and Microsoft's customers' computers and computing devices; and intellectual property violations to the injury of Microsoft and Microsoft's customers. Microsoft seeks a preliminary injunction directing the registry associated with these Internet domains to take all steps necessary to disable access to and operation of these Internet domains to ensure that changes or access to the Internet domains cannot be made absent a court order and that all content and material associated with these Internet domains are to be isolated and preserved pending resolution of the dispute. Microsoft seeks a permanent injunction, other equitable relief and damages. Full copies of the pleading documents are available at www.noticeofpleadings.net/gamarue
>
> NOTICE TO DEFENDANT: READ THESE PAPERS CAREFULLY! You must "appear" in this case or the other side will win automatically. To "appear" you must file with the court a legal document called a "motion" or "answer." The "motion" or "answer" must be given to the court clerk or administrator within 21 days of the date of first publication specified herein. It must be in proper form and have proof of service on Microsoft's attorneys, Michael Zweiback at Alston & Bird LLP, 333 South Hope Street, 16th Floor, Los Angeles, CA 90071. If you have questions, you should consult with your own attorney immediately."

19. When sending each of the above e-mails, Alston requested both confirmation of delivery to the destination e-mail server and read receipts. A confirmation of delivery to the destination e-mail server was received by Alston after each e-mail sent to dertyert.info@regprivate.ru and contact@whoissecret.org. Further, five read receipts were received from the-schwarz@linuxmail.org. Although the destination e-mail server for the Gmail e-mail addresses did not

provide a confirmation of delivery (and no read receipts were sent), Alston did not receive any delivery failure notifications. Alston also included a remotely hosted 1x1 pixel image with each e-mail, and the tracking service indicated that these images were loaded several times over several days.

Other Methods of Service

20. When registering a domain name, the registrant provides identifying and contact information, including the registrant's name, postal address, e-mail address, phone number, administrative contact details, and technical contact details. This information is referred to as "WHOIS" data. (Dkt. 1, ¶¶ 28-29; Dkt. 7, ¶¶ 21-28.)

21. Based on my prior experience and from Microsoft's research, I believe that the most reliable contact information for effecting communication with Defendants are e-mail addresses that have been discovered to be associated with Defendants' domains. From my research, I conclude that such e-mail addresses are likely to be valid, as it is necessary to obtain web hosting services or Internet domain names and receive communications from the registrar.

22. Many of the mailing addresses provided to the domain registrars by Defendants are incomplete. Further, based on my research and prior experience, I believe that the physical mailing addresses provided by the Defendants are likely

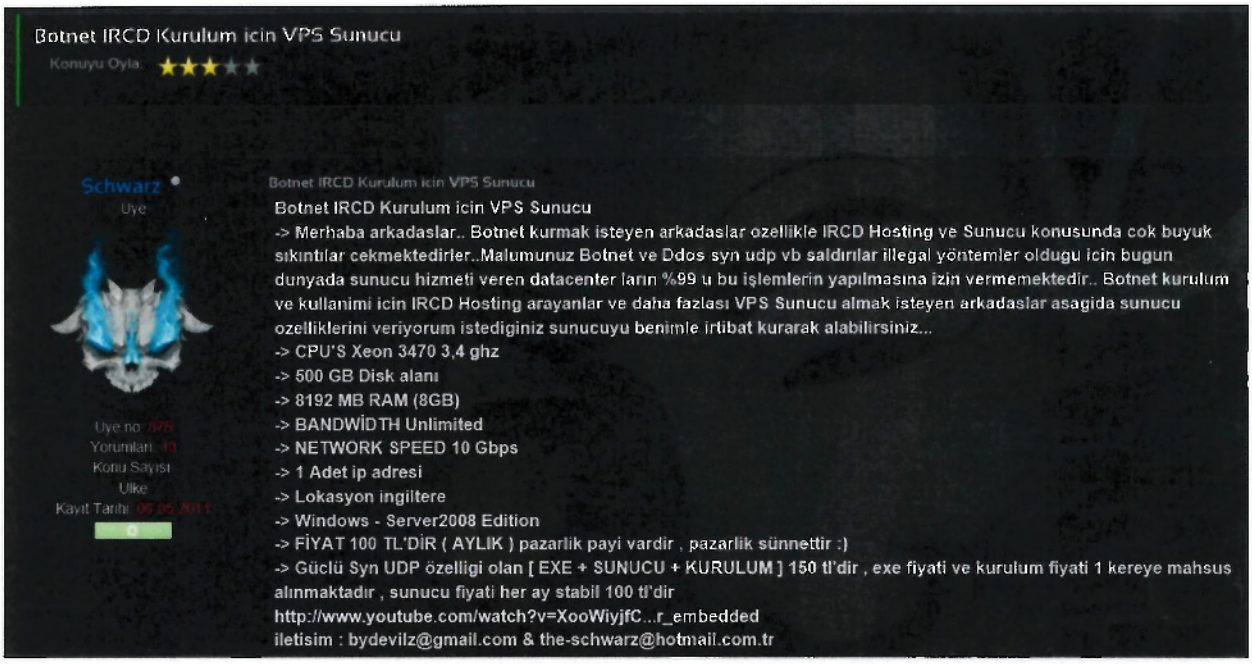
fraudulent. Accordingly, we have not attempted service on any mailing addresses or using The Hague processes.

Contact by Defendants

23. As of December 19, 2017, I have only been contacted via e-mail by one individual using the e-mail address bydevilz@gmail.com in connection with this case. The individual's first correspondence was received shortly after the TRO was executed, and this individual, who identified himself as Tolga Baskan, was subsequently served with the Complaint, summons, and provided a link to the website www.noticeofpleadings.net/gamarue, as described above in paragraphs 12 through 19.

24. Based in part on a public post at http://cryptr.org/Konu-Botnet-IRCD-Kurulum-icin-VPS-Sunucu.html offering to provide hosting services in connection with a botnet, a true and correct copy of which is attached hereto as **Exhibit 5** and an excerpt of which is included below as **Figure 1**, I believe that this individual operates both the e-mail addresses bydevilz@gmail.com and the-schwarz@linuxmail.org.

Figure 1



I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct to the best of my knowledge. Executed on this 19th day of December, 2017, in Los Angeles, California.

Michael Zweiback

CERTIFICATE OF SERVICE

I hereby certify that on the 19th day of December, 2017, the foregoing was electronically filed with the Clerk of Court using the CM/ECF system. Copies of the forgoing were also served on the defendants listed below by electronic mail:

John Does 1-51

ishad2022222@gmail.com

contact@whoissecret.org

jad.dodo1@gmail.com

dertyert.info@regprivate.ru

the-schwarz@linuxmail.org

bydevilz@gmail.com

ALSTON & BIRD LLP

/s/ Erin Coleman

Erin Coleman
CA State Bar No. 281092
Attorney for Plaintiff Microsoft Corp.
ALSTON & BIRD LLP
333 South Hope Street, 16th Floor
Los Angeles, CA 90071
Telephone: (213) 576-1000
Fax: (213) 576-1100
Email: erin.coleman@alston.com

EXHIBIT 1

ANDROMEDA BOTNET DISMANTLED IN INTERNATIONAL CYBER OPERATION

04 December 2017

Press Release

On 29 November 2017, the Federal Bureau of Investigation (FBI), in close cooperation with the Luneburg Central Criminal Investigation Inspectorate in Germany, Europol's European Cybercrime Centre (EC3), the Joint Cybercrime Action Task Force (J-CAT), Eurojust and private-sector partners, dismantled one of the longest running malware families in existence called Andromeda (also known as Gamarue).

This widely distributed malware created a network of infected computers called the Andromeda botnet[1] . According to Microsoft, Andromeda's main goal was to distribute other malware families. Andromeda was associated with 80 malware families and, in the last six months, it was detected on or blocked an average of over 1 million machines every month. Andromeda was also used in the infamous Avalanche network, which was dismantled in a huge international cyber operation (https://www.europol.europa.eu/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-operation)in 2016.

Steven Wilson, the Head of Europol's European Cybercrime Centre: "This is another example of international law enforcement working together with industry partners to tackle the most significant cyber criminals and the dedicated infrastructure they use to distribute malware on a global scale. The clear message is that public-private partnerships can impact these criminals and make the internet safer for all of us."

One year ago, on 30 November 2016, after more than four years of investigation, the Public Prosecutor's Office Verden and the Luneburg Police in Germany, the United States Attorney's Office for the Western District of Pennsylvania, the Department of Justice, the FBI, Europol, Eurojust and global partners, had dismantled the international criminal infrastructure Avalanche. This was used as a delivery platform to launch and manage mass global malware attacks such as Andromeda, and money mule recruitment campaigns.

Insights gained during the Avalanche case by the investigating German law enforcement entities were shared, via Europol, with the FBI and supported this year's investigations to dismantle the Andromeda malware last week.

Jointly, the international partners took action against servers and domains, which were used to spread the Andromeda malware. Overall, 1500 domains of the malicious software were subject to sinkholing[2] . According to Microsoft, during 48 hours of sinkholing, approximately 2 million unique Andromeda victim IP addresses from 223 countries were captured. The involved law enforcement authorities also executed the search and arrest of a suspect in Belarus.

Simultaneously, the German sinkhole measures of the Avalanche case have been extended by another year. An extension of this measure was necessary, as globally 55 per cent of the computer systems originally infected in Avalanche are still infected today.

The measures to combat the malicious Andromeda software as well as the extension of the Avalanche measures involved the following EU Member States: Austria, Belgium, Finland, France, Italy, the Netherlands, Poland, Spain, the United Kingdom, and the following non-EU Member States: Australia, Belarus, Canada, Montenegro, Singapore and Taiwan.

The operation was supported by the following private and institutional partners: Shadowserver Foundation, Microsoft, Registrar of Last Resort, Internet Corporation for Assigned Names and Numbers (ICANN) and associated domain registries, Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE), and the German Federal Office for Information Security (BSI).

The operation was coordinated from the command post hosted at Europol's HQ.

---

[1] Botnets are networks of computers infected with malware, which are under the control of a cybercriminal. Botnets allow criminals to harvest sensitive information from infected computers, such as online banking credentials and credit card information. A criminal can also use a botnet to perform cyberattacks on other computer systems, such as denial-of-service attacks.

[2] Sinkholing is an action whereby traffic between infected computers and a criminal infrastructure is redirected to servers controlled by law enforcement authorities and/or an IT security company. This may be done by assuming control of the domains used by the criminals or IP addresses. When employed at a 100% scale, infected computers can no longer reach the criminal command-and-control computer systems and criminals can therefore no longer control the infected computers. The sinkholing infrastructure captures victims' IP addresses, which can subsequently be used for notification and follow-up through dissemination to National CERTs and network owners.

CRIME AREAS

Cybercrime (/crime-areas-and-trends/crime-areas/cybercrime) •
Forgery of Administrative Documents and Trafficking therein (/crime-areas-and-trends/crime-areas/forgery-of-administrative-documents-and-trafficking-therein)

TARGET GROUPS

General Public (/target-groups/general-public) • Law Enforcement (/target-groups/law-enforcement) •
Academia (/target-groups/academia) • Professor (/target-groups/professor) • Students (/target-groups/students) •
Researcher (/target-groups/researcher) • Press/Journalists (/target-groups/press-journalists) •
Other (/target-groups/other)

ENTITIES

European Cybercrime Center (EC3) (/entities/european-cybercrime-center-ec3) •
Joint Cybercrime Action Taskforce (J-CAT) (/entities/joint-cybercrime-action-taskforce-j-cat)

ORGANISATIONS

Eurojust (/organisations/eurojust) •
Federal Bureau of Investigation (FBI) (/organisations/federal-bureau-of-investigation-fbi)

SUPPORT & SERVICES

Operational coordination (/support-services/operational-coordination) •
Operational support (/support-services/operational-support) •
Information exchange (/support-services/information-exchange) • Analysis (/support-services/analysis)

EXHIBIT 2

Microsoft teams up with law enforcement and other partners to disrupt Gamarue (Andromeda)

Rate this article ★★★★★

msft-mmpc (https://social.technet.microsoft.com/profile/msft-mmpc) December 4, 2017

Today, with help from Microsoft security researchers, law enforcement agencies around the globe (https://www.europol.europa.eu/newsroom/news/andromeda-botnet-dismantled-in-international-cyber-operation), in cooperation with Microsoft Digital Crimes Unit (DCU), announced the disruption of Gamarue (https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Gamarue), a widely distributed malware that has been used in networks of infected computers collectively called the Andromeda botnet.

The disruption is the culmination of a journey that started in December 2015, when the Microsoft Windows Defender research team and DCU activated a Coordinated Malware Eradication (CME) campaign for Gamarue. In partnership with internet security firm ESET (https://www.eset.com/us/about/newsroom/press-releases/eset-unites-with-microsoft-and-law-enforcement-agencies-to-disrupt-gamarue-botnets/), we performed in-depth research into the Gamarue malware and its infrastructure.

Our analysis of more than 44,000 malware samples uncovered Gamarue's sprawling infrastructure. We provided detailed information about that infrastructure to law enforcement agencies around the world, including:

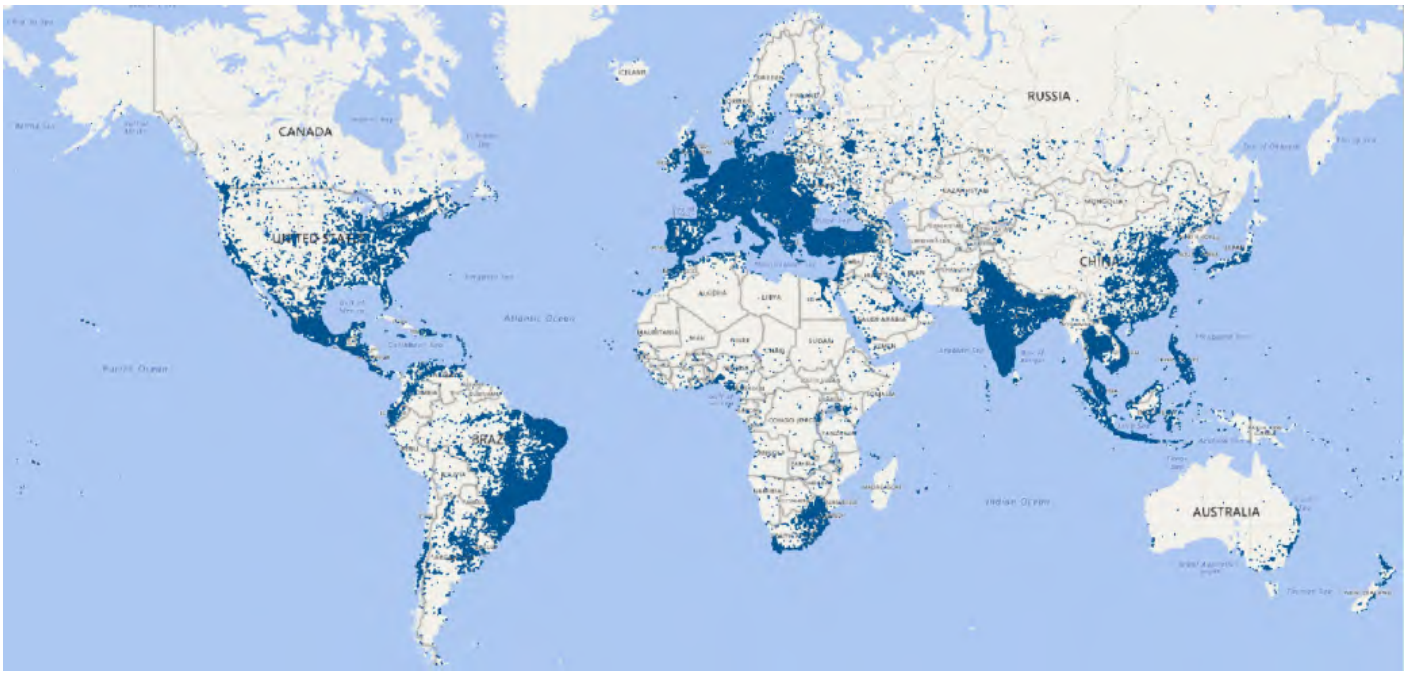
- 1,214 domains and IP addresses of the botnet's command and control servers
- 464 distinct botnets
- More than 80 associated malware families

The coordinated global operation resulted in the takedown of the botnet's servers, disrupting one of the largest malware operations in the world. Since 2011, Gamarue has been distributing a plethora of other threats, including:

- Petya (https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Petya) and Cerber (https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Cerber) ransomware
- Kasidet (https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Kasidet) malware (also known as Neutrino bot), which is used for DDoS attacks
- Lethic (https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Lethic), a spam bot
- Info-stealing malware Ursnif (https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=win32/ursnif), Carberp (https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Carberp), and Fareit (https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Fareit), among others

A global malware operation

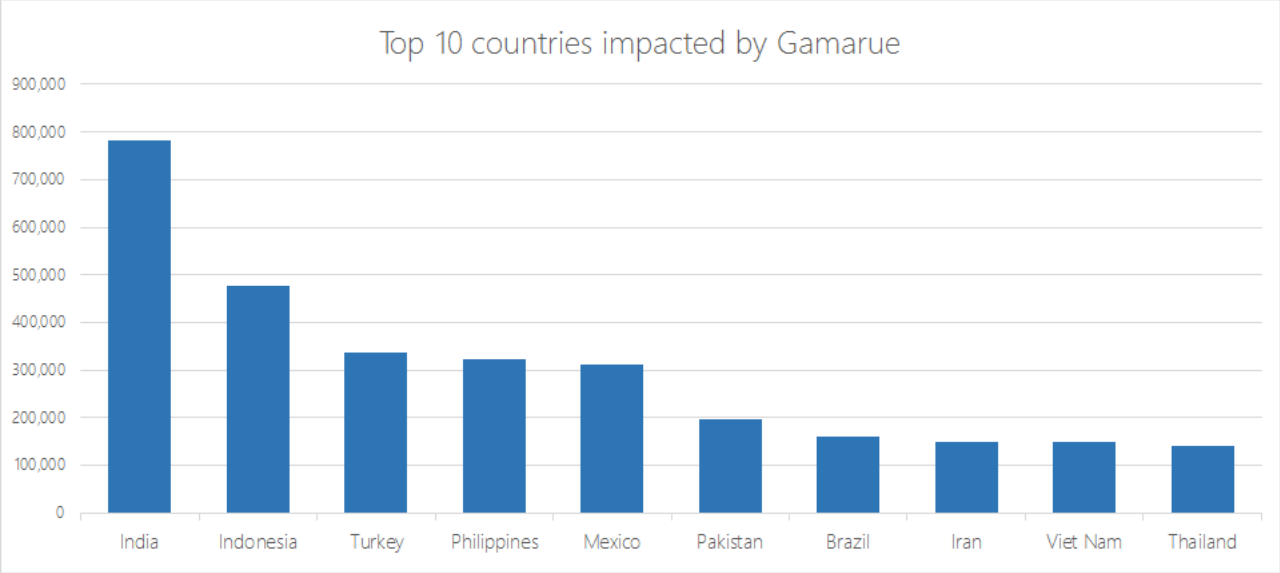
For the past six years, Gamarue has been a very active malware operation that, until the takedown, showed no signs of slowing down. Windows Defender telemetry in the last six months shows Gamarue's global prevalence.



(https://msdnshared.blob.core.windows.net/media/2017/12/gamarue-geo-chart.png)

Figure 1. Gamarue's global prevalence from May to November 2017

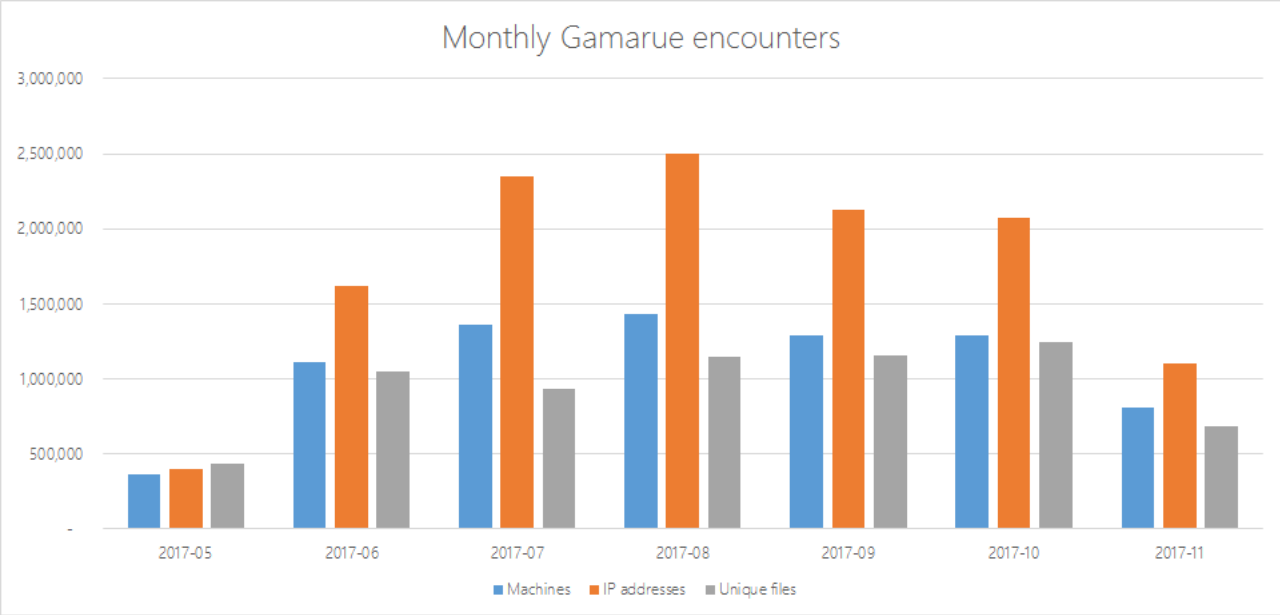
While the threat is global, the list of top 10 countries with Gamarue encounters is dominated by Asian countries.



(https://msdnshared.blob.core.windows.net/media/2017/12/top-10-gamarue-andromeda-impacted-countries.png)

Figure 2. Top 10 countries with the most Gamarue encounters from May to November 2017

In the last six months, Gamarue was detected or blocked on approximately 1,095,457 machines every month on average.



(https://msdnshared.blob.core.windows.net/media/2017/12/monthly-gamarue-andromeda-encounters.png)

Figure 3. Machines, IPs, and unique file encounters for Gamarue from May to November 2017; data does not include LNK detections

The Gamarue bot

Gamarue is known in the underground cybercrime market as Andromeda bot. A bot is a program that allows an attacker to take control of an infected machine. Like many other bots, Gamarue is advertised as a crime kit that hackers can purchase.

The Gamarue crime kit includes the following components:

- **Bot-builder**, which builds the malware binary that infects computers
- **Command-and-control application**, which is a PHP-based dashboard application that allows hackers to manage and control the bots
- **Documentation** on how to create a Gamarue botnet

A botnet is a network of infected machines that communicate with command-and-control (C&C) servers, which are computer servers used by the hacker to control infected machines.

The evolution of the Gamarue bot has been the subject of many thorough analyses by security researchers. At the time of takedown, there were five known active Gamarue versions: 2.06, 2.07, 2.08, 2.09, and 2.10. The latest and the most active is version 2.10.

Gamarue is modular, which means that its functionality can be extended by plugins that are either included in the crime kit or available for separate purchase. The Gamarue plugins include:

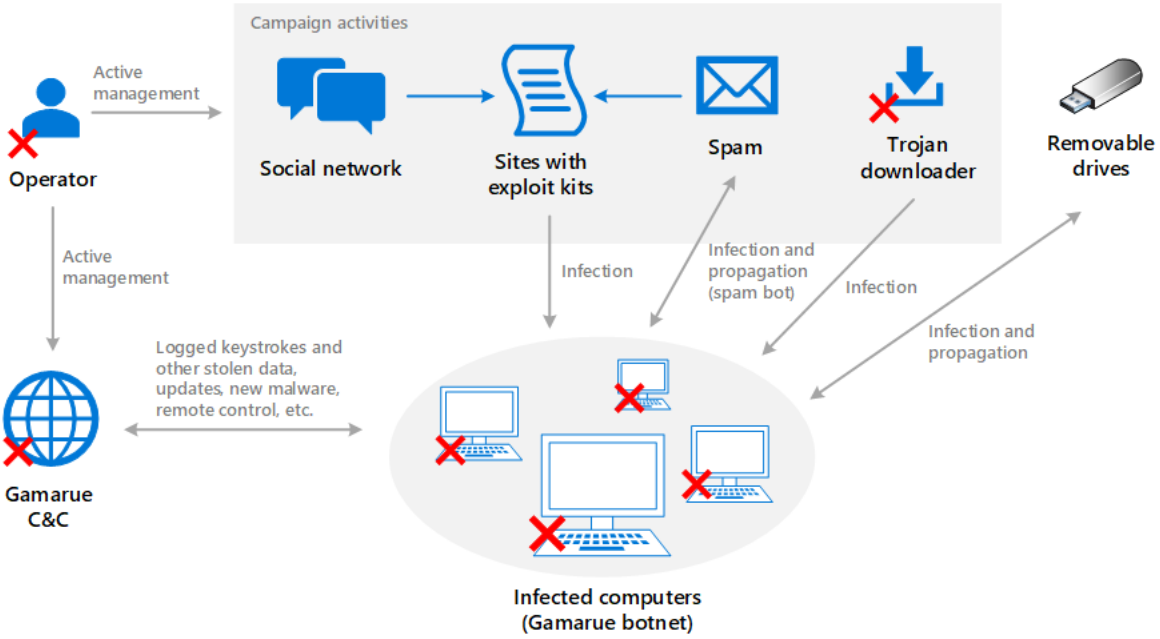
- **Keylogger ($150)** – Used for logging keystrokes and mouse activity in order to steal user names and passwords, financial information, etc
- **Rootkit (included in crime kit)** – Injects rootkit codes into all processes running on a victim computer to give Gamarue persistence
- **Socks4/5 (included in crime kit)** – Turns victim computer into a proxy server for serving malware or malicious instructions to other computers on the internet
- **Formgrabber ($250)** – Captures any data submitted through web browsers (Chrome, Firefox, and Internet Explorer)
- **Teamviewer ($250)** – Enables attacker to remotely control the victim machine, spy on the desktop, perform file transfer, among other functions
- **Spreader** – Adds capability to spread Gamarue malware itself via removable drives (for example, portable hard drives or flash drives connected via a USB port); it also uses Domain Name Generation (DGA) for the servers where it downloads updates

Gamarue attack kill-chain

Over the years, various attack vectors have been used to distribute Gamarue. These include:

- Removable drives
- Social media (such as Facebook) messages with malicious links to websites that host Gamarue
- Drive-by downloads/exploit kits
- Spam emails with malicious links
- Trojan downloaders

Once Gamarue has infected a machine, it contacts the C&C server, making the machine part of the botnet. Through the C&C server, the hacker can control Gamarue-infected machines, steal information, or issue commands to download additional malware modules.



(https://msdnshared.blob.core.windows.net/media/2017/12/gamarue-attack-kill-chain.png)

Figure 4. Gamarue's attack kill-chain

Gamarue's main goal is to distribute other prevalent malware families. During the CME campaign, we saw at least 80 different malware families distributed by Gamarue. Some of these malware families include:

- Petya (https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Petya) (ransomware)
- Cerber (https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Cerber) (ransomware)
- Troldesh (https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Troldesh) (ransomware)
- Ursnif (https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Ursnif) (info-stealing and banking trojan)
- Carberp (https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Carberp) (info-stealing and banking trojan)
- Fareit (https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Fareit) (info-stealing and DDoS malware)
- Kasidet (https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Kasidet) (worm and DDoS malware)
- Lethic (https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Lethic) (spam bot)
- Cutwail (https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Cutwail) (spam bot)
- Neurevt (https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Neurevt) (click-fraud malware)
- Ursnif (https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=win32/ursnif) (click-fraud malware)
- Fynloski (https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Fynloski) (backdoor)

The installation of other malware broadens the scale of what hackers can do with the network of infected machines.

Command-and-control communication

When the Gamarue malware triggers the infected machine to contact the C&C server, it provides information like the hard disk's volume serial number (used as the bot ID for the computer), the Gamarue build ID, the operating system of the infected machine, the local IP address, an indication whether the signed in user has administrative rights, and keyboard language setting for the infected machine. This information is sent to the C&C server via HTTP using the JSON format:

```
{"id":%lu,"bid":%lu,"os":%lu,"la":%lu,"rg":%lu,"bb":%lu',0
```
(https://msdnshared.blob.core.windows.net/media/2017/12/gamarue-Cnc-comm-2.png)
(https://msdnshared.blob.core.windows.net/media/2017/12/gamarue-Cnc-comm.png)

Figure 5. Information sent by Gamarue to C&C server

The information about keyboard language setting is very interesting, because the machine will not be further infected if the keyboard language corresponds to the following countries:

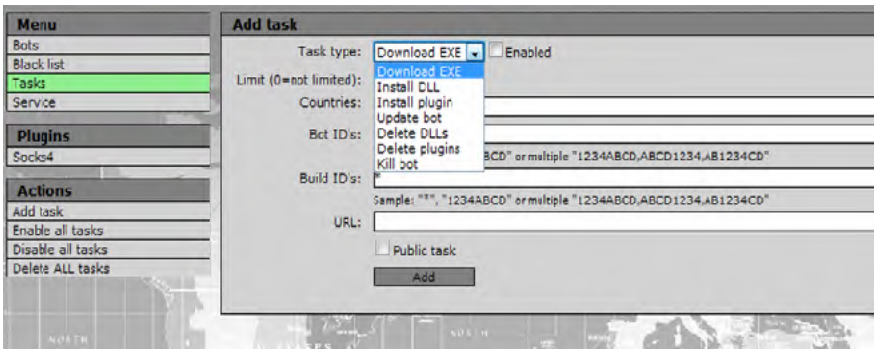
- Belarus
- Russia
- Ukraine
- Kazahkstan

Before sending to the C&C server, this information is encrypted with RC4 algorithm using a key hardcoded in the Gamarue malware body.

(https://msdnshared.blob.core.windows.net/media/2017/12/gamarye-cnc-comm-encrypted.png)

Figure 6. Encrypted C&C communication

Once the C&C server receives the message, it sends a command that is pre-assigned by the hacker in the control dashboard.



(https://msdnshared.blob.core.windows.net/media/2017/12/gamarue-control-dashboard.png)

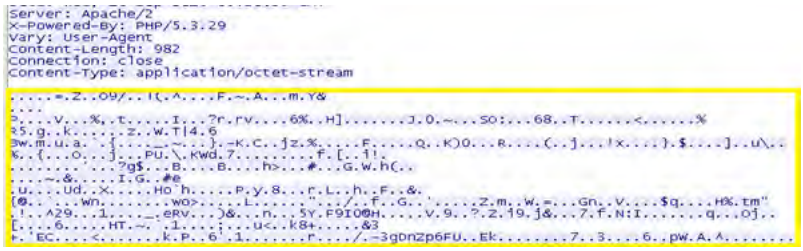
Figure 7. Sample control dashboard used by attackers to communicate to Gamarue bots

The command can be any of the following:

- Download EXE (i.e., additional executable malware files)
- Download DLL (i.e., additional malware; removed in version 2.09 and later)
- Install plugin
- Update bot (i.e., update the bot malware)
- Delete DLLs (removed in version 2.09 and later)
- Delete plugins
- Kill bot

The last three commands can be used to remove evidence of Gamarue presence in machines.

The reply from the C&C server is also encrypted with RC4 algorithm using the same key used to encrypt the message from the infected machine.



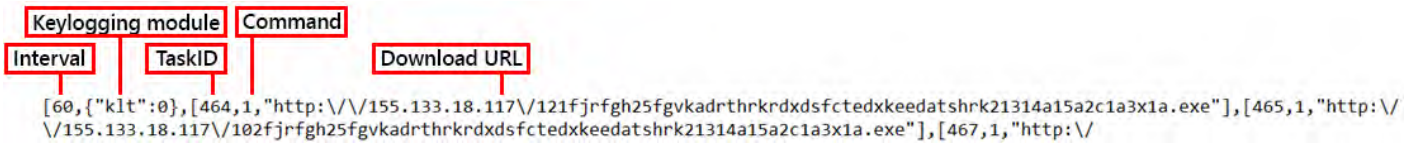
(https://msdnshared.blob.core.windows.net/media/2017/12/gamarue-encrypted-cnc-reply.png)

Figure 8. Encrypted reply from C&C server

When decrypted, the reply contains the following information:

- Time interval in minutes – time to wait for when to ask the C2 server for the next command
- Task ID - used by the hacker to track if there was an error performing the task
- Command – one of the command mentioned above
- Download URL - from which a plugin/updated binary/other malware can be downloaded depending on the command.

(https://msdnshared.blob.core.windows.net/media/2017/12/gamarye-cnc-reply-decrypted.png)



(https://msdnshared.blob.core.windows.net/media/2017/12/gamarye-cnc-reply-decrypted-2.png)

Figure 9. Decrypted reply from C&C server

Anti-sandbox techniques

Gamarue employs anti-AV techniques to make analysis and detection difficult. Prior to infecting a machine, Gamarue checks a list hashes of the processes running on a potential victim's machine. If it finds a process that may be associated with malware analysis tools, such as virtual machines or sandbox tools, Gamarue does not infect the machine. In older versions, a fake payload is manifested when running in a virtual machine.

```
analysis_prog_hash_list dd 99DD4432h    ; DATA XREF: chk_dbg+C8↓r
                                        ; chk_dbg+DD↓r
                                        ; vmwareuser.exe
                dd 2D859DB4h            ; vmwareservice.exe
                dd 64340DCEh            ; vboxservice.exe
                dd 63C54474h            ; vboxtray.exe
                dd 349C9C8Bh            ; sandboxiedcomlaunch.exe
                dd 3446EBCEh            ; sandboxierpcss.exe
                dd 5BA9B1FEh            ; procmon.exe
                dd 3CE2BEF3h            ; regmon.exe
                dd 3D46F02Bh            ; filemon.exe
                dd 77AE10F7h            ; wireshark.exe
                dd 0F344E95Dh           ; netmon.exe
```

(https://msdnshared.blob.core.windows.net/media/2017/12/gamarue-list-processes.png)

Figure 10. Gamarue checks if any of the running processes are associated with malware analysis tools

Stealth mechanisms

Gamarue uses cross-process injection (https://blogs.technet.microsoft.com/mmpc/tag/cross-process-injection/) techniques to stay under the radar. It injects its code into the following legitimate processes:

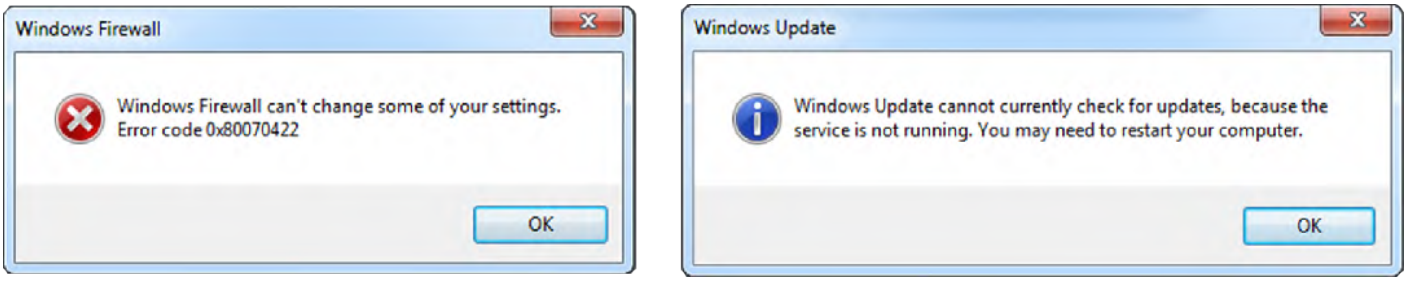
- msiexec.exe (Gamarue versions 2.07 to 2.10)
- wuauclt.exe, wupgrade.exe, svchost.exe (version 2.06)

It can also use a rootkit plugin to hide the Gamarue file and its autostart registry entry.

Gamarue employs a stealthy technique to store and load its plugins as well. The plugins are stored fileless, either saved in the registry or in an alternate data stream of the Gamarue file.

OS tampering

Gamarue attempts to tamper with the operating systems of infected computers by disabling Firewall, Windows Update, and User Account Control functions. These functionalities cannot be re-enabled until the Gamarue infection has been removed from the infected machine. This OS tampering behavior does not work on Windows 10



(https://msdnshared.blob.core.windows.net/media/2017/12/gamarue-firewall-disabled-2.png)

Figure 11. Disabled Firewall and Windows Update

Monetization

There are several ways hackers earn using Gamarue. Since Gamarue's main purpose is to distribute other malware, hackers earn using pay-per-install scheme. Using its plugins, Gamarue can also steal user information; stolen information can be sold to other hackers in cybercriminal underground markets. Access to Gamarue-infected machines can also be sold, rented, leased, or swapped by one criminal group to another.

Remediation

To help prevent a Gamarue infection, as well as other malware and unwanted software, take these precautions:

- Be cautious when opening emails or social media messages from unknown users.
- Be wary about downloading software from websites other than the program developers.

More importantly, ensure you have the right security solutions that can protect your machine from Gamarue and other threats. Windows Defender Antivirus detects and removes the Gamarue malware. With advanced machine learning models, as well as generic and heuristic techniques, Windows Defender AV detects new as well as never-before-seen malware (https://blogs.technet.microsoft.com/mmpc/2017/07/18/windows-defender-antivirus-cloud-protection-service-advanced-real-time-defense-against-never-before-seen-malware?ocid=cx-blog-mmpc) in real-time via the cloud protection service. Alternatively, standalone tools, such as Microsoft Safety Scanner (https://www.microsoft.com/wdsi/products/scanner) and the Malicious Software Removal Tool (MSRT) (https://www.microsoft.com/download/malicious-software-removal-tool-details.aspx), can also detect and remove Gamarue.

Microsoft Edge (https://docs.microsoft.com/en-us/microsoft-edge/deploy/index?ocid=cx-blog-mmpc) can block Gamarue infections from the web, such as those from malicious links in social media messages and drive-by downloads or exploit kits. Microsoft Edge is a secure browser that opens pages within low privilege app containers and uses reputation-based blocking of malicious downloads.

In enterprise environments, additional layers of protection are available. Windows Defender Advanced Threat Protection (https://www.microsoft.com/en-us/windowsforbusiness/windows-atp?ocid=cx-blog-mmpc) can help security operations personnel to detect Gamarue activities, including cross-process injection techniques, in the network so they can investigate and respond to attacks. Windows Defender ATP's enhanced behavioral and machine learning detection libraries flag malicious behavior across the malware infection process, from delivery and installation, to persistence mechanisms, and command-and-control communication.

Microsoft Exchange Online Protection (EOP) (https://products.office.com/en-us/exchange/exchange-email-security-spam-protection?ocid=cx-blog-mmpc) can block Gamarue infections from email uses built-in anti-spam filtering capabilities that help protect Office 365 customers. Office 365 Advanced Threat Protection (https://products.office.com/en-us/exchange/online-email-threat-protection?ocid=cx-blog-mmpc) helps secure mailboxes against email attacks by blocking emails with unsafe attachments, malicious links, and linked-to files leveraging time-of-click protection.

Windows Defender Exploit Guard (https://blogs.technet.microsoft.com/mmpc/2017/10/23/windows-defender-exploit-guard-reduce-the-attack-surface-against-next-generation-malware/) can block malicious documents (such as those that distribute Gamarue) and scripts. The Attack Surface Reduction (ASR) (https://docs.microsoft.com/en-us/windows/threat-protection/windows-defender-exploit-guard/attack-surface-reduction-exploit-guard?ocid=cx-blog-mmpc) feature in Windows Defender Exploit Guard uses a set of built-in intelligence that can block malicious behaviors observed in malicious documents. ASR rules can also be turned on to block malicious attachments (https://docs.microsoft.com/en-us/windows/threat-protection/windows-defender-exploit-guard/attack-surface-reduction-exploit-guard?ocid=cx-blog-mmpc) from being run or launched from Microsoft Outlook or webmail (such as Gmail, Hotmail, or Yahoo).

Microsoft is also continuing the collaborative effort to help clean Gamarue-infected computers by providing a one-time package with samples (through the Virus Information Alliance (https://www.microsoft.com/en-us/wdsi/alliances/virus-information-alliance)) to help organizations protect their customers.

Microsoft Digital Crimes Unit *and* ***Windows Defender Research team***

Get more info on the Gamarue (Andromeda) takedown from the following sources:

- Europol: Andromeda botnet dismantled in international cyber operation (https://www.europol.europa.eu/newsroom/news/andromeda-botnet-dismantled-in-international-cyber-operation)
- ESET: ESET unites with Microsoft and law enforcement agencies to disrupt Gamarue botnets (https://www.eset.com/us/about/newsroom/press-releases/eset-unites-with-microsoft-and-law-enforcement-agencies-to-disrupt-gamarue-botnets/)

Talk to us

Questions, concerns, or insights on this story? Join discussions at the Microsoft community (https://answers.microsoft.com/en-us/protect).

Follow us on Twitter @WDSecurity (https://twitter.com/WDSecurity) and Facebook Microsoft Malware Protection Center (https://www.facebook.com/msftmmpc/)

Tags Andromeda (https://blogs.technet.microsoft.com/mmpc/tag/andromeda/) bot (https://blogs.technet.microsoft.com/mmpc/tag/bot/) botnet (https://blogs.technet.microsoft.com/mmpc/tag/botnet/) Carberp (https://blogs.technet.microsoft.com/mmpc/tag/carberp/) Cerber (https://blogs.technet.microsoft.com/mmpc/tag/cerber/) Coordinated Malware Eradication Program (https://blogs.technet.microsoft.com/mmpc/tag/coordinated-malware-eradication-program/) disruption (https://blogs.technet.microsoft.com/mmpc/tag/disruption/) fareit (https://blogs.technet.microsoft.com/mmpc/tag/fareit/) Gamarue (https://blogs.technet.microsoft.com/mmpc/tag/gamarue/) info-stealing malware (https://blogs.technet.microsoft.com/mmpc/tag/info-stealing-malware/) Kasidet (https://blogs.technet.microsoft.com/mmpc/tag/kasidet/) keylogger (https://blogs.technet.microsoft.com/mmpc/tag/keylogger/) Lethic (https://blogs.technet.microsoft.com/mmpc/tag/lethic/) Microsoft DCU (https://blogs.technet.microsoft.com/mmpc/tag/microsoft-dcu/) Microsoft Digital Crimes Unit (https://blogs.technet.microsoft.com/mmpc/tag/microsoft-digital-crimes-unit/) Netutrino (https://blogs.technet.microsoft.com/mmpc/tag/netutrino/) Petya (https://blogs.technet.microsoft.com/mmpc/tag/petya/) rootkit (https://blogs.technet.microsoft.com/mmpc/tag/rootkit/) spam bot (https://blogs.technet.microsoft.com/mmpc/tag/spam-bot/) takedown (https://blogs.technet.microsoft.com/mmpc/tag/takedown/) Ursnif (https://blogs.technet.microsoft.com/mmpc/tag/ursnif/) Win32/Gamarue (https://blogs.technet.microsoft.com/mmpc/tag/win32gamarue/)

Recent posts

- Detonating a bad rabbit: Windows Defender Antivirus and layered machine learning defenses (https://blogs.technet.microsoft.com/mmpc/2017/12/11/detonating-a-bad-rabbit-windows-defender-antivirus-and-layered-machine-learning-defenses/)
- Microsoft teams up with law enforcement and other partners to disrupt Gamarue (Andromeda) (https://blogs.technet.microsoft.com/mmpc/2017/12/04/microsoft-teams-up-with-law-enforcement-and-other-partners-to-disrupt-gamarue-andromeda/)
- Windows Defender ATP machine learning and AMSI: Unearthing script-based attacks that 'live off the land' (https://blogs.technet.microsoft.com/mmpc/2017/12/04/windows-defender-atp-machine-learning-and-amsi-unearthing-script-based-attacks-that-live-off-the-land/)
- New tech support scam launches communication or phone call app (https://blogs.technet.microsoft.com/mmpc/2017/11/20/new-tech-support-scam-launches-communication-or-phone-call-app/)
- #AVGater vulnerability does not affect Windows Defender Antivirus, MSE, or SCEP (https://blogs.technet.microsoft.com/mmpc/2017/11/13/avgater-vulnerability-does-not-affect-windows-defender-antivirus/)
- Detecting reflective DLL loading with Windows Defender ATP (https://blogs.technet.microsoft.com/mmpc/2017/11/13/detecting-reflective-dll-loading-with-windows-defender-atp/)

Social

@WDSecurity (https://twitter.com/WDSecurity)

MsftWDSI (https://www.facebook.com/MsftWDSI)

Security@Microsoft (https://www.linkedin.com/groups?gid=3660709&trk=myg_ugrp_ovr)

RSS (http://blogs.technet.com/b/mmpc/rss.aspx)

Security Newsletter (http://technet.microsoft.com/en-us/security/cc307424.aspx)

About

(https://blogs.technet.microsoft.com/mmpc/about/)

Categories

- Advanced persistent threats (https://blogs.technet.microsoft.com/mmpc/category/research/apt/) (22)
- Cloud protection (https://blogs.technet.microsoft.com/mmpc/category/technologies/cloud-protection/) (7)
- Device Guard (https://blogs.technet.microsoft.com/mmpc/category/technologies/device-guard/) (2)
- Exploits (https://blogs.technet.microsoft.com/mmpc/category/research/exploits/) (16)
- Java malware (https://blogs.technet.microsoft.com/mmpc/category/research/java-malware/) (1)
- JavaScript malware (https://blogs.technet.microsoft.com/mmpc/category/research/javascript/) (6)
- Macro-based malware (https://blogs.technet.microsoft.com/mmpc/category/research/macro-malware/) (16)
- Malvertising (https://blogs.technet.microsoft.com/mmpc/category/research/malvertising-campaign/) (2)
- Microsoft Edge (https://blogs.technet.microsoft.com/mmpc/category/technologies/microsoft-edge/) (7)
- MSRT (https://blogs.technet.microsoft.com/mmpc/category/technologies/msrt/) (38)
- Objective Criteria (https://blogs.technet.microsoft.com/mmpc/category/technologies/objective-criteria/) (19)
- Office (https://blogs.technet.microsoft.com/mmpc/category/technologies/office/) (5)
- Office 365 Advanced Threat Protection (https://blogs.technet.microsoft.com/mmpc/category/technologies/office-365-advanced-threat-protection/) (6)
- Phishing (https://blogs.technet.microsoft.com/mmpc/category/research/phishing/) (3)
- PowerShell (https://blogs.technet.microsoft.com/mmpc/category/technologies/powershell/) (2)
- Ransomware (https://blogs.technet.microsoft.com/mmpc/category/research/ransomware/) (47)
- Rogue (https://blogs.technet.microsoft.com/mmpc/category/research/rogue/) (2)
- Spam (https://blogs.technet.microsoft.com/mmpc/category/research/spam/) (14)
- Tech support scam (https://blogs.technet.microsoft.com/mmpc/category/research/supportscam/) (5)
- Trojan (https://blogs.technet.microsoft.com/mmpc/category/research/trojan/) (27)
- Uncategorized (https://blogs.technet.microsoft.com/mmpc/category/uncategorized/) (472)
- Unwanted software (https://blogs.technet.microsoft.com/mmpc/category/research/unwanted-software/) (22)
- Windows 10 (https://blogs.technet.microsoft.com/mmpc/category/technologies/windows-10/) (46)
- Windows 10 Creators Update (https://blogs.technet.microsoft.com/mmpc/category/technologies/creators-update/) (19)
- Windows 10 Fall Creators Update (https://blogs.technet.microsoft.com/mmpc/category/technologies/fall-creators-update/) (11)
- Windows 10 S (https://blogs.technet.microsoft.com/mmpc/category/technologies/windows-10-s/) (4)
- Windows Defender Application Control (https://blogs.technet.microsoft.com/mmpc/category/technologies/windows-defender-application-control/) (1)
- Windows Defender Application Guard (https://blogs.technet.microsoft.com/mmpc/category/technologies/windows-defender-application-guard/) (2)
- Windows Defender ATP (https://blogs.technet.microsoft.com/mmpc/category/technologies/windows-defender-atp/) (38)
- Windows Defender AV (https://blogs.technet.microsoft.com/mmpc/category/technologies/windows-defender/) (51)
- Windows Defender Exploit Guard (https://blogs.technet.microsoft.com/mmpc/category/technologies/windows-defender-exploit-guard/) (3)
- Windows Defender Security Intelligence (https://blogs.technet.microsoft.com/mmpc/category/research/) (135)
- Windows Defender System Guard (https://blogs.technet.microsoft.com/mmpc/category/technologies/windows-defender-system-guard/) (1)
- Windows Hello (https://blogs.technet.microsoft.com/mmpc/category/technologies/windows-hello/) (1)
- Windows security product tips (https://blogs.technet.microsoft.com/mmpc/category/tips/) (50)
- Windows security technologies (https://blogs.technet.microsoft.com/mmpc/category/technologies/) (73)
- Worms (https://blogs.technet.microsoft.com/mmpc/category/research/worms/) (4)

EXHIBIT 3

welivesecurity
News, views, and insight from the ESET security community

ESET takes part in global operation to disrupt Gamarue

BY JEAN-IAN BOUTIN POSTED 4 DEC 2017 - 07:01PM

Today, we announce that a major law enforcement operation disrupted many botnets using a malware family that has been plaguing the internet for quite a long time: Gamarue, also known as Andromeda. This joint operation, involving law enforcement agencies world-wide, Microsoft, and ESET, has been ongoing for more than a year now.

Gamarue, mostly detected by ESET as Win32/TrojanDownloader.Wauchos, has been around since at least September 2011 and was, for the most part, sold as a crimekit on underground forums. This crimekit proved very popular amongst cybercriminals and, that being the case, there are multiple, independent Wauchos botnets. In the past, Wauchos has been the most detected malware family amongst ESET users, so when approached by Microsoft to take part in a joint disruption effort against it, to better protect our users and the general public at large, it was a no-brainer to agree.

ESET provided technical analysis to this operation by closely tracking Wauchos botnets, identifying their C&C servers for takedown, and monitoring what its operators installed on victims' systems. Through Microsoft, the information provided to law enforcement agencies as part of this operation included:

- 1,214 domains and IP addresses of the botnet's command and control servers
- 464 distinct botnets
- 80 associated malware families

In Figure 1 you can see Wauchos's prevalence map based on our telemetry data. Evidently, Wauchos is a global problem and any attempt to disrupt it is worth making. As you will notice throughout the article, the data shown are about a year old. This is when Wauchos's activity was at its peak, according to our telemetry. As legal procedures do take some time, especially when arrests are involved, we chose these older data, as they are more representative of the period at which most of the research took place.

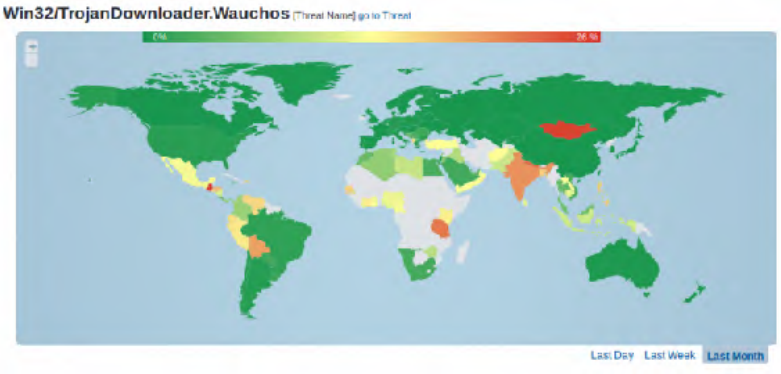


Figure 1. Wauchos Prevalence Map (December 2016 – source http://virusradar.com/)

If you are worried that your Windows system might be compromised by this threat and are not an ESET customer, you can download and use the **ESET Online Scanner**, which will remove any threats, including Wauchos, it might find on your system.

What is Wauchos?

This very prevalent malware has been around for several years and has been covered in the past by multiple blog posts [1][2][3][4]. In this section, we will review the technical basics of this malware: what it is and how it is spread. The following section will cover technical details that we uncovered while tracking this malware family.

Wauchos is mostly used to steal credentials and download and install additional malware onto a system. Thus, if a system is compromised with Wauchos, it's likely that there will be several other malware families lurking on the same system.

Wauchos is modular malware whose functionalities can easily be expanded by adding plugins. Plugins used include a **keylogger**, a formgrabber, a **rootkit**, a SOCKS proxy and a TeamViewer bot. There are five known major build versions of Wauchos, based on its own versioning scheme: 2.06, 2.07, 2.08, 2.09 and 2.10. For the first three versions, the build version was included in the first POST request sent to the C&C by the bot, so version identification was easy. Later versions of Wauchos removed the `bv` parameter in the POST request, but it is still relatively simple to identify the bot version by looking at the identification string sent to the server [3]:

Version	Identification string
<= 2.06	id:%lu|bid:%lu|bv:%lu|sv:%lu|pa:%lu|la:%lu|ar:%lu
2.07 – 2.08	id:%lu|bid:%lu|bv:%lu|os:%lu|la:%lu|rg:%lu
2.09	id:%lu|bid:%lu|os:%lu|la:%lu|rg:%lu
2.10 *	{"id":%lu,"bid":%lu,"os":%lu,"la":%lu,"rg":%lu}

(* Note the switch to JSON format.)

A typical POST request is shown in Figure 2. The identification string is RC4 encrypted and then encoded using base64.

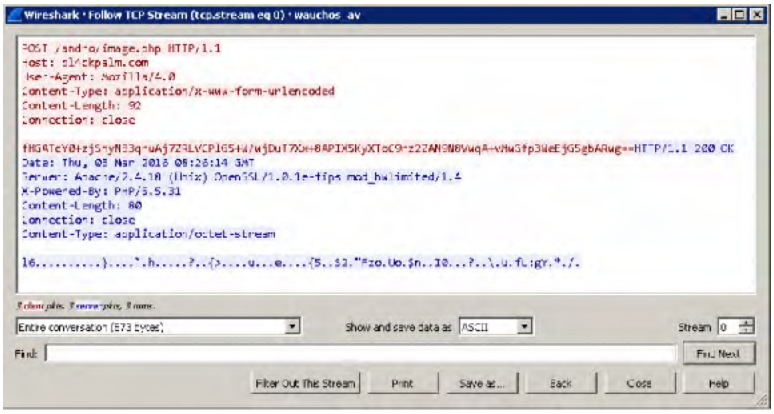


Figure 2. Typical POST Request

Since a builder for version 2.06 was leaked a few years ago, we have seen quite a bit of that version of this botnet in our telemetry. However, according to our crawler data the latest version, 2.10, is the most prevalent.

The truly global nature of this threat is also seen in the diversity of the command and control servers its operators use. Throughout our monitoring of this threat, we were able to discover dozens of Wauchos's C&C servers every month. Figure 3 shows a snapshot of the different TLDs used by the C&Cs while Figure 4 shows the geographic distribution of these C&C server IPs when our crawler was connecting to them in November and December 2016.

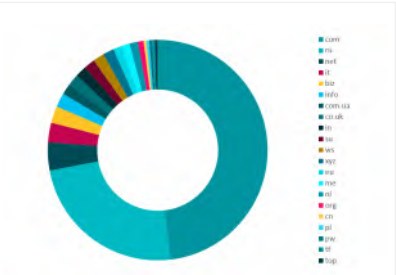


Figure 3. C&C TLDs for November and December 2016

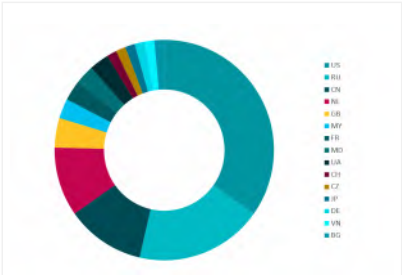


Figure 4. C&C IP Geolocation for November and December 2016

Interestingly, a lot of samples we analyzed check the system's keyboard layout and does not proceed with the infection if it matches one of the following:

- Russia
- Ukraine
- Belarus
- Kazakhstan

Infection vector

As Wauchos is bought and then distributed by a variety of cybercriminals, the infection vectors used to disseminate this threat vary greatly. Historically, Wauchos samples have been distributed through social media, instant messaging, removable media, spam, and exploit kits. Figure 5 shows a typical email spam with a Wauchos sample attached.

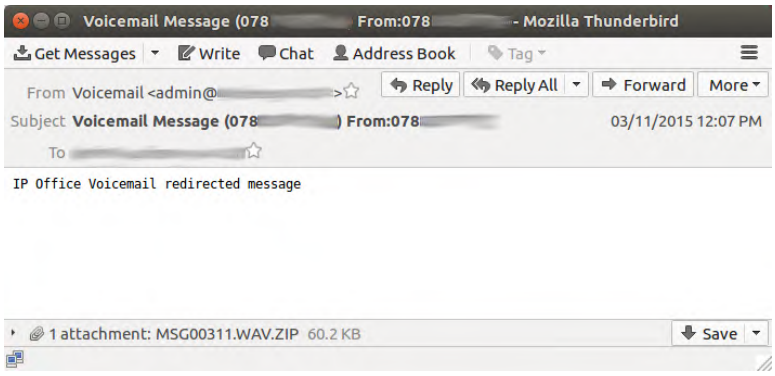


Figure 5. Typical email spam distributing Wauchos

Pay-per-install malware

As described previously, Wauchos is mostly used to distribute other malware families. Through our automatic systems, we were able to derive statistics on what was downloaded by the Wauchos bots we were tracking. Figure 6 shows the different plugins that were downloaded by our crawler when first connecting to the C&C.

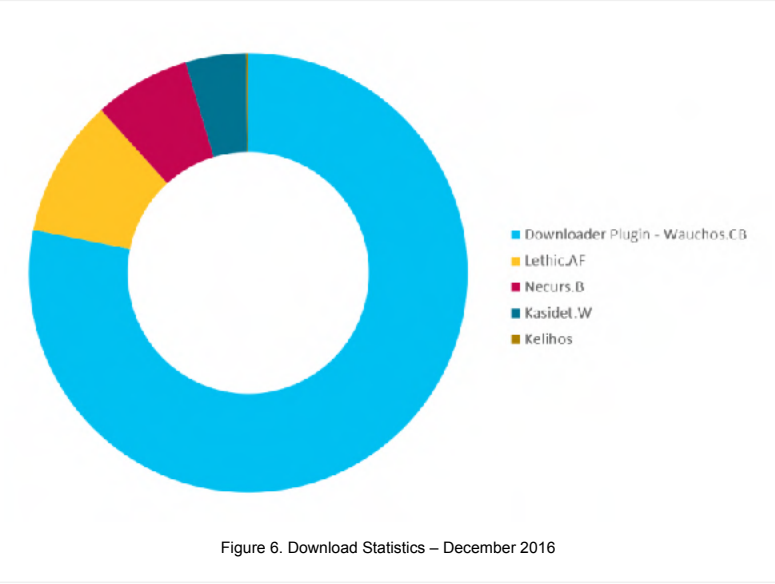


Figure 6. Download Statistics – December 2016

The first download is usually a plugin — more specifically, the downloader plugin we will discuss in a subsequent section. In terms of installed malware, most of the malware we saw distributed in December 2016 were spambots such as **Win32/Kasidet**, **Win32/Kelihos** or **Win32/Lethic**. Of course, as it is a pay-per-install scheme, these statistics tend to change from time to time. There was, as one might expect, other malware downloaded by Wauchos, but according to our telemetry data, the ones shown above are the most prevalent.

Technical analysis

In this section, we will present some technical details that have not been widely discussed in public and that provide context in light of the recent takedown. In particular, we will discuss two plugins that can provide side-channel communication to the botmaster, increasing the botnet's resiliency to a takedown operation.

Wauchos variants

First, to help our fellow researchers interested in this malware family, we will briefly describe the major variants, using ESET's naming and to what they correspond.

Win32/Wauchos.B is the most prevalent detection for 2.06 Wauchos component while version 2.10 is mainly detected as Win32/Wauchos.AW. The other variants grouped under the Win32/Wauchos family are either plugins, packed versions of the aforementioned versions or other versions of the Wauchos malware, such as 2.07, 2.08 or 2.09; these are less prevalent according to our telemetry and thus less relevant to this discussion.

In the latest version of Wauchos (2.10), the bot supports the current commands:

Command ID	Description
1	Download and run a binary file
2	Download a plugin
3	Download malware update
6	Delete all plugins
9	Uninstall

Plugins

Wauchos is an extensible bot that allows its owner to create and use custom plugins. However, there are some plugins that are widely available and that are used by many different botnets. In this section we will review the different plugins our tracking mechanism was able to download.

Title	Detection name	Description
SOCKS Proxy	Win32/TrojanDownloader.Wauchos.O	Accepts connections and acts as a network proxy
TeamViewer	Win32/TrojanDownloader.Wauchos.BA	Embeds TeamViewer application that will launch in hidden mode and allow criminals to connect back and control compromised system
Form Grabber	Win32/TrojanDownloader.Wauchos.AZ	Steals content entered into web forms by the user

When a bot downloads a plugin, it must first decrypt its header with the RC4 key. The header contains the unique key required to decrypt the payload. Once decrypted, the last operation is to decompress the plugin using aPLib. Once this is done, the malware uses a custom loader to load this binary blob into memory. As the binary blobs are already memory-page aligned they can be loaded *directly* into memory and executed.

The number of different RC4 keys collected by our tracking system amongst all different botnets is surprisingly small, at around 40. This makes it pretty easy to decrypt any downloaded components without even needing to analyze the sample. It is interesting to note here that the same RC4 key is used to encrypt both sample strings and network communication, but reversed for the latter.

In terms of C&C communication, all the samples we analyzed were using Google's DNS infrastructure directly to resolve the C&C domains. Version 2.06 is trying to resolve the C&C server IP address using raw UDP sockets to 8.8.4.4:53. If it is unsuccessful, it first falls back to the DnsQueryA() Windows API and second to the gethostbyname() API. Version 2.10 hooks GetAddrInfoW() and all calls to it are resolved using raw UDP packets to 8.8.4.4:53 with fallback to the original GetAddrInfoW() API if unsuccessful.

New persistence mechanisms

In this section we cover two plugins that appeared this year and that we believe are an attempt to prevent takedown operations like this one from succeeding, by providing a side-channel communication to the botmaster. This behavior has also been discussed here [4].

The first one is a USB spreader while the second implements a fileless attack through a downloader stored in the registry that is launched via a PowerShell script at startup.

USB spreader – Win32/Bundpil.CS

This plugin is able to hook DNS API functions, tries to spread through removable media and uses a DGA (Domain Generation Algorithm) to download additional data.

There is one thread that scans for inserted removable media and, if it finds any, puts a copy of the malware on it. The other functionality of this plugin is to hook DNS APIs and replace specific domains by a hardcoded one. For example, one sample we analyzed was redirecting any requests to these old Wauchos domains:

- designfuture.ru
- disorderstatus.ru
- atomictrivia.ru
- differentia.ru

to gvaq70s7he.ru.

There is also a DGA component to this plugin that will try to connect to the automatically generated domain to download additional data to the compromised system. The DGA algorithm pseudo-code can be found on our **Github page**. The URLs it tries to reach match these patterns:

- <dga_domain>.ru/mod
- ww1.<dga_domain>.ru/1
- ww2.<dga_domain>.ru/2

We were able to download a binary blob from this DGA scheme. What we obtained was an encrypted blob starting with 'MZ'. The plugin will remove these two bytes and store the blob directly to the Windows registry.

The main Wauchos bot will then decrypt the RC4 encrypted payload, decompress it with aPLib and load it as a regular plugin. Note here that the same RC4 keys used to encrypt the plugins are used for this process. The binary we obtained this way was an updated version of the USB spreader. We therefore hypothesized that through DNS hooking, it would be possible for botmasters to regain control of their bots by downloading a fresh version of this module from a domain they control, which will then redirect the hard coded-domains in the main Wauchos binary.

Downloader

The last plugin we want to talk about is a small downloader using a DGA to reach out to URLs like these, depending on the version:

- <dga_domain>.ru/ld.so
- <dga_domain>.ru/last.so
- <dga_domain>.ru/nonc.so

It is used to download a binary blob that it stores in the registry. This binary blob can be decrypted with the RC4 key contained in the main Wauchos payload.

One of the malware variants that was downloaded by this plugin is another downloader detected as TrojanDownloader.Small.AHI. This malware is particularly interesting as its sole purpose is to download an updated version of the downloader plugin and store it encrypted in the registry, but with a little twist. It also adds a run key with a PowerShell script that decrypts and executes the encrypted binary from the registry key each time the machine is started. Right now, this binary is merely updating itself. However, its DGA could be used as a secondary communication channel to download a new payload and regain control over bots, should someone try to take them over. Figure 7 shows the overall process.

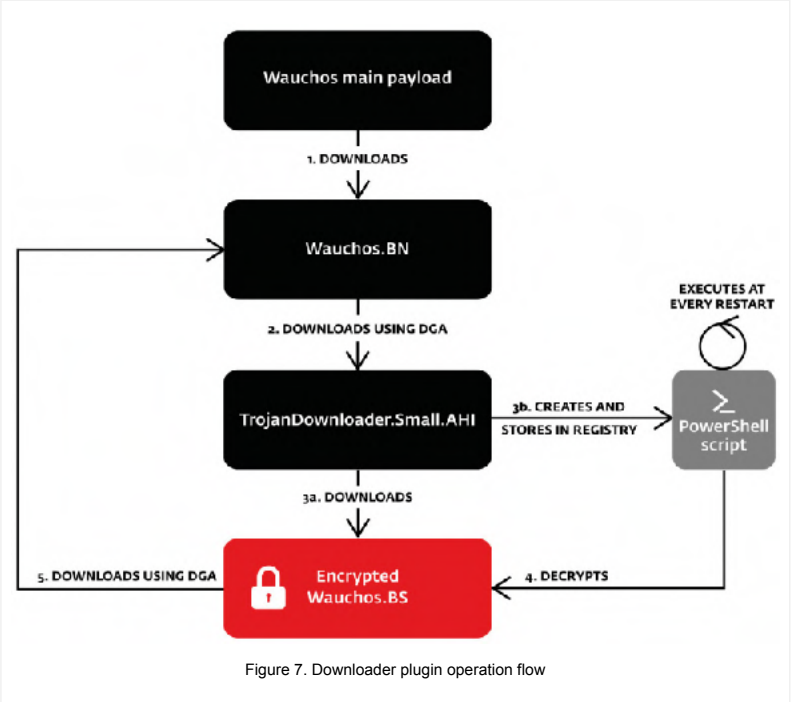


Figure 7. Downloader plugin operation flow

It is interesting to note here that we have also seen Necurs.B being downloaded through DGA and through this plugin. However, the vast majority of downloads we saw were for Win32/TrojanDownloader.Small.AHI. In fact, the latter malware has been seen numerous times, according to our cloud statistics. Interestingly, we saw a lot of activity in August 2016 for this particular module, via our crawler, but nothing since then. We did not investigate further to try to determine whether we were just blacklisted or if they only tested this feature for a brief period of time.

Conclusion

Wauchos is an old botnet that has been reinventing itself through the years. Its command and control infrastructure is one of the many that ESET tracks. This information is vital in order to keep track of changes in malware behavior and to be able to provide actionable data to help with disruption and takedown efforts.

Wauchos uses old tricks to compromise new systems. Users should be cautious when opening files on removable media, as well as files they receive through email or social media. If you believe that you are infected with Wauchos, we have **a free tool for you**. ESET products currently detect thousands of variations of Wauchos modules along with the different malware distributed by the Wauchos botnets.

Special thanks to Juraj Jánošík, Viktor Lucza, Filip Mazán, Zoltán Rusnák and Richard Vida for their help in this research.

Hashes

SHA-1	Detection
CC9AC16847427CC15909A60B130CB7E67D2D3804	Win32/TrojanDownloader.Wauchos.B
BCD45398983EB58B33294DFE852B57B1ADD5117E	Win32/TrojanDownloader.Wauchos.AK
6FA5E48AD60B53761A42725A4B9EC12B85963F90	Win32/TrojanDownloader.Small.AHI
6D5051580DA73570944BBE79A9EA7F2E4D006699	Win32/TrojanDownloader.Wauchos.O

References

- [1] **https://blog.fortinet.com/2014/04/16/a-good-look-at-the-Andromeda-botnet**
- [2] **https://blog.avast.com/Andromeda-under-the-microscope**
- [3] **http://eternal-todo.com/blog/Andromeda-gamarue-loves-json**
- [4] **http://blog.trendmicro.com/trendlabs-security-intelligence/usb-malware-implicated-fileless-attacks**

EXHIBIT 4

Date of First Publication: December 4, 2017

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF GEORGIA

Atlanta Division

MICROSOFT CORPORATION, a Washington Corporation, Plaintiff, v. JOHN DOES 1-51, CONTROLLING MULTIPLE COMPUTER BOTNETS THEREBY INJURING MICROSOFT AND ITS CUSTOMERS Defendants.	)	Civil Action No: 1:17-cv-4566

Plaintiff Microsoft Corporation ("Microsoft") has sued Defendants John Does 1-51 associated with the Internet domains listed below. Microsoft alleges that Defendants have violated various Federal and state laws by hosting a cybercriminal operation through these Internet domains, causing unlawful intrusion into Microsoft and Microsoft's customers' computers and computing devices; and intellectual property violations to the injury of Microsoft and Microsoft's customers. Microsoft seeks a preliminary injunction directing the registry associated with these Internet domains to take all steps necessary to disable access to and operation of these Internet domains to ensure that changes or access to the Internet domains cannot be made absent a court order and that all content and material associated with these Internet domains are to be isolated and preserved pending resolution of the dispute. Microsoft seeks a permanent injunction, other equitable relief and damages. Full copies of the pleading documents are available at www.noticeofpleadings.net/gamarue.

NOTICE TO DEFENDANT: READ THESE PAPERS CAREFULLY! You must "appear" in this case or the other side will win automatically. To "appear" you must file with the court a legal document called a "motion" or "answer." The "motion" or "answer" must be given to the court clerk or administrator within 21 days of the date of first publication specified herein. It must be in proper form and have proof of service on Microsoft's attorneys, Michael Zweiback at Alston & Bird LLP, 333 South Hope Street, 16th Floor, Los Angeles, CA 90071. If you have questions, you should consult with your own attorney immediately.

COMPLAINT AND SUMMONS

Complaint (files/Complaint_And_Summons/Complaint.pdf)

Summons for Doe Defendants 1-51 (files/Complaint_And_Summons/Summons.pdf)

COURT ORDERS

Emergency Ex Parte Temporary Restraining Order and Order to Show Cause Re: Preliminary Injunction (files/Court_Orders/Emergency_Ex_Parte_TRO_and_Order_to_Show_Cause_re_Preliminary_Injunction.pdf)

Order Granting Motion for Protective Order Temporarily Sealing Documents (files/Court_Orders/Order_Granting_Motion_for_Protective_Order_Temporarily_Sealing_Documents.pdf)

Order Granting Motion for Leave to Exceed Page Limits Re: Microsoft's Brief in Support of Microsoft's TRO Application (files/Court_Orders/Order_Granting_Motion_for_leave_to_Exceed_Page_Limits.pdf)

Standing Order Regarding Civil Litigation (files/Court_Orders/Standing_Order_Regarding_Civil_Litigation.pdf)

Order Granting Microsoft's Emergency Motion Re: Unsealing of Case (files/Court_Orders/Order_Unsealing_Case.pdf)

Order Extending Microsoft's Emergency Ex Parte Temporary Restraining Order And Order To Show Cause Re: Preliminary Injunction (files/Court_Orders/Order_Extending_TRO.pdf)

APPLICATION FOR EMERGENCY EX PARTE TEMPORARY RESTRAINING ORDER (TRO) AND PRELIMINARY INJUNCTION

Emergency Motion Pursuant to Local Rule 7.2B (files/Application_For_TRO/Emergency_Motion_LR_7_2B.pdf)

Notice of Hearing Re: Application of Microsoft for an Emergency Ex Parte TRO and Order to Show Cause Re: Preliminary Injunction (files/Application_For_TRO/Notice_of_Hearing_re_TRO.pdf)

Application of Microsoft for an Emergency Ex Parte TRO and Order to Show Cause Re: Preliminary Injunction (files/Application_For_TRO/Application_for_TRO.pdf)

Brief in Support of Microsoft's Emergency Ex Parte TRO and Order to Show Cause Re: Preliminary Injunction (files/Application_For_TRO/Brief_ISO_TRO_Application.pdf)

Declaration of Jean-Ian Boutin in Support of Microsoft's Application for an Emergency Ex Parte TRO and Order to Show Cause Re: Preliminary Injunction; Exhibits 1-4 to Declaration of Jean-Ian Boutin (files/Application_For_TRO/Boutin_TRO_Decl_Ex_1_4.pdf)

Declaration of Rodelio G. Fiñones in Support of Microsoft's Application for an Emergency Ex Parte TRO and Order to Show Cause Re: Preliminary Injunction; Exhibit 1 to Declaration of Rodelio G. Fiñones (files/Application_For_TRO/Finones_TRO_Decl_Ex_1.pdf)

Declaration of Vishant Patel in Support of Microsoft's Application for an Emergency Ex Parte TRO and Order to Show Cause Re: Preliminary Injunction; Exhibit 1-2 to Declaration of Vishant Patel (files/Application_For_TRO/Patel_TRO_Decl_Ex_1_2.pdf)

Declaration of Michael Zweiback in Support of Microsoft's Application for an Emergency Ex Parte TRO and Order to Show Cause Re: Preliminary Injunction; Exhibits 1-7 to Declaration of Michael Zweiback (files/Application_For_TRO/8_0_Zweiback_TRO_Decl_Ex_1_7.pdf)

Exhibits 8-20 to Declaration of Michael Zweiback (files/Application_For_TRO/8_1_Zweiback_TRO_Decl_Ex_8_20.pdf)

Exhibits 21-37 to Declaration of Michael Zweiback (files/Application_For_TRO/8_2_Zweiback_TRO_Decl_Ex_21_37.pdf)

MOTION FOR ORDER TEMPORARILY SEALING DOCUMENTS

Notice of Hearing Re: Motion for Protective Order Temporarily Sealing Documents (files/Motion_To_Temporarily_Seal_Docs/Notice_of_Hearing_re_Protective_Order.pdf)

Microsoft's Motion for Protective Order Temporarily Sealing Documents (files/Motion_To_Temporarily_Seal_Docs/Motion_for_Protective_Order.pdf)

Memorandum in Support of Motion for Protective Order Temporarily Sealing Documents (files/Motion_To_Temporarily_Seal_Docs/Memo_ISO_Motion_to_Seal.pdf)

Declaration of Michael Zweiback in Support of Motion for Protective Order Temporarily Sealing Documents (files/Motion_To_Temporarily_Seal_Docs/Zweiback_Sealing_Decl.pdf)

MOTION TO EXCEED PAGE LIMITS

Notice of Hearing Re: Microsoft's Motion for Leave to Exceed Page Limits Re: Microsoft's Brief in Support of Microsoft's Application for an Emergency Ex Parte TRO and Order to Show Cause Re: Preliminary Injunction (files/Motion_For_Page_Limits/Notice_of_Hearing_re_Motion_to_Exceed.pdf)

Microsoft's Motion for Leave to Exceed Page Limits Re: Brief in Support of Microsoft's Application for an Emergency Ex Parte TRO and Order to Show Cause Re: Preliminary Injunction (files/Motion_For_Page_Limits/Motion_to_Exceed_Pages.pdf)

Brief in Support of Microsoft's Motion for Leave to Exceed Page Limits Re: Brief in Support of Microsoft's Application for an Emergency Ex Parte TRO and Order to Show Cause Re: Preliminary Injunction (files/Motion_For_Page_Limits/Brief_ISO_Motion_to_Exceed_Pages.pdf)

NOTICE OF EXECUTION AND MOTION TO UNSEAL

Emergency Motion Pursuant to Local Rule 7.2B (files/Notice_Of_Execution_And_Motion_To_Unseal/Emergency_Motion_LR_7.2B.pdf)

Notice of Execution of Emergency Ex Parte Temporary Restraining Order and Notice of Emergency Motion Re: Unsealing of Case (files/Notice_Of_Execution_And_Motion_To_Unseal/Notice_of_Execution_Notice_of_Hearing_re_Unsealing_Motion.pdf)

Microsoft's Emergency Motion Re: Unsealing of Case (files/Notice_Of_Execution_And_Motion_To_Unseal/Emergency_Unsealing_Motion.pdf)

MISCELLANEOUS

Civil Cover Sheet (files/Miscellaneous/Civil_Cover_Sheet.pdf)

Financial Interest Disclosure Statement (files/Miscellaneous/Financial_Interest_Disclosure_Statement.pdf)

Trademark Report Form (files/Miscellaneous/USPTO_Notice_Trademark_Report_Form.pdf)

Civil Minutes Entry – November 14, 2017 Hearing (files/Miscellaneous/Civil_Minutes_Nov_14_Sealing_Hearing.pdf)

Civil Minutes Entry – November 15, 2017 Hearing (files/Miscellaneous/Civil_Minutes_Nov_15_TRO_Hearing.pdf)

Civil Minutes Entry – November 30, 2017 Hearing (files/Miscellaneous/Civil_Minutes_Nov_30_Unsealing_Hearing.pdf)

CONTACT US

If you wish to contact us by e-mail, fax, phone or letter please contact us at:

Michael Zweiback
Alston & Bird LLP
333 South Hope Street
16th Floor
Los Angeles, CA 90071

Telephone: (213) 576-1000
Facsimile: (213) 576-1100
Email: michael.zweiback@alston.com (mailto:michael.zweiback@alston.com)

EXHIBIT 5

CRYPTR.org

Server Optimization

The Unique Soldiers of Turkey

ANASAYFA ARAMA PORTAL ÜYELER FORUM TAKIMI

Oturum Aç Kayıt Ol

Cryptr Arge / Cryptr Satış / Black Market Botnet IRCD Kurulum icin VPS Sunucu

Botnet IRCD Kurulum icin VPS Sunucu

Konuyu Oyla:

Goruntuleme Modu
Normal Mod | Çizgisel Görünüm

Schwarz
Üye

Üye no: 875
Yorumları: 13
Konu Sayısı:
Ülke
Kayıt Tarihi: 06-05-2011
0

Botnet IRCD Kurulum icin VPS Sunucu — Yorum: #1

Botnet IRCD Kurulum icin VPS Sunucu
-> Merhaba arkadaslar.. Botnet kurmak isteyen arkadaslar ozellikle IRCD Hosting ve Sunucu konusunda cok buyuk sıkıntılar cekmektedirler..Malumunuz Botnet ve Ddos syn udp vb saldırılar illegal yöntemler oldugu icin bugun dunyada sunucu hizmeti veren datacenter ların %99 u bu işlemlerin yapılmasına izin vermemektedir.. Botnet kurulum ve kullanimi icin IRCD Hosting arayanlar ve daha fazlası VPS Sunucu almak isteyen arkadaslar asagida sunucu ozelliklerini veriyorum istediginiz sunucuyu benimle irtibat kurarak alabilirsiniz...
-> CPU'S Xeon 3470 3,4 ghz
-> 500 GB Disk alanı
-> 8192 MB RAM (8GB)
-> BANDWİDTH Unlimited
-> NETWORK SPEED 10 Gbps
-> 1 Adet ip adresi
-> Lokasyon ingiltere
-> Windows - Server2008 Edition
-> FİYAT 100 TL'DİR (AYLIK) pazarlik payi vardir , pazarlik sünnettir :)
-> Güçlü Syn UDP özelligi olan [EXE + SUNUCU + KURULUM] 150 tl'dir , exe fiyati ve kurulum fiyati 1 kereye mahsus alınmaktadır , sunucu fiyati her ay stabil 100 tl'dir
http://www.youtube.com/watch?v=XooWiyjfC...r_embedded
iletisim : bydevilz@gmail.com & the-schwarz@hotmail.com.tr

Son Düzenleme: 27-01-2012, Saat: 01:40, Düzenleyen: Schwarz.

27-01-2012, Saat: 01:39 Ara Beğen Alıntı Yap

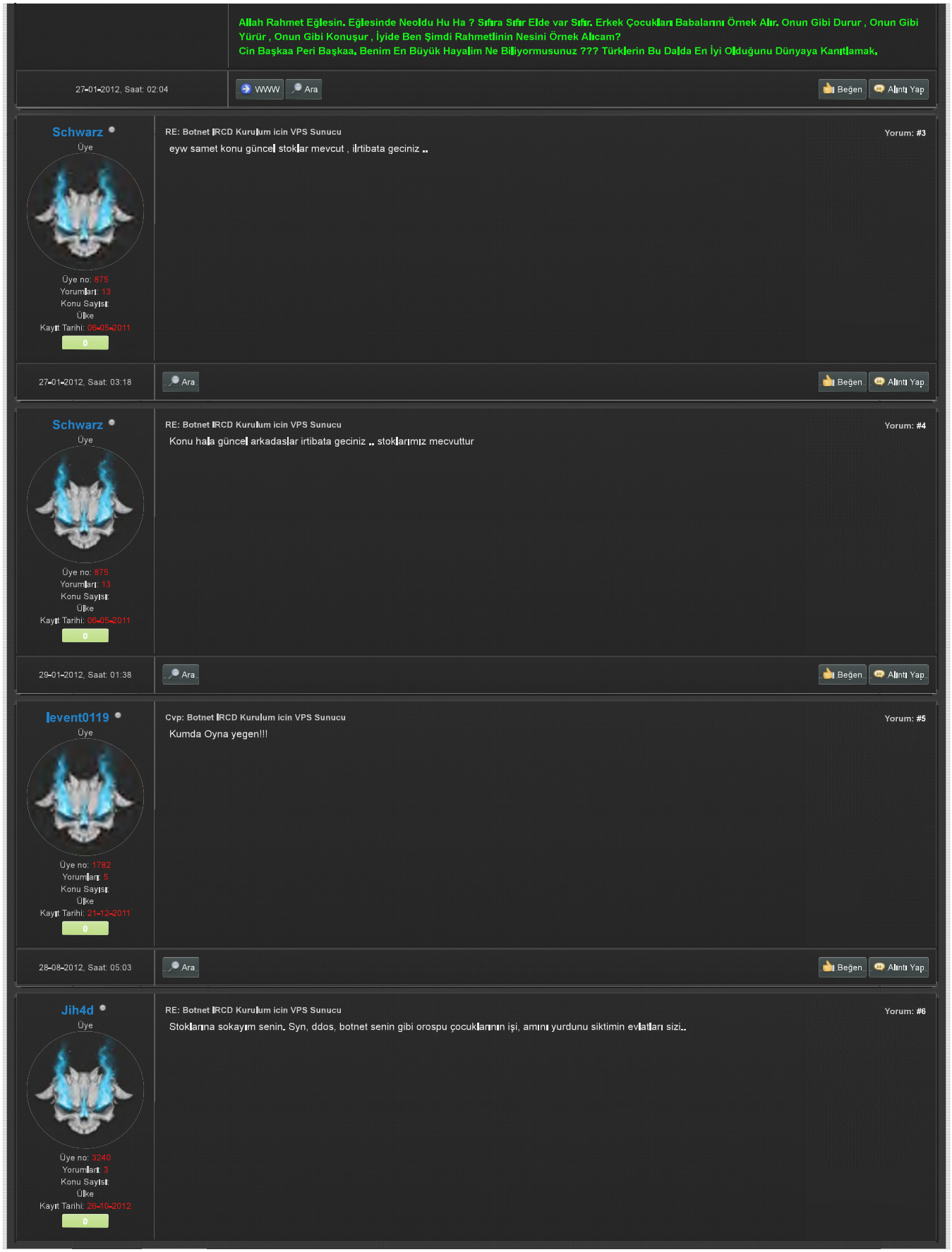
Ap0x
Administrator & Forum Leader

Üye no: 3
Yorumları: 2,946
Konu Sayısı:
Ülke
Kayıt Tarihi: 08-09-2010
22

RE: Botnet IRCD Kurulum icin VPS Sunucu — Yorum: #2

Konunun Yeri Burası Değil Black Market'e Açmalısın Taşıyorum...

Adım Samet Namıdiyar Ap0x Adı : Samet Soyadı : Karaeski
İnsanoğluyum
Hayatım Boyunca Herhangi bir Mesleğe Bağlı Kalmadım, Hastasıda Olmadım.
Benim Hastalığım Başka. Yılın 365 gününün 101 ini Hack Yaparak Geçiririm 35 Gününü All The Time Pompa Yaparak Geçiriyorum Desek, 45 Gününüde Arkadaşlarımla Beraber Geçiriyorum Beyin Fırtınası Misali Desek, 60 Gününüde Alışveriş Rakı Partileri Desek, Geriye Kalır 125 Gün 125 Günde Ne Mi Yapılabilir Evlenilebilir, Dünya Turuna Çıkılabilir, Jigolo Olunabilir, Borsa Bahis At Yarışı Futbol Turnuvaları Yapılabilir,
Kilo Alıp Verilebilir , Sıkıldığın Sevgilinden Ayrılıp Bir Başkasıyla Çıkılabilir , Sıkı Çalışırsa İnceden Fit Bir Vucuda Sahip Olunabilir Sonrasında Brazzers'a Başvurulabilir , Herşey Yapılabilir.
Varoş Bir Ailenin Tek Erkek Evladıyım. Rahmetli Babamın En Büyük Mirası Hayalleriydi,İyi Kotu Ev , İyi Kotu Arabamız Olucaktı Geçinip Gidicektik.



Allah Rahmet Eğlesin. Eğlesinde Neoldu Hu Ha ? Sıfıra Sıfır Elde var Sıfır. Erkek Çocukları Babalarını Örnek Alır. Onun Gibi Durur , Onun Gibi Yürür , Onun Gibi Konuşur , İyide Ben Şimdi Rahmetlinin Nesini Örnek Alıcam?
Cin Başkaa Peri Başkaa. Benim En Büyük Hayalim Ne Biliyormusunuz ??? Türklerin Bu Dalda En İyi Olduğunu Dünyaya Kanıtlamak.

27-01-2012, Saat: 02:04 — WWW — Ara — Beğen — Alıntı Yap

Schwarz
Üye
Üye no: 875
Yorumları: 13
Konu Sayısı:
Ülke
Kayıt Tarihi: 06-05-2011
0

RE: Botnet IRCD Kurulum icin VPS Sunucu — Yorum: #3

eyw samet konu güncel stoklar mevcut , iletişim geciniz ..

27-01-2012, Saat: 03:18 — Ara — Beğen — Alıntı Yap

Schwarz
Üye
Üye no: 875
Yorumları: 13
Konu Sayısı:
Ülke
Kayıt Tarihi: 06-05-2011
0

RE: Botnet IRCD Kurulum icin VPS Sunucu — Yorum: #4

Konu hala güncel arkadaslar irtibata geciniz .. stoklarımız mecvuttur

29-01-2012, Saat: 01:38 — Ara — Beğen — Alıntı Yap

levent0119
Üye
Üye no: 1782
Yorumları: 5
Konu Sayısı:
Ülke
Kayıt Tarihi: 21-12-2011
0

Cvp: Botnet IRCD Kurulum icin VPS Sunucu — Yorum: #5

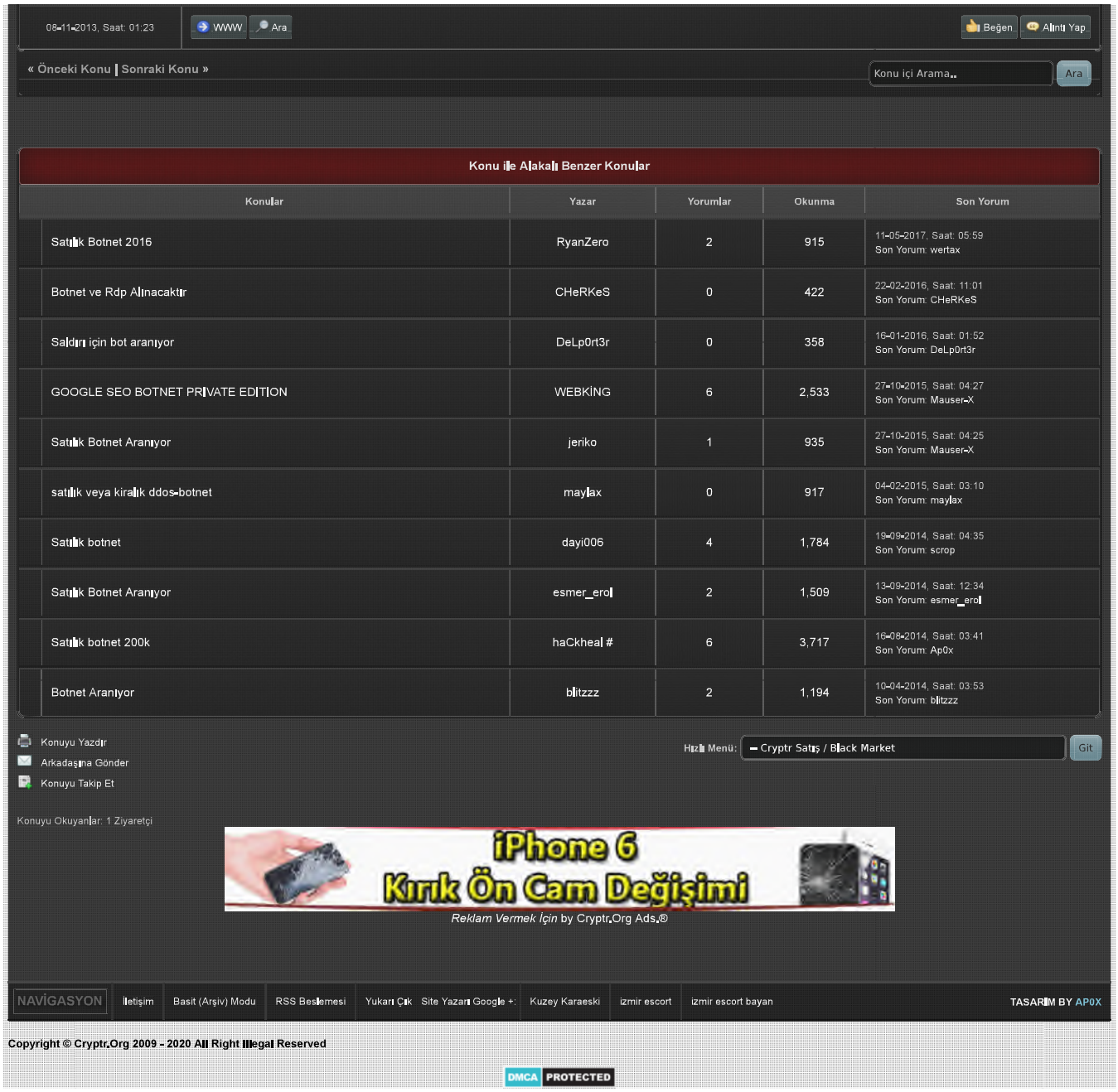
Kumda Oyna yegen!!!

28-08-2012, Saat: 05:03 — Ara — Beğen — Alıntı Yap

Jih4d
Üye
Üye no: 3240
Yorumları: 3
Konu Sayısı:
Ülke
Kayıt Tarihi: 26-10-2012
0

RE: Botnet IRCD Kurulum icin VPS Sunucu — Yorum: #6

Stoklarına sokayım senin. Syn, ddos, botnet senin gibi orospu çocuklarının işi, amını yurdunu siktimin evlatları sizi..


08-11-2013, Saat: 01:23
WWW
Ara
Beğen
Alıntı Yap
« Önceki Konu | Sonraki Konu »
Konu içi Arama..
Ara
Konu ile Alakalı Benzer Konular
Konular
Yazar
Yorumlar
Okunma
Son Yorum
Satılık Botnet 2016
RyanZero
2
915
11-05-2017, Saat: 05:59
Son Yorum: wertax
Botnet ve Rdp Alınacaktır
CHeRKeS
0
422
22-02-2016, Saat: 11:01
Son Yorum: CHeRKeS
Saldırı için bot aranıyor
DeLp0rt3r
0
358
16-01-2016, Saat: 01:52
Son Yorum: DeLp0rt3r
GOOGLE SEO BOTNET PRIVATE EDITION
WEBKİNG
6
2,533
27-10-2015, Saat: 04:27
Son Yorum: Mauser-X
Satılık Botnet Aranıyor
jeriko
1
935
27-10-2015, Saat: 04:25
Son Yorum: Mauser-X
satılık veya kiralık ddos-botnet
maylax
0
917
04-02-2015, Saat: 03:10
Son Yorum: maylax
Satılık botnet
dayi006
4
1,784
19-09-2014, Saat: 04:35
Son Yorum: scrop
Satılık Botnet Aranıyor
esmer_erol
2
1,509
13-09-2014, Saat: 12:34
Son Yorum: esmer_erol
Satılık botnet 200k
haCkheal #
6
3,717
16-08-2014, Saat: 03:41
Son Yorum: Ap0x
Botnet Aranıyor
blitzzz
2
1,194
10-04-2014, Saat: 03:53
Son Yorum: blitzzz
Konuyu Yazdır
Arkadaşına Gönder
Konuyu Takip Et
Hızlı Menü:
Cryptr Satış / Black Market
Git
Konuyu Okuyanlar: 1 Ziyaretçi
iPhone 6
Kırık Ön Cam Değişimi
Reklam Vermek İçin by Cryptr.Org Ads.®
NAVİGASYON
İletişim
Basit (Arşiv) Modu
RSS Beslemesi
Yukarı Çık
Site Yazarı Google +:
Kuzey Karaeski
izmir escort
izmir escort bayan
TASARIM BY AP0X
Copyright © Cryptr.Org 2009 - 2020 All Right Illegal Reserved
DMCA PROTECTED