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

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

DECLARATION OF JEAN-IAN BOUTIN IN SUPPORT OF MICROSOFT'S APPLICATION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE: PRELIMINARY INJUNCTION

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

FILED UNDER SEAL

DECLARATION OF JEAN-IAN BOUTIN IN SUPPORT OF MICROSOFT'S APPLICATION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE: PRELIMINARY INJUNCTION

I, Jean-Ian Boutin, declare as follows:

1. I am a senior malware researcher with ESET, spol. s r.o. ("ESET"), a company which specializes in providing Internet security services and antivirus products. I make this declaration in support of Microsoft's Application For An Emergency *Ex Parte* Temporary Restraining Order And Order To Show Cause Re: Preliminary Injunction. I make this declaration of my own personal knowledge, and,

if called as a witness, I could and would testify competently to the truth of the matters set forth herein.

2. In my role in ESET's Security Intelligence Program, I supervise a team investigating incidents related to online attacks, security threats, botnets and fraud. In particular, over the past six years I've been involved in identifying and mitigating online threats for millions of ESET product end users. My role at ESET has provided me an in-depth insight into how malware authors deploy and utilize online threats for their monetary gain. Prior to joining ESET, I was a senior software developer for a cellular network planning company. In 2009, I received a Master of Engineering degree in Electrical & Computer Engineering from Concordia University in Montreal, Canada. In 2005, I received a Bachelor of Engineering degree in Electrical Engineering from McGill University in Montreal, Canada. I am a regular contributor to ESET's security blog: welivesecurity.com. A true and correct copy of the current version of my curricula vitae is attached to this declaration as **Exhibit 1**.

I. OVERVIEW OF INTERNET BOTNETS

3. A botnet is a group of compromised end-user computers, all controlled by malicious actors or organizations, without the knowledge or consent of the computer's owner or user. Botnets can be comprised of hundreds or thousands of

compromised computers owned by individuals and businesses. Some recent botnets, including the botnet at issue in this case, have pulled in hundreds of thousands of infected end-user computers, and some comprise over a million computers.

4. Cybercriminals secretly control these botnets in order to conduct illegal acts. Cybercriminals can tell their botnet armies to, for example, install keystroke-logging programs, which will then report the end-users' sensitive information, such as banking passwords or credit card numbers.

5. Cybercriminals can also use botnets to perform coordinated attacks. In 2007, major portions of the Internet in Estonia were shut down due to denial-of-service attacks carried out by botnets, and websites of the government of the country of Georgia were severely disabled by botnets in 2008. A botnet called the "Rustock" botnet was capable of sending many billions of spam emails. Financial-fraud botnets such as "Zeus," "Citadel," "Shylock," "Ramnit," and the botnet in question in this case, "Gamarue," have been collectively responsible for the theft of millions—and potentially even hundreds of millions—of dollars from online banking accounts.

6. Botnets are grown by infecting multiple computers with malicious software and connecting them to a common infrastructure of command and control servers ("C2 servers") over the Internet, through which they may all be directed. Infection may occur through a variety of means, the most common being misleading

victims into installing the software, vulnerability exploitation, and leveraging pre-existing infections on a victim's computer. To facilitate control of a botnet, these infected computers receive commands from a controller to retrieve stolen information, conduct reconnaissance into the networks of individual botnet nodes, and more. These means are commonly referred to as the "command and control" (or "C2") structure of the botnet, and those structures vary in implementation.

7. Credible evidence indicates that botnets are often controlled by sophisticated, organized groups who participate in global, well-developed underground economies. These organizations operate similarly to legitimate businesses, in that specific tasks may be outsourced, products and services are offered in a competitive market, and incentives and value-adds are offered to "customers." These gangs are quick to adapt to new technologies, to new law enforcement tactics, and to new opportunities. Often, the controllers of a botnet will rent access to the botnet for specific tasks, and may even sell off sections of the botnet. For these reasons, botnets are dangerous instrumentalities that pose a threat to the infrastructure of the Internet and computer users worldwide.

II. OVERVIEW AND HISTORY OF GAMARUE

8. This declaration describes the functionality, operation and injury caused by a malware family known as "Gamarue." Security researchers and other

industry members also refer to this same malware family as "Andromeda" or "Wauchos." For purposes of this declaration, I will refer to the malware as Gamarue.

9. In my role as senior malware researcher at ESET, I have carried out a study of Gamarue, working with a team of ESET malware analysts located in Bratislava, Slovakia. Gamarue's primary purpose is to give cybercriminals control of infected computers, deliver additional malware to victims' computers, steal account credentials and then money from the users of infected computers, or deliver other malware such as ransomware in order to extort money from victims (as further described in paragraphs 33 and 35, below). Variants of this malware family are detected and identified by ESET products as Win32/TrojanDownloader.Wauchos.A, Win32/TrojanDownloader.Wauchos.B, Win32/TrojanDownloader.Wauchos.C, and so forth through Win32/TrojanDownloader.Wauchos.CY.[1]

10. ESET classified the Gamarue malware family on April 12, 2012. *See* Win32/TrojanDownloader.Wauchos Threat Detail, ESET Threat Encyclopedia, *available at* http://virusradar.com/en/Win32_TrojanDownloader.Wauchos/detail, a true and correct copy of which is attached hereto as **Exhibit 3**. Gamarue malware has been observed in many different countries. Following our initial detection,

[1] See David Harley, Wauchos Warhorse Rides Again (Nov. 8, 2012 7:11 AM), available at https://www.welivesecurity.com/2012/11/08/wauchos-warhorse-gallops-again/, a true and correct copy of which is attached hereto as **Exhibit 2**.

ESET has observed Gamarue spread prolifically across the Internet. On October 22, 2016, Gamarue and its associated plugins accounted for 7.64% of malware detections reported by ESET products, which represented the highest proportion of Gamarue detections reported by ESET's products. *See id.* The attached report shows a sample set of Gamarue variants analyzed during the same week. *See* ESET Threat Intelligence, Botnet Activity Report, Global Statistics: Week 42/2016, at 68-72, a true and correct copy of which is attached hereto as **Exhibit 4**.

III. TECHNICAL ANALYSIS OF GAMARUE MALWARE

11. Under my guidance and with my participation, ESET reverse-engineered a Gamarue malware sample to understand its internal operation and structure. One of Gamarue's more noteworthy features is that the malware that initially infects the computer is relatively limited in its capabilities. However, it is designed to allow other malware applications (referred to as "modules" or "plugins") to be downloaded. Gamarue bots therefore typically download an assortment of more specialized malware modules, which are then plugged into the malware already on the machine, further expanding its capabilities and functionality.

12. Operators of Gamarue malware use common tools, a common codebase, and common tactics to establish and run these botnets. Part III.1, below, describes how the Gamarue malware has been spread by Defendants through the use

of exploits in infected files or links delivered via compromised networks or websites, and through infected devices such as USB drives. Part III.2, below, explains how the Gamarue malware can be used to download and install other malicious programs without the victims' knowledge or consent. Part III.3, below, describes the additional malware delivered by the Defendants using the Gamarue malware—the additional malware enables the Defendants to steal information and money directly from victims, or extort victims using ransomware. Finally, Part III.4, below, explains how the Gamarue malware depends on a C2 infrastructure made up of Internet domains, name servers, and IP addresses, all maintained on an interconnected network via the Internet.

1. Infecting Victims with Gamarue Malware

13. Victims can become infected with Gamarue in several ways. A victim may use an infected thumb-drive borrowed from a friend or coworker that contains the malware; access a malicious link or compromised website where the malware downloader is staged; or download other malware which then downloads Gamarue without the users consent.

14. For example, a victim might receive a spam e-mail message that appears to be authored by a friend or family member, but was in fact sent by one of the Defendants. These messages will include a malicious attachment, and when the

victim opens the attachment, the Gamarue malware is secretly installed on the victim's device. As evidenced by Gamarue's rapid spread, the Defendants have employed these techniques very effectively.

15. As further described in paragraphs 21 to 28, below, the Gamarue malware can download additional malware modules after infection. One commonly downloaded plugin, which ESET products identify as Win32/Bundpil.CS, is a worm that enables the Gamarue malware to spread by infecting removable drives, including USB devices. A "worm" is type of stand-alone malware that can replicate itself in order to infect other computers. The most commonly downloaded plugin by far, however, is the standalone Gamarue downloader (".BN" and variants). This technique has facilitated Gamarue's updates and persistence.

2. Gamarue's Initial Capabilities Upon Infection

16. One of the modules downloaded during the initial Gamarue infection creates what is referred to as a "backdoor." After a successful infection of Gamarue on a victim's computer, one of the Gamarue malware's first tasks is to establish a connection with the C2 server network via the Internet. C2 servers refer to either physical server computers or software running on computers that support the Gamarue malware (i.e., the botnets). In other words, Gamarue is able to communicate and receive instructions or additional modules from computers

elsewhere on the Internet, and Defendants use and control these C2 servers to deliver instructions to and maintain ongoing control of victim computers.

17. After connecting with the C2 servers, the Gamarue malware provides information about an infected device. This information includes a volume serial number for the victim computer (this is used as a bot ID for the computer), the Gamarue version with which the computer has been infected,[2] the operating system that is running on the victim computer, the local IP address for the victim computer, an indication as to whether the victim account has administrative rights on the victim computer, and the keyboard language setting for the victim computer.

18. The Gamarue malware then waits for a C2 server to provide instructions. There are several built-in commands that the Gamarue malware can execute, and these include:

- Download Binary: Downloads and runs additional malware onto the infected machine as a binary file;
- Install Plugin: Downloads and installs additional plugins onto the infected machine;

[2] Some variants of Gamarue do not report the version of Gamarue.

- Update Gamarue Malware: Downloads and installs an update to the Gamarue malware program;
- Uninstall Plugins: Removes Gamarue plugins from the infected machine; and
- Uninstall Gamarue Malware: Removes Gamarue malware and evidence of its presence on the infected machine.

19. Immediately after Gamarue's installation, we have observed that the Gamarue malware typically executes the "Download Binary," "Install Plugin," and Updated Gamarue Malware" commands. This practice infects the computer with additional malware, adds additional functionality to Gamarue through additional plugins, and keeps the main Gamarue malware up-to-date.

20. The Gamarue malware's ability to update itself makes it difficult to effectively remediate. Several versions of the Gamarue malware exist, and the functionality described in this declaration is primarily for the latest version, which is also the most prevalent version amongst ESET's customers.

3. Additional Malware Modules and Plugins Downloaded from Gamarue C2 Servers

21. Defendants can also use the C2 servers to download, install, or remove additional plugins; spy on the victim by capturing keystrokes and mouse actions and

viewing the victim's desktop; capture any data (e.g., credentials) submitted by a victim online; and turn the computer into a proxy server.[3] Most, if not all, owners of Gamarue-infected computing devices are unaware that their machines are infected and operating as part of the Gamarue malware. Even with professional assistance, it can be very difficult to clean an infected computer.

22. In addition to a number of unidentified plugins, I have identified several known malware modules that Gamarue downloads from the C2 servers. I have described seven modules below, using the Microsoft Defender malware family names for clarity and their descriptions as provided by Microsoft's Malware Encyclopedia, which I have reviewed and with which I am familiar.

23. First, I have observed that Gamarue downloads Fareit, a malware commonly used to steal passwords. Fareit can also be used to spread other malware and execute brute-force attacks.

24. Second, I have observed that Gamarue downloads Lethic, a "trojan" that allows hackers to gain remote access and control of an infected device. Some Lethic variants utilize code injection to hinder detection and removal, and some

[3] Some malware dropped by Gamarue also has its own C2 server infrastructure, and we do not have visibility into these separate C2 servers or the harm perpetuated by them.

variants drop copies of itself into different file names in the Windows system folder. Lethic's primary use is to send spam messages.

25. The third and fourth modules that I have seen Gamarue download are Bagsu and Dynamer, which are "trojan" modules as well.

26. Fifth, I have observed Gamarue download a module known as Kasidet, which can be used to steal sensitive information (including credit card data), record victim keystrokes, and execute a type of cyberattack called a Denial of Service ("DoS") attack. This involves using multiple compromised systems (e.g., infected computers or networks in a botnet) to simultaneously target a single computer system. For example, a botnet operator can cause all of the infected computers in his botnet to simultaneously flood the target computer or network with requests, thereby overloading the target computer system and making it impossible for the target computer system to respond to legitimate requests. This effectively shuts down the target computer system. For example, Distributed Denial of Service ("DDoS") malware may be used in an attack against a computer system or shut it down and prevent legitimate users from accessing it.

27. A sixth module that I have seen downloaded by Gamarue is Cerber, a form of "ransomware." When installed on a victim's computer, "ransomware" secretly encrypts all files on the victim's device, including photos and other

documents. This encryption blocks the victim's access to their files. The victim is then notified, and payment is demanded in order to decrypt the files. Even if the ransom is paid, the victims have no assurances that they will recover their files unaltered—in some instances files are left encrypted and are thus permanently lost.

28. Finally, I have observed Gamarue download Banload, a "trojan" designed to steal banking credentials and other sensitive data, in addition to downloading other malware. Banload sends stolen information to a remote computer using the HTTP or FTP protocols.

4. **Gamarue Malware Command and Control Infrastructure and Associated Domains**

29. Defendants carry out overall control of the Gamarue malware through C2 servers and associated domains, which Defendants use to provide instructions from the C2 servers to the infected computers.

30. The C2 servers reside at locations on the Internet referred to as domains. Each resource on the web, such as a website like cnn.com, can be accessed through a unique domain. This domain is often presented as a user friendly name like "cnn.com," while it actually corresponds to a unique alpha-numeric value IP address, such as 157.166.226.26. The IP address can be thought of as the physical location on the Internet that corresponds to a particular domain name.

31. To create an active domain, Defendants must register the domain with any one of the many domain name registrars in the world. During the registration process, Defendants must associate the domain with one or more specific IP addresses. After a domain has been registered, the registry service responsible for managing domains then associates a domain registered by an entity with a name server. Either the registrar or the entity that registered the domain uses the name server to publish the IP address for the domain.

32. Using the domain names registered by Defendants, Gamarue is able to connect infected users to their C2 servers in the botnet infrastructure. All of the infected computers will regularly connect to C2 servers to upload stolen information and to receive new commands. In this fashion, the computers of hundreds of thousands of victims around the world, including many located in the United States, have and continue to funnel highly sensitive personal financial information to Defendants.

IV. <u>INJURY CAUSED BY GAMARUE</u>

33. Gamarue causes harm to a number of parties. First, of course, serious harm is caused to end users whose computers are infected with Gamarue. Through the Gamarue malware, Defendants can steal sensitive credentials and identifying

information from the victim, and Defendants could then use those credentials to steal money from the user's financial accounts.

34. Additionally, users who detect that their computer is infected with Gamarue face the often daunting and time-consuming task of figuring out how to remove it from their computers and restore their computers settings, including its security defenses, to the original and proper configuration. In my experience, users faced with this sort of aggravating situation are prone to extreme frustration, lost time, financial costs, and when removal is done improperly, sometimes infections from other malware.

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 13th day of November, 2017, in Atlanta, Georgia.

Jean-Ian Boutin

1

Jean-Ian Boutin

Senior Security Researcher

Experience

2011–present **Senior Malware Researcher**, *ESET Canada Recherche*, Montreal.
Working as a senior malware researcher - Team Coordinator in ESET's security intelligence program.
Responsible for investigating trends in malware and finding effective techniques to counter new threats.
Work on large operations against cybercrime involving multiple organizations across different disciplines: private sector, government and academia.
Main research interests include investigation of financially motivated threat actors and state-sponsored espionage groups.

2016–present **Strategic Projects Selection Panel – Information and Communications Technologies**, *Natural Sciences and Engineering Research Council of Canada (NSERC)*.
Asked to serve as a member of the strategic projects selection panel by the NSERC, due to strong expertise in cybersecurity research.
Reviewed and ranked selected applications from professors applying to this prestigious grant.

2014–present **Scientific Advisory Committee Member**, *SERENE-RISC*, Montreal.
The Smart Cybersecurity Network (SERENE-RISC) is a knowledge mobilization network created to improve the general public's awareness of cybersecurity risks and to empower all to reduce those risks through knowledge.
The scientific advisory committee advises the board on technical and scientific matters relating to the SERENE network

2009-2011 **Senior Software Engineer**, *Mendev Canada*, Gatineau.
Mendev Canada specializes in the design and development of IP and RF planning, assurance and optimization software solutions.
Responsible for the design and implementation of several wave propagation models in Mendev's flagship product Mentum Planet.
Main duties were coding and maintaining the code base both in C++ and .NET.

2006–present **Senior Software Designer**, *InterDigital Canada Ltee*, Montreal.
Experience in the full software development cycle: system design, software design, unit testing, system testing and integration.
Development, optimization and profiling of a L2/3 3GPP R5 cellular protocol stack.
Software development and design of a mobility middleware (IEEE 802.21) for Windows XP and Windows Mobile platforms allowing ultramobile devices to perform seamless handovers across heterogeneous radio access technologies (WLAN, cellular, WiMAX).

2004 **Intern - Software Prototyping**, *InterDigital Canada Ltee*, Montreal.
Eight months, full-time internship in the WLAN prototyping division.
Implementation and design of new algorithms to increase access point functionalities.
Performed background research work and produced internal reports showing experimental results to support algorithm development.

Relevant skills

Reverse Engineering IDA, ollydbg, windbg, hiew

Threat intelligence	VirusTotal hunting, YARA, MISP
Coding	Python, C/C++, .NET, git
Experienced speaker	Presented at several conferences and different events such as Virus Bulletin, CARO, ZeroNights
conference program committee	Botconf conference, SERENE-RISC workshops

Education

2006–2008 **Masters of Engineering - M. Eng**, *Concordia University*, Montreal, *Cumulative Grade-Point Average 4.23/4.3.*

2001–2005 **Bachelor of Engineering - Honours Electrical Engineering**, *McGill University*, Montreal, *Cumulative Grade-Point Average 3.84/4.00.*

Languages

French	**Fluent**	***My native Language.***
English	**Fluent**	***Speaking, reading and writing.***

Awards

2009 **The F.A. Gerard Prize - MEng & M Applied Computer Science**, *Awarded annually, when merited, to the most deserving graduate of the Master of/ Magisteriate in Engineering and Applied Computer Science programs (non-thesis).*

2005 **Fonds Quebecois de Recherche sur Nature et les Technologies Scholarship**, *Quebec Government Master's Research Scholarship.*

2005 **McGill Dean's Honours List**, *Awarded to the top* 10% *of the Faculty of Engineering.*

2002 **Motorola Scholarship**, *Grant for Outstanding Academic Standing.*

Interests

Music	I play piano and love music in general
Sports	I love squash, tennis and hockey
Travel	I enjoy discovering new places

2

welivesecurity

News, views, and insight from the ESET security community

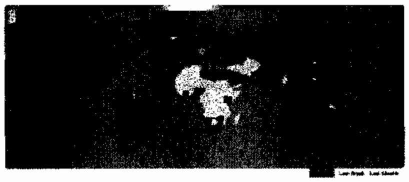
Type your keyword... Search

Wauchos Warhorse rides again

BY DAVID HARLEY POSTED 8 NOV 2012 - 07:11AM

Stephen Cobb, my friend and colleague at ESET North America brought to my attention this morning a spike, local to the United Kingdom, in detections of **Win32/TrojanDownloader.Wauchos**. This is interesting, but kind of strange, considering that the malware in question goes back to May 2012 and we haven't had to modify our detection (signature, if you must…) for quite a while.

At the moment it accounts for 24.69% of UK detections picked up by our telemetry – it accounts for 0.83% of detections worldwide, and previously peaked at 3.23% worldwide on May 14th. While highly generic detections can fluctuate wildly in volume and locality, it's kind of unusual for a more specific detection to show up again in such unusually high volumes.



As you can see from the screenshot It's also spiking in Germany: not quite so dramatically (14.3%, which is still pretty dramatic, but doesn't merit a bright red). It's also presenting an upward trend – but in much smaller volumes so far – in other parts of Europe. If you check the **actual map** on Virus Radar you'll see that its prevalence is only very slightly above the average in the US.

White areas are those for which we have no telemetry data.

Our data from-the-cloud suggests distribution by spam campaign, using file names like E-ticket-BritishAirways.pdf.exe, Vodafone_MMS.jpg.exe, Facebook-message-Foto.jpeg.exe, and Pay_by_Phone_Parking_Receipt.pdf.exe. (Tip of the hat to Pierre-Marc and Dusan for the information about the spam campaign.)

Obviously, we have good detection coverage, and given the age of the malware, I'd expect other vendors to be on top of it too, so while there are obviously people out there who don't have or don't maintain good AV protection (and may be fooled by this quaintly old-fashioned trick of giving malware a double filename extension to make it harder to spot that it's actually an .EXE), this apparent spike may represent an intensive spam campaign rather than an epidemic of actual infections.

David Harley CITP FBCS CISSP
ESET Senior Research Fellow

3

Home Threat Encyclopaedia Glossary Statistics Update Info Tools Reports **Search**

Threat Radar Report, February 2014

HOME > Threat Encyclopaedia > Threat Detail

Threat Timeline Prevalence Map

Win32/TrojanDownloader.Wauchos [Threat Name]

Detection created	**2012-04-12**
World activity peak	**2016-10-22 (7.64 %)**

Threat Variants with Description

Threat Variant Name	**Date Added**	**Threat Type**
Win32/TrojanDownloader.Wauchos.CB	2016-09-23	trojan
Win32/TrojanDownloader.Wauchos.AK	2014-09-11	trojan
Win32/TrojanDownloader.Wauchos.AF	2014-06-30	trojan
Win32/TrojanDownloader.Wauchos.X	2013-11-27	trojan
Win32/TrojanDownloader.Wauchos.L	2013-04-19	trojan
Win32/TrojanDownloader.Wauchos.I	2013-02-20	trojan
Win32/TrojanDownloader.Wauchos.C	2012-05-18	trojan
Win32/TrojanDownloader.Wauchos.A	2012-05-12	trojan
Win32/TrojanDownloader.Wauchos.B	2012-04-12	trojan

Contact | Privacy | Legal Information | Sitemap

4

Win32/TrojanDownloader.Wauchos [Threat Name]

Detection created	2012-04-12
World activity peak	2016-10-22 (7.64 %)

Threat Variants with Description

Threat Variant Name	Date Added	Threat Type
Win32/TrojanDownloader.Wauchos.CB	2016-09-23	trojan
Win32/TrojanDownloader.Wauchos.AK	2014-09-11	trojan
Win32/TrojanDownloader.Wauchos.AF	2014-06-30	trojan
Win32/TrojanDownloader.Wauchos.X	2013-11-27	trojan
Win32/TrojanDownloader.Wauchos.L	2013-04-19	trojan
Win32/TrojanDownloader.Wauchos.I	2013-02-20	trojan
Win32/TrojanDownloader.Wauchos.C	2012-05-18	trojan
Win32/TrojanDownloader.Wauchos.A	2012-05-12	trojan
Win32/TrojanDownloader.Wauchos.B	2012-04-12	trojan

4

Global Statistics: Week 42/2016

DATE	SAMPLES	C&C	NEW C&C	TARGETS	NEW TARGETS
2016-10-17	4147	678	22	190	1
2016-10-18	2385	797	19	261	1
2016-10-19	2769	1150	53	403	19
2016-10-20	3154	895	15	340	5
2016-10-21	2617	834	16	258	6
2016-10-22	2248	850	34	230	0
2016-10-23	1630	972	61	242	1

FAMILY	SAMPLES	C&C	NEW C&C	TARGETS	NEW TARGETS
Dorkbot	8434	466	1	68	2
Zbot	7807	219	100	369	25
Wauchos	3494	100	80	0	0
Papras	1500	166	2	0	0
SpyBanker	607	11	0	17	0
Bebloh	309	100	0	0	0
Banload	213	21	13	0	0
Retefe	111	29	16	61	6
Waski	95	362	0	0	0
Battdil	89	89	0	0	0
Tinba	53	175	8	0	0
Elenoocka	5	0	0	0	0

Botnet-specific report: Banload Week 42/2016

Samples

VARIANT	COUNT
Win32_TrojanDownloader_Banload_XRD_trojan	133
Win32_TrojanDownloader_Banload_XQS_trojan	11
Win32_TrojanDownloader_Banload_XOV_trojan	10
Win32_TrojanDownloader_Banload_XRH_trojan	3
Win32_TrojanDownloader_Banload_SGN_trojan	3
MSIL_TrojanDownloader_Banload_FF_trojan	3
Win32_TrojanDownloader_Banload_WZQ_trojan	3
Win32_TrojanDownloader_Banload_TZM_trojan	3
Win32_TrojanDownloader_Banload_XBU_trojan	3
Win32_TrojanDownloader_Banload_UHG_trojan	2
Win32_TrojanDownloader_Banload_WCV_trojan	2
Win32_TrojanDownloader_Banload_VHE_trojan	2
Win32_TrojanDownloader_Banload_USU_trojan	1
Win32_TrojanDownloader_Banload_XNW_trojan	1
Win32_TrojanDownloader_Banload_SQV_trojan	1
Win32_TrojanDownloader_Banload_RVO_trojan	1
Win32_TrojanDownloader_Banload_UZT_trojan	1
Win32_TrojanDownloader_Banload_XLG_trojan	1
Win32_TrojanDownloader_Banload_UFF_trojan	1
Win32_TrojanDownloader_Banload_VAT_trojan	1
Win32_TrojanDownloader_Banload_TUD_trojan	1
Win32_TrojanDownloader_Banload_XLL_trojan	1
Win32_TrojanDownloader_Banload_VQK_trojan	1
Win32_TrojanDownloader_Banload_VJU_trojan	1
Win32_TrojanDownloader_Banload_XKV_trojan	1
Win32_TrojanDownloader_Banload_XLV_trojan	1
Win32_TrojanDownloader_Banload_TLV_trojan	1

VARIANT	COUNT
Win32_TrojanDownloader_Banload_RHC_trojan	1
Win32_TrojanDownloader_Banload_URG_trojan	1
Win32_TrojanDownloader_Banload_XFX_trojan	1
Win32_TrojanDownloader_Banload_TUV_trojan	1
MSIL_TrojanDownloader_Banload_BG_trojan	1
Win32_TrojanDownloader_Banload_UUR_trojan	1
Win32_TrojanDownloader_Banload_PXR_trojan	1
Win32_TrojanDownloader_Banload_VJP_trojan	1
Win32_TrojanDownloader_Banload_UPX_trojan	1
Win32_TrojanDownloader_Banload_VWJ_trojan	1
Win32_TrojanDownloader_Banload_XLC_trojan	1
Win32_TrojanDownloader_Banload_VVV_trojan	1
Win32_TrojanDownloader_Banload_XPH_trojan	1
Win32_TrojanDownloader_Banload_VYT_trojan	1
Win32_TrojanDownloader_Banload_WSI_trojan	1
MSIL_TrojanDownloader_Banload_BA_trojan	1
Win32_TrojanDownloader_Banload_XQO_trojan	1
Win32_TrojanDownloader_Banload_WYF_trojan	1
Win32_TrojanDownloader_Banload_VAP_trojan	1
Win32_TrojanDownloader_Banload_TXV_trojan	1

Command & Control servers

	SERVER URL	LAST ALIVE	STATUS	COUNT
ℹ	http://healtechys[dot]com.br/banner/gold.gif	2016-10-18	new	2
ℹ	http://www[dot]4shared.com/download/n8p_um2kce/pro20-01-novinho.zip	2016-10-22	new	2
ℹ	http://www[dot]rioguiden.com/css/clientes/chromo/yxafsjx.zip	2016-10-21	new	2
ℹ	http://caf[dot]orangeamer.com/index/modsyuws.rar	2016-10-19	new	1
ℹ	http://howardbelfer[dot]com/webalizer/img/ai.png	2016-10-17	new	1

BOTNET ACTIVITY REPORT

	SERVER URL	LAST ALIVE	STATUS	COUNT
ⓘ	http://storage[dot]googleapis.com/sorte/in.zip	2016-10-19	new	1
ⓘ	http://wrstecnologia[dot]url.ph/j2/acesso.php	2016-10-19	new	1
ⓘ	http://www[dot]cumk.de/cro/hdbust.zlib	2016-10-18	new	1
ⓘ	http://www[dot]progresso2016.com.br/america/notify.php	2016-10-20	new	1
ⓘ	http://www[dot]progresso2016.com.br/download-capionsnow/captions-now.zip	2016-10-20	new	1
ⓘ	http://www[dot]thornhillpharmacy.ca/images/banners/css/javaw.exe	2016-10-17	new	1
ⓘ	http://www[dot]whey.nl/wp-includes/text/diff/renderer/upx/chromo/uzrcexq.zip	2016-10-21	new	1
ⓘ	https://s3[dot]amazonaws.com/f.cl.ly/items/3p3o1g3e0r1t1x2a0l17/install.exe?AWSAccessKeyId=AKIAJEFUZRCWSLB2QA5Q&Expires=1476833072&Signature=0vDcYngSHQN9LcBfgo9FIgaowKk%3D&response-content-disposition=attachment	2016-10-19	new	1
	http://www[dot]w3.org/2000/xmlns/	2016-05-26	inactive	2
	http://www[dot]w3.org/2001/XMLSchema	2016-05-26	inactive	2
	http://www[dot]w3.org/2001/XMLSchema-instance	2016-05-25	inactive	[illegible]
	http://ns[dot]adobe.com/xap/1.0/	2016-06-25	inactive	1
	http://www[dot]leemanchemical.com/logs/index/zobcx.zlib	2016-09-29	inactive	1
	http://www3[dot]cedare.int/joomla/images/documents/ok/1.txt	2016-08-05	inactive	1
	https://get[dot]adobe.com/br/reader/	2016-06-02	inactive	1
	https://www[dot]frpromotora.com.br/adm/modelo1.txt	2016-05-26	inactive	1

Botnet-specific report: Battdil Week 42/2016

Samples

VARIANT	COUNT
Win32_Battdil_AL_trojan	88
Win32_Battdil_J_trojan	1

Command & Control servers

SERVER URL	LAST ALIVE	STATUS	COUNT
https://108[dot]61.176.154:4443	2015-11-16	inactive	86
https://109[dot]199.11.51:443	2015-11-04	inactive	86
https://12[dot]206.248.195:443	2016-03-19	inactive	86
https://150[dot]129.49.163:443	2015-11-05	inactive	86
https://159[dot]148.19.195:443	2015-11-20	inactive	86
https://172[dot]250.73.193:4443	2015-11-05	inactive	86
https://173[dot]248.22.227:443	2016-05-17	inactive	86
https://176[dot]100.195.216:4443	2015-11-05	inactive	86
https://177[dot]8.255.6:443	2015-11-04	inactive	86
https://178[dot]18.75.14:443	2016-05-17	inactive	86
https://181[dot]211.112.250:443	2015-11-20	inactive	86
https://184[dot]59.100.51:443	2015-11-04	inactive	86
https://185[dot]23.14.198:443	2015-11-05	inactive	86
https://185[dot]49.69.35:4443	2015-11-16	inactive	86
https://188[dot]122.24.154:443	2016-08-18	inactive	86
https://193[dot]13.37.183:443	2015-11-19	inactive	86
https://193[dot]43.231.104:443	2016-05-17	inactive	86
https://195[dot]117.119.187:443	2015-11-04	inactive	86
https://197[dot]210.196.26:443	2015-11-05	inactive	86
https://197[dot]210.214.12:443	2015-11-05	inactive	86
https://199[dot]120.97.238:4443	2015-11-05	inactive	86

BOTNET ACTIVITY REPORT

SERVER URL	LAST ALIVE	STATUS	COUNT
https://202[dot]69.38.234:443	2015-11-05	inactive	86
https://202[dot]95.137.247:443	2015-11-04	inactive	86
https://212[dot]22.69.28:443	2015-11-02	inactive	86
https://213[dot]173.64.129:443	2015-11-04	inactive	86
https://213[dot]250.199.170:443	2015-11-05	inactive	86
https://217[dot]11.135.88:443	2015-11-05	inactive	86
https://46[dot]174.214.195:443	2015-11-19	inactive	86
https://46[dot]249.181.138:4443	2015-11-04	inactive	86
https://5[dot]149.250.254:4443	2015-11-10	inactive	86
https://5[dot]149.251.163:4443	2015-11-10	inactive	86
https://5[dot]149.251.164:4443	2015-11-10	inactive	86
https://5[dot]152.196.218:4443	2015-11-10	inactive	86
https://50[dot]24.53.233:4443	2015-11-05	inactive	86
https://50[dot]24.94.197:4443	2015-11-19	inactive	86
https://67[dot]221.146.148:4443	2015-11-04	inactive	86
https://67[dot]221.156.188:4443	2015-11-23	inactive	86
https://69[dot]193.145.138:4443	2015-11-24	inactive	86
https://77[dot]45.102.62:443	2015-11-04	inactive	86
https://80[dot]48.138.165:4443	2015-11-05	inactive	86
https://84[dot]237.216.158:443	2016-05-17	inactive	86
https://86[dot]104.134.164:4443	2015-11-10	inactive	86
https://89[dot]234.208.115:443	2016-05-16	inactive	86
https://93[dot]175.224.143:4443	2015-11-05	inactive	86
https://93[dot]185.4.90:4443	2015-11-05	inactive	86
https://94[dot]40.82.91:443	2015-11-05	inactive	86
https://107[dot]161.199.59:4443	2015-06-18	inactive	1
https://176[dot]120.201.9:443	2015-10-30	inactive	1
https://178[dot]219.10.23:443	2015-08-03	inactive	1
https://178[dot]22.222.89:443	2015-06-18	inactive	1

SERVER URL	LAST ALIVE	STATUS	COUNT
https://181[dot]189.152.131:443	2015-08-16	inactive	1
https://184[dot]164.97.60:443	2015-06-18	inactive	1
https://185[dot]31.33.98:443	2016-05-02	inactive	1
https://188[dot]123.34.203:443	2015-06-18	inactive	1
https://188[dot]255.236.227:4443	2015-06-18	inactive	1
https://188[dot]255.241.22:4443	2015-06-18	inactive	1
https://194[dot]28.190.84:443	2015-08-17	inactive	1
https://194[dot]28.191.213:443	2015-08-05	inactive	1
https://195[dot]206.255.131:443	2016-03-10	inactive	1
https://195[dot]34.206.204:443	2015-08-12	inactive	1
https://212[dot]37.81.96:4443	2015-08-07	inactive	1
https://212[dot]69.14.89:443	2015-07-09	inactive	1
https://217[dot]23.194.237:443	2015-06-18	inactive	1
https://31[dot]42.170.118:443	2016-05-18	inactive	1
https://38[dot]124.169.163:4443	2015-07-02	inactive	1
https://46[dot]175.23.130:443	2015-07-01	inactive	1
https://46[dot]37.205.163:443	2015-06-18	inactive	1
https://67[dot]206.96.30:443	2015-07-29	inactive	1
https://67[dot]206.97.238:443	2015-07-29	inactive	1
https://67[dot]207.228.144:443	2015-08-17	inactive	1
https://67[dot]219.166.113:443	2015-07-24	inactive	1
https://69[dot]118.144.195:4443	2015-07-30	inactive	1
https://69[dot]146.233.162:4443	2015-07-23	inactive	1
https://69[dot]9.204.37:443	2015-07-10	inactive	1
https://75[dot]134.44.251:443	2016-01-04	inactive	1
https://77[dot]104.206.150:443	2015-06-18	inactive	1
https://77[dot]234.235.48:443	2015-07-21	inactive	1
https://77[dot]95.192.36:443	2015-06-18	inactive	1
https://80[dot]234.34.137:443	2015-07-28	inactive	1

SERVER URL	LAST ALIVE	STATUS	COUNT
https://80[dot]87.219.35:443	2016-09-13	inactive	1
https://83[dot]168.164.18:443	2015-07-03	inactive	1
https://84[dot]16.54.22:443	2015-08-03	inactive	1
https://84[dot]16.55.122:443	2015-08-16	inactive	1
https://84[dot]237.229.49:443	2015-06-18	inactive	1
https://87[dot]116.153.216:443	2016-05-02	inactive	1
https://91[dot]232.157.139:443	2015-10-30	inactive	1
https://91[dot]240.97.141:443	2015-06-18	inactive	1
https://93[dot]91.154.243:443	2015-08-17	inactive	1
https://95[dot]143.131.73:443	2015-08-05	inactive	1

Botnet-specific report: Bebloh Week 42/2016

Samples

VARIANT	COUNT
Win32_Spy_Bebloh_K_trojan	309

Command & Control servers

SERVER URL	LAST ALIVE	STATUS	COUNT
http://11tz3sevjhhei[dot]net/auth/	2016-07-25	inactive	309
http://15o3mzr23my1[dot]com/auth/	2016-07-25	inactive	309
http://1cuiykb45wfxd[dot]net/auth/	2016-07-25	inactive	309
http://1qgquooa4lgq4ta[dot]com/auth/	2016-07-25	inactive	309
http://2mbbsm3epe3y23e[dot]com/auth/	2016-07-25	inactive	309
http://394vv13ita9[dot]com/auth/	2016-07-25	inactive	309
http://3bzwcks5puh[dot]com/auth/	2016-07-25	inactive	309
http://4rj9mgdchgcbh[dot]com/auth/	2016-07-25	inactive	309
http://5fot4r1kyzxdpya[dot]com/auth/	2016-07-25	inactive	309
http://9a3g1ghu9hn[dot]com/auth/	2016-07-25	inactive	309
http://9puzhqyl1ijeaop[dot]net/auth/	2016-07-25	inactive	309
http://9ymupehqhr5qb[dot]net/auth/	2016-07-25	inactive	309
http://af59ebcnwul9opz[dot]net/auth/	2016-07-25	inactive	309
http://alyvfll4oub4h[dot]net/auth/	2016-07-25	inactive	309
http://aymjbgn2dkt5h[dot]net/auth/	2016-07-25	inactive	309
http://btnxuhczzdsvg[dot]net/auth/	2016-07-25	inactive	309
http://cyhiz4j1s3k[dot]net/auth/	2016-07-25	inactive	309
http://evqo4nrtmds[dot]com/auth/	2016-07-25	inactive	309
http://gakzrpllvaw[dot]com/auth/	2016-07-25	inactive	309
http://gax2zjfyrt4[dot]net/auth/	2016-07-25	inactive	309
http://ghnnfywqpcx[dot]net/auth/	2016-07-25	inactive	309
http://gjo1na3ne44jq1j[dot]com/auth/	2016-07-25	inactive	309

BOTNET ACTIVITY REPORT

SERVER URL	LAST ALIVE	STATUS	COUNT
http://gn1nyhnjbdof[dot]net/auth/	2016-07-25	inactive	309
http://i2l2s4x3jtrxb4z[dot]net/auth/	2016-07-25	inactive	309
http://j1bqeyb1ffj[dot]net/auth/	2016-07-25	inactive	309
http://k4r3divsnsqu1mr[dot]net/auth/	2016-07-25	inactive	309
http://kf3rlioibrumjnnla[dot]com/auth/	2016-07-25	inactive	309
http://l1ubnlrr54[dot]com/auth/	2016-07-25	inactive	309
http://ljtrv5bsqhzl[dot]com/auth/	2016-07-25	inactive	309
http://lub3csg2t5h[dot]net/auth/	2016-07-25	inactive	309
http://nfjxd9mglt91o[dot]com/auth/	2016-07-25	inactive	309
http://odbnfhbyagyz4{dot]net/auth/	2016-10-17	active	309
http://oey2351k9foxd[dot]com/auth/	2016-07-25	inactive	309
http://ohw5c1cls4fyonu[dot]com/auth/	2016-07-25	inactive	309
http://owce3l5a4mfsawx[dot]com/auth/	2016-07-25	inactive	309
http://panttlrw2ohhv[dot]com/auth/	2016-07-25	inactive	309
http://phz9hlvvs1ddymk[dot]net/auth/	2016-07-25	inactive	309
http://pj59z2rgos3[dot]com/auth/	2016-07-25	inactive	309
http://qfwjp4n3mrfan[dot]net/auth/	2016-07-25	inactive	309
http://rr53b1jgdac[dot]net/auth/	2016-07-25	inactive	309
http://ueavl4eequooda[dot]net/auth/	2016-07-25	inactive	309
http://ul1eadtv4ladvu9[dot]net/auth/	2016-07-25	inactive	309
http://vgwi1mg9uxl[dot]net/auth/	2016-07-25	inactive	309
http://vrid5qspmwddv[dot]com/auth/	2016-07-25	inactive	309
http://xepnalivoquea[dot]com/auth/	2016-07-25	inactive	309
http://xqg25x35nvw[dot]com/auth/	2016-07-25	inactive	309
http://xw4yb5lw3fdb5[dot]com/auth/	2016-07-25	inactive	309
http://yric5p9pibhzklj[dot]com/auth/	2016-07-25	inactive	309
http://z5vkx4tkwn[dot]net/auth/	2016-07-25	inactive	309
http://zbxcxjltfkofsny[dot]net/auth/	2016-07-25	inactive	309
https://11tz3sevjhhei[dot]net/auth/	2016-07-25	inactive	309

SERVER URL	LAST ALIVE	STATUS	COUNT
https://15o3mzr23my1[dot]com/auth/	2016-07-25	inactive	309
https://1cuiykb45wfxd[dot]net/auth/	2016-07-25	inactive	309
https://1qgquooa4lgq4ta[dot]com/auth/	2016-07-25	inactive	309
https://2mbbsm3epe3y23e[dot]com/auth/	2016-07-25	inactive	309
https://394vv13ita9[dot]com/auth/	2016-07-25	inactive	309
https://3bzwcks5puh[dot]com/auth/	2016-07-25	inactive	309
https://4rj9mgdchgcbh[dot]com/auth/	2016-07-25	inactive	309
https://5fot4i1kyzxdpya[dot]com/auth/	2016-07-25	inactive	309
https://9a3g1ghu9hn[dot]com/auth/	2016-07-25	inactive	309
https://9puzhqyl1ijeaop[dot]net/auth/	2016-07-25	inactive	309
https://9ymupehqhr5qb[dot]net/auth/	2016-07-25	inactive	309
https://af59ebcnwul9opz[dot]net/auth/	2016-07-25	inactive	309
https://alyvfll4oub4h[dot]net/auth/	2016-07-25	inactive	309
https://aymjbgn2dkt5h[dot]net/auth/	2016-07-25	inactive	309
https://btixuhzzdsvg[dot]net/auth/	2016-07-25	inactive	309
https://cyhiz4j1s3k[dot]net/auth/	2016-07-25	inactive	309
https://evqq4nrtmds[dot]com/auth/	2016-07-25	inactive	309
https://gakzrpllvaw[dot]com/auth/	2016-07-25	inactive	309
https://gax2zjfyit4[dot]net/auth/	2016-07-25	inactive	309
https://ghnnfywqpcx[dot]net/auth/	2016-07-25	inactive	309
https://gjo1na3ne44jq1j[dot]com/auth/	2016-07-25	inactive	309
https://gn1nyhnjbdof[dot]net/auth/	2016-07-25	inactive	309
https://i2l2s4x3jtrxb4z[dot]net/auth/	2016-07-25	inactive	309
https://j1bqeyb1ffj[dot]net/auth/	2016-07-25	inactive	309
https://k4r3divsnsqu1mr[dot]net/auth/	2016-07-25	inactive	309
https://kf3rhoibnmjnnla[dot]com/auth/	2016-07-25	inactive	309
https://l1ubnlri54[dot]com/auth/	2016-07-25	inactive	309
https://ljtrv5bsqhzl[dot]com/auth/	2016-07-25	inactive	309
https://lub3csg2t5h[dot]net/auth/	2016-07-25	inactive	309

SERVER URL	LAST ALIVE	STATUS	COUNT
https://nfjxd9rnglt91o[dot]com/auth/	2016-07-25	inactive	309
https://odbnfhbyagyz4[dot]net/auth/	2016-10-17	active	309
https://oey2351k9foxd[dot]com/auth/	2016-07-25	inactive	309
https://ohw5c1cls4fyonu[dot]com/auth/	2016-07-25	inactive	309
https://owce3l5a4rnfsawx[dot]com/auth/	2016-07-25	inactive	309
https://panttlrw2ohhv[dot]com/auth/	2016-07-25	inactive	309
https://phz9hlvvs1ddymk[dot]net/auth/	2016-07-25	inactive	309
https://pj59z2rgos3[dot]com/auth/	2016-07-25	inactive	309
https://qfwjp4n3mrfan[dot]net/auth/	2016-07-25	inactive	309
https://rr53b1jgdac[dot]net/auth/	2016-07-25	inactive	309
https://ueavl4eequooda[dot]net/auth/	2016-07-25	inactive	309
https://ul1eadtv4ladvu9[dot]net/auth/	2016-07-25	inactive	309
https://vgwi1mg9uxl[dot]net/auth/	2016-07-25	inactive	309
https://vrid5qspmwddv[dot]com/auth/	2016-07-25	inactive	309
https://xepnalivoquea[dot]com/auth/	2016-07-25	inactive	309
https://xqg25x35nvw[dot]com/auth/	2016-07-25	inactive	309
https://xw4yb5lw3fdb5[dot]com/auth/	2016-07-25	inactive	309
https://yric5p9pibhzklj[dot]com/auth/	2016-07-25	inactive	309
https://z5vkx4tkwn[dot]net/auth/	2016-07-25	inactive	309
https://zbxcxjltfkofsny[dot]net/auth/	2016-07-25	inactive	309

Botnet-specific report: Dorkbot Week 42/2016

Samples

VARIANT	COUNT
Win32_Dorkbot_I_worm	5041
Win32_Dorkbot_B_worm	1786
Win32_Dorkbot_H_worm	1534
Win32_Dorkbot_L_worm	50
Win32_Dorkbot_A_worm	22
Win32_Dorkbot_M_worm	1

Command & Control servers

SERVER URL	LAST ALIVE	STATUS	COUNT
tcp://69[dot]172.201.217:0	2016-10-21	new	3
udp://pop[dot]mibjkib.ru:8670	2015-07-29	inactive	4744
udp://pop[dot]pjhzure.ru:8670	2015-07-29	inactive	4744
udp://pop[dot]qlmkxqlx.com:8670	2015-07-29	inactive	4744
udp://pop[dot]qzibngc.ru:8670	2015-07-29	inactive	4744
udp://pop[dot]ukmsske.ru:8670	2015-07-29	inactive	4744
udp://pop[dot]w8start.ru:8670	2015-07-29	inactive	4744
udp://pop[dot]vfukgsuopav.ru:8670	2015-07-29	inactive	4739
udp://pop[dot]natntbuo.ru:8670	2016-10-23	active	4737
udp://pop[dot]cpegnjp.ru:8670	2015-07-29	inactive	2702
udp://pop[dot]etvnzswkt.com:8670	2015-07-29	inactive	2702
udp://pop[dot]ghbzfbftq.com:8670	2015-07-29	inactive	2702
udp://pop[dot]gzjjprkuf.com:8670	2015-07-29	inactive	2702
udp://pop[dot]ifzsrlfew.com:8670	2015-07-29	inactive	2702
udp://pop[dot]iywjiyxur.com:8670	2015-07-29	inactive	2702
udp://pop[dot]jeuuinloc.com:8670	2015-07-29	inactive	2702
udp://pop[dot]jiomqnk.ru:8670	2015-07-29	inactive	2702

SERVER URL	LAST ALIVE	STATUS	COUNT
udp://pop[dot]kcwloqp.ru:8670	2015-07-29	inactive	2702
udp://pop[dot]llhoggcq.ru:8670	2015-07-29	inactive	2702
udp://pop[dot]lltiufg.ru:8670	2015-07-29	inactive	2702
udp://pop[dot]lqtmgjw.ru:8670	2015-07-29	inactive	2702
udp://pop[dot]mswteam.ru:8670	2015-07-29	inactive	2702
udp://pop[dot]nnzrwmt.ru:8670	2015-07-29	inactive	2702
udp://pop[dot]nuyftxn.ru:8670	2015-07-29	inactive	2702
udp://pop[dot]ocesuej.ru:8670	2015-07-29	inactive	2702
udp://pop[dot]prbmgxklr.com:8670	2015-07-29	inactive	2702
udp://pop[dot]qnqcwlj.ru:8670	2015-07-29	inactive	2702
udp://pop[dot]qstopsi.ru:8670	2015-07-29	inactive	2702
udp://pop[dot]riyfoawpx.com:8670	2015-07-29	inactive	2702
udp://pop[dot]ronjyfj.ru:8670	2015-07-29	inactive	2702
udp://pop[dot]rzhheil.ru:8670	2015-07-29	inactive	2702
udp://pop[dot]srzbyrt.ru:8670	2015-07-29	inactive	2702
udp://pop[dot]sxazgprlz.com:8670	2015-07-29	inactive	2702
udp://pop[dot]tpalenc.ru:8670	2015-07-29	inactive	2702
udp://pop[dot]trrppxw.ru:8670	2015-07-29	inactive	2702
udp://pop[dot]tvugttl.ru:8670	2015-07-29	inactive	2702
udp://pop[dot]ypqctjbwk.com:8670	2015-07-29	inactive	2702
udp://pop[dot]zfzhpps.ru:8670	2015-07-29	inactive	2702
udp://pop[dot]zhrelfk.ru:8670	2015-07-29	inactive	2702
udp://pop[dot]zrwolqp.ru:8670	2015-07-29	inactive	2702
udp://pop[dot]ctuiwslxa.com:8670	2015-07-29	inactive	2698
udp://pop[dot]etyrmcain.com:8670	2015-07-29	inactive	2698
udp://pop[dot]fnyswnkvk.com:8670	2015-07-29	inactive	2698
udp://pop[dot]guepcvzsr.com:8670	2015-07-29	inactive	2698
udp://pop[dot]inqmzqvxx.com:8670	2015-07-29	inactive	2698
udp://pop[dot]ketnxrsck.com:8670	2015-07-29	inactive	2698

BOTNET ACTIVITY REPORT

SERVER URL	LAST ALIVE	STATUS	COUNT
udp://pop[dot]ktqqaowqt.com:8670	2015-07-29	inactive	2698
udp://pop[dot]srpfrgvvm.com:8670	2015-07-29	inactive	2698
udp://pop[dot]uvieegpuz.com:8670	2015-07-29	inactive	2698
udp://pop[dot]vlinnbcqyw.com:8670	2015-07-29	inactive	2698
udp://pop[dot]vijvseapa.com:8670	2015-07-29	inactive	2698
udp://pop[dot]vivfcpmzj.com:8670	2015-07-29	inactive	2698
udp://pop[dot]whxwcavvg.com:8670	2015-07-29	inactive	2698
udp://pop[dot]xosecjxic.com:8670	2015-07-29	inactive	2698
udp://pop[dot]hiznnvmvu.com:8670	2015-07-29	inactive	2692
udp://89[dot]206.219.239:8670	2016-07-09	inactive	2446
udp://93[dot]190.140.243:8670	2016-10-23	active	2377
http://38[dot]130.218.55/qxl2nijj.gif	2016-10-23	active	2332
tcp://s[dot]trxspgpzz.ru:0	2016-09-07	inactive	1067
tcp://136[dot]243.118.242:0	2016-10-24	active	1066
tcp://195[dot]38.137.100:0	2016-10-23	active	410
tcp://204[dot]95.99.243:0	2016-10-23	active	410
tcp://216[dot]170.116.105:0	2016-10-23	active	410
tcp://n[dot]abjuylahr.com:0	2015-12-03	inactive	410
tcp://n[dot]abmadwhcr.com:0	2015-12-03	inactive	410
tcp://n[dot]adhelcnoh.com:0	2015-12-03	inactive	410
tcp://n[dot]adkxlenod.ru:0	2015-12-03	inactive	410
tcp://n[dot]akyjwkkqj.ru:0	2015-12-03	inactive	410
tcp://n[dot]aoyylwyxd.ru:0	2015-12-03	inactive	410
tcp://n[dot]aumzkzwrl.com:0	2015-12-03	inactive	410
tcp://n[dot]avebiwdbf.ru:0	2015-12-03	inactive	410
tcp://n[dot]axitdflcr.ru:0	2015-12-03	inactive	410
tcp://n[dot]bffihxjxo.com:0	2015-12-03	inactive	410
tcp://n[dot]bhsbqjysh.ru:0	2015-12-03	inactive	410
tcp://n[dot]bjadvjfdx.ru:0	2015-12-03	inactive	410

SERVER URL	LAST ALIVE	STATUS	COUNT
tcp://n[dot]bjlajcvcy.com:0	2015-12-03	inactive	410
tcp://n[dot]bkgywvtsx.ru:0	2015-12-03	inactive	410
tcp://n[dot]bvjbygkhq.com:0	2015-12-03	inactive	410
tcp://n[dot]cbceluvnf.com:0	2015-12-03	inactive	410
tcp://n[dot]cdtclxicx.ru:0	2015-12-03	inactive	410
tcp://n[dot]celujntse.com:0	2015-12-03	inactive	410
tcp://n[dot]cfqqxfduf.ru:0	2015-12-03	inactive	410
tcp://n[dot]cirgfzcxh.com:0	2015-12-03	inactive	410
tcp://n[dot]cjwxfmimx.ru:0	2015-12-03	inactive	410
tcp://n[dot]ckcwacpts.com:0	2015-12-03	inactive	410
tcp://n[dot]cusviecqs.ru:0	2015-12-03	inactive	410
tcp://n[dot]cvnuxxysj.com:0	2015-12-03	inactive	410
tcp://n[dot]cygzrpdct.com:0	2015-12-03	inactive	410
tcp://n[dot]dclhmfkcb.ru:0	2015-12-03	inactive	410
tcp://n[dot]dsnkjlklu.com:0	2015-12-03	inactive	410
tcp://n[dot]eaxeebvnx.com:0	2015-12-03	inactive	410
tcp://n[dot]ecnpjynwc.com:0	2015-12-03	inactive	410
tcp://n[dot]eepixnqaa.com:0	2015-12-03	inactive	410
tcp://n[dot]elnytydma.com:0	2016-08-31	inactive	410
tcp://n[dot]eoifjgjxl.ru:0	2015-12-03	inactive	410
tcp://n[dot]eoxhxlxax.com:0	2015-12-03	inactive	410
tcp://n[dot]epbdyornt.ru:0	2015-12-03	inactive	410
tcp://n[dot]ezjhyxxbf.ru:0	2015-12-03	inactive	410
tcp://n[dot]fwmfdsrdo.com:0	2015-12-03	inactive	410
tcp://n[dot]fxagapbcw.ru:0	2015-12-03	inactive	410
tcp://n[dot]fxazudqiv.ru:0	2015-12-03	inactive	410
tcp://n[dot]gbckjrrzu.ru:0	2015-12-03	inactive	410
tcp://n[dot]gbfelbdjz.ru:0	2015-12-03	inactive	410
tcp://n[dot]ghovcuips.com:0	2015-12-03	inactive	410

SERVER URL	LAST ALIVE	STATUS	COUNT
tcp://n[dot]gurvnrthi.com:0	2015-12-03	inactive	410
tcp://n[dot]gxltnbgks.ru:0	2015-12-03	inactive	410
tcp://n[dot]gznzenuve.ru:0	2015-12-03	inactive	410
tcp://n[dot]hbukvpirg.ru:0	2015-12-03	inactive	410
tcp://n[dot]hceymatul.ru:0	2015-12-03	inactive	410
tcp://n[dot]heiylmruc.ru:0	2015-12-03	inactive	410
tcp://n[dot]hhxxcplyd.com:0	2015-12-03	inactive	410
tcp://n[dot]hmiblgoja.ru:0	2015-10-20	inactive	410
tcp://n[dot]hpufkdrqr.ru:0	2015-12-03	inactive	410
tcp://n[dot]iclcakajd.ru:0	2015-12-03	inactive	410
tcp://n[dot]iegvyabpm.com:0	2015-12-03	inactive	410
tcp://n[dot]igmkzotyp.com:0	2015-12-03	inactive	410
tcp://n[dot]ipdcuzrbj.ru:0	2015-12-03	inactive	410
tcp://n[dot]ipzfjqnzj.com:0	2015-12-03	inactive	410
tcp://n[dot]irhwtkyov.com:0	2015-12-03	inactive	410
tcp://n[dot]ivqxnsonc.com:0	2015-12-03	inactive	410
tcp://n[dot]jcapalebj.com:0	2015-12-03	inactive	410
tcp://n[dot]jcawsrxup.com:0	2015-12-03	inactive	410
tcp://n[dot]jijvoiiqf.com:0	2015-12-03	inactive	410
tcp://n[dot]jntbxduhz.ru:0	2015-11-19	inactive	410
tcp://n[dot]jqltfflhx.ru:0	2015-12-03	inactive	410
tcp://n[dot]jractocvx.ru:0	2015-12-03	inactive	410
tcp://n[dot]jspowmxsl.ru:0	2015-12-03	inactive	410
tcp://n[dot]jthxriotb.ru:0	2015-12-03	inactive	410
tcp://n[dot]jupoofsnc.ru:0	2015-12-03	inactive	410
tcp://n[dot]jveblfxqs.ru:0	2015-12-03	inactive	410
tcp://n[dot]jxgxgdmnh.com:0	2015-12-03	inactive	410
tcp://n[dot]kbsdxnoqc.com:0	2015-12-03	inactive	410
tcp://n[dot]kbwuxntle.ru:0	2015-12-03	inactive	410

SERVER URL	LAST ALIVE	STATUS	COUNT
tcp://n[dot]kdrlowylt.com:0	2015-12-03	inactive	410
tcp://n[dot]keqenlhsc.ru:0	2015-12-03	inactive	410
tcp://n[dot]khqrqoqoe.ru:0	2015-12-03	inactive	410
tcp://n[dot]kntrejzkq.ru:0	2015-12-03	inactive	410
tcp://n[dot]knyszaijv.ru:0	2015-12-03	inactive	410
tcp://n[dot]koiqczjzt.com:0	2015-12-03	inactive	410
tcp://n[dot]kpmcbjlmz.com:0	2015-12-03	inactive	410
tcp://n[dot]kpypmhotd.com:0	2015-12-03	inactive	410
tcp://n[dot]krpjpyuvr.com:0	2015-12-03	inactive	410
tcp://n[dot]kvupdstwh.ru:0	2015-12-03	inactive	410
tcp://n[dot]kyhoimuag.com:0	2015-12-03	inactive	410
tcp://n[dot]lbxfqfcxj.ru:0	2015-12-03	inactive	410
tcp://n[dot]lgcpogvly.ru:0	2015-12-03	inactive	410
tcp://n[dot]lmfbywtms.com:0	2015-12-03	inactive	410
tcp://n[dot]lsisqkwax.com:0	2015-12-03	inactive	410
tcp://n[dot]lujjeazun.ru:0	2015-12-03	inactive	410
tcp://n[dot]lumzwlhum.ru:0	2015-12-03	inactive	410
tcp://n[dot]lurgcdqwk.ru:0	2015-12-03	inactive	410
tcp://n[dot]lwoucvztu.com:0	2015-12-03	inactive	410
tcp://n[dot]lxbluoryz.ru:0	2015-12-03	inactive	410
tcp://n[dot]mmhjrarii.ru:0	2015-12-03	inactive	410
tcp://n[dot]mqjcctzdu.ru:0	2015-12-03	inactive	410
tcp://n[dot]mrjwqrvhe.com:0	2015-12-03	inactive	410
tcp://n[dot]msosxcmuh.com:0	2015-12-03	inactive	410
tcp://n[dot]mvhrrpbab.com:0	2015-12-03	inactive	410
tcp://n[dot]myyhalxbr.com:0	2015-12-03	inactive	410
tcp://n[dot]nfjmrolyt.com:0	2015-12-03	inactive	410
tcp://n[dot]nikejqiis.ru:0	2015-12-03	inactive	410
tcp://n[dot]nmdlqnsqv.com:0	2015-12-03	inactive	410

SERVER URL	LAST ALIVE	STATUS	COUNT
tcp://n[dot]nnzykujty.ru:0	2015-12-03	inactive	410
tcp://n[dot]nothauweh.com:0	2015-12-03	inactive	410
tcp://n[dot]nwsxkwjtb.com:0	2015-12-03	inactive	410
tcp://n[dot]nxnprnedd.com:0	2015-12-03	inactive	410
tcp://n[dot]nxoyntdzt.com:0	2015-12-03	inactive	410
tcp://n[dot]oaclzemyh.ru:0	2015-12-03	inactive	410
tcp://n[dot]obfzdniwo.com:0	2015-12-03	inactive	410
tcp://n[dot]oceardpku.ru:0	2015-12-03	inactive	410
tcp://n[dot]odeujslqf.com:0	2015-12-03	inactive	410
tcp://n[dot]offbizvki.com:0	2015-12-03	inactive	410
tcp://n[dot]onnaznfpi.com:0	2015-12-03	inactive	410
tcp://n[dot]onqxlsjsu.com:0	2015-12-03	inactive	410
tcp://n[dot]orvjwcvqt.ru:0	2015-12-03	inactive	410
tcp://n[dot]owjbbpdam.ru:0	2015-12-03	inactive	410
tcp://n[dot]oysaqcxbi.ru:0	2015-12-03	inactive	410
tcp://n[dot]phbndvdsy.ru:0	2015-12-03	inactive	410
tcp://n[dot]pszpnkbib.com:0	2015-12-03	inactive	410
tcp://n[dot]pubacyixo.com:0	2015-12-03	inactive	410
tcp://n[dot]pucpdbgjm.com:0	2015-12-03	inactive	410
tcp://n[dot]pxktczqpg.com:0	2015-12-03	inactive	410
tcp://n[dot]qktjrlxil.ru:0	2015-12-03	inactive	410
tcp://n[dot]qtcyitbce.com:0	2015-12-03	inactive	410
tcp://n[dot]raqimfebe.ru:0	2015-12-03	inactive	410
tcp://n[dot]rejtobfsz.com:0	2015-12-03	inactive	410
tcp://n[dot]rjywkggko.com:0	2015-12-03	inactive	410
tcp://n[dot]rpbzpxiyg.ru:0	2015-12-03	inactive	410
tcp://n[dot]rqbupminx.ru:0	2015-12-03	inactive	410
tcp://n[dot]rsxnjdvgu.com:0	2015-12-03	inactive	410
tcp://n[dot]rxehjwklo.com:0	2015-12-03	inactive	410

SERVER URL	LAST ALIVE	STATUS	COUNT
tcp://n[dot]rzhfwlaaj.com:0	2015-12-03	inactive	410
tcp://n[dot]rzyyjafvk.ru:0	2015-12-03	inactive	410
tcp://n[dot]saluqauqxz.ru:0	2015-12-03	inactive	410
tcp://n[dot]sbliadsxt.com:0	2015-12-03	inactive	410
tcp://n[dot]sgteglshe.com:0	2015-12-03	inactive	410
tcp://n[dot]sjkguntum.ru:0	2015-12-03	inactive	410
tcp://n[dot]sokjrsoge.ru:0	2015-12-03	inactive	410
tcp://n[dot]spdsazjaj.ru:0	2015-12-03	inactive	410
tcp://n[dot]spgpenwqk.ru:0	2015-12-03	inactive	410
tcp://n[dot]srcbrtetb.ru:0	2015-12-03	inactive	410
tcp://n[dot]srobpranm.ru:0	2015-12-03	inactive	410
tcp://n[dot]srxkwklks.ru:0	2015-12-03	inactive	410
tcp://n[dot]tnylqmwer.com:0	2015-12-03	inactive	410
tcp://n[dot]tsmdeqpxz.ru:0	2015-12-03	inactive	410
tcp://n[dot]uafvkahxq.com:0	2015-12-03	inactive	410
tcp://n[dot]uahauuzyr.com:0	2015-12-03	inactive	410
tcp://n[dot]uczcgpuxv.com:0	2015-12-03	inactive	410
tcp://n[dot]uhwumfxht.ru:0	2015-12-03	inactive	410
tcp://n[dot]ukgorgrom.com:0	2015-12-03	inactive	410
tcp://n[dot]ulffiidks.com:0	2015-12-03	inactive	410
tcp://n[dot]unvsceumt.com:0	2015-12-03	inactive	410
tcp://n[dot]uqeuhlpbo.ru:0	2015-12-03	inactive	410
tcp://n[dot]vbemnggcj.ru:0	2015-12-03	inactive	410
tcp://n[dot]vimaspimf.com:0	2015-12-03	inactive	410
tcp://n[dot]vlwibqnup.com:0	2015-12-03	inactive	410
tcp://n[dot]votjsbqxi.ru:0	2015-12-03	inactive	410
tcp://n[dot]vvspbjbsj.com:0	2015-12-03	inactive	410
tcp://n[dot]wbakrhdqe.ru:0	2015-12-03	inactive	410
tcp://n[dot]wesocfgdj.com:0	2015-12-03	inactive	410

SERVER URL	LAST ALIVE	STATUS	COUNT
tcp://n[dot]wewhftcna.com:0	2015-12-03	inactive	410
tcp://n[dot]whukpjket.ru:0	2015-12-03	inactive	410
tcp://n[dot]wnkgkwbbb.com:0	2015-12-03	inactive	410
tcp://n[dot]wpsnxnegs.com:0	2015-12-03	inactive	410
tcp://n[dot]wxctgbeou.com:0	2015-12-03	inactive	410
tcp://n[dot]wxvwsagfj.ru:0	2015-12-03	inactive	410
tcp://n[dot]xcuygznmk.ru:0	2015-12-03	inactive	410
tcp://n[dot]xiablhaoi.ru:0	2015-12-03	inactive	410
tcp://n[dot]xqbwkgtli.com:0	2015-12-03	inactive	410
tcp://n[dot]xqrnrfjkk.com:0	2015-12-03	inactive	410
tcp://n[dot]xrbqavrjw.com:0	2015-12-03	inactive	410
tcp://n[dot]xyxbbuxhw.ru:0	2015-12-03	inactive	410
tcp://n[dot]yfxmjmbpd.ru:0	2015-12-03	inactive	410
tcp://n[dot]yjeuatihg.ru:0	2015-12-03	inactive	410
tcp://n[dot]ylbotqjmk.com:0	2015-12-03	inactive	410
tcp://n[dot]ynxjwgdec.com:0	2015-12-03	inactive	410
tcp://n[dot]ysmilxqbp.ru:0	2015-12-03	inactive	410
tcp://n[dot]ysrzbwrhy.com:0	2015-12-03	inactive	410
tcp://n[dot]yugypkhvl.ru:0	2015-12-03	inactive	410
tcp://n[dot]yxntnyrap.ru:0	2015-12-03	inactive	410
tcp://n[dot]yykzejasl.com:0	2015-12-03	inactive	410
tcp://n[dot]zccgyxwfa.ru:0	2015-12-03	inactive	410
tcp://n[dot]zdxappufr.ru:0	2015-12-03	inactive	410
tcp://n[dot]zepjdorss.com:0	2015-12-03	inactive	410
tcp://n[dot]zervwpzra.ru:0	2015-12-03	inactive	410
tcp://n[dot]zfluvuuez.com:0	2015-12-03	inactive	410
tcp://n[dot]zgfvfhtli.ru:0	2015-12-03	inactive	410
tcp://n[dot]zhgcuntif.ru:0	2015-12-03	inactive	410
tcp://n[dot]zhjdwkpaz.ru:0	2015-12-03	inactive	410

SERVER URL	LAST ALIVE	STATUS	COUNT
tcp://n[dot]zhlhvgfpj.com:0	2015-12-03	inactive	410
tcp://n[dot]zjadtsvrd.ru:0	2015-12-03	inactive	410
tcp://n[dot]zjfprawyu.com:0	2015-12-03	inactive	410
tcp://n[dot]zmvlqrhsl.com:0	2015-12-03	inactive	410
tcp://n[dot]zodoyucra.com:0	2015-12-03	inactive	410
tcp://n[dot]zqpkvolqc.ru:0	2015-12-03	inactive	410
tcp://n[dot]zzwwnrwum.com:0	2015-12-03	inactive	410
tcp://n[dot]ggxvmjwgy.ru:0	2015-12-03	inactive	409
tcp://n[dot]lhklpacah.com:0	2015-12-03	inactive	409
tcp://n[dot]nzebzahio.com:0	2015-12-03	inactive	409
tcp://n[dot]tekwkrsll.ru:0	2015-12-03	inactive	409
tcp://n[dot]yothepdgz.ru:0	2015-12-03	inactive	409
udp://inbox[dot]fcoklyak.ru:8670	2015-07-29	inactive	297
udp://inbox[dot]keyywcmo.com:8670	2015-07-29	inactive	297
udp://inbox[dot]lyfccggc.ru:8670	2015-07-29	inactive	297
udp://inbox[dot]otlkxlqc.com:8670	2015-07-29	inactive	297
udp://inbox[dot]tinyupdates.ru:8670	2016-09-25	inactive	297
udp://inbox[dot]zbnwaipr.com:8670	2015-07-29	inactive	297
tcp://192[dot]42.116.41:0	2016-10-23	active	249
tcp://192[dot]42.119.41:0	2016-10-23	active	161
tcp://199[dot]2.137.29:0	2016-10-23	active	21
tcp://199[dot]2.137.22:0	2016-10-20	active	11
tcp://103[dot]234.37.4:0	2016-10-23	active	9
tcp://a[dot]aaasr02.com:0	2016-01-13	inactive	7
tcp://a[dot]amasr00.com:0	2015-12-06	inactive	7
tcp://a[dot]bbasr02.com:0	2016-01-13	inactive	7
tcp://a[dot]bmasr00.com:0	2015-12-06	inactive	7
tcp://a[dot]ccasr0002.com:0	2016-01-13	inactive	7
tcp://a[dot]cmasr0000.com:0	2015-12-06	inactive	7

SERVER URL	LAST ALIVE	STATUS	COUNT
tcp://a[dot]najwahaifamelema1.com:0	2015-11-24	inactive	6
tcp://a[dot]najwahaifamelema10.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema100.com:0	2015-12-07	inactive	6
tcp://a[dot]najwahaifamelema11.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema12.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema13.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema14.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema15.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema16.com:0	2015-12-07	inactive	6
tcp://a[dot]najwahaifamelema17.com:0	2015-11-18	inactive	6
tcp://a[dot]najwahaifamelema18.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema19.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema2.com:0	2015-12-07	inactive	6
tcp://a[dot]najwahaifamelema20.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema21.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema22.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema23.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema24.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema25.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema26.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema27.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema28.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema29.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema3.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema30.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema31.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema32.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema33.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema34.com:0	2015-12-03	inactive	6

SERVER URL	LAST ALIVE	STATUS	COUNT
tcp://a[dot]najwahaifamelema35.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema36.com:0	2015-10-20	inactive	6
tcp://a[dot]najwahaifamelema37.com:0	2015-10-20	inactive	6
tcp://a[dot]najwahaifamelema38.com:0	2015-10-20	inactive	6
tcp://a[dot]najwahaifamelema39.com:0	2015-10-20	inactive	6
tcp://a[dot]najwahaifamelema4.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema40.com:0	2015-10-20	inactive	6
tcp://a[dot]najwahaifamelema41.com:0	2015-10-20	inactive	6
tcp://a[dot]najwahaifamelema42.com:0	2015-10-20	inactive	6
tcp://a[dot]najwahaifamelema43.com:0	2015-10-20	inactive	6
tcp://a[dot]najwahaifamelema44.com:0	2015-10-20	inactive	6
tcp://a[dot]najwahaifamelema45.com:0	2015-10-20	inactive	6
tcp://a[dot]najwahaifamelema46.com:0	2015-12-07	inactive	6
tcp://a[dot]najwahaifamelema47.com:0	2015-12-07	inactive	6
tcp://a[dot]najwahaifamelema48.com:0	2015-12-07	inactive	6
tcp://a[dot]najwahaifamelema49.com:0	2015-12-07	inactive	6
tcp://a[dot]najwahaifamelema5.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema50.com:0	2015-10-20	inactive	6
tcp://a[dot]najwahaifamelema51.com:0	2015-10-20	inactive	6
tcp://a[dot]najwahaifamelema52.com:0	2015-10-20	inactive	6
tcp://a[dot]najwahaifamelema53.com:0	2015-12-07	inactive	6
tcp://a[dot]najwahaifamelema54.com:0	2015-12-07	inactive	6
tcp://a[dot]najwahaifamelema55.com:0	2015-12-07	inactive	6
tcp://a[dot]najwahaifamelema56.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema57.com:0	2015-12-07	inactive	6
tcp://a[dot]najwahaifamelema58.com:0	2015-12-07	inactive	6
tcp://a[dot]najwahaifamelema59.com:0	2015-12-07	inactive	6
tcp://a[dot]najwahaifamelema6.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema60.com:0	2015-12-07	inactive	6

SERVER URL	LAST ALIVE	STATUS	COUNT
tcp://a[dot]najwahaifamelema61.com:0	2015-12-07	inactive	6
tcp://a[dot]najwahaifamelema62.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema63.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema64.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema65.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema66.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema67.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema68.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema69.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema7.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema70.com:0	2015-10-20	inactive	6
tcp://a[dot]najwahaifamelema71.com:0	2015-10-20	inactive	6
tcp://a[dot]najwahaifamelema72.com:0	2015-10-20	inactive	6
tcp://a[dot]najwahaifamelema73.com:0	2015-10-20	inactive	6
tcp://a[dot]najwahaifamelema74.com:0	2015-10-20	inactive	6
tcp://a[dot]najwahaifamelema75.com:0	2015-10-20	inactive	6
tcp://a[dot]najwahaifamelema76.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema77.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema78.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema79.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema8.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema80.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema81.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema82.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema83.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema84.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema85.com:0	2015-10-20	inactive	6
tcp://a[dot]najwahaifamelema86.com:0	2015-12-07	inactive	6
tcp://a[dot]najwahaifamelema87.com:0	2015-12-07	inactive	6

SERVER URL	LAST ALIVE	STATUS	COUNT
tcp://a[dot]najwahaifamelema88.com:0	2015-12-07	inactive	6
tcp://a[dot]najwahaifamelema89.com:0	2015-12-07	inactive	6
tcp://a[dot]najwahaifamelema9.com:0	2015-12-07	inactive	6
tcp://a[dot]najwahaifamelema91.com:0	2015-10-26	inactive	6
tcp://a[dot]najwahaifamelema92.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema93.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema94.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema95.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema96.com:0	2015-12-03	inactive	6
tcp://a[dot]najwahaifamelema97.com:0	2015-12-07	inactive	6
tcp://a[dot]najwahaifamelema98.com:0	2015-12-07	inactive	6
tcp://a[dot]najwahaifamelema99.com:0	2015-12-07	inactive	6
tcp://c[dot]ejhvdqw5ladies13.com:0	2015-12-05	inactive	5
tcp://c[dot]ejhvdqw5ladies42.com:0	2016-02-17	inactive	5
tcp://c[dot]ejjjqws5fkxx42.com:0	2016-02-17	inactive	5
tcp://c[dot]najwahaifamelema100.com:0	2015-12-05	inactive	5
tcp://c[dot]najwahaifamelema32.com:0	2015-12-05	inactive	5
tcp://c[dot]najwahaifamelema33.com:0	2015-12-05	inactive	5
tcp://c[dot]najwahaifamelema35.com:0	2015-12-05	inactive	5
tcp://c[dot]najwahaifamelema36.com:0	2015-10-20	inactive	5
tcp://c[dot]najwahaifamelema37.com:0	2015-10-20	inactive	5
tcp://c[dot]najwahaifamelema38.com:0	2015-10-20	inactive	5
tcp://c[dot]najwahaifamelema47.com:0	2015-12-05	inactive	5
tcp://c[dot]najwahaifamelema48.com:0	2015-12-05	inactive	5
tcp://c[dot]najwahaifamelema49.com:0	2015-12-05	inactive	5
tcp://c[dot]najwahaifamelema50.com:0	2015-10-20	inactive	5
tcp://c[dot]najwahaifamelema51.com:0	2015-10-20	inactive	5
tcp://c[dot]najwahaifamelema52.com:0	2015-10-20	inactive	5
tcp://c[dot]najwahaifamelema53.com:0	2015-12-05	inactive	5

SERVER URL	LAST ALIVE	STATUS	COUNT
tcp://c[dot]najwahaifamelema54.com:0	2015-12-05	inactive	5
tcp://c[dot]najwahaifamelema86.com:0	2015-12-05	inactive	5
tcp://c[dot]najwahaifamelema87.com:0	2015-12-05	inactive	5
tcp://c[dot]najwahaifamelema88.com:0	2015-12-05	inactive	5
tcp://c[dot]najwahaifamelema89.com:0	2015-12-05	inactive	5
tcp://c[dot]najwahaifamelema97.com:0	2015-12-05	inactive	5
tcp://c[dot]najwahaifamelema98.com:0	2015-12-05	inactive	5
tcp://c[dot]najwahaifamelema99.com:0	2015-12-05	inactive	5
tcp://c[dot]roonggeyyy4.com:0	2015-12-05	inactive	5
tcp://c[dot]saao20000.com:0	2015-12-05	inactive	5
tcp://c[dot]so1aa00.com:0	2015-12-05	inactive	5
tcp://c[dot]zabrak0vmin0kov1.com:0	2015-12-05	inactive	5
tcp://c[dot]zabrak0vmin0kov10.com:0	2015-12-05	inactive	5
tcp://c[dot]zabrak0vmin0kov11.com:0	2015-12-05	inactive	5
tcp://c[dot]zabrak0vmin0kov12.com:0	2015-12-05	inactive	5
tcp://c[dot]zabrak0vmin0kov14.com:0	2015-12-05	inactive	5
tcp://c[dot]zabrak0vmin0kov15.com:0	2015-12-05	inactive	5
tcp://c[dot]zabrak0vmin0kov2.com:0	2015-12-05	inactive	5
tcp://c[dot]zabrak0vmin0kov3.com:0	2015-12-05	inactive	5
tcp://c[dot]zabrak0vmin0kov4.com:0	2015-12-05	inactive	5
tcp://c[dot]zabrak0vmin0kov5.com:0	2015-12-05	inactive	5
tcp://c[dot]zabrak0vmin0kov6.com:0	2015-10-20	inactive	5
tcp://c[dot]zabrak0vmin0kov7.com:0	2015-12-05	inactive	5
tcp://c[dot]zabrak0vmin0kov8.com:0	2015-12-05	inactive	5
tcp://c[dot]zabrak0vmin0kov9.com:0	2015-12-05	inactive	5
tcp://j[dot]daweeb1.com:0	2015-12-04	inactive	4
tcp://j[dot]daweeb2.com:0	2015-12-04	inactive	4
tcp://j[dot]daweeb3.com:0	2015-12-04	inactive	4
tcp://j[dot]daweeb4.com:0	2015-12-04	inactive	4

BOTNET ACTIVITY REPORT

SERVER URL	LAST ALIVE	STATUS	COUNT
tcp://a[dot]acaraka1lagroup42.com:0	2015-12-04	inactive	3
tcp://a[dot]adoyou1understandme42.com:0	2015-12-04	inactive	3
tcp://a[dot]aire1bobohayawen42.com:0	2015-12-04	inactive	3
tcp://a[dot]ajhvdqw1ladies42.com:0	2015-12-04	inactive	3
tcp://a[dot]ajjjqws1fkxx42.com:0	2016-07-24	inactive	3
tcp://a[dot]amous1epadsafa42.com:0	2015-12-04	inactive	3
tcp://a[dot]anabok1hasn1aser42.com:0	2015-12-04	inactive	3
tcp://a[dot]athemall1gonowhaha42.com:0	2015-12-04	inactive	3
tcp://a[dot]bcaraka2lagroup42.com:0	2015-12-04	inactive	3
tcp://a[dot]bdoyou2understandme42.com:0	2015-12-04	inactive	3
tcp://a[dot]biphon2egalaxyblack42.com:0	2015-10-20	inactive	3
tcp://a[dot]bire2bobohayawen42.com:0	2015-12-04	inactive	3
tcp://a[dot]bjhvdqw2ladies42.com:0	2015-12-04	inactive	3
tcp://a[dot]bjjjqws2fkxx42.com:0	2015-12-04	inactive	3
tcp://a[dot]bmous2epadsafa42.com:0	2015-11-25	inactive	3
tcp://a[dot]bnabok2hasn1aser42.com:0	2015-12-04	inactive	3
tcp://a[dot]bthemall2gonowhaha42.com:0	2015-12-04	inactive	3
tcp://a[dot]cdoyou3understandme42.com:0	2016-02-16	inactive	3
tcp://a[dot]ciphon3egalaxyblack42.com:0	2016-02-16	inactive	3
tcp://a[dot]cjhvdqw3ladies42.com:0	2016-02-16	inactive	3
tcp://a[dot]cjjjqws3fkxx42.com:0	2016-02-16	inactive	3
tcp://a[dot]cmous3epadsafa42.com:0	2015-12-04	inactive	3
tcp://a[dot]cnabok3hasn1aser42.com:0	2016-02-16	inactive	3
tcp://a[dot]cthemall3gonowhaha42.com:0	2015-12-02	inactive	3
tcp://a[dot]ddoyou4understandme42.com:0	2015-10-20	inactive	3
tcp://a[dot]diphon4egalaxyblack42.com:0	2016-02-16	inactive	3
tcp://a[dot]dire4bobohayawen42.com:0	2015-12-04	inactive	3
tcp://a[dot]djhvdqw4ladies42.com:0	2016-02-16	inactive	3
tcp://a[dot]djjjqws4fkxx42.com:0	2016-02-16	inactive	3

SERVER URL	LAST ALIVE	STATUS	COUNT
tcp://a[dot]dmous4epadsafa42.com:0	2015-12-04	inactive	3
tcp://a[dot]dnabok4hasn1aser42.com:0	2016-02-16	inactive	3
tcp://a[dot]dthemall4gonowhaha42.com:0	2015-12-02	inactive	3
tcp://a[dot]edoyou5understandme42.com:0	2015-10-20	inactive	3
tcp://a[dot]eiphon5egalaxyblack42.com:0	2016-02-16	inactive	3
tcp://a[dot]ejhvdqw5ladies42.com:0	2016-02-16	inactive	3
tcp://a[dot]ejjjqws5fkxx42.com:0	2016-02-16	inactive	3
tcp://a[dot]emous5epadsafa42.com:0	2015-12-04	inactive	3
tcp://a[dot]enabok5hasn1aser42.com:0	2016-02-16	inactive	3
tcp://a[dot]roooggeyyy2.com:0	2015-12-04	inactive	3
tcp://a[dot]roooggeyyy3.com:0	2015-12-04	inactive	3
tcp://a[dot]roooggeyyy4.com:0	2015-12-04	inactive	3
tcp://a[dot]saao20000.com:0	2015-12-05	inactive	3
tcp://a[dot]so1aa00.com:0	2015-12-04	inactive	3

Targets in configurations

TARGET	STATUS	COUNT
login[dot]live./*	new	6
no-ip/login*i	new	5
[dot]moneybookers./*login.pl	known	3339
:2083/login	known	3339
:2086/login	known	3339
aol[dot]/*login.psp*	known	3339
bigstring[dot]/*index.php*	known	3339
dyndns/account*	known	3339
facebook[dot]/login.php*	known	3339
fastmail[dot]/mail/*	known	3339
gmx[dot]/*FormLogin*	known	3339

TARGET	STATUS	COUNT
google[dot]/*ServiceLoginAuth*	known	3339
login[dot]yahoo./*login*	known	3339
*officebanking[dot]cl/*login.asp*	known	3339
screenname[dot]aol./login.psp*	known	3339
*twitter[dot]com/sessions	known	3339
steampowered/login*	known	3338
runescape/*weblogin*	known	3337
secure[dot]logmein./*logincheck*	known	3336
no-ip/login*	known	3334
login[dot]live./*post.srf*	known	3333
hackforums[dot]/member.php	known	3330
paypal[dot]/webscr?cmd=_login-submit*	known	3327
1and1[dot]com/xml/config	known	3317
4shared[dot]com/login	known	3317
:2082/login	known	3317
:2222/CMD_LOGIN	known	3317
*dotster[dot]com/*login*	known	3317
enom[dot]com/login	known	3317
fileserv[dot]com/login	known	3317
*filesonic[dot]com/*login*	known	3317
freakshare[dot]com/login	known	3317
godaddy[dot]com/login	known	3317
hotfile[dot]com/login	known	3317
letitbit[dot]net	known	3317
*mediafire[dot]com/*login*	known	3317
megaupload[dot]/*login*	known	3317
members[dot]iknowthatgirl*/members*	known	3317
members[dot]brazzers.com	known	3317
*moniker[dot]com/*Login*	known	3317

TARGET	STATUS	COUNT
*namecheap[dot]com/*login*	known	3317
*netflix[dot]com/*ogin*	known	3317
netload[dot]in/index	known	3317
sendspace[dot]com/login	known	3317
*signin[dot]ebay*SignIn	known	3317
sms4file[dot]com//signin-do*	known	3317
speedyshare[dot]com/login	known	3317
thepiratebay[dot]org/login	known	3317
*uploaded[dot]to/*login*	known	3317
*uploading[dot]com/*login*	known	3317
vip-file[dot]com//signin-do*	known	3317
*webnames[dot]ru/*user_login*	known	3317
what[dot]cd/login	known	3317
*whcms*dologin*	known	3317
youporn[dot]/login*	known	3317
alertpay[dot]com/login	known	3316
depositfiles[dot]/*/login*	known	3316
oron[dot]com/login	known	3312
*bcointernacional*login*	known	3308
*torrentleech[dot]org/*login*	known	3307
[dot]alertpay./*login.aspx	known	22
fileserve[dot]/login*	known	22
megaupload[dot]/*login	known	22
paypal[dot]/webscr?cmd=_logi	known	12
*	known	10
*hack	known	9
*,	known	3
*a	known	1

Botnet-specific report: Elenoocka Week 42/2016

Samples

VARIANT	COUNT
Win32_TrojanDownloader_Elenoocka_A_trojan	5

Botnet-specific report: Papras Week 42/2016

Samples

VARIANT	COUNT
Win32_PSW_Papras_CX_trojan	617
Win32_PSW_Papras_DR_trojan	477
Win32_PSW_Papras_EC_trojan	278
Win32_PSW_Papras_EH_trojan	87
Win32_PSW_Papras_EJ_trojan	24
Win32_PSW_Papras_DT_trojan	13
Win32_PSW_Papras_DU_trojan	4

Command & Control servers

SERVER URL	LAST ALIVE	STATUS	COUNT
http://containinges[dot]bid	2016-10-20	new	2
http://embarrassmentyy[dot]bid	2016-10-20	new	2
http://195[dot]130.192.106/viewforum.php	2015-03-18	inactive	322
http://195[dot]130.192.110/viewforum.php	2015-03-18	inactive	322
http://146[dot]185.233.38/viewforum.php	2015-03-18	inactive	230
http://146[dot]185.233.80/viewforum.php	2015-03-18	inactive	230
http://46[dot]38.51.216/viewforum.php	2015-03-18	inactive	213
http://80[dot]243.184.239/viewforum.php	2015-03-18	inactive	213
http://195[dot]130.192.65/work/1.php	2015-03-18	inactive	183
http://195[dot]130.192.91/work/1.php	2015-03-18	inactive	183
http://kopirabus[dot]com/work/1.php	2015-03-18	inactive	183
http://manulizza[dot]com/work/1.php	2015-03-18	inactive	183
http://mitlerbis[dot]com/work/1.php	2015-03-18	inactive	183
http://macoroxaz[dot]com/work/1.php	2015-03-18	inactive	162
http://lofiiik[dot]su/app/manager/	2015-03-18	inactive	157
http://maxuber[dot]su/app/manager/	2015-03-18	inactive	157

SERVER URL	LAST ALIVE	STATUS	COUNT
http://185[dot]13.32.67/viewforum.php	2015-03-18	inactive	155
http://185[dot]13.32.80/viewforum.php	2015-03-18	inactive	155
http://146[dot]185.233.91/viewforum.php	2015-03-18	inactive	138
http://146[dot]185.233.97/viewforum.php	2015-03-18	inactive	138
http://furenga[dot]com/forum/post.php?topic=	2015-03-18	inactive	117
http://monitbent[dot]su/forum/post.php?topic=	2015-03-18	inactive	117
http://monitkey[dot]com/forum/post.php?topic=	2015-03-18	inactive	117
http://monitoring-web[dot]su/forum/post.php?topic=	2015-03-18	inactive	117
http://nunpeko[dot]com/forum/post.php?topic=	2015-03-18	inactive	117
http://78[dot]153.149.219/work/1.php	2015-03-18	inactive	111
http://efuelia[dot]com/work/1.php	2015-03-18	inactive	111
http://analytica-uk[dot]su/app/manager/	2015-03-18	inactive	93
http://brightlounge[dot]su/stores/servlet/OrderItemDisplay?storeId=	2015-05-13	inactive	93
http://egor555[dot]su/app/manager/	2015-03-18	inactive	93
http://jabberstorm[dot]su/stores/servlet/OrderItemDisplay?storeId=	2015-06-17	inactive	93
http://photohubchart[dot]com/stores/servlet/OrderItemDisplay?storeId=	2015-07-08	inactive	93
http://pongola[dot]su/app/manager/	2015-03-18	inactive	93
http://thoughtdog[dot]net/stores/servlet/OrderItemDisplay?storeId=	2015-06-09	inactive	93
http://altlane[dot]com/stores/servlet/OrderItemDisplay?storeId=	2015-07-14	inactive	91
http://cbcomm[dot]ru/stores/servlet/OrderItemDisplay?storeId=	2015-07-14	inactive	91
http://devomchart[dot]com/stores/servlet/OrderItemDisplay?storeId=	2015-06-17	inactive	91
http://natext[dot]ru/stores/servlet/OrderItemDisplay?storeId=	2015-07-14	inactive	91
http://signtower[dot]com/stores/servlet/OrderItemDisplay?storeId=	2015-07-13	inactive	91
http://woodlab[dot]su/stores/servlet/OrderItemDisplay?storeId=	2015-07-13	inactive	91
http://yourstart[dot]su/stores/servlet/OrderItemDisplay?storeId=	2015-07-13	inactive	91
http://188[dot]190.126.93/forumdisplay.php	2015-03-18	inactive	89
http://lastiks[dot]su/app/manager/	2015-03-18	inactive	64
http://solokip[dot]su/app/manager/	2015-03-18	inactive	64

SERVER URL	LAST ALIVE	STATUS	COUNT
http://146[dot]185.233.38/forumdisplay.php	2015-03-18	inactive	59
http://146[dot]185.233.80/forumdisplay.php	2015-03-18	inactive	59
http://46[dot]38.48.92/work/1.php	2015-03-18	inactive	51
http://kiodlers[dot]com/work/1.php	2015-03-18	inactive	51
http://pilkodran[dot]com/work/1.php	2015-03-18	inactive	51
http://pudloxan[dot]com/work/1.php	2015-03-18	inactive	51
http://botias[dot]ru/stores/servlet/OrderItemDisplay?storeId=	2015-07-08	inactive	41
http://counsel[dot]su/stores/servlet/OrderItemDisplay?storeId=	2015-07-08	inactive	41
http://deserver[dot]ru/stores/servlet/OrderItemDisplay?storeId=	2015-07-08	inactive	41
http://ecologyint[dot]com/stores/servlet/OrderItemDisplay?storeId=	2015-07-08	inactive	41
http://owmarket[dot]com/stores/servlet/OrderItemDisplay?storeId=	2015-07-08	inactive	41
http://wittersphere[dot]net/stores/servlet/OrderItemDisplay?storeId=	2015-07-08	inactive	41
http://muzalabels[dot]com/mer/res/	2015-05-13	inactive	37
http://folxnis[dot]com/app/manager/	2015-03-24	inactive	36
http://jordaninogre[dot]net/app/manager/	2016-02-06	inactive	36
http://lebrotreiding[dot]com/app/manager/	2015-03-24	inactive	36
http://monitoring-info[dot]su/app/manager/	2015-03-24	inactive	36
http://starhiler[dot]su/app/manager/	2015-03-24	inactive	36
http://185[dot]13.32.67/forumdisplay.php	2015-03-18	inactive	31
http://185[dot]13.32.80/forumdisplay.php	2015-03-18	inactive	31
http://bennimag[dot]com/forumdisplay.php	2015-03-18	inactive	28
http://humpold[dot]com/forumdisplay.php	2015-03-18	inactive	28
http://maxigolon[dot]com/forumdisplay.php	2015-03-18	inactive	28
http://mondiaz[dot]com/forumdisplay.php	2015-03-18	inactive	28
http://sandoxon[dot]com/forumdisplay.php	2015-03-18	inactive	28
http://terekilpane[dot]com/forumdisplay.php	2015-03-18	inactive	28
http://blubadar[dot]com/param/	2015-03-18	inactive	27
http://dinklip[dot]com/param/	2015-03-18	inactive	27
http://dukeregi[dot]com/param/	2015-03-18	inactive	27

SERVER URL	LAST ALIVE	STATUS	COUNT
http://kidrion[dot]pw/param/	2015-03-18	inactive	27
http://lorseda[dot]com/param/	2015-03-18	inactive	27
http://perdonik[dot]com/param/	2015-03-18	inactive	27
http://pinello[dot]net/param/	2015-03-18	inactive	27
http://sellida[dot]com/param/	2015-03-18	inactive	27
http://92[dot]63.99.122/work/1.php	2015-03-18	inactive	21
http://balookung[dot]com/work/1.php	2015-03-18	inactive	21
http://bunerix[dot]com/work/1.php	2015-03-18	inactive	21
http://celloverse[dot]su/mer/res/	2015-05-13	inactive	21
http://epromax[dot]su/mer/res/	2015-05-13	inactive	21
http://eximbpc[dot]su/mer/res/	2015-05-13	inactive	21
http://headberry[dot]com/mer/res/	2015-05-13	inactive	21
http://nextfork[dot]com/mer/res/	2015-05-13	inactive	21
http://numkisad[dot]com/work/1.php	2015-03-18	inactive	21
http://overtura[dot]su/mer/res/	2015-05-13	inactive	21
http://ploxinmat[dot]com/work/1.php	2015-03-18	inactive	21
http://pludran[dot]com/work/1.php	2015-03-18	inactive	21
http://vimrealty[dot]com/stores/servlet/OrderItemDisplay?storeId=	2015-10-21	inactive	21
http://cleargym[dot]com/stores/servlet/OrderItemDisplay?storeId=	2015-10-21	inactive	16
http://expressread[dot]com/stores/servlet/OrderItemDisplay?storeId=	2015-10-21	inactive	16
http://loftsrent[dot]com/mer/res/	2015-05-13	inactive	16
http://newart[dot]su/stores/servlet/OrderItemDisplay?storeId=	2015-10-21	inactive	16
http://pixarsal[dot]com/mer/res/	2015-05-13	inactive	16
http://pollbox[dot]net/mer/res/	2015-05-13	inactive	16
http://senseboat[dot]com/mer/res/	2015-05-13	inactive	16
http://tolonit[dot]su/mer/res/	2015-05-13	inactive	16
http://broodcom[dot]net/collection/	2015-05-29	inactive	13
http://foliumslip[dot]net/collection/	2015-09-11	inactive	13
http://Tovakan[dot]com/mer/res/	2015-05-19	inactive	12

SERVER URL	LAST ALIVE	STATUS	COUNT
http://givepname[dot]net/mer/res/	2015-05-19	inactive	12
http://nyenamo[dot]com/mer/res/	2015-05-19	inactive	12
http://paypname[dot]com/mer/res/	2015-05-19	inactive	12
http://monitbay[dot]ru/spreadsheets/	2015-05-19	inactive	8
http://monitfunct[dot]su/spreadsheets/	2015-05-21	inactive	8
http://monitfyv[dot]ru/spreadsheets/	2015-05-21	inactive	8
http://monitjack[dot]com/spreadsheets/	2015-05-21	inactive	8
http://monitlate[dot]su/spreadsheets/	2015-05-19	inactive	8
http://monitmass[dot]su/spreadsheets/	2015-05-19	inactive	8
http://monitover[dot]ru/spreadsheets/	2015-05-19	inactive	8
http://monitsus[dot]su/spreadsheets/	2015-05-21	inactive	8
http://monitzany[dot]su/spreadsheets/	2015-05-19	inactive	8
http://monitztx[dot]ru/spreadsheets/	2015-05-21	inactive	8
http://hisdivine[dot]com/collection/	2015-09-04	inactive	7
http://incubatenet[dot]com/collection/	2015-05-29	inactive	7
http://orielnet[dot]com/collection/	2015-09-03	inactive	7
http://streakpic[dot]com/collection/	2015-09-03	inactive	7
http://transfercom[dot]net/collection/	2015-09-05	inactive	7
http://Bygromo[dot]com/mer/res/	2015-05-19	inactive	6
http://Freedomsu[dot]su/mer/res/	2015-05-19	inactive	6
http://culear[dot]net/collection/	2015-09-19	inactive	6
http://fafiekee[dot]net/collection/	2015-10-01	inactive	6
http://fourapp[dot]com/forumdisplay.php	2015-03-18	inactive	6
http://ganeeneex[dot]net/collection/	2015-09-28	inactive	6
http://geelov[dot]com/collection/	2015-09-19	inactive	6
http://ideals[dot]su/forumdisplay.php	2015-03-18	inactive	6
http://koonodea[dot]net/collection/	2015-10-03	inactive	6
http://kuvefiecud[dot]net/collection/	2015-09-18	inactive	6
http://liemeihibo[dot]net/collection/	2015-09-13	inactive	6

SERVER URL	LAST ALIVE	STATUS	COUNT
http://lofege[dot]net/collection/	2015-09-11	inactive	6
http://onlinemix[dot]net/forumdisplay.php	2015-03-18	inactive	6
http://osochas[dot]com/mer/res/	2015-05-19	inactive	6
http://quickregme[dot]su/mer/res/	2015-05-19	inactive	6
http://waiter[dot]su/forumdisplay.php	2015-03-18	inactive	6
http://coobeab[dot]com/company/	2015-11-23	inactive	5
http://fituhr[dot]com/company/	2015-11-21	inactive	5
http://goovaponar[dot]su/company/	2015-11-18	inactive	5
http://keasooseeg[dot]net/company/	2015-10-26	inactive	5
http://neevepa[dot]com/company/	2015-11-20	inactive	5
http://ordure[dot]net/company/	2015-10-26	inactive	5
http://pidoolei[dot]com/company/	2015-10-26	inactive	5
http://seekeifoof[dot]com/company/	2015-08-26	inactive	5
http://seekeifoof[dot]net/company/	2015-10-26	inactive	5
http://spiritgroup[dot]ru/stores/servlet/OrderItemDisplay?storeId=	2015-07-16	inactive	5
http://veafikan[dot]com/company/	2015-10-26	inactive	5
http://xihuz[dot]net/company/	2015-10-26	inactive	5
http://zifato[dot]com/company/	2015-10-26	inactive	5
http://auramontofont[dot]com/forumdisplay.php	2015-03-18	inactive	2
http://auromontofont[dot]com/forumdisplay.php	2015-03-18	inactive	2
http://cmedia[dot]cloud	2016-06-20	inactive	2
http://degvabelando[dot]com/forumdisplay.php	2015-03-18	inactive	2
http://handelbarg[dot]com/forumdisplay.php	2015-03-18	inactive	2
http://hramano[dot]com/forumdisplay.php	2015-03-18	inactive	2
http://nereenx[dot]com/forumdisplay.php	2015-03-18	inactive	2
http://paleenkos[dot]com/forumdisplay.php	2015-03-18	inactive	2
http://plus[dot]google.com	2016-01-12	inactive	2
http://wellentarel[dot]com/forumdisplay.php	2015-03-18	inactive	2
http://ceikeee[dot]su/company/	2015-08-21	inactive	1

SERVER URL	LAST ALIVE	STATUS	COUNT
http://ciwuzired[dot]su/company/	2015-06-16	inactive	1
http://geemeaz[dot]su/company/	2015-06-16	inactive	1
http://heehak[dot]su/company/	2015-08-21	inactive	1
http://hundred[dot]su/company/	2015-06-16	inactive	1
http://leadac[dot]su/company/	2015-06-16	inactive	1
http://sovoo[dot]su/company/	2015-06-16	inactive	1

Botnet-specific report: Retefe Week 42/2016

Samples

VARIANT	COUNT
JS_Retefe_C%ScriptAlg_trojan	110
JS_Retefe_A%ScriptAlg_trojan	1

Command & Control servers

SERVER URL	LAST ALIVE	STATUS	COUNT
http://oymvkvxxzblk6suf[dot]onion/	2016-10-20	new	7
tcp://oymvkvxxzblk6suf[dot]onion:88	2016-10-20	new	7
udp://oymvkvxxzblk6suf[dot]onion:88	2016-10-20	new	7
http://p7lvwva45jx5zsw3[dot]onion/	2016-10-20	new	6
http://2ia23deqi44wrull[dot]onion/	2016-10-20	new	5
http://xswdriwlpe7wmpwy[dot]onion/	2016-10-20	new	5
tcp://2ia23deqi44wrull[dot]onion:88	2016-10-20	new	5
tcp://p7lvwva45jx5zsw3[dot]onion:88	2016-10-20	new	5
tcp://xswdriwlpe7wmpwy[dot]onion:88	2016-10-20	new	5
udp://2ia23deqi44wrull[dot]onion:88	2016-10-20	new	5
udp://p7lvwva45jx5zsw3[dot]onion:88	2016-10-20	new	5
udp://xswdriwlpe7wmpwy[dot]onion:88	2016-10-20	new	5
http://cxwfgckwjwlen54k[dot]onion/	2016-10-21	new	1
https://kexif6cl7uarcl44[dot]onion.to/	2016-10-20	new	1
tcp://cxwfgckwjwlen54k[dot]onion:88	2016-10-21	new	1
udp://cxwfgckwjwlen54k[dot]onion:88	2016-10-21	new	1
http://api[dot]ipify.org/	2016-10-12	inactive	111
http://ug6nw7vl6csbuqzs[dot]onion/	2016-10-23	active	27
http://3ne2scma55oczag6[dot]onion/	2016-10-23	active	25
tcp://3ne2scma55oczag6[dot]onion:88	2016-10-23	active	25
tcp://ug6nw7vl6csbuqzs[dot]onion:88	2016-10-23	active	25

SERVER URL	LAST ALIVE	STATUS	COUNT
udp://3ne2scma55oczag6[dot]onion:88	2016-10-23	active	25
udp://ug6nw7vl6csbuqzs[dot]onion:88	2016-10-23	active	25
http://6kux6tnxjptryfg7[dot]onion/	2016-10-24	active	19
tcp://6kux6tnxjptryfg7[dot]onion:88	2016-10-24	active	16
udp://6kux6tnxjptryfg7[dot]onion:88	2016-10-24	active	16
http://vl46saaxvfsosg3y[dot]onion/	2016-10-22	active	15
tcp://vl46saaxvfsosg3y[dot]onion:88	2016-10-22	active	12
udp://vl46saaxvfsosg3y[dot]onion:88	2016-10-22	active	12

Targets in configurations

	TARGET	STATUS	COUNT
ℹ	*bankthalwil[dot]ch	new	83
ℹ	*piguetgalland[dot]ch	new	51
ℹ	ch[dot]chchb.chon	new	51
ℹ	*triba[dot]ch	new	24
ℹ	hosts[dot]length	new	1
ℹ	nking[dot]at	new	1
	*[dot]bankaustria.at	known	110
	*[dot]bawag.com	known	110
	*[dot]bawagpsk.com	known	110
	*[dot]bekb.ch	known	110
	*[dot]bkb.ch	known	110
	*[dot]clientis.ch	known	110
	*[dot]credit-suisse.com	known	110
	*[dot]easybank.at	known	110
	*[dot]eek.ch	known	110
	*[dot]lukb.ch	known	110
	*[dot]onba.ch	known	110

TARGET	STATUS	COUNT
*[dot]raiffeisen.at	known	110
*[dot]raiffeisen.ch	known	110
*[dot]static-ubs.com	known	110
*[dot]ubs.com	known	110
*[dot]ukb.ch	known	110
*[dot]urkb.ch	known	110
*[dot]zkb.ch	known	110
*abs[dot]ch	known	110
*baloise[dot]ch	known	110
*bcf[dot]ch	known	110
*bcj[dot]ch	known	110
*bcn[dot]ch	known	110
*bcv[dot]ch	known	110
*bcvs[dot]ch	known	110
*blkb[dot]ch	known	110
*cash[dot]ch	known	110
*glkb[dot]ch	known	110
*juliusbaer[dot]com	known	110
*nkb[dot]ch	known	110
*oberbank[dot]at	known	110
*owkb[dot]ch	known	110
*shkb[dot]ch	known	110
*szkb[dot]ch	known	110
*valiant[dot]ch	known	110
*wir[dot]ch	known	110
*zuercherlandbank[dot]ch	known	110
clientis[dot]ch	known	110
cs[dot]directnet.com	known	110
e-banking[dot]gkb.ch	known	110

TARGET	STATUS	COUNT
eb[dot]akb.ch	known	110
ebanking[dot]raiffeisen.ch	known	110
netbanking[dot]bcge.ch	known	110
tb[dot]raiffeisendirect.ch	known	110
urkb[dot]ch	known	110
www[dot]banking.co.at	known	110
www[dot]oberbank-banking.at	known	110
wwwsec[dot]ebanking.zugerkb.ch	known	110
*[dot]onion	known	109
*cic[dot]ch	known	109
*postfinance[dot]ch	known	109
*[dot]postfinance.ch	known	96
*[dot]cic.ch	known	94
nk[dot]chchb.chon	known	45
nking[dot]atonion	known	5

Botnet-specific report: SpyBanker Week 42/2016

Samples

VARIANT	COUNT
Win32_Spy_Banker_ACJB_trojan	376
Win32_Spy_Banker_ACZW~mem_trojan	55
Win32_Spy_Banker_ADHE_trojan	24
Win32_Spy_Banker_ACZN_trojan	17
Win32_Spy_Banker_ADFK_trojan	11
Win32_Spy_Banker_ADHX_trojan	10
Win32_Spy_Banker_ADHI_trojan	8
Win32_Spy_Banker_ADDB_trojan	6
Win32_Spy_Banker_ULM_trojan	6
Win32_Spy_Banker_AAPB_gen_trojan	5
Win32_Spy_Banker_ADBJ_trojan	4
Win32_Spy_Banker_ACZP_trojan	4
Win32_Spy_Banker_ADBR_trojan	4
Win32_Spy_Banker_VER_trojan	3
Win32_Spy_Banker_ADIB_trojan	3
Win32_Spy_Banker_ADIK_trojan	3
Win32_Spy_Banker_ACYT_trojan	3
Win32_Spy_Banker_AABY_trojan	3
Win32_Spy_Banker_ACZD_trojan	3
Win32_Spy_Banker_AAGD_trojan	3
Win32_Spy_Banker_ADHS_trojan	2
Win32_Spy_Banker_ADDD_trojan	2
Win32_Spy_Banker_AALI_trojan	2
Win32_Spy_Banker_ACZC_trojan	2
Win32_Spy_Banker_ABCU_trojan	2
Win32_Spy_Banker_AAHF_trojan	2
Win32_Spy_Banker_AAHA_trojan	2

VARIANT	COUNT
Win32_Spy_Banker_ADIH_trojan	2
Win32_Spy_Banker_ADIC_trojan	2
Win32_Spy_Banker_ADIR_trojan	2
Win32_Spy_Banker_ACWJ_trojan	2
Win32_Spy_Banker_ACRW_trojan	2
Win32_Spy_Banker_ABWN_trojan	2
Win32_Spy_Banker_ADHW_trojan	1
Win32_Spy_Banker_AABW_trojan	1
Win32_Spy_Banker_ADAM_trojan	1
Win32_Spy_Banker_ACMP_trojan	1
Win32_Spy_Banker_QEP_trojan	1
Win32_Spy_Banker_AANA_trojan	1
Win32_Spy_Banker_WUH_trojan	1
Win32_Spy_Banker_ADGT_trojan	1
Win32_Spy_Banker_ACWL_trojan	1
Win32_Spy_Banker_ACYS_trojan	1
Win32_Spy_Banker_AAPM_trojan	1
Win32_Spy_Banker_ACWN_trojan	1
Win32_Spy_Banker_AADK_trojan	1
Win32_Spy_Banker_VQI_trojan	1
Win32_Spy_Banker_ADCL_trojan	1
Win32_Spy_Banker_AAIT_trojan	1
Win32_Spy_Banker_AAWO_trojan	1
Win32_Spy_Banker_ADHP_trojan	1
Win32_Spy_Banker_ADFO_trojan	1
Win32_Spy_Banker_ACJM_trojan	1
Win32_Spy_Banker_ABGD_trojan	1
Win32_Spy_Banker_ACYZ_trojan	1
Win32_Spy_Banker_ACUR_trojan	1

VARIANT	COUNT
Win32_Spy_Banker_SMU_trojan	1
Win32_Spy_Banker_ZYS_trojan	1
Win32_Spy_Banker_ACAP_trojan	1
Win32_Spy_Banker_ABKT_trojan	1
Win32_Spy_Banker_ZDO_trojan	1
Win32_Spy_Banker_ZIE_trojan	1
Win32_Spy_Banker_AAXD_trojan	1

Command & Control servers

SERVER URL	LAST ALIVE	STATUS	COUNT
http://football[dot]championat.biz/info/menu.php	2016-10-23	active	167
http://google997[dot]com/info/menu.php	2016-08-18	inactive	78
http://microsoft775[dot]com/info/menu.php	2016-08-18	inactive	78
http://icq[dot]chatovod.info/info/menu.php	2016-10-23	active	74
http://ndfl[dot]pravcons.biz/info/menu.php	2016-10-21	active	38
http://rss[dot]sport-express.biz/info/menu.php	2016-10-23	active	36
http://forum[dot]zaycev.biz/info/menu.php	2016-10-22	active	26
http://buh[dot]klerk.us/law/main.php	2016-10-18	active	15
http://glavbukh[dot]biz/service/menu.php	2015-11-30	inactive	8
http://topic[dot]buhgalter-info.com/support/menu.php	2016-03-24	inactive	8
http://buhnews[dot]com/info/menu.php	2016-10-10	inactive	4

Targets in configurations

TARGET	STATUS	COUNT
accounts[dot]google.com	known	3
acesso[dot]uol.com.br/login	known	3
email[dot]uol.com.br	known	3
http://email[dot]uol.com.br/	known	3

TARGET	STATUS	COUNT
http://gmail[dot]com	known	3
http://mail[dot]terra.com.br	known	3
http://outlook[dot]com	known	3
http://www[dot]bb.com.br	known	3
http://www[dot]cef.com.br	known	3
http://www[dot]itau.com.br	known	3
http://www[dot]santanderempresarial.com.br	known	3
http://www[dot]tam.com.br	known	3
http://www[dot]voegol.com.br	known	3
login[dot]live.com	known	3
mail[dot]terra.com	known	3
webmail[dot]terraempresas.com	known	3
www[dot]uol.com.br	known	3

Botnet-specific report: Tinba Week 42/2016

Samples

VARIANT	COUNT
Win32_Tinba_BT_trojan	32
Win32_Tinba_AX_trojan	21

Command & Control servers

	SERVER URL	LAST ALIVE	STATUS	COUNT
ⓘ	http://ljyuwhybrqrk[dot]biz:80/	2016-10-21	new	3
ⓘ	http://ljyuwhybrqrk[dot]co.in:80/	2016-10-21	new	3
ⓘ	http://ljyuwhybrqrk[dot]me.uk:80/	2016-10-21	new	3
ⓘ	http://ljyuwhybrqrk[dot]me:80/	2016-10-21	new	3
ⓘ	http://pjvkdltedclw[dot]biz:80/	2016-10-21	new	3
ⓘ	http://pjvkdltedclw[dot]co.in:80/	2016-10-21	new	3
ⓘ	http://pjvkdltedclw[dot]me.uk:80/	2016-10-21	new	3
ⓘ	http://pjvkdltedclw[dot]me:80/	2016-10-21	new	3
	http://itanews[dot]pw:80/	2016-09-28	inactive	12
	http://fairystale[dot]ru/uo/	2015-06-30	inactive	9
	http://bkdivhoplvdv[dot]biz:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
	http://bkdivhoplvdv[dot]co.in:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
	http://bkdivhoplvdv[dot]me.uk:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
	http://bkdivhoplvdv[dot]me:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
	http://bmcluywwvyyw[dot]biz:80/	2016-10-03	inactive	8
	http://bmcluywwvyyw[dot]co.in:80/	2016-10-03	inactive	8
	http://bmcluywwvyyw[dot]me.uk:80/	2016-10-03	inactive	8
	http://bmcluywwvyyw[dot]me:80/	2016-10-03	inactive	8
	http://gcdvvuudggvj[dot]biz:80/	2016-10-03	inactive	8
	http://gcdvvuudggvj[dot]co.in:80/	2016-10-03	inactive	8
	http://gcdvvuudggvj[dot]me.uk:80/	2016-10-03	inactive	8

SERVER URL	LAST ALIVE	STATUS	COUNT
http://gcdwuudggvj[dot]me:80/	2016-10-03	inactive	8
http://iosbqigxhsjm[dot]biz:80/	2016-10-03	inactive	8
http://iosbqigxhsjm[dot]co.in:80/	2016-10-03	inactive	8
http://iosbqigxhsjm[dot]me.uk:80/	2016-10-03	inactive	8
http://iosbqigxhsjm[dot]me:80/	2016-10-03	inactive	8
http://kocjupilkwgf[dot]biz:80/	2016-10-03	inactive	8
http://kocjupilkwgf[dot]co.in:80/	2016-10-03	inactive	8
http://kocjupilkwgf[dot]me.uk:80/	2016-10-03	inactive	8
http://kocjupilkwgf[dot]me:80/	2016-10-03	inactive	8
http://ljyuwhybrqrs[dot]biz:80/	2016-10-03	inactive	8
http://ljyuwhybrqrs[dot]co.in:80/	2016-10-03	inactive	8
http://ljyuwhybrqrs[dot]me.uk:80/	2016-10-03	inactive	8
http://ljyuwhybrqrs[dot]me:80/	2016-10-03	inactive	8
http://lqkkqjkskckd[dot]pw:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
http://mcjfgtyjgddi[dot]biz:80/	2016-10-03	inactive	8
http://mcjfgtyjgddi[dot]co.in:80/	2016-10-03	inactive	8
http://mcjfgtyjgddi[dot]me.uk:80/	2016-10-03	inactive	8
http://mcjfgtyjgddi[dot]me:80/	2016-10-03	inactive	8
http://mlooticbghcr[dot]biz:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
http://mlooticbghcr[dot]co.in:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
http://mlooticbghcr[dot]me.uk:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
http://mlooticbghcr[dot]me:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
http://pjvkdltedcru[dot]biz:80/	2016-10-03	inactive	8
http://pjvkdltedcru[dot]co.in:80/	2016-10-03	inactive	8
http://pjvkdltedcru[dot]me.uk:80/	2016-10-03	inactive	8
http://pjvkdltedcru[dot]me:80/	2016-10-03	inactive	8
http://qhwneepsrvbr[dot]biz:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
http://qhwneepsrvbr[dot]co.in:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
http://qhwneepsrvbr[dot]me.uk:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8

BOTNET ACTIVITY REPORT

SERVER URL	LAST ALIVE	STATUS	COUNT
http://qhwneepsrvbr[dot]me:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
http://spejgoduxmni[dot]biz:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
http://spejgoduxmni[dot]co.in:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
http://spejgoduxmni[dot]me.uk:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
http://spejgoduxmni[dot]me:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
http://thfnqfwdeexj[dot]biz:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
http://thfnqfwdeexj[dot]co.in:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
http://thfnqfwdeexj[dot]me.uk:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
http://thfnqfwdeexj[dot]me:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
http://tptlttmjrjgf[dot]biz:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
http://tptlttmjrjgf[dot]co.in:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
http://tptlttmjrjgf[dot]me.uk:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
http://tptlttmjrjgf[dot]me:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
http://uuqpojihdkwr[dot]biz:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
http://uuqpojihdkwr[dot]co.in:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
http://uuqpojihdkwr[dot]me.uk:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
http://uuqpojihdkwr[dot]me:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
http://xtxxphxqdxgx[dot]biz:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
http://xtxxphxqdxgx[dot]co.in:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
http://xtxxphxqdxgx[dot]me.uk:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
http://xtxxphxqdxgx[dot]me:80/iuyfjyfcjgcjj/	2016-10-15	inactive	8
http://yyipsocikpdk[dot]biz:80/	2016-10-03	inactive	8
http://yyipsocikpdk[dot]co.in:80/	2016-10-03	inactive	8
http://yyipsocikpdk[dot]me.uk:80/	2016-10-03	inactive	8
http://yyipsocikpdk[dot]me:80/	2016-10-03	inactive	8
http://gfjis78jj79[dot]ru/li/	2015-07-07	inactive	6
http://wedratikul[dot]ru/pk/	2015-07-08	inactive	5
http://bmcluvwgnpyx[dot]biz:80/	2016-09-28	inactive	4
http://bmcluvwgnpyx[dot]co.in:80/	2016-09-28	inactive	4

SERVER URL	LAST ALIVE	STATUS	COUNT
http://bmcluvwgnpyx[dot]me.uk:80/	2016-09-28	inactive	4
http://bmcluvwgnpyx[dot]me:80/	2016-09-28	inactive	4
http://gcdvvunqlksr[dot]biz:80/	2016-09-28	inactive	4
http://gcdvvunqlksr[dot]co.in:80/	2016-09-28	inactive	4
http://gcdvvunqlksr[dot]me.uk:80/	2016-09-28	inactive	4
http://gcdvvunqlksr[dot]me:80/	2016-09-28	inactive	4
http://iosbqigbxgxb[dot]biz:80/	2016-09-28	inactive	4
http://iosbqigbxgxb[dot]co.in:80/	2016-09-28	inactive	4
http://iosbqigbxgxb[dot]me.uk:80/	2016-09-28	inactive	4
http://iosbqigbxgxb[dot]me:80/	2016-09-28	inactive	4
http://kocjupilkchq[dot]biz:80/	2016-09-28	inactive	4
http://kocjupilkchq[dot]co.in:80/	2016-09-28	inactive	4
http://kocjupilkchq[dot]me.uk:80/	2016-09-28	inactive	4
http://kocjupilkchq[dot]me:80/	2016-09-28	inactive	4
http://mcjfgtyjgdmf[dot]biz:80/	2016-09-28	inactive	4
http://mcjfgtyjgdmf[dot]co.in:80/	2016-09-28	inactive	4
http://mcjfgtyjgdmf[dot]me.uk:80/	2016-09-28	inactive	4
http://mcjfgtyjgdmf[dot]me:80/	2016-09-28	inactive	4
http://yyipsociemqn[dot]biz:80/	2016-09-28	inactive	4
http://yyipsociemqn[dot]co.in:80/	2016-09-28	inactive	4
http://yyipsociemqn[dot]me.uk:80/	2016-09-28	inactive	4
http://yyipsociemqn[dot]me:80/	2016-09-28	inactive	4
http://edgfebcmjqur[dot]biz:80/new0fo782d78j2dh/	2016-02-16	inactive	2
http://edgfebcmjqur[dot]co.in:80/new0fo782d78j2dh/	2016-02-16	inactive	2
http://edgfebcmjqur[dot]me.uk:80/new0fo782d78j2dh/	2016-02-16	inactive	2
http://edgfebcmjqur[dot]me:80/new0fo782d78j2dh/	2016-02-16	inactive	2
http://edmjknrfpqsh[dot]biz:80/new0fo782d78j2dh/	2016-02-16	inactive	2
http://edmjknrfpqsh[dot]co.in:80/new0fo782d78j2dh/	2016-02-16	inactive	2
http://edmjknrfpqsh[dot]me.uk:80/new0fo782d78j2dh/	2016-02-16	inactive	2

SERVER URL	LAST ALIVE	STATUS	COUNT
http://edmjknrfpqsh[dot]me:80/new0fo782d78j2dh/	2016-02-16	inactive	2
http://enwhhdvfolsn[dot]biz:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://enwhhdvfolsn[dot]co.in:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://enwhhdvfolsn[dot]me.uk:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://enwhhdvfolsn[dot]me:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://epxylvumlrfe[dot]biz:80/new0fo782d78j2dh/	2016-02-16	inactive	2
http://epxylvumlrfe[dot]co.in:80/new0fo782d78j2dh/	2016-02-16	inactive	2
http://epxylvumlrfe[dot]me.uk:80/new0fo782d78j2dh/	2016-02-16	inactive	2
http://epxylvumlrfe[dot]me:80/new0fo782d78j2dh/	2016-02-16	inactive	2
http://fcsjbbbpenim[dot]biz:80/new0fo782d78j2dh/	2016-02-16	inactive	2
http://fcsjbbbpenim[dot]co.in:80/new0fo782d78j2dh/	2016-02-16	inactive	2
http://fcsjbbbpenim[dot]me.uk:80/new0fo782d78j2dh/	2016-02-16	inactive	2
http://fcsjbbbpenim[dot]me:80/new0fo782d78j2dh/	2016-02-16	inactive	2
http://fgxlkkfiptid[dot]biz:80/new0fo782d78j2dh/	2016-02-16	inactive	2
http://fgxlkkfiptid[dot]co.in:80/new0fo782d78j2dh/	2016-02-16	inactive	2
http://fgxlkkfiptid[dot]me.uk:80/new0fo782d78j2dh/	2016-02-16	inactive	2
http://fgxlkkfiptid[dot]me:80/new0fo782d78j2dh/	2016-02-16	inactive	2
http://fqelkidudcwb[dot]biz:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://fqelkidudcwb[dot]co.in:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://fqelkidudcwb[dot]me.uk:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://fqelkidudcwb[dot]me:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://hquuyplmjbjw[dot]biz:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://hquuyplmjbjw[dot]co.in:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://hquuyplmjbjw[dot]me.uk:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://hquuyplmjbjw[dot]me:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://i28h63gdb67uehdi[dot]cc:80/new0fo782d78j2dh/	2016-02-16	inactive	2
http://iqfeershiybb[dot]biz:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://iqfeershiybb[dot]co.in:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://iqfeershiybb[dot]me.uk:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2

SERVER URL	LAST ALIVE	STATUS	COUNT
http://iqfeershiybb[dot]me:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://j73gdy64reff625r[dot]cc:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://llnwryfjnqyx[dot]biz:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://llnwryfjnqyx[dot]co.in:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://llnwryfjnqyx[dot]me.uk:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://llnwryfjnqyx[dot]me:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://ndstcbhkvjkh[dot]biz:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://ndstcbhkvjkh[dot]co.in:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://ndstcbhkvjkh[dot]me.uk:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://ndstcbhkvjkh[dot]me:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://nreycgqhollw[dot]biz:80/new0fo782d78j2dh/	2016-02-16	inactive	2
http://nreycgqhollw[dot]co.in:80/new0fo782d78j2dh/	2016-02-16	inactive	2
http://nreycgqhollw[dot]me.uk:80/new0fo782d78j2dh/	2016-02-16	inactive	2
http://nreycgqhollw[dot]me:80/new0fo782d78j2dh/	2016-02-16	inactive	2
http://okgskwwvunml[dot]biz:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://okgskwwvunml[dot]co.in:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://okgskwwvunml[dot]me.uk:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://okgskwwvunml[dot]me:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://ormlknfcstik[dot]biz:80/new0fo782d78j2dh/	2016-02-16	inactive	2
http://ormlknfcstik[dot]co.in:80/new0fo782d78j2dh/	2016-02-16	inactive	2
http://ormlknfcstik[dot]me.uk:80/new0fo782d78j2dh/	2016-02-16	inactive	2
http://ormlknfcstik[dot]me:80/new0fo782d78j2dh/	2016-02-16	inactive	2
http://ortscdtpxmof[dot]biz:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://ortscdtpxmof[dot]co.in:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://ortscdtpxmof[dot]me.uk:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://ortscdtpxmof[dot]me:80/jdhe7301he73yhd7i/	2016-03-01	inactive	2
http://uutdiihloccx[dot]biz:80/new0fo782d78j2dh/	2016-02-16	inactive	2
http://uutdiihloccx[dot]co.in:80/new0fo782d78j2dh/	2016-02-16	inactive	2
http://uutdiihloccx[dot]me.uk:80/new0fo782d78j2dh/	2016-02-16	inactive	2

SERVER URL	LAST ALIVE	STATUS	COUNT
http://uutdiihloccx[dot]me:80/new0fo782d78j2dh/	2016-02-16	inactive	2
http://ljyuwhybrqrd[dot]biz:80/	2016-09-28	inactive	1
http://ljyuwhybrqrd[dot]co.in:80/	2016-09-28	inactive	1
http://ljyuwhybrqrd[dot]me.uk:80/	2016-09-28	inactive	1
http://ljyuwhybrqrd[dot]me:80/	2016-09-28	inactive	1
http://pjvkdltedclq[dot]biz:80/	2016-09-28	inactive	1
http://pjvkdltedclq[dot]co.in:80/	2016-09-28	inactive	1
http://pjvkdltedclq[dot]me.uk:80/	2016-09-28	inactive	1
http://pjvkdltedclq[dot]me:80/	2016-09-28	inactive	1

Botnet-specific report: Waski Week 42/2016

Samples

VARIANT	COUNT
Win32_TrojanDownloader_Waski_F_trojan	46
Win32_TrojanDownloader_Waski_Z_trojan	39
Win32_TrojanDownloader_Waski_AG_trojan	9
Win32_TrojanDownloader_Waski_A_trojan	1

Command & Control servers

SERVER URL	LAST ALIVE	STATUS	COUNT
http://107[dot]161.207.151/misi12.png	2015-12-15	inactive	11
http://176[dot]223.153.138/misi12.png	2015-12-15	inactive	11
http://195[dot]228.219.230/misi12.png	2015-12-15	inactive	11
http://212[dot]92.6.123/misi12.png	2015-12-15	inactive	11
http://216[dot]245.211.242/misi12.png	2015-12-15	inactive	11
http://216[dot]51.193.145/misi12.png	2015-12-15	inactive	11
http://66[dot]215.30.118/misi12.png	2015-12-15	inactive	11
http://68[dot]70.242.203/misi12.png	2015-12-15	inactive	11
http://73[dot]22.119.204/misi12.png	2015-12-15	inactive	11
http://87[dot]255.64.223/misi12.png	2015-12-15	inactive	11
http://91[dot]144.83.19/misi12.png	2015-12-15	inactive	11
http://93[dot]119.102.70/misi12.png	2015-12-15	inactive	11
http://93[dot]185.4.90/misi12.png	2015-12-15	inactive	11
http://96[dot]40.19.168/misi12.png	2015-12-15	inactive	11
http://96[dot]46.100.49/misi12.png	2015-12-15	inactive	11
http://96[dot]46.103.232/misi12.png	2015-12-15	inactive	11
http://96[dot]46.99.183/misi12.png	2015-12-15	inactive	11
http://178[dot]219.10.23/modoc12.pdf	2015-12-16	inactive	5
http://178[dot]79.58.15/modoc12.pdf	2015-12-16	inactive	5

SERVER URL	LAST ALIVE	STATUS	COUNT
http://178[dot]79.58.27/modoc12.pdf	2015-12-16	inactive	5
http://178[dot]79.58.28/modoc12.pdf	2015-12-16	inactive	5
http://184[dot]164.107.28/static12.pdf	2015-12-16	inactive	5
http://184[dot]164.107.36/static12.pdf	2015-12-16	inactive	5
http://184[dot]164.97.236/static12.pdf	2015-12-16	inactive	5
http://184[dot]164.97.238/static12.pdf	2015-12-16	inactive	5
http://184[dot]164.97.239/static12.pdf	2015-12-16	inactive	5
http://184[dot]164.97.242/static12.pdf	2015-12-16	inactive	5
http://194[dot]106.166.22/modoc12.pdf	2015-12-16	inactive	5
http://199[dot]180.92.27/static12.pdf	2015-12-16	inactive	5
http://209[dot]193.67.173/static12.pdf	2015-12-16	inactive	5
http://209[dot]193.86.177/static12.pdf	2015-12-16	inactive	5
http://212[dot]69.7.79/modoc12.pdf	2015-12-16	inactive	5
http://216[dot]245.211.242/modoc12.pdf	2015-12-16	inactive	5
http://216[dot]245.211.242/static12.pdf	2015-12-16	inactive	5
http://38[dot]124.60.82/modoc12.pdf	2015-12-16	inactive	5
http://64[dot]184.235.209/static12.pdf	2015-12-16	inactive	5
http://64[dot]184.239.248/static12.pdf	2015-12-16	inactive	5
http://64[dot]184.255.69/static12.pdf	2015-12-16	inactive	5
http://65[dot]79.201.39/modoc12.pdf	2015-12-16	inactive	5
http://67[dot]207.228.144/modoc12.pdf	2015-12-16	inactive	5
http://67[dot]219.166.113/modoc12.pdf	2015-12-16	inactive	5
http://68[dot]170.52.35/static12.pdf	2015-12-16	inactive	5
http://69[dot]8.48.221/modoc12.pdf	2015-12-16	inactive	5
http://69[dot]9.204.37/modoc12.pdf	2015-12-16	inactive	5
http://75[dot]127.23.245/static12.pdf	2015-12-16	inactive	5
http://75[dot]127.28.70/static12.pdf	2015-12-16	inactive	5
http://79[dot]101.2.254/modoc12.pdf	2015-12-16	inactive	5
http://79[dot]101.42.247/modoc12.pdf	2015-12-16	inactive	5

SERVER URL	LAST ALIVE	STATUS	COUNT
http://91[dot]211.17.201/modoc12.pdf	2015-12-16	inactive	5
http://91[dot]211.17.201/static12.pdf	2015-12-16	inactive	5
http://93[dot]87.3.169/modoc12.pdf	2015-12-16	inactive	5
http://109[dot]111.109.48/bliser2.zip	2015-11-27	inactive	4
http://109[dot]75.154.46/picc22.png	2015-12-16	inactive	4
http://110[dot]78.166.230/bliser2.zip	2015-11-27	inactive	4
http://112[dot]133.203.43/bliser2.zip	2015-11-27	inactive	4
http://173[dot]248.31.6/bliser2.zip	2015-11-27	inactive	4
http://181[dot]143.71.20/bliser2.zip	2015-11-27	inactive	4
http://185[dot]14.28.206/bliser2.zip	2015-11-27	inactive	4
http://186[dot]31.224.64/bliser2.zip	2015-11-27	inactive	4
http://188[dot]167.93.231/bliser2.zip	2015-11-27	inactive	4
http://190[dot]0.99.80/bliser2.zip	2015-11-27	inactive	4
http://195[dot]146.118.46/picc22.png	2015-12-16	inactive	4
http://197[dot]149.90.166/bliser2.zip	2015-11-27	inactive	4
http://202[dot]70.89.57/bliser2.zip	2015-11-27	inactive	4
http://202[dot]79.57.155/bliser2.zip	2015-11-27	inactive	4
http://203[dot]129.197.50/bliser2.zip	2015-11-27	inactive	4
http://203[dot]223.42.3/bliser2.zip	2015-11-27	inactive	4
http://208[dot]117.68.78/bliser2.zip	2015-11-27	inactive	4
http://212[dot]5.207.78/bliser2.zip	2015-11-27	inactive	4
http://213[dot]81.199.121/bliser2.zip	2015-11-27	inactive	4
http://216[dot]245.211.242/picc22.png	2015-12-16	inactive	4
http://24[dot]148.217.188/bliser2.zip	2015-11-27	inactive	4
http://24[dot]33.131.116/bliser2.zip	2015-11-27	inactive	4
http://27[dot]109.20.53/bliser2.zip	2015-11-27	inactive	4
http://37[dot]19.85.9/bliser2.zip	2015-11-27	inactive	4
http://43[dot]248.24.50/bliser2.zip	2015-11-27	inactive	4
http://67[dot]222.201.105/bliser2.zip	2015-11-27	inactive	4

SERVER URL	LAST ALIVE	STATUS	COUNT
http://72[dot]230.82.80/bliser2.zip	2015-11-27	inactive	4
http://77[dot]48.30.156/picc22.png	2015-12-16	inactive	4
http://77[dot]95.195.68/picc22.png	2015-12-16	inactive	4
http://81[dot]90.164.134/picc22.png	2015-12-16	inactive	4
http://82[dot]115.76.211/bliser2.zip	2015-11-27	inactive	4
http://82[dot]160.64.45/bliser2.zip	2015-11-27	inactive	4
http://85[dot]143.220.31/bliser2.zip	2015-11-27	inactive	4
http://86[dot]100.25.233/bliser2.zip	2015-11-27	inactive	4
http://86[dot]106.251.174/bliser2.zip	2015-11-27	inactive	4
http://87[dot]244.175.114/bliser2.zip	2015-11-27	inactive	4
http://87[dot]248.191.142/bliser2.zip	2015-11-27	inactive	4
http://87[dot]249.149.40/picc22.png	2015-12-16	inactive	4
http://88[dot]101.108.254/bliser2.zip	2015-11-27	inactive	4
http://88[dot]209.249.139/bliser2.zip	2015-11-27	inactive	4
http://91[dot]211.17.201/picc22.png	2015-12-16	inactive	4
http://91[dot]221.217.139/picc22.png	2015-12-16	inactive	4
http://91[dot]240.236.122/bliser2.zip	2015-11-27	inactive	4
http://92[dot]38.41.38/picc22.png	2015-12-16	inactive	4
http://93[dot]115.172.232/bliser2.zip	2015-11-27	inactive	4
http://93[dot]183.155.22/bliser2.zip	2015-11-27	inactive	4
http://95[dot]143.128.70/picc22.png	2015-12-16	inactive	4
http://95[dot]143.130.63/picc22.png	2015-12-16	inactive	4
http://95[dot]143.131.160/picc22.png	2015-12-16	inactive	4
http://95[dot]143.131.73/picc22.png	2015-12-16	inactive	4
http://95[dot]143.132.118/picc22.png	2015-12-16	inactive	4
http://95[dot]143.134.103/picc22.png	2015-12-16	inactive	4
http://95[dot]143.141.50/picc22.png	2015-12-16	inactive	4
http://109[dot]199.11.51/osaka21.jpg	2015-12-15	inactive	3
http://109[dot]199.11.51/updf12.tar	2015-11-28	inactive	3

SERVER URL	LAST ALIVE	STATUS	COUNT
http://112[dot]133.203.43/osaka21.jpg	2015-12-15	inactive	3
http://112[dot]133.203.43/updf12.tar	2015-11-28	inactive	3
http://150[dot]129.49.11/osaka21.jpg	2015-12-15	inactive	3
http://173[dot]216.247.74/osaka21.jpg	2015-12-15	inactive	3
http://173[dot]216.247.74/updf12.tar	2015-11-28	inactive	3
http://173[dot]248.31.6/osaka21.jpg	2015-12-15	inactive	3
http://173[dot]248.31.6/updf12.tar	2015-11-28	inactive	3
http://176[dot]101.135.103/osaka21.jpg	2015-12-15	inactive	3
http://176[dot]221.77.21/dron22.png	2015-12-16	inactive	3
http://178[dot]22.217.166/dron22.png	2015-12-16	inactive	3
http://178[dot]22.222.89/dron22.png	2015-12-16	inactive	3
http://178[dot]222.250.35/dron22.png	2015-12-16	inactive	3
http://178[dot]249.175.151/updf12.tar	2015-11-28	inactive	3
http://178[dot]253.216.40/dron22.png	2015-12-16	inactive	3
http://178[dot]79.58.16/dron22.png	2015-12-16	inactive	3
http://178[dot]79.58.18/dron22.png	2015-12-16	inactive	3
http://181[dot]143.71.20/updf12.tar	2015-11-28	inactive	3
http://185[dot]31.33.98/dron22.png	2015-12-16	inactive	3
http://185[dot]47.89.141/dron22.png	2015-12-16	inactive	3
http://185[dot]89.64.160/osaka21.jpg	2015-12-15	inactive	3
http://186[dot]31.224.64/updf12.tar	2015-11-28	inactive	3
http://186[dot]68.94.38/osaka21.jpg	2015-12-15	inactive	3
http://188[dot]167.93.231/updf12.tar	2015-11-28	inactive	3
http://190[dot]0.99.80/updf12.tar	2015-11-28	inactive	3
http://190[dot]95.138.66/updf12.tar	2015-11-28	inactive	3
http://194[dot]28.191.245/osaka21.jpg	2015-12-15	inactive	3
http://195[dot]158.109.24/updf12.tar	2015-11-28	inactive	3
http://197[dot]149.90.166/osaka21.jpg	2015-12-15	inactive	3
http://197[dot]149.90.166/updf12.tar	2015-11-28	inactive	3

SERVER URL	LAST ALIVE	STATUS	COUNT
http://197[dot]210.199.21/osaka21.jpg	2015-12-15	inactive	3
http://197[dot]210.199.21/updf12.tar	2015-11-28	inactive	3
http://197[dot]254.56.126/updf12.tar	2015-11-28	inactive	3
http://200[dot]25.207.173/updf12.tar	2015-11-28	inactive	3
http://202[dot]70.89.57/updf12.tar	2015-11-28	inactive	3
http://202[dot]79.57.155/updf12.tar	2015-11-28	inactive	3
http://203[dot]115.103.27/osaka21.jpg	2015-12-15	inactive	3
http://203[dot]129.197.50/osaka21.jpg	2015-12-15	inactive	3
http://203[dot]129.197.50/updf12.tar	2015-11-28	inactive	3
http://208[dot]117.68.78/osaka21.jpg	2015-12-15	inactive	3
http://208[dot]117.68.78/updf12.tar	2015-11-28	inactive	3
http://209[dot]27.49.117/osaka21.jpg	2015-12-15	inactive	3
http://212[dot]200.112.6/dron22.png	2015-12-16	inactive	3
http://212[dot]5.207.78/updf12.tar	2015-11-28	inactive	3
http://213[dot]81.199.121/updf12.tar	2015-11-28	inactive	3
http://213[dot]92.138.154/osaka21.jpg	2015-12-15	inactive	3
http://216[dot]245.211.242/dron22.png	2015-12-16	inactive	3
http://24[dot]148.217.188/osaka21.jpg	2015-12-15	inactive	3
http://24[dot]148.217.188/updf12.tar	2015-11-28	inactive	3
http://24[dot]33.131.116/osaka21.jpg	2015-12-15	inactive	3
http://24[dot]33.131.116/updf12.tar	2015-11-28	inactive	3
http://27[dot]109.20.53/osaka21.jpg	2015-12-15	inactive	3
http://27[dot]109.20.53/updf12.tar	2015-11-28	inactive	3
http://31[dot]47.104.149/updf12.tar	2015-11-28	inactive	3
http://37[dot]19.85.9/updf12.tar	2015-11-28	inactive	3
http://37[dot]57.144.177/osaka21.jpg	2015-12-15	inactive	3
http://38[dot]66.20.98/dron22.png	2015-12-16	inactive	3
http://43[dot]248.24.50/updf12.tar	2015-11-28	inactive	3
http://45[dot]64.159.18/osaka21.jpg	2015-12-15	inactive	3

SERVER URL	LAST ALIVE	STATUS	COUNT
http://50[dot]24.13.21/updf12.tar	2015-11-28	inactive	3
http://63[dot]248.156.246/osaka21.jpg	2015-12-15	inactive	3
http://65[dot]33.236.173/osaka21.jpg	2015-12-15	inactive	3
http://67[dot]207.229.215/osaka21.jpg	2015-12-15	inactive	3
http://67[dot]221.147.66/osaka21.jpg	2015-12-15	inactive	3
http://67[dot]222.201.105/updf12.tar	2015-11-28	inactive	3
http://67[dot]222.201.222/osaka21.jpg	2015-12-15	inactive	3
http://67[dot]222.201.61/osaka21.jpg	2015-12-15	inactive	3
http://68[dot]70.242.203/osaka21.jpg	2015-12-15	inactive	3
http://69[dot]144.171.44/osaka21.jpg	2015-12-15	inactive	3
http://69[dot]144.171.44/updf12.tar	2015-11-28	inactive	3
http://69[dot]9.204.114/osaka21.jpg	2015-12-15	inactive	3
http://69[dot]9.204.114/updf12.tar	2015-11-28	inactive	3
http://72[dot]230.82.80/osaka21.jpg	2015-12-15	inactive	3
http://72[dot]230.82.80/updf12.tar	2015-11-28	inactive	3
http://77[dot]104.206.150/dron22.png	2015-12-16	inactive	3
http://77[dot]48.30.156/osaka21.jpg	2015-12-15	inactive	3
http://77[dot]95.192.36/dron22.png	2015-12-16	inactive	3
http://78[dot]108.101.67/osaka21.jpg	2015-12-15	inactive	3
http://78[dot]72.233.105/osaka21.jpg	2015-12-15	inactive	3
http://80[dot]95.103.138/updf12.tar	2015-11-28	inactive	3
http://80[dot]95.103.167/updf12.tar	2015-11-28	inactive	3
http://82[dot]115.76.211/osaka21.jpg	2015-12-15	inactive	3
http://82[dot]115.76.211/updf12.tar	2015-11-28	inactive	3
http://82[dot]160.64.45/osaka21.jpg	2015-12-15	inactive	3
http://82[dot]160.64.45/updf12.tar	2015-11-28	inactive	3
http://84[dot]22.52.129/dron22.png	2015-12-16	inactive	3
http://85[dot]135.104.170/osaka21.jpg	2015-12-15	inactive	3
http://85[dot]67.227.249/updf12.tar	2015-11-28	inactive	3

SERVER URL	LAST ALIVE	STATUS	COUNT
http://86[dot]100.25.233/updf12.tar	2015-11-28	inactive	3
http://86[dot]106.251.174/updf12.tar	2015-11-28	inactive	3
http://87[dot]249.142.189/osaka21.jpg	2015-12-15	inactive	3
http://88[dot]101.108.254/updf12.tar	2015-11-28	inactive	3
http://88[dot]209.248.135/updf12.tar	2015-11-28	inactive	3
http://88[dot]209.249.139/updf12.tar	2015-11-28	inactive	3
http://89[dot]239.120.43/osaka21.jpg	2015-12-15	inactive	3
http://91[dot]211.17.201/dron22.png	2015-12-16	inactive	3
http://91[dot]240.236.122/updf12.tar	2015-11-28	inactive	3
http://92[dot]247.244.122/updf12.tar	2015-11-28	inactive	3
http://93[dot]115.172.232/updf12.tar	2015-11-28	inactive	3
http://93[dot]123.88.180/updf12.tar	2015-11-28	inactive	3
http://93[dot]183.155.22/updf12.tar	2015-11-28	inactive	3
http://94[dot]141.130.9/osaka21.jpg	2015-12-15	inactive	3
http://94[dot]154.107.172/dron22.png	2015-12-16	inactive	3
http://94[dot]40.82.66/osaka21.jpg	2015-12-15	inactive	3
http://109[dot]111.109.48/pic_172.jpg	2015-12-14	inactive	2
http://109[dot]199.11.51/fupd12.zip	2015-11-27	inactive	2
http://110[dot]78.166.230/pic_172.jpg	2015-12-14	inactive	2
http://112[dot]133.203.43/fupd12.zip	2015-11-27	inactive	2
http://112[dot]133.203.43/pic_172.jpg	2015-12-14	inactive	2
http://173[dot]216.247.74/fupd12.zip	2015-11-27	inactive	2
http://173[dot]248.31.6/fupd12.zip	2015-11-27	inactive	2
http://173[dot]248.31.6/pic_172.jpg	2015-12-14	inactive	2
http://177[dot]240.223.45/fupd12.zip	2015-11-27	inactive	2
http://181[dot]143.54.146/fupd12.zip	2015-11-27	inactive	2
http://181[dot]143.71.20/pic_172.jpg	2015-12-14	inactive	2
http://185[dot]14.28.206/pic_172.jpg	2015-12-14	inactive	2
http://186[dot]31.224.64/fupd12.zip	2015-11-27	inactive	2

SERVER URL	LAST ALIVE	STATUS	COUNT
http://186[dot]31.224.64/pic_172.jpg	2015-12-14	inactive	2
http://188[dot]167.93.231/fupd12.zip	2015-11-27	inactive	2
http://188[dot]167.93.231/pic_172.jpg	2015-12-14	inactive	2
http://190[dot]0.99.80/pic_172.jpg	2015-12-14	inactive	2
http://190[dot]121.164.10/fupd12.zip	2015-11-27	inactive	2
http://190[dot]254.98.82/fupd12.zip	2015-11-27	inactive	2
http://190[dot]255.42.99/fupd12.zip	2015-11-27	inactive	2
http://190[dot]95.138.66/fupd12.zip	2015-11-27	inactive	2
http://197[dot]149.90.166/fupd12.zip	2015-11-27	inactive	2
http://197[dot]149.90.166/pic_172.jpg	2015-12-14	inactive	2
http://197[dot]210.199.21/fupd12.zip	2015-11-27	inactive	2
http://197[dot]254.116.190/fupd12.zip	2015-11-27	inactive	2
http://197[dot]254.56.126/fupd12.zip	2015-11-27	inactive	2
http://200[dot]122.196.138/fupd12.zip	2015-11-27	inactive	2
http://200[dot]25.207.173/fupd12.zip	2015-11-27	inactive	2
http://202[dot]70.89.57/fupd12.zip	2015-11-27	inactive	2
http://202[dot]70.89.57/pic_172.jpg	2015-12-14	inactive	2
http://202[dot]79.57.155/fupd12.zip	2015-11-27	inactive	2
http://202[dot]79.57.155/pic_172.jpg	2015-12-14	inactive	2
http://203[dot]129.197.50/fupd12.zip	2015-11-27	inactive	2
http://203[dot]129.197.50/pic_172.jpg	2015-12-14	inactive	2
http://203[dot]223.42.3/pic_172.jpg	2015-12-14	inactive	2
http://208[dot]117.68.78/fupd12.zip	2015-11-27	inactive	2
http://208[dot]117.68.78/pic_172.jpg	2015-12-14	inactive	2
http://212[dot]5.207.78/pic_172.jpg	2015-12-14	inactive	2
http://213[dot]81.199.121/pic_172.jpg	2015-12-14	inactive	2
http://213[dot]92.138.154/fupd12.zip	2015-11-27	inactive	2
http://24[dot]148.217.188/fupd12.zip	2015-11-27	inactive	2
http://24[dot]148.217.188/pic_172.jpg	2015-12-14	inactive	2

SERVER URL	LAST ALIVE	STATUS	COUNT
http://24[dot]33.131.116/fupd12.zip	2015-11-27	inactive	2
http://24[dot]33.131.116/pic_172.jpg	2015-12-14	inactive	2
http://27[dot]109.20.53/fupd12.zip	2015-11-27	inactive	2
http://27[dot]109.20.53/pic_172.jpg	2015-12-14	inactive	2
http://37[dot]19.85.9/pic_172.jpg	2015-12-14	inactive	2
http://37[dot]57.144.177/fupd12.zip	2015-11-27	inactive	2
http://43[dot]248.24.50/fupd12.zip	2015-11-27	inactive	2
http://43[dot]248.24.50/pic_172.jpg	2015-12-14	inactive	2
http://50[dot]24.13.21/fupd12.zip	2015-11-27	inactive	2
http://67[dot]222.201.105/fupd12.zip	2015-11-27	inactive	2
http://67[dot]222.201.105/pic_172.jpg	2015-12-14	inactive	2
http://67[dot]222.201.61/fupd12.zip	2015-11-27	inactive	2
http://68[dot]70.242.203/fupd12.zip	2015-11-27	inactive	2
http://69[dot]144.171.44/fupd12.zip	2015-11-27	inactive	2
http://69[dot]9.204.114/fupd12.zip	2015-11-27	inactive	2
http://72[dot]230.82.80/fupd12.zip	2015-11-27	inactive	2
http://72[dot]230.82.80/pic_172.jpg	2015-12-14	inactive	2
http://78[dot]108.101.67/fupd12.zip	2015-11-27	inactive	2
http://82[dot]115.76.211/fupd12.zip	2015-11-27	inactive	2
http://82[dot]115.76.211/pic_172.jpg	2015-12-14	inactive	2
http://82[dot]160.64.45/fupd12.zip	2015-11-27	inactive	2
http://82[dot]160.64.45/pic_172.jpg	2015-12-14	inactive	2
http://85[dot]143.220.31/pic_172.jpg	2015-12-14	inactive	2
http://86[dot]100.25.233/pic_172.jpg	2015-12-14	inactive	2
http://86[dot]106.251.174/pic_172.jpg	2015-12-14	inactive	2
http://87[dot]126.65.67/fupd12.zip	2015-11-27	inactive	2
http://87[dot]244.175.114/pic_172.jpg	2015-12-14	inactive	2
http://87[dot]248.191.142/pic_172.jpg	2015-12-14	inactive	2
http://88[dot]101.108.254/pic_172.jpg	2015-12-14	inactive	2

SERVER URL	LAST ALIVE	STATUS	COUNT
http://88[dot]209.249.139/pic_172.jpg	2015-12-14	inactive	2
http://91[dot]240.236.122/fupd12.zip	2015-11-27	inactive	2
http://91[dot]240.236.122/pic_172.jpg	2015-12-14	inactive	2
http://91[dot]240.236.148/fupd12.zip	2015-11-27	inactive	2
http://93[dot]115.172.232/fupd12.zip	2015-11-27	inactive	2
http://93[dot]115.172.232/pic_172.jpg	2015-12-14	inactive	2
http://93[dot]183.155.22/fupd12.zip	2015-11-27	inactive	2
http://93[dot]183.155.22/pic_172.jpg	2015-12-14	inactive	2
http://94[dot]40.82.66/fupd12.zip	2015-11-27	inactive	2
http://104[dot]131.250.211/tab12.tar	2015-12-14	inactive	1
http://104[dot]174.123.66/soks11.png	2016-02-02	inactive	1
http://104[dot]36.232.219/soks11.png	2016-02-02	inactive	1
http://109[dot]111.109.48/tab12.tar	2015-12-14	inactive	1
http://109[dot]86.226.85/soks11.png	2016-02-02	inactive	1
http://112[dot]133.203.43/tab12.tar	2015-12-14	inactive	1
http://162[dot]255.126.8/soks11.png	2016-02-02	inactive	1
http://173[dot]216.240.56/soks11.png	2016-02-02	inactive	1
http://173[dot]248.29.43/soks11.png	2016-02-02	inactive	1
http://173[dot]248.31.6/tab12.tar	2015-12-14	inactive	1
http://176[dot]36.251.208/soks11.png	2016-02-02	inactive	1
http://178[dot]249.175.151/tab12.tar	2015-12-14	inactive	1
http://181[dot]143.71.20/tab12.tar	2015-12-14	inactive	1
http://184[dot]164.107.28/static11.pdf	2016-01-21	inactive	1
http://184[dot]164.107.36/static11.pdf	2016-01-21	inactive	1
http://184[dot]164.97.236/static11.pdf	2016-01-21	inactive	1
http://184[dot]164.97.238/static11.pdf	2016-01-21	inactive	1
http://184[dot]164.97.239/static11.pdf	2016-01-21	inactive	1
http://184[dot]164.97.242/static11.pdf	2016-01-21	inactive	1
http://186[dot]31.224.64/tab12.tar	2015-12-14	inactive	1

SERVER URL	LAST ALIVE	STATUS	COUNT
http://188[dot]167.93.231/tab12.tar	2015-12-14	inactive	1
http://188[dot]231.34.130/soks11.png	2016-02-02	inactive	1
http://188[dot]255.134.177/soks11.png	2016-02-02	inactive	1
http://188[dot]255.165.154/soks11.png	2016-02-02	inactive	1
http://188[dot]255.241.59/soks11.png	2016-02-02	inactive	1
http://190[dot]0.99.80/tab12.tar	2015-12-14	inactive	1
http://190[dot]95.138.66/tab12.tar	2015-12-14	inactive	1
http://197[dot]149.90.166/tab12.tar	2015-12-14	inactive	1
http://197[dot]210.199.21/tab12.tar	2015-12-14	inactive	1
http://197[dot]254.56.126/tab12.tar	2015-12-14	inactive	1
http://199[dot]180.92.27/static11.pdf	2016-01-21	inactive	1
http://202[dot]70.89.57/tab12.tar	2015-12-14	inactive	1
http://202[dot]79.57.155/tab12.tar	2015-12-14	inactive	1
http://203[dot]129.197.50/tab12.tar	2015-12-14	inactive	1
http://203[dot]223.42.3/tab12.tar	2015-12-14	inactive	1
http://208[dot]117.68.78/tab12.tar	2015-12-14	inactive	1
http://209[dot]193.67.173/static11.pdf	2016-01-21	inactive	1
http://209[dot]193.86.177/static11.pdf	2016-01-21	inactive	1
http://212[dot]5.207.78/tab12.tar	2015-12-14	inactive	1
http://213[dot]81.199.121/tab12.tar	2015-12-14	inactive	1
http://216[dot]245.211.242/static11.pdf	2016-01-21	inactive	1
http://24[dot]148.217.188/tab12.tar	2015-12-14	inactive	1
http://24[dot]159.153.153/soks11.png	2016-02-02	inactive	1
http://24[dot]220.92.193/soks11.png	2016-02-02	inactive	1
http://24[dot]33.131.116/tab12.tar	2015-12-14	inactive	1
http://27[dot]109.20.53/tab12.tar	2015-12-14	inactive	1
http://37[dot]19.85.9/tab12.tar	2015-12-14	inactive	1
http://38[dot]75.38.186/soks11.png	2016-02-02	inactive	1
http://43[dot]248.24.50/tab12.tar	2015-12-14	inactive	1

SERVER URL	LAST ALIVE	STATUS	COUNT
http://46[dot]37.201.165/tab12.tar	2015-12-14	inactive	1
http://64[dot]184.235.209/static11.pdf	2016-01-21	inactive	1
http://64[dot]184.239.248/static11.pdf	2016-01-21	inactive	1
http://64[dot]184.255.69/static11.pdf	2016-01-21	inactive	1
http://64[dot]203.121.6/soks11.png	2016-02-02	inactive	1
http://67[dot]222.201.105/tab12.tar	2015-12-14	inactive	1
http://68[dot]170.52.35/static11.pdf	2016-01-21	inactive	1
http://69[dot]144.171.44/tab12.tar	2015-12-14	inactive	1
http://72[dot]230.82.80/tab12.tar	2015-12-14	inactive	1
http://75[dot]127.23.245/static11.pdf	2016-01-21	inactive	1
http://75[dot]127.28.70/static11.pdf	2016-01-21	inactive	1
http://82[dot]115.76.211/tab12.tar	2015-12-14	inactive	1
http://82[dot]160.64.45/tab12.tar	2015-12-14	inactive	1
http://86[dot]100.25.233/tab12.tar	2015-12-14	inactive	1
http://86[dot]106.251.174/tab12.tar	2015-12-14	inactive	1
http://87[dot]244.175.114/tab12.tar	2015-12-14	inactive	1
http://88[dot]101.108.254/tab12.tar	2015-12-14	inactive	1
http://88[dot]209.249.139/tab12.tar	2015-12-14	inactive	1
http://91[dot]192.131.229/tab12.tar	2015-12-14	inactive	1
http://91[dot]211.17.201/static11.pdf	2016-01-21	inactive	1
http://91[dot]240.236.122/tab12.tar	2015-12-14	inactive	1
http://93[dot]115.172.232/tab12.tar	2015-12-14	inactive	1
http://93[dot]183.155.22/tab12.tar	2015-12-14	inactive	1
http://93[dot]185.4.90/soks11.png	2016-02-02	inactive	1

Botnet-specific report: Wauchos Week 42/2016

Samples

VARIANT	COUNT
Win32_TrojanDownloader_Wauchos_BH~mem_trojan	1411
Win32_TrojanDownloader_Wauchos_CB_trojan	1396
Win64_TrojanDownloader_Wauchos_A_trojan	511
Win32_TrojanDownloader_Wauchos_BF~mem_trojan	95
Win32_TrojanDownloader_Wauchos_CA~mem_trojan	25
Win64_TrojanDownloader_Wauchos_A~mem_trojan	18
Win32_TrojanDownloader_Wauchos_BB~mem_trojan	14
Win32_TrojanDownloader_Wauchos_BZ_trojan	13
Win32_TrojanDownloader_Wauchos_BX_trojan	5
Win32_TrojanDownloader_Wauchos_CA_trojan	2
Win32_TrojanDownloader_Wauchos_BK~mem_trojan	2
Win32_TrojanDownloader_Wauchos_BC~mem_trojan	1
Win32_TrojanDownloader_Wauchos_BY~mem_trojan	1

Command & Control servers

	SERVER URL	LAST ALIVE	STATUS	COUNT
ⓘ	http://ofytcx99yi[dot]ru/last.so	2016-10-17	new	768
ⓘ	http://109[dot]236.84.25/121egreregregrege55454.exe	2016-10-22	new	24
ⓘ	http://109[dot]236.84.25/123egreregregrege55454.exe	2016-10-22	new	24
ⓘ	http://109[dot]236.84.25/156aegreregregrege55454.exe	2016-10-22	new	24
ⓘ	http://109[dot]236.84.25/156begreregregrege55454.exe	2016-10-22	new	24
ⓘ	http://109[dot]236.84.25/161egreregregrege55454.exe	2016-10-22	new	24
ⓘ	http://109[dot]236.84.25/17egreregregrege55454.exe	2016-10-22	new	24
ⓘ	http://109[dot]236.84.25/226egreregregrege55454.exe	2016-10-22	new	24
ⓘ	http://109[dot]236.84.25/38egreregregrege55454.exe	2016-10-22	new	24
ⓘ	http://109[dot]236.84.25/74egreregregrege55454.exe	2016-10-22	new	24

	SERVER URL	LAST ALIVE	STATUS	COUNT
ⓘ	http://109[dot]236.84.25/85egreregregrege55454.exe	2016-10-22	new	24
ⓘ	http://109[dot]236.84.25/smoke927145.exe	2016-10-22	new	24
ⓘ	http://109[dot]236.84.25/121frgegerg6e6565.exe	2016-10-23	new	20
ⓘ	http://109[dot]236.84.25/121nite43.exe	2016-10-23	new	20
ⓘ	http://109[dot]236.84.25/123frgegerg6e6565.exe	2016-10-23	new	20
ⓘ	http://109[dot]236.84.25/123nite43.exe	2016-10-23	new	20
ⓘ	http://109[dot]236.84.25/156afrgegerg6e6565.exe	2016-10-23	new	20
ⓘ	http://109[dot]236.84.25/156bfrgegerg6e6565.exe	2016-10-23	new	20
ⓘ	http://109[dot]236.84.25/161frgegerg6e6565.exe	2016-10-23	new	20
ⓘ	http://109[dot]236.84.25/161nite43.exe	2016-10-23	new	20
ⓘ	http://109[dot]236.84.25/17frgegerg6e6565.exe	2016-10-23	new	20
ⓘ	http://109[dot]236.84.25/17nite43.exe	2016-10-23	new	20
ⓘ	http://109[dot]236.84.25/226frgegerg6e6565.exe	2016-10-23	new	20
ⓘ	http://109[dot]236.84.25/226nite43.exe	2016-10-23	new	20
ⓘ	http://109[dot]236.84.25/38frgegerg6e6565.exe	2016-10-23	new	20
ⓘ	http://109[dot]236.84.25/38nite43.exe	2016-10-23	new	20
ⓘ	http://109[dot]236.84.25/74frgegerg6e6565.exe	2016-10-23	new	20
ⓘ	http://109[dot]236.84.25/74nite43.exe	2016-10-23	new	20
ⓘ	http://109[dot]236.84.25/85frgegerg6e6565.exe	2016-10-23	new	20
ⓘ	http://109[dot]236.84.25/85nite43.exe	2016-10-23	new	20
ⓘ	http://109[dot]236.84.25/smoke927146.exe	2016-10-23	new	20
ⓘ	http://109[dot]236.84.25/121eff3f34f496969.exe	2016-10-23	new	12
ⓘ	http://109[dot]236.84.25/123eff3f34f496969.exe	2016-10-23	new	12
ⓘ	http://109[dot]236.84.25/156aeff3f34f496969.exe	2016-10-23	new	12
ⓘ	http://109[dot]236.84.25/156beff3f34f496969.exe	2016-10-23	new	12
ⓘ	http://109[dot]236.84.25/161eff3f34f496969.exe	2016-10-23	new	12
ⓘ	http://109[dot]236.84.25/17eff3f34f496969.exe	2016-10-23	new	12
ⓘ	http://109[dot]236.84.25/226eff3f34f496969.exe	2016-10-23	new	12
ⓘ	http://109[dot]236.84.25/38eff3f34f496969.exe	2016-10-23	new	12

	SERVER URL	LAST ALIVE	STATUS	COUNT
ⓘ	http://109[dot]236.84.25/74eff3f34f496969.exe	2016-10-23	new	12
ⓘ	http://109[dot]236.84.25/85eff3f34f496969.exe	2016-10-23	new	12
ⓘ	http://109[dot]236.84.25/smoke927147.exe	2016-10-23	new	12
ⓘ	http://109[dot]236.84.25/121nite44.exe	2016-10-23	new	8
ⓘ	http://109[dot]236.84.25/123nite44.exe	2016-10-23	new	8
ⓘ	http://109[dot]236.84.25/161nite44.exe	2016-10-23	new	8
ⓘ	http://109[dot]236.84.25/17nite44.exe	2016-10-23	new	8
ⓘ	http://109[dot]236.84.25/226nite44.exe	2016-10-23	new	8
ⓘ	http://109[dot]236.84.25/38nite44.exe	2016-10-23	new	8
ⓘ	http://109[dot]236.84.25/74nite44.exe	2016-10-23	new	8
ⓘ	http://109[dot]236.84.25/85nite44.exe	2016-10-23	new	8
ⓘ	http://109[dot]236.84.25/121fwgrgfregre6g56e.exe	2016-10-24	new	6
ⓘ	http://109[dot]236.84.25/123fwgrgfregre6g56e.exe	2016-10-24	new	6
ⓘ	http://109[dot]236.84.25/156afwgrgfregre6g56e.exe	2016-10-24	new	6
ⓘ	http://109[dot]236.84.25/156bfwgrgfregre6g56e.exe	2016-10-24	new	6
ⓘ	http://109[dot]236.84.25/161fwgrgfregre6g56e.exe	2016-10-24	new	6
ⓘ	http://109[dot]236.84.25/17fwgrgfregre6g56e.exe	2016-10-24	new	6
ⓘ	http://109[dot]236.84.25/226fwgrgfregre6g56e.exe	2016-10-24	new	6
ⓘ	http://109[dot]236.84.25/38fwgrgfregre6g56e.exe	2016-10-24	new	6
ⓘ	http://109[dot]236.84.25/74fwgrgfregre6g56e.exe	2016-10-24	new	6
ⓘ	http://109[dot]236.84.25/85fwgrgfregre6g56e.exe	2016-10-24	new	6
ⓘ	http://109[dot]236.84.25/smoke927148.exe	2016-10-24	new	6
ⓘ	http://109[dot]236.84.25/121fefewff3vcxzzcvv.exe	2016-10-19	new	2
ⓘ	http://109[dot]236.84.25/121nite39.exe	2016-10-19	new	2
ⓘ	http://109[dot]236.84.25/123fefewff3vcxzzcvv.exe	2016-10-19	new	2
ⓘ	http://109[dot]236.84.25/123nite39.exe	2016-10-19	new	2
ⓘ	http://109[dot]236.84.25/156afefewff3vcxzzcvv.exe	2016-10-19	new	2
ⓘ	http://109[dot]236.84.25/156bfefewff3vcxzzcvv.exe	2016-10-19	new	2
ⓘ	http://109[dot]236.84.25/161fefewff3vcxzzcvv.exe	2016-10-19	new	2

BOTNET ACTIVITY REPORT

	SERVER URL	LAST ALIVE	STATUS	COUNT
ⓘ	http://109[dot]236.84.25/161nite39.exe	2016-10-19	new	2
ⓘ	http://109[dot]236.84.25/17fefewff3vcxzzcvv.exe	2016-10-19	new	2
ⓘ	http://109[dot]236.84.25/17nite39.exe	2016-10-19	new	2
ⓘ	http://109[dot]236.84.25/226fefewff3vcxzzcvv.exe	2016-10-19	new	2
ⓘ	http://109[dot]236.84.25/226nite39.exe	2016-10-19	new	2
ⓘ	http://109[dot]236.84.25/38fefewff3vcxzzcvv.exe	2016-10-19	new	2
ⓘ	http://109[dot]236.84.25/38nite39.exe	2016-10-19	new	2
ⓘ	http://109[dot]236.84.25/74fefewff3vcxzzcvv.exe	2016-10-19	new	2
ⓘ	http://109[dot]236.84.25/74nite39.exe	2016-10-19	new	2
ⓘ	http://109[dot]236.84.25/85fefewff3vcxzzcvv.exe	2016-10-19	new	2
ⓘ	http://109[dot]236.84.25/85nite39.exe	2016-10-19	new	2
ⓘ	http://109[dot]236.84.25/smoke927138.exe	2016-10-19	new	2
	http://4nbizac8[dot]ru/diff.php	2016-10-24	active	1453
	http://76236osm1[dot]ru/diff.php	2016-10-24	active	1453
	http://ac6ruv8t[dot]ru/diff.php	2016-10-24	active	1453
	http://differentia[dot]ru/diff.php	2016-10-24	active	1453
	http://gvaq70s7he[dot]ru/diff.php	2016-10-24	active	1453
	http://185[dot]112.82.50/future	2016-10-24	active	1169
	http://4nbizac8[dot]ru/atomic.php	2016-10-24	active	1157
	http://76236osm1[dot]ru/atomic.php	2016-10-24	active	1157
	http://ac6ruv8t[dot]ru/atomic.php	2016-10-24	active	1157
	http://atomictrivia[dot]ru/atomic.php	2016-10-24	active	1157
	http://gvaq70s7he[dot]ru/atomic.php	2016-10-24	active	1157
	http://4nbizac8[dot]ru/order.php	2016-10-23	active	296
	http://76236osm1[dot]ru/order.php	2016-10-23	active	296
	http://ac6ruv8t[dot]ru/order.php	2016-10-23	active	296
	http://disorderstatus[dot]ru/order.php	2016-10-23	active	296
	http://gvaq70s7he[dot]ru/order.php	2016-10-23	active	296
	http://and31[dot]amainworldnancy4.com/bla31/gate.php	2016-10-01	inactive	64

SERVER URL	LAST ALIVE	STATUS	COUNT
http://and31[dot]blllaaaaaazblaaa1.com/bla31/gate.php	2016-10-24	active	64
http://and31[dot]blllaaaaaazblaaa2.com/bla31/gate.php	2016-10-01	inactive	64
http://and31[dot]blllaaaaaazblaaa3.com/bla31/gate.php	2016-10-01	inactive	64

Botnet-specific report: Zbot Week 42/2016

Samples

VARIANT	COUNT
Win32_Spy_Zbot_YW_trojan	2978
Win32_Spy_Zbot_AAU_trojan	1740
Win32_Spy_Zbot_JF_trojan	1504
Win32_Spy_Zbot_ABV_trojan	528
Win32_Spy_Zbot_ACG_trojan	422
Win32_Spy_Zbot_ACM~mem_trojan	345
Win32_Spy_Zbot_AAO_trojan	122
Win32_Spy_Zbot_ABS_trojan	44
Win32_Spy_Zbot_ACB_trojan	28
Win32_Spy_Zbot_ABX_trojan	28
Win64_Spy_Zbot_M_trojan	18
Win32_Spy_Zbot_AAQ_trojan	16
Win32_Spy_Zbot_ACM_trojan	9
Win32_Spy_Zbot_ACO~mem_trojan	6
Win32_Spy_Zbot_ACF_trojan	6
Win32_Spy_Zbot_ACQ~mem_trojan	5
Win32_Spy_Zbot_ZR_trojan	4
Win32_Spy_Zbot_ACP_trojan	3
Win32_Spy_Zbot_UN_trojan	1

Command & Control servers

	SERVER URL	LAST ALIVE	STATUS	COUNT
ℹ	http://anothersideofpeace[dot]org/guv/file.php	2016-10-17	new	270
ℹ	https://addfais[dot]website/1eqzeithucooxfycequyx.dat	2016-10-19	new	157
ℹ	https://addfais[dot]website/1eqzeithucooxfycequyx.exe	2016-10-19	new	157
ℹ	https://addfais[dot]website/backsocks.bin	2016-10-19	new	157

SERVER URL	LAST ALIVE	STATUS	COUNT
https://addfais[dot]website/grabber.bin	2016-10-19	new	157
https://addfais[dot]website/vnc32.bin	2016-10-19	new	157
https://addfais[dot]website/vnc64.bin	2016-10-19	new	157
https://addfais[dot]website/webinjects.dat	2016-10-19	new	157
http://sunte-hk[dot]com/jag/file.php	2016-10-18	new	112
http://poetrybykhalidkhan[dot]com/.smileys/.gif/ify/uname/file.php	2016-10-21	new	104
http://l3d[dot]pp.ru/forum/file.php	2016-10-21	new	40
http://klgreetings[dot]com/.bin/simon/server/cfg.bin	2016-10-21	new	36
http://davewalshphoto[dot]com/slideshows/file.php	2016-10-20	new	32
https://scopus[dot]website/1ozozoveniwidyhqiukka.dat	2016-10-19	new	16
https://scopus[dot]website/1ozozoveniwidyhqiukka.exe	2016-10-19	new	16
https://scopus[dot]website/backsocksmon.bin	2016-10-19	new	16
https://scopus[dot]website/grabbermon.bin	2016-10-19	new	16
https://scopus[dot]website/vnc32mon.bin	2016-10-19	new	16
https://scopus[dot]website/vnc64mon.bin	2016-10-19	new	16
https://scopus[dot]website/webinjectsmon.dat	2016-10-19	new	16
http://cctoday[dot]info/wp-rss/filetype.php	2016-10-20	new	10
http://globalapps[dot]info/wp-rss/filetype.php	2016-10-20	new	10
https://wegas[dot]info/wp-rss/filetype.php	2016-10-20	new	10
http://growyourownteacher[dot]co.uk/eme/file.php	2016-10-18	new	6
http://bartus-umzuege[dot]de/images/ico-med9a.png	2016-10-23	new	4
http://www[dot]kpresident.com/dmp/file.php	2016-10-23	new	4
https://bacucucu[dot]top	2016-10-23	new	3
https://birounous[dot]top	2016-10-23	new	3
https://madagaba[dot]pw	2016-10-23	new	3
https://madagaba[dot]top	2016-10-23	new	3
https://madagaba[dot]top/2muisimymiwkigilepuki.dat	2016-10-23	new	3
https://madagaba[dot]top/2muisimymiwkigilepuki.exe	2016-10-23	new	3
https://madagaba[dot]top/backsocks.bin	2016-10-23	new	3

	SERVER URL	LAST ALIVE	STATUS	COUNT
ℹ	https://madagaba[dot]top/grabber.bin	2016-10-23	new	3
ℹ	https://madagaba[dot]top/vnc32.bin	2016-10-23	new	3
ℹ	https://madagaba[dot]top/vnc64.bin	2016-10-23	new	3
ℹ	https://madagaba[dot]top/webinjects_new.dat	2016-10-23	new	3
ℹ	https://moussaka[dot]pw	2016-10-23	new	3
ℹ	https://moussaka[dot]pw/4azinepatylyfamkyamyl.dat	2016-10-23	new	3
ℹ	https://moussaka[dot]pw/4azinepatylyfamkyamyl.exe	2016-10-23	new	3
ℹ	https://moussaka[dot]pw/backsocks.bin	2016-10-23	new	3
ℹ	https://moussaka[dot]pw/grabber.bin	2016-10-23	new	3
ℹ	https://moussaka[dot]pw/vnc32.bin	2016-10-23	new	3
ℹ	https://moussaka[dot]pw/vnc64.bin	2016-10-23	new	3
ℹ	https://moussaka[dot]pw/webinjects_new.dat	2016-10-23	new	3
ℹ	https://moussaka[dot]top	2016-10-23	new	3
ℹ	http://216[dot]170.119.107/sp/serverphp/config.bin	2016-10-17	new	2
ℹ	http://beanbags[dot]lk/data/config.bin	2016-10-18	new	2
ℹ	http://bizconnect247[dot]com/wp-admin/zee/config.bin	2016-10-19	new	2
ℹ	http://bizconnect247[dot]com/wp-admin/zee/gate.php	2016-10-19	new	2
ℹ	http://config[dot]com/file.php	2016-10-23	new	2
ℹ	http://contonskovkiys[dot]ru/file.php	2016-10-22	new	2
ℹ	http://drpzone[dot]org/pronz/config.bin	2016-10-18	new	2
ℹ	http://dualforcegate[dot]com/completed/success/private/upgrade.php	2016-10-22	new	2
ℹ	http://seguralawfirm[dot]com/css/file.php	2016-10-17	new	2
ℹ	http://winerelapse[dot]net/eis2/bin/cfg.php	2016-10-23	new	2
ℹ	http://www[dot]alfatechly.com/config.bin	2016-10-19	new	2
ℹ	http://www[dot]rolsmith.com/scp/images/icons/jpg/fax.bin	2016-10-18	new	2
ℹ	http://www[dot]vivahammer.com/wp-admin/images/img/config.bin	2016-10-19	new	2
ℹ	https://alyaqwer1141[dot]com	2016-10-18	new	2
ℹ	https://extensivee[dot]bid/000l7bo11nq36ou 9cfjfb0rdz17e7ulo_4agents/gate.php	2016-10-22	new	2
ℹ	https://fofancanada2016[dot]com/1imoxziziumdugecanafe.dat	2016-10-18	new	2

BOTNET ACTIVITY REPORT

SERVER URL	LAST ALIVE	STATUS	COUNT
https://fofancanada2016[dot]com/1imoxziziumdugecanafe.exe	2016-10-18	new	2
https://fofancanada2016[dot]com/backsocks.bin	2016-10-18	new	2
https://fofancanada2016[dot]com/grabber.bin	2016-10-18	new	2
https://fofancanada2016[dot]com/vnc32.bin	2016-10-18	new	2
https://fofancanada2016[dot]com/vnc64.bin	2016-10-18	new	2
https://fofancanada2016[dot]com/webinjects.dat	2016-10-18	new	2
https://fofancanada2017[dot]com	2016-10-18	new	2
https://fofancanade20111[dot]com	2016-10-18	new	2
https://madagaba[dot]pw/1arxegyotfigyxepemiud.dat	2016-10-23	new	2
https://madagaba[dot]pw/1arxegyotfigyxepemiud.exe	2016-10-23	new	2
https://madagaba[dot]pw/backsocks.bin	2016-10-23	new	2
https://madagaba[dot]pw/grabber.bin	2016-10-23	new	2
https://madagaba[dot]pw/vnc32.bin	2016-10-23	new	2
https://madagaba[dot]pw/vnc64.bin	2016-10-23	new	2
https://madagaba[dot]pw/webinjects_new.dat	2016-10-23	new	2
https://simpsonlok1221[dot]com	2016-10-18	new	2
https://ayane[dot]online	2016-10-20	new	1
https://lkpaal1[dot]xyz	2016-10-20	new	1
https://lkpaal2[dot]xyz	2016-10-20	new	1
https://lkpaal3[dot]xyz	2016-10-20	new	1
https://lkpaal4[dot]xyz	2016-10-20	new	1
https://lkpaal5[dot]xyz	2016-10-20	new	1
https://nihapred[dot]top/2ferogoereselnyyzowka.dat	2016-10-17	new	1
https://nihapred[dot]top/2ferogoereselnyyzowka.exe	2016-10-17	new	1
https://nihapred[dot]top/backsocks.bin	2016-10-17	new	1
https://nihapred[dot]top/grabber.bin	2016-10-17	new	1
https://nihapred[dot]top/vnc32.bin	2016-10-17	new	1
https://nihapred[dot]top/vnc64.bin	2016-10-17	new	1

	SERVER URL	LAST ALIVE	STATUS	COUNT
ⓘ	https://nihapred[dot]top/webinjects.dat	2016-10-17	new	1
ⓘ	https://wirpacel[dot]top/1siumdyidanepceluvava.dat	2016-10-17	new	1
ⓘ	https://wirpacel[dot]top/1siumdyidanepceluvava.exe	2016-10-17	new	1
ⓘ	https://wirpacel[dot]top/3efxaimekecelucenigmo.dat	2016-10-17	new	1
ⓘ	https://wirpacel[dot]top/3efxaimekecelucenigmo.exe	2016-10-17	new	1
ⓘ	https://wirpacel[dot]top/backsocks.bin	2016-10-17	new	1
ⓘ	https://wirpacel[dot]top/grabber.bin	2016-10-17	new	1
ⓘ	https://wirpacel[dot]top/vnc32.bin	2016-10-17	new	1
ⓘ	https://wirpacel[dot]top/vnc64.bin	2016-10-17	new	1
ⓘ	https://wirpacel[dot]top/webinjects.dat	2016-10-17	new	1
	http://bzfdcp[dot]com/cfg.bin	2015-05-08	inactive	539
	http://cpdesigns-za[dot]com/lopz/frintz/bnhb.bin	2015-04-15	inactive	384
	http://adres34[dot]sytes.net/sitem/cfg.bin	2015-03-18	inactive	364
	http://1211news[dot]com/copyrite/webmoney2.xls	2015-08-19	inactive	286
	http://wisetoolz[dot]com/lala/config.jpg	2016-08-29	inactive	246
	http://enginbilgidenizi[dot]com/wp-admin/includes/.filters/mono/eng/vjc.jpg	2016-10-03	inactive	207
	http://newdink[dot]org/d.bin	2015-08-25	inactive	192
	http://universithig[dot]at/eg.jpg	2015-08-19	inactive	190
	http://enginbilgidenizi[dot]com/wp-admin/includes/.filters/mono/eng/ssl.php	2016-10-21	active	169
	https://kasdima[dot]top	2016-08-10	inactive	159
	https://larodimas[dot]top	2016-08-10	inactive	159
	https://addfais[dot]website	2016-10-23	active	158
	https://kkjaoil[dot]trade	2016-10-03	inactive	158
	https://wsdfpoaa[dot]site	2016-09-12	inactive	158
	http://datma[dot]info/wp-admin/images/shots/config.bin	2015-03-18	inactive	152
	https://abbonatimailclustersite[dot]com	2016-10-23	active	141
	https://abbonatimailclustersite[dot]com/backsocks.bin	2016-09-18	inactive	141
	https://abbonatimailclustersite[dot]com/grabber.bin	2016-09-18	inactive	141

SERVER URL	LAST ALIVE	STATUS	COUNT
https://abbonatimailclustersite[dot]com/vnc32.bin	2016-09-18	inactive	141
https://abbonatimailclustersite[dot]com/vnc64.bin	2016-09-18	inactive	141
https://abbonatimailclustersite[dot]com/webinjects.dat	2016-09-18	inactive	141
https://benchmarkemailsite[dot]com	2016-09-18	inactive	141
https://couriermailsrvsite[dot]com	2016-09-18	inactive	141
https://ipcluxlistsite[dot]com	2016-09-18	inactive	141
https://mail25website[dot]com	2016-09-18	inactive	141
https://mailcorpsite[dot]com	2016-09-18	inactive	141
http://dlink4[dot]biz/o.bin	2015-08-25	inactive	122
http://164[dot]132.31.214/login/f.php	2016-08-19	inactive	120
http://blog201507[dot]com/admin/config.bin	2015-03-24	inactive	120
http://www[dot]botcat.la/cfg.bin	2015-08-20	inactive	94
https://abbonatimailclustersite[dot]com/1iqasusaxmadeorenuxic.dat	2016-10-07	inactive	90
https://abbonatimailclustersite[dot]com/1iqasusaxmadeorenuxic.exe	2016-10-07	inactive	90
http://iknowuwantme[dot]com/etc/config/index.php	2015-03-18	inactive	82
http://filebale[dot]ru/blocked.php	2015-03-18	inactive	80
http://yrganossbas3[dot]net/vbsa/cc.bin	2015-08-19	inactive	72
http://in-quiry[dot]net/soft/scout/9/s3.bin	2015-03-24	inactive	62
http://mncaauifdf[dot]ru/file.php	2016-09-28	inactive	62
http://mncxzbvuifdf[dot]ru/googlead/file.php	2016-09-28	inactive	62
http://186[dot]202.127.132/~villadochafarizc/.temp/cgi-bin/aces/eye.jpg	2016-10-10	inactive	60
http://186[dot]202.127.132/~villadochafarizc/.temp/cgi-bin/aces/xx.php	2016-10-21	active	60
http://dlink8[dot]net/v.bin	2015-08-19	inactive	58
https://abbonatimailclustersite[dot]com/1zafawexiheumhyagapza.dat	2016-09-30	inactive	51
https://abbonatimailclustersite[dot]com/1zafawexiheumhyagapza.exe	2016-09-30	inactive	51
http://nwarkansas[dot]org/wp-blog/config/index.php	2015-03-25	inactive	44
http://188[dot]165.206.163/login/f.php	2016-10-19	active	32
http://188[dot]165.206.163/login/g.php	2016-10-19	active	32

SERVER URL	LAST ALIVE	STATUS	COUNT
http://biotapharmas[dot]com/slamm/fresh/cidphp/file.php	2015-12-28	inactive	32
http://ibriossolar[dot]org.br/gallery/ibrio.bin	2015-03-25	inactive	26
https://bradesco[dot]tech	2016-07-25	inactive	23
https://novoparadiciona[dot]tech	2016-08-19	inactive	23
https://scopus[dot]host	2016-07-25	inactive	23
https://scopus[dot]website	2016-10-23	active	23
https://tecnoservice[dot]online	2016-07-25	inactive	23
http://habilitacionesdebomberos[dot]com/images/test/config.bin	2015-03-24	inactive	20
http://www[dot]kachilab.net/pony/pnn/config.jpg	2016-05-24	inactive	20
http://www[dot]shinden-model.com/wp-comment/config/index.php	2015-03-25	inactive	14
http://188[dot]225.33.143/ssdc32716372/file.php	2015-03-25	inactive	10
http://188[dot]225.33.163/ssdc32716372/file.php	2015-03-25	inactive	10
http://tamarindoreas[dot]info/fort/forum/index.php?p=4	2015-07-14	inactive	10
http://46[dot]28.55.100/ssdc32716372/file.php	2015-03-19	inactive	8
http://rqxba[dot]com/cfg.bin	2015-04-29	inactive	8
http://sadertokenupd[dot]ru/file.php	2015-11-25	inactive	6
http://secmicroupdate[dot]ru/file.php	2015-11-25	inactive	6
http://widexsecconnect[dot]ru/file.php	2015-11-25	inactive	6
https://aurmidh[dot]pw	2016-07-11	inactive	6
https://bainloth[dot]pw	2016-07-11	inactive	6
https://belegestel[dot]pw	2016-07-11	inactive	6
https://calengil[dot]pw	2016-07-11	inactive	6
https://cuinmalenel[dot]pw	2016-07-11	inactive	6
https://eluidess[dot]pw	2016-08-16	inactive	6
https://emmasirn[dot]pw	2016-06-20	inactive	5
https://olubev[dot]online	2016-06-21	inactive	5
https://prianvis[dot]site	2016-06-20	inactive	5
https://rodonn[dot]online	2016-06-20	inactive	5
https://sakovel[dot]xyz	2016-06-20	inactive	5

SERVER URL	LAST ALIVE	STATUS	COUNT
https://ylecaerels[dot]xyz	2016-06-20	inactive	5
http://188[dot]225.32.208/ssdc32716372/file.php	2015-03-18	inactive	4
http://188[dot]225.32.209/ssdc32716372/file.php	2015-03-25	inactive	4
http://92[dot]53.105.175/ssdc32716372/file.php	2015-04-01	inactive	4
http://92[dot]53.105.245/ssdc32716372/file.php	2015-04-01	inactive	4
http://146[dot]185.221.196/lyck/config.jpg	2015-12-12	inactive	2
http://500w[dot]su/500.jpg	2015-11-12	inactive	2
http://78[dot]24.216.58/lesson/site	2015-11-08	inactive	2
http://angryshippflyforok[dot]su/support1/mol/door.jpg	2015-11-22	inactive	2
http://apre-delfud1225[dot]com/zs/john.bin	2016-01-27	inactive	2
http://extremarazao[dot]com.br/timers/config.bin	2016-07-21	inactive	2
http://fourth[dot]su/foto_120x48_1425380539.jpg	2016-01-26	inactive	2
http://hezslqy[dot]com/bazfx/cfg.bin	2015-05-06	inactive	2
http://lobsterliveverromez[dot]com/rome2ceasar/config.php	2016-03-18	inactive	2
http://sabwexuyq[dot]com/ncete/cfg.bin	2015-05-06	inactive	2
http://unityidea[dot]com/will_smith.jpg	2016-01-26	inactive	2
http://usagetorrenen[dot]com/aws/ferfa.php	2015-10-02	inactive	2
http://valuationservice[dot]com/file.php	2015-06-16	inactive	2
http://wintersnowsunshaines[dot]su/support1/vujs/haad.jpg	2015-11-06	inactive	2
http://www[dot]gkmexico.com/sos/css/bor.bin	2015-06-03	inactive	2
http://www[dot]microsoft-analytics.xyz/reporting/data/microsoft/usage-analytics/borr.php	2016-07-04	inactive	2
http://www[dot]microsoft-error-reporting.xyz/analytics_engine/receiverd/inputs/data/borr.php	2016-07-04	inactive	2
http://www[dot]windows-troubleshooting.xyz/rep_data/analytics/processnode/output/borr.php	2016-07-04	inactive	2
http://x7urf7gig647mott[dot]onion/server/config.bin	2016-03-03	inactive	2
http://yvtwibsp[dot]com/ldpyd/cfg.bin	2015-05-08	inactive	2
https://fofancanada2016[dot]com	2016-10-20	active	2
https://hdd[dot]altacom.it/fkgir222.jpg	2015-11-19	inactive	2
https://wow[dot]mb190slclubitalia.it/tab123.jpg	2015-11-16	inactive	2

SERVER URL	LAST ALIVE	STATUS	COUNT
http://lincolnkaraoke[dot]com/lincdev/linc.jpg	2016-02-18	inactive	1
http://vpzsr[dot]com/lgnwfvhf/cfg.bin	2015-11-07	inactive	1
http://www[dot]irrsbergmusi.com/img/irrs.jpg	2016-02-01	inactive	1
http://www[dot]milkworks.org/mwtrichard/milk.jpg	2016-02-09	inactive	1
https://connect[dot]timstackleshop.es/gkdlw.jpg	2016-10-19	active	1
https://milkascvan[dot]top	2016-08-10	inactive	1
https://moll[dot]repack.it/up/ton/error.exe	2016-10-19	active	1
https://nihapred[dot]top	2016-10-17	active	1
https://oarnducoh[dot]top	2016-07-25	inactive	1
https://pp[dot]clanpontaccio.com/smotra.jpg	2016-10-19	active	1
https://sdfogwqq[dot]xyz	2016-09-12	inactive	1
https://sss[dot]mb190slclubitalia.it/tab123.jpg	2016-10-19	active	1
https://tioparcod[dot]top	2016-07-25	inactive	1
https://trk[dot]metalcer.it/newser/changestat.php	2016-10-19	active	1
https://urascmhe[dot]top	2016-09-27	inactive	1
https://wirpacel[dot]top	2016-10-17	active	1

Targets in configurations

TARGET	STATUS	COUNT
www[dot]nab.com.au/etc/designs/nabrwd/clientlibs.js	new	154
https://*[dot]anz.com/IBAU/web/L001/css/newsite/bootstrap/bootstrap.min.css	new	154
https://*[dot]my.commbank.com.au/netbank/Portfolio/WebResource.axd*	new	154
https://banking[dot]westpac.com.au/*/banking/Scripts/Desktop/Core/SkipAutoRegistration/modernizr.js*	new	154
https://banking[dot]westpac.com.au/wbc/banking/Resources/Desktop/WBC/Assets/Scripts/an_promo.min.js	new	154
https://banking[dot]westpac.com.au/wbc/banking/scripts/desktop/core/0010combined.js*	new	154
https://banking[dot]westpac.com.au/wbc/banking/scripts/desktop/fiserv.ps.authentication/0000combined.js*	new	154
https://ib[dot]nab.com.au/nabib/scripts/fancybox/jquery.fancybox-1.3.1.css*	new	154
https://ib[dot]nab.com.au/nabib/styles/nabstyle.css*	new	154

	TARGET	STATUS	COUNT
ⓘ	https://ihb[dot]cedacri.it/hb/authentication/login.seam	new	154
ⓘ	https://ihb[dot]cedacri.it/hb/authentication/login.seam?abi=05424	new	154
ⓘ	https://ihb2[dot]cedacri.it/hb/authentication/login.seam?abi=03105	new	154
ⓘ	https://ihb2[dot]cedacri.it/hb/authentication/login.seam?abi=03127	new	154
ⓘ	https://www[dot]anz.com/common/css/new/layout.css	new	154
ⓘ	https://www[dot]commbank.com.au/etc/designs/commbank-neo/neo/clientlibs/common.cs*	new	154
ⓘ	https://*[dot]anz.com/IBAU/web/L001/script/common.js	new	93
ⓘ	https://ihb[dot]cedacri.it/hb/authentication/login.seam?abi=05385&	new	93
ⓘ	https://ihb2[dot]cedacri.it/hb/authentication/login.seam?abi=05704*	new	93
ⓘ	https://ihb2[dot]cedacri.it/hb/authentication/login.seam?abi=06090	new	93
ⓘ	https://ihb2[dot]cedacri.it/hb/authentication/login.seam?abi=06090&productCode=&conversationId=*	new	93
ⓘ	https://waf1x[dot]anz.com/inetban*/Lrt.js	new	90
ⓘ	https://ihb[dot]cedacri.it/hb/authentication/login.seam?abi=05385&amp	new	61
ⓘ	https://www[dot]inbiz.intesasanpaolo.com/scriptFvca0/LinksWAR/master/fvcproductbonschistory/recuperaStoricoPresentazioniBonSCT.do?CODPRODOTTO=_FUN_PRODDISP_HISTORY	new	61
ⓘ	https://banking[dot]westpac.com.au/wbc/banking/Themes/Default/Desktop/WBC/Core/000-0001combined.css*	new	32
ⓘ	https://wupos[dot]westernunion.com/agent-app/home*	new	1
	!*[dot]microsoft.com/*	known	232
	!http://*myspace[dot]com*	known	232
	!http://*odnoklassniki[dot]ru/*	known	231
	!http://vkontakte[dot]ru/*	known	231
	@*/atl[dot]osmp.ru/*	known	231
	@*/login[dot]osmp.ru/*	known	231
	https://www[dot]gruposantander.es/*	known	231
	$http://digg[dot]com/news*	known	230
	$http://www[dot]apple.com/mac/	known	230
	http://ya[dot]ru*	known	229

TARGET	STATUS	COUNT
https://support[dot]comodo.com/*	known	229
*/etc/designs/sbg/stg/clientlibs/js/head[dot]min.js	known	154
*/ibank2/javascript/util/jquery-1[dot]7.1.min.js	known	154
ibank2/javascript/screen/accountDetails[dot]js	known	154
ibank2/javascript/util/s_code[dot]js	known	154
nab/resources/omniture/s_code[dot]js	known	154
static[dot]my.commbank.com.au/static/transactionhistory/js/online.transactionhistory	known	154
http*//www[dot]inbiz.intesasanpaolo.com/portalEiam0/sma/login_otp.f*	known	154
http*//www[dot]inbiz.intesasanpaolo.com/portalEiam0/sma/loginmode_vetrina.f*	known	154
https://*[dot]anz.com/base/resources/JScript/IB/supertag.js*	known	154
https://*[dot]anz.com/inetbank/banklink/common_all.js	known	154
https://aziendaonline[dot]mps.it/cbl/exec/loginSi*	known	154
https://banking*[dot]anz.com/IBAU/BANKAWAYTRAN*	known	154
https://ib[dot]nab.com.au/nabib/scripts/jquery/jquery-1.10.2.js*	known	154
https://ib[dot]nab.com.au/nabib/scripts/libs/browserdata/getBrowserData*.js*	known	154
https://ibbweb[dot]tecmarket.it/tmibbwebsecurity/05034/login.as*	known	154
https://ibk[dot]icbpi.it/gvb*	known	154
https://scrigno[dot]popso.it/ihb/run	known	154
https://scrigno[dot]popso.it/ihb/run1	known	154
https://static[dot]my.commbank.com.au/static/core/js/core-merge*.js	known	154
https://static[dot]my.commbank.com.au/static/core/js/instrumentation-merge*.js	known	154
https://static[dot]my.commbank.com.au/static/core/js/microsoftajaxwebforms*.js*	known	154
https://static[dot]my.commbank.com.au/static/core/theme/core/css/coreshared*.css	known	154
https://static[dot]my.commbank.com.au/static/netbank/js/func*.js	known	154
https://static[dot]my.commbank.com.au/static/netbank/js/tracking-merge*.js	known	154
https://static[dot]my.commbank.com.au/static/netbank/theme/fo/css/logon-merge*.css	known	154
https://www[dot]bancaprossima.com/script/ServiceLogin/ib/logi*	known	154
https://www[dot]gbw2.it/cbl/exec/loginSi*	known	154
https://www[dot]inbank.it/function/login.ht*	known	154

TARGET	STATUS	COUNT
easyweb[dot]td.com	known	126
http*://*acc*desjardins[dot]com*	known	126
http*scotiabank[dot]com*	known	126
https://*[dot]cibc.com/*	known	126
https://secure[dot]tangerine.ca/web/*	known	126
http*alterna*[dot]c*	known	123
http*beaubear[dot]ca*	known	123
http*bvi[dot]bnc.ca*	known	123
http*caissepopclare[dot]com*	known	123
http*ccunl[dot]c*	known	123
http*conexus[dot]c*	known	123
http*copperfin[dot]c*	known	123
http*credit*[dot]c*	known	123
http*cu[dot]*c*	known	123
http*cua[dot]c*	known	123
http*direct[dot]net*	known	123
http*entegra[dot]ca*	known	123
http*financial[dot]c*	known	123
http*firstcalgary[dot]com*	known	123
http*gffg[dot]com*	known	123
http*hald-nor[dot]on.ca*	known	123
http*hscunl[dot]ca*	known	123
http*implicity[dot]ca*	known	123
http*memberone[dot]ca*	known	123
http*mtlehman[dot]com*	known	123
http*northsave[dot]com*	known	123
http*noventis[dot]ca*	known	123
http*omista[dot]com*	known	123
http*prospera[dot]ca*	known	123

TARGET	STATUS	COUNT
http*provincialemployees[dot]com*	known	123
http*reddyk[dot]net*	known	123
http*savings[dot]c*	known	123
http*solutions[dot]c*	known	123
http*tandia[dot]com*	known	123
http*valleyfirst[dot]com*	known	123
http*vancity[dot]com*	known	123
http*wherewebank[dot]com*	known	123
[dot]royalbank.com	known	121
usaa[dot]com	known	121
*usaa[dot]com*BkAccounts?target=AccountSummary*	known	121
http*://*discover*[dot]com*	known	121
http*://*wer[dot]com.au*	known	121
http*amazon[dot]*	known	121
http*americanexpress[dot]com*	known	121
http*bmo[dot]com*	known	121
http*ebay[dot]*	known	121
http*wellsfargo[dot]com*	known	121
https://*bankofscotland[dot]co.uk/personal/*	known	121
https://*capitalone[dot]com*	known	121
https://*halifax-online[dot]co.uk/personal/*	known	121
https://*lloydsbank[dot]co.uk/personal/*	known	121
https://*tsb[dot]co.uk/personal/*	known	121
https://bank[dot]barclays.co.uk/olb/auth/LoginLink.action	known	121
https://bank[dot]barclays.co.uk/olb/balances/PersonalFinancialSummary*	known	121
https://banking[dot]chase.com/AccountActivity/*	known	121
https://chaseonline[dot]chase.com/MyAccounts.aspx	known	121
https://payments[dot]chase.com/PnT/*	known	121
https://secure[dot]bankofamerica.com/*.go*	known	121

TARGET	STATUS	COUNT
https://www[dot]bankofamerica.com/	known	121
https://www[dot]bankofamerica.com/*.go*	known	121
https://www[dot]chase.com/	known	121
https://online-retail[dot]unicredit.it/nb/it/MiniBoxLogin*	known	93
https://waf1x[dot]anz.com/inetbank1/Lrt.js	known	64
http://uyeler[dot]mynet.com/	known	32
http*//banco[dot]bradesco/html/classic/controller*	known	15
http*//banco[dot]bradesco/html/classic/index.shtm	known	15
http*//banco[dot]bradesco/html/classic/sobre/*.shtm	known	15
http*://*boq[dot]com.au*	known	15
http://banco[dot]bradesco/html/exclusive/index.shtm	known	15
http://banco[dot]bradesco/html/prime/index.shtm	known	15
http://banco[dot]bradesco/html/private/index.shtm	known	15
http://www[dot]bradesco.com.br/html/classic/index.shtm	known	15
https://www[dot]itau.com.br/_arquivosestaticos/Itau/defaultTheme/js/mapa*	known	15
https://www2[dot]bancobrasil.com.br/aapf/login.jsp	known	15
https://*bmo[dot]com/onlinebanking/*	known	5
https://*royalbank[dot]com/*	known	5
*[dot]ebay.com/*eBayISAPI.dll?*	known	2
*//mail[dot]yandex.ru/	known	2
*//mail[dot]yandex.ru/index.xml	known	2
*//money[dot]yandex.ru/	known	2
*//money[dot]yandex.ru/index.xml	known	2
*/my[dot]ebay.com/*CurrentPage=MyeBayPersonalInfo*	known	2
banking[dot]berliner-bank.de/trxm/bb	known	2
banquepopulaire[dot]fr/	known	2
e-bank[dot]wuestenrot.de/ebanking/eb/index.htm	known	2
entry?rzid=XC&rzbk=	known	2
fineco[dot]it//error	known	2

TARGET	STATUS	COUNT
fineco[dot]it/it/public	known	2
ideal[dot]ing.nl	known	2
ideal[dot]regiobank.nl/internetbankieren/	known	2
ideal[dot]snsreaal.nl/secure/sns/Pages/Payment	known	2
kunden[dot]commerzbank.de/lp/login	known	2
meine[dot]deutsche-bank.de/trxm/db	known	2
meine[dot]norisbank.de/trxm/noris	known	2
mijn[dot]ing.nl/internetbankieren/SesamLoginServlet*	known	2
okpay[dot]com/account/login.html	known	2
*pintan[dot]santanderbank.de/*PinUser*	known	2
*regiobank[dot]nl/internetbankieren/homepage/secure/homepage/homepage.html	known	2
*regiobank[dot]nl/internetbankieren/secure/login.html	known	2
*regiobank[dot]nl/internetbankieren/secure/login.html*action_prepareStepTwo=Inloggen	known	2
*regiobank[dot]nl/internetbankieren/secure/logout/logoutConfirm.html	known	2
*snsbank[dot]nl/mijnsns/bankieren/secure/betalen/overschrijvenbinnenland.html	known	2
snsbank[dot]nl/mijnsns/bankieren/secure/verzendlijst/verzendlijst.html	known	2
*snsbank[dot]nl/mijnsns/homepage/secure/homepage/homepage.html	known	2
*snsbank[dot]nl/mijnsns/secure/login.html	known	2
*snsbank[dot]nl/mijnsns/secure/login.html*action_prepareStepTwo=Inloggen	known	2
*snsbank[dot]nl/mijnsns/secure/logout/logoutConfirm.html	known	2
wellsfargo[dot]com/	known	2
http://*[dot]osmp.ru/	known	2
http://caixasabadell[dot]net/banca2/tx0011/0011.jsp	known	2
http://casino[dot]bet365.com/home/*	known	2
http://www[dot]hsbc.co.uk/1/2/personal/internet-banking*	known	2
http://www[dot]nrwbank.de/de*	known	2
https*de*portal/portal*	known	2
https*www[dot]*commerzbank.de*	known	2
https://*/*heck*ut*	known	2

TARGET	STATUS	COUNT
https://*/*order*	known	2
https://*/cart/*	known	2
https://*Account*Activity*	known	2
https://*AccountDetail[dot]*	known	2
https://*ban*[dot]*/*card*	known	2
https://*ban*[dot]*/*transfers*	known	2
https://*ban*ummary*	known	2
https://*bill*ummary*	known	2
https://*ccount*ummary*	known	2
https://areariservata[dot]bancamarche.it/wps/portal/*	known	2
https://areasegura[dot]banif.es/bog/bogbsn*	known	2
https://banca[dot]cajaen.es/Jaen/INclient.jsp	known	2
https://bancaonline[dot]openbank.es/servlet/PProxy?*	known	2
https://bancopostaonline[dot]poste.it/bpol/bancoposta/formslogin.asp	known	2
https://banesnet[dot]banesto.es/*/loginEmpresas.htm	known	2
https://banking*[dot]anz.com/*	known	2
https://banking[dot]donner-reuschel.de/*	known	2
https://banking[dot]fidor.de/users/*	known	2
https://banking[dot]postbank.de/rai*	known	2
https://cardsonline-consumer[dot]com/RBSG_Consumer/VerifyLogin.do	known	2
https://carnet[dot]cajarioja.es/banca3/tx0011/0011.jsp	known	2
https://cfi[dot]mb.seb.se/pqq_portal/sebflow/*	known	2
https://cristalcard[dot]de/*	known	2
https://easyweb*[dot]tdcanadatrust.com/servlet/*FinancialSummaryServlet*	known	2
https://ebanking[dot]procreditbank.de/User/*	known	2
https://empresas[dot]gruposantander.es/WebEmpresas/servlet/webempresas.servlets.*	known	2
https://extranet[dot]banesto.es/*/loginParticulares.htm	known	2
https://extranet[dot]banesto.es/npage/OtrosLogin/LoginIBanesto.htm	known	2
https://hb[dot]quiubi.it/newSSO/x11logon.htm	known	2

TARGET	STATUS	COUNT
https://home[dot]cbonline.co.uk/login.html*	known	2
https://home[dot]ybonline.co.uk/login.html*	known	2
https://home[dot]ybonline.co.uk/ral/loginmgr/*	known	2
https://home2ae[dot]cd.citibank.ae/CappWebAppAE/producttwo/capp/action/signoncq.do	known	2
https://ibank[dot]barclays.co.uk/olb/x/LoginMember.do	known	2
https://ibank[dot]internationalbanking.barclays.com/logon/icebapplication*	known	2
https://intbank[dot]crediteurope.nl/FWFIB/*	known	2
https://intelvia[dot]cajamurcia.es/2043/entrada/01entradaencrip.htm	known	2
https://internetbanking[dot]aib.ie/hb1/roi/signon	known	2
https://klant[dot]alex.nl/logon/index*	known	2
https://kunde[dot]comdirect.de/lp/wt/*	known	2
https://kunde[dot]onvista-bank.de/*	known	2
https://light[dot]webmoney.ru/default.aspx	known	2
https://lot-port[dot]bcs.ru/names.nsf?#ogin*	known	2
https://mijn[dot]gilissen.nl/authentication/*	known	2
https://moj[dot]raiffeisenpolbank.*	known	2
https://montevia[dot]elmonte.es/cgi-bin/INclient_2098*	known	2
https://oi[dot]cajamadrid.es/CajaMadrid/oi/pt_oi/Login/login	known	2
https://oie[dot]cajamadridempresas.es/CajaMadrid/oie/pt_oie/Login/login_oie_1	known	2
https://olb2[dot]nationet.com/MyAccounts/frame_MyAccounts_WP2.asp*	known	2
https://olb2[dot]nationet.com/signon/signon*	known	2
https://online*[dot]lloydstsb.co.uk/logon.ibc	known	2
https://online-business[dot]lloydstsb.co.uk/customer.ibc	known	2
https://online-offshore[dot]lloydstsb.com/customer.ibc	known	2
https://online[dot]atbank.nl/atb-retail/*	known	2
https://online[dot]ingbank.pl/bskonl/login.html*	known	2
https://online[dot]mbank.pl/pl/Logi*	known	2
https://online[dot]wamu.com/Servicing/Servicing.aspx?targetPage=AccountSummary	known	2
https://online[dot]wellsfargo.com/das/cgi-bin/session.cgi*	known	2

TARGET	STATUS	COUNT
https://online[dot]wellsfargo.com/login*	known	2
https://online[dot]wellsfargo.com/signon*	known	2
https://onlinebanking#[dot]wachovia.com/myAccounts.aspx?referrer=authService	known	2
https://onlinebanking[dot]nationalcity.com/OLB/secure/AccountList.aspx	known	2
https://onlineeast#[dot]bankofamerica.com/cgi-bin/ias/*/GotoWelcome	known	2
https://pastornetparticulares[dot]bancopastor.es/SrPd*	known	2
https://payangocard[dot]de/*	known	2
https://persoonlijk[dot]knab.nl/account/*	known	2
https://privati[dot]internetbanking.bancaintesa.it/sm/login/IN/box_login.jsp	known	2
https://probanking[dot]procreditbank.bg/main/main.asp*	known	2
https://resources[dot]chase.com/MyAccounts.aspx	known	2
https://rupay[dot]com/index.php	known	2
https://scrigno[dot]popso.it*	known	2
https://sports[dot]gamebookers.com/*	known	2
https://token[dot]kasbank.com/secure/logon*	known	2
https://web[dot]da-us.citibank.com/*BS_Id=MemberHomepage*	known	2
https://web[dot]da-us.citibank.com/cgi-bin/citifi/portal/l/autherror.do*	known	2
https://web[dot]da-us.citibank.com/cgi-bin/citifi/portal/l/l.do	known	2
https://web[dot]secservizi.it/siteminderagent/forms/login.fcc	known	2
https://welcome23[dot]smile.co.uk/SmileWeb/start.do	known	2
https://welcome27[dot]co-operativebank.co.uk/CBIBSWeb/start.do	known	2
https://www#[dot]citizensbankonline.com/*/index-wait.jsp	known	2
https://www#[dot]usbank.com/internetBanking/LoginRouter	known	2
https://www*[dot]banking.first-direct.com/1/2/*	known	2
https://www[dot]53.com/servlet/efsonline/index.html*	known	2
https://www[dot]asl.com/cas/login?service=*	known	2
https://www[dot]atbonlinebusiness.com/CorporateBankingWeb/Core/Login.aspx*	known	2
https://www[dot]bancajaproximaempresas.com/ControlEmpresas*	known	2
https://www[dot]bancoherrero.com/es/*	known	2

TARGET	STATUS	COUNT
https://www[dot]bbvanetoffice.com/local_bdno/login_bbvanetoffice.html	known	2
https://www[dot]bgnetplus.com/niloinet/login.jsp	known	2
https://www[dot]bwin.com/*	known	2
https://www[dot]caixagirona.es/cgi-bin/INclient_2030*	known	2
https://www[dot]caixalaietana.es/cgi-bin/INclient_2042	known	2
https://www[dot]caixaontinyent.es/cgi-bin/INclient_2045	known	2
https://www[dot]caixatarragona.es/esp/sec_1/oficinacodigo.jsp	known	2
https://www[dot]caja-granada.es/cgi-bin/INclient_2031	known	2
https://www[dot]cajabadajoz.es/cgi-bin/INclient_6010*	known	2
https://www[dot]cajacanarias.es/cgi-bin/INclient_6065	known	2
https://www[dot]cajacirculo.es/ISMC/Circulo/acceso.jsp	known	2
https://www[dot]cajadeavila.es/cgi-bin/INclient_6094	known	2
https://www[dot]cajalaboral.com/home/acceso.asp	known	2
https://www[dot]cajasoldirecto.es/2106/*	known	2
https://www[dot]cajavital.es/Appserver/vitalnet*	known	2
https://www[dot]ccm.es/cgi-bin/INclient_6105	known	2
https://www[dot]citibank.de*	known	2
https://www[dot]clavenet.net/cgi-bin/INclient_7054	known	2
https://www[dot]dab-bank.com*	known	2
https://www[dot]dkb.de/*	known	2
https://www[dot]e-gold.com/acct/balance.asp*	known	2
https://www[dot]e-gold.com/acct/li.asp	known	2
https://www[dot]ebank.hsbc.co.uk/main/IBLogon.jsp	known	2
https://www[dot]fibancmediolanum.es/BasePage.aspx*	known	2
https://www[dot]gruposantander.es/bog/sbi*?ptns=acceso*	known	2
https://www[dot]gruppocarige.it/grps/vbank/jsp/login.jsp	known	2
https://www[dot]halifax-online.co.uk/MyAccounts/MyAccounts.aspx*	known	2
https://www[dot]halifax-online.co.uk/_mem_bin/*	known	2
https://www[dot]halifax-online.co.uk/_mem_bin/formslogin.asp*	known	2

TARGET	STATUS	COUNT
https://www[dot]icscards.nl/*	known	2
https://www[dot]insidecard.de/*	known	2
https://www[dot]isbank.com.tr/Internet/ControlLoader.aspx*	known	2
https://www[dot]isideonline.it/relaxbanking/sso.Login*	known	2
https://www[dot]iwbank.it/private/index_pub.jhtml*	known	2
https://www[dot]mijn-icsbusiness.nl/icsbusiness/*	known	2
https://www[dot]mybank.alliance-leicester.co.uk/login/*	known	2
https://www[dot]nwolb.com/Login.asp*	known	2
https://www[dot]nwolb.com/Login.aspx*	known	2
https://www[dot]paypal.com/*	known	2
https://www[dot]paypal.com/*/webscr?cmd=_account	known	2
https://www[dot]paypal.com/*/webscr?cmd=_login-done*	known	2
https://www[dot]rbsdigital.com/Login.asp*	known	2
https://www[dot]sabadellatlantico.com/es/*	known	2
https://www[dot]suntrust.com/portal/server.pt*parentname=Login*	known	2
https://www[dot]syzgroup.com/	known	2
https://www[dot]targobank.de/de/online-banking/*	known	2
https://www[dot]ubibanca.com/*	known	2
https://www[dot]unicaja.es/PortalServlet*	known	2
https://www[dot]uno-e.com/local_bdnt_unoe/Login_unoe2.html	known	2
https://www[dot]us.hsbc.com/*	known	2
https://www[dot]wellsfargo.com/*	known	2
https://www[dot]xoom.com*	known	2
https://www[dot]xoom.com/*	known	2
https://www2[dot]bancopopular.es/AppBPE/servlet/servin*	known	2
!*apps[dot]facebook.com*	known	1
!*facebook[dot]com/ajax/*	known	1
!*google[dot]com/chat/*	known	1
!*googleusercontent[dot]com*	known	1

TARGET	STATUS	COUNT
!*mail[dot]google.com/*	known	1
!*pipe[dot]skype.com*	known	1
!*plus[dot]googleapis.com*	known	1
!*twitter[dot]com/i/jot*	known	1
#*bancopostaimpresaonline[dot]poste.it*	known	1
#*banklinknet2[dot]cariparma.it*	known	1
#*banklinknet2[dot]carispezia.it*	known	1
#*chebanca[dot]it*	known	1
#*corporate[dot]friuladria.it*	known	1
#*credem[dot]it*	known	1
https://bancopostaimpresaonline[dot]poste.it/*/*	known	1
https://wupos[dot]westernunion.com/agent-app/login*	known	1
|*Banner[dot]html*	known	1
|*analytics-control[dot]com*	known	1
|*banner[dot]html*	known	1
|*check[dot]lloydsbank.co.uk*	known	1
|*check[dot]tsb.co.uk*	known	1
|*cs[dot]directnet.com/dn/csd/*	known	1
|*fbds7[dot]ingdirect.ca/*	known	1
|*grey[dot]smile.co.uk/*	known	1
|*iba[dot]npbs.co.uk*	known	1
|*ideal[dot]ing.nl/lpt/*	known	1
|*ideal[dot]ing.nl/mpz/startpaginarekeninginfo.do*	known	1
|*isbank[dot]com.tr/Internet/images7/*	known	1
|*mc3[dot]retail.santander.co.uk/*	known	1
|*mijn[dot]ing.nl/lpt/*	known	1
|*mijn[dot]ing.nl/mpz/startpaginarekeninginfo.do*	known	1
|*mijnzakelijk[dot]ing.nl/lpt/*	known	1
|*mijnzakelijk[dot]ing.nl/mpz/startpaginarekeninginfo.do*	known	1

TARGET	STATUS	COUNT
|*nab[dot]directnet.com/dn/csd*	known	1
|*onlinebanking[dot]iombank.com*	known	1
|*pane[dot]bankofamerica.com*	known	1
|*rbsdigital[dot]com/*	known	1
|*roll[dot]nationwide.co.uk/*	known	1
|*stage[dot]quadrange.com/*	known	1
|*staticres[dot]klikbca.com/*	known	1
|*t32[dot]pnc.com/pressroom*	known	1
|*tppa[dot]bmo.com/*	known	1
|*uni[dot]ibank.nbg.gr/*	known	1
|*wp[dot]tb.raiffeisendirect.ch*	known	1
|*www[dot]defcompare.com/*	known	1
|*www[dot]fe.axa.be/trends/*	known	1
|*www7[dot]nwolb.com/*	known	1
|*www7[dot]ulsterbankanytimebanking.ie*	known	1

Explanations

Global statistics (for each day and for each tracked family)

Number of malware samples checked by ESET Threat Intelligence.

Number of all Command & Control (C&C) servers and new C&C servers seen.

Number of all Targets and new Targets seen in configurations.

More details for each tracked family are available in botnet-specific reports.

Botnet-specific reports (for each tracked family)

SAMPLES	List of variants tracked, with number of checked samples.
COMMAND & CONTROL SERVERS	List of all servers seen, with seen count, last seen (alive) date and statuses: Blue = new (first seen during this period) Gray = inactive (did not work during this period) Black = active (did work, not new) First, all new servers are listed, then all other servers are sorted by count (descending order).
TARGETS IN CONFIGURATIONS	List of all targets seen, with seen count and status: Blue = new (first seen during this period) Black = known (already seen before)