Bredolab Botnet – Botnet Analysis Report

Malware Analysis Project
MSc in Cybersecurity

Prateek Pulastya
Student ID: X21112541

School of Computing
National College of Ireland

Lecturer: Mr. Vikas Sahni

Bredolab Botnet – Botnet Analysis Report

Prateek Pulastya
X21112541

1 Executive Summary

Bredolab is a highly advanced piece of malware that can be used to download and install other types of harmful programs. It has made a steady amount of money throughout the year, making up for its monthly losses with a new campaign every day. Although it was initially categorized as a downloadable program, Bredolab has grown over time and become a malware distribution centre. Bredolab infections are also linked to various other threats, such as identity theft and spam.

One of the main methods of Bredolab Botnet spreading is through unsolicited mail. These are usually caused by malicious links, macro-enabled documents, and malicious scripts. Bredolab emails are designed to look like they are from a reputable company or a well-known payment method. They can then be tricked into clicking on a link or a particular message, such as "Your Invoice." This type of email has been around for a few years, and the attackers have evolved.

The Bredolab campaign used email as an attack vector, and it took it to a new level. Besides sending out shipping notifications and invoices, it also used email campaigns to trick people into clicking on links in infected websites. One of the main features of the Bredolab operation is its method of spreading its payload, which involved tricking users into visiting malicious resources.

Bredolab Botnet

- Group: Trojan Horse, Malware Loader
- Lifetime: First discovered in 2009 and shut down in 2011
- Spread Technique: Social engineering, Spam emails

Capabilities

- Data Theft: Yes
- Backdoor Capability: Yes
- Files Infection: Yes

Behaviour

- A malware management server that allows it to distribute and hack newly developed malware samples. It's additionally used to authenticate the credentials of the BredoLab users.
- A VPN server is used for various purposes, such as managing other servers and launching attacks against other websites. It can also be used to communicate with individuals and groups.
- The database server used by BredoLab stores information about the various types of malware samples and infected bots that it has distributed.
- A Jabber server is used to send commands to Zeus malware. It's also used to control the bots that it has distributed.

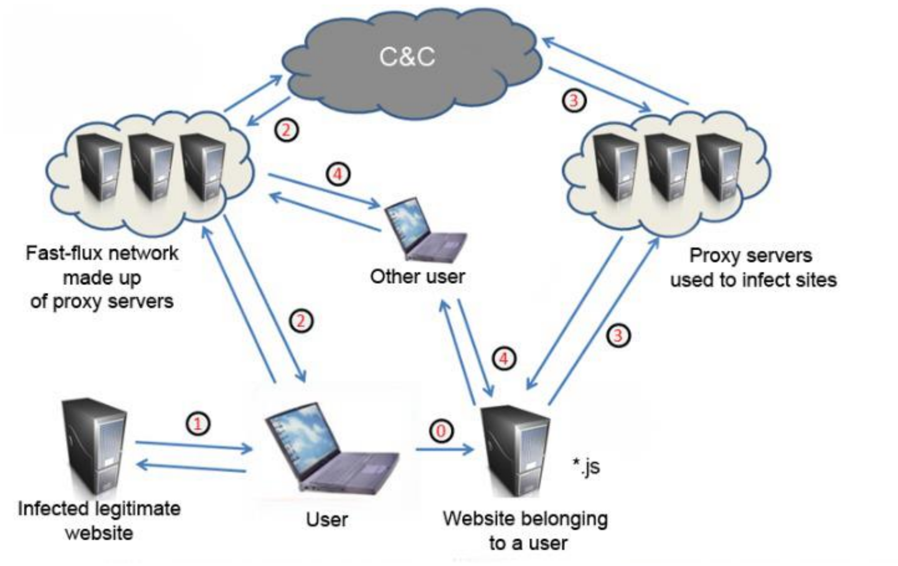

C&C
Fast-flux network made up of proxy servers
Other user
Proxy servers used to infect sites
Infected legitimate website
User
Website belonging to a user
*.js
0
1
2
2
3
3
4
4

Figure 1 Cyber-kill chain of Bredolab Botnet

The Bredolab botnet's infection chain is shown in Figure.1. It describes the various steps involved in maintaining a network after an attacker attacks it.

In this report, we first discussed the Bredolab Botnet and its various characteristics. After a thorough analysis and investigation, the details of the Bredolab botnet have been presented in a brief description. This report also provides recommendations and mitigations that can help prevent the exploitation of this type of botnet in the future.

2 Methodology

To perform the research on Bredolab various botnets, I have used a combination of strategies and techniques. For instance, I have searched for the most popular and longest running bot attacks, as well as the most dangerous ones.

After reading and evaluating the various reports about the Bredolab Botnets, I have decided to investigate and study the targeted botnet. In order to do so, I have used various analytical techniques such as network analysis, static analysis, and manual debugging. For instance, I have used the multiple threat reports of Bredolab to perform my research.

A report that provides a comprehensive analysis of the Bredolab Botnets has been presented to help inform the users about its various capabilities. It also provides a good knowledge about its kill chain and infection cycle. [1]

The report also discussed the history of the Bredolab Botnets. It's believed that the group was inspired by the Oficla banking Trojan, which was mainly used in viral e-mail spam. In addition, they discussed the threat actor that is responsible for the Bredolab botnet. Several names have been given to the entity that is responsible for the operation of the botnet.

Bredolab has been known to target various industries such as finance, healthcare, and manufacturing. It has also been used in multiple campaigns against government and other organizations. [2]

This paper aims to provide a comprehensive analysis of the Bredolab Botnet and its various variants. It also describes the steps taken by the NHTCU in the removal of the botnet. The authors have presented a variety of attack strategies and techniques that were used to attack the botnet. In the end, the paper shows the results of the experiment. [1]

A cyber threat analysis report published by the company mentioned that Bredolab has been known to distribute various types of documents. These include .exe or .dat files, which are usually used to download the Bredolab loader. They also use AutoOpen macros to execute a code, which then allows them to download the documents. After that, they showed a variety of tools and techniques that can be used to analyze the data collected by the Bredolab. [3]

2.1 Analysis

Two datasets have been analyzed and identified for performing a proper analysis of Bredolab. One of these is a tutorial that shows the various activities that occurred in the network during the time of the Bredolab infection. The other is a packet capture analysis tool called Wireshark. The tutorial talks about the chain of events that led to the infection. The malicious software used in the attack was downloaded or infected through a JavaScript webpage. [2]

The attached ZIP archive can contain a PDF file that can be used by the attacker to download the malicious software. Some of the emails contained links that can be used to download a PDF document. Figure 2 shows a flowchart that describes the various activities that occurred in the network during the time of the Bredolab infection. In the past decade, the initial binary file used in the attack was a Windows EXE file. [2]

One interesting fact about the various activities that occurred during the time of the Bredolab infection is that all of the links that were sent through the malicious software pointed to Port 8080. The servers that were used to respond to the requests were most likely using a type of HTTP server known as Nginx, which is commonly used as a reverse proxy. After clicking on the link, the users were redirected to the control center of the infected network. All of the requests to download the malicious software were sent through the fast-flux network's proxy servers. [4]

Most of the domains that were registered on the fast-flux network during the period of the Bredolab infection were owned by the cybercriminals. However, in the summer of 2010, some of these domains started to appear that were third-level. These third-level domains were placed on legitimate websites, which was a clear indication that the attackers were able to control the settings of these sites. [5] It's believed that the attackers were able to gain access to these websites through user account details. Two of the third-level domains are: -

- Koll****.sky##***on.com
- Aos**$#.do##$***tation.com

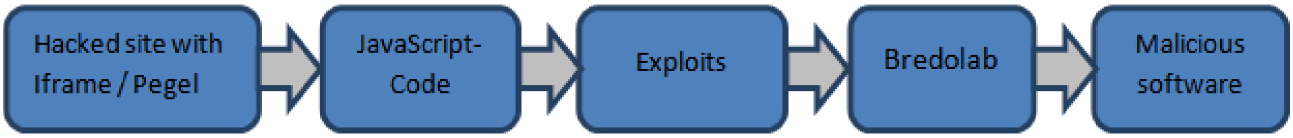


Figure 2 The phases of a target device's attack

3 Botnet Investigation & Findings

A type of malicious software known as Bredolab can steal various details from an infected computer, such as its password and login details. It has become a threat to users worldwide due to its size. The program can be spread through a fast-flux technique, which allows it to infect millions of computers at the same time. Its control panel is similar to that of Zeus. The various types of malwares it can install include rootkits, banking trojans, and spam. [6]

The Bredolab spam messages that were sent out by the network typically contained malicious attachments that looked like they came from DHL invoices. They were then used to trick users into clicking on the link in the message. The servers used for Bredolab were owned by a reseller of Dutch hosting company Lease web. Other malware such as SASFIS and CUTWAIL were also able to download the BREDOLAB variants. Users who visit compromised pages that contain malicious iframes might additionally be infected with the program. Black hat search engine optimization is another technique that allows users to get affected by the scam. [7]

Bredolab operations are carried out through a process known as a botnet. It copies itself into the registry entries of the affected computers. It then modifies the settings for the autorun process in order to remain active. The malware also allows its users to download additional payloads. Through its various infection processes, the program can send and receive data from the infected computer. The last step in the process is to wait for the control servers to perform their operations. [5]

This Trojan drops the following files:
%Application Data%\avdrn.dat
%Application Data%\wiaservg.log
%Application Data%\avkgp.dat

3.1 Bredolab Botnet Identification

One of the main features of the Bredolab botnet was its method of operation. It was able to spread its payload by visiting legitimate websites, which were then redirected to malicious resources. After clicking on these links, the computers of the infected users would automatically be infected with the Trojan.Win32.Bredolab. [5]

Another example of the Bredolab botnet is the Trojan.Downloader.Bredolab.CJ, which has a high damage rate and is mainly composed of around 40kb of code. The affected system would show the presence of two related files: %AppData%avdrn.dat and %Startuprarype32.exe. This program is disguised as a word document and tricks the users into downloading it. After successfully accessing the infected computer, it copies itself into the victim's %Startuprarype32.exe file, which then deletes all traces of its previous files. The main component of the Trojan.Downloader.Bredolab.CJ is a downloader that is injected into other programs, such as explorer.exe. [5]

According to Virustotal, the technical details about above two examples of Bredolab Botnet:

SHA256 Hash: - e6d10fd429e4103fd0212904a87e49d0f7401aa7b8643991557bd4a987801b78
MD5 Hash: - 04af1d1d111083ea142d8a7d03baeff5
File size: - 1014.05 KB
File Type: - Win32 EXE
File Name: - netspybox.exe
File Description: - Alternate of Trojan.Win32.Bredolab

SHA256 Hash: - 55129212b43e9255cdb9cff463eef0c08c3fc85f2bc964c27387b8eae9554e4c
MD5 Hash: - a45c6243f068d421c897fe8c4559f766
File size: - 26.02 KB
File Type: - Win32 EXE
File Name: - sever5737.exe
File Description: - Alternate of Trojan.Downloader.Bredolab.CJ

3.2 Bredolab Botnet Size, Damage and Evolution

The Bredolab Botnet file size is estimated at around 100 KB. It's mainly composed of a malicious link that's embedded in the file. After conducting a bit of research, I discovered that most of the files that are related to the Bredolab botnet are around 40 to 90 KB in size. The file is a part of a malware-as-a service that allows it to download and install other malware.

Individuals and organizations such as governments, schools, and financial institutions have been targeted by the Bredolab malware. It's a type of banking Trojan that targets different types of businesses and organizations. The Bredolab Trojan was mainly used to attack these individuals and groups through its download management system. It was offered for sale on various hacker forums. According to the Dutch police, the botnet, which was created in mid-2009, had over 30 million users globally. The software that developed the Bredolab botnet was purchased on the dark web. [2]

According to Kaspersky lab, in 2010 the Bredolab Botnet trojan horse attack, attacks the most users who are in USA.

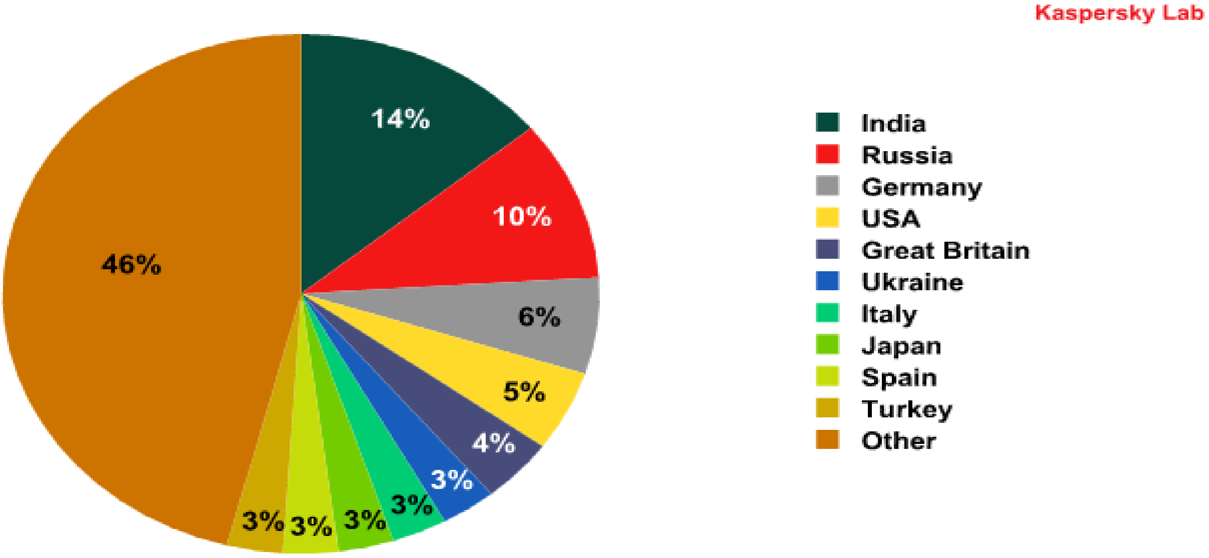


Figure 3 Distribution of Bredolab Botnet in January-October 2010 by nation

3.3 Bredolab Botnet Architecture

The Bredolab botnets are composed of a variety of components, including a dynamic link library and a configuration file. In cybersecurity, this type of activity is referred to as network sniffing. In order to monitor the activity of the attackers, network sniffing involves logging the data collected from outgoing traffic. [1]

It has been revealed that the IP addresses used in the attack came from various dedicated servers, as well as virtual dedicated servers. Further analysis revealed that Port 80, which is used to communicate with popular websites, is also used by these servers. After a certain amount of time, the compromised account details are transferred to the infected website.

Some of the components of the Bredolab botnets are used to access the website's contents. However, not all of them are downloaded from the server. This means that the files that start with index, default, main, and index.js are targeted. These files are then injected with malicious code. [2]

The download and upload operations of the Bredolab botnets are remarkably simple. They can be performed through a variety of IP addresses. Each file is then transferred from one IP address to another.

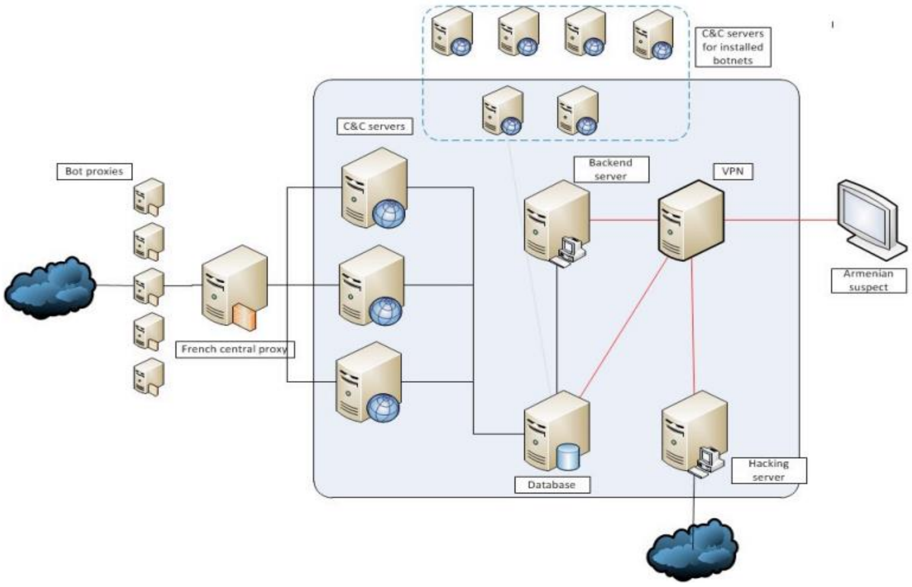


Figure 4 Architecture of Bredolab Botnet

The BredoLab architecture included a central proxy server, a database server, a variety of proxy servers, a personal hacking server, and a VPN server. The blue square shows the servers that were wiretapped, while the red lines represent the traffic generated by the VPN server. The data collected by the wiretap analysis tools showed that the traffic coming from the three C&C server's various components consisted of HTTP and MySQL traffic going to a proxy server in France, as well as the usual traffic from a database server. The VPN server was also used to manage other servers. [2]

3.4 Bredolab Botnet Takedown

In 2010, Leaseweb, a large hosting company in the Netherlands, started a community outreach project called Community Outreach. On October 26, 2010, the Dutch Police received a complaint about a member of the project, Abuse.ch, a non-profit organization that focuses on identifying threats on the Internet. Through this organization, Leaseweb was informed that a large botnet infrastructure was likely to be connected to their network due to the Zeus malware that was distributed by BredoLab. The National High Tech Crime Unit (NHTCU) then conducted wiretaps on 11 servers at Leaseweb to monitor the communication between the bots and the company's network. [4]

The Public Office said that LeaseWeb disabled 143 servers, which were part of a global distribution hub for malware known as Bredolab. Earlier this year, security researchers and hosting providers disabled a number of servers used by the Pushdo bot network to distribute spam and other malware. In March, Microsoft and other security firms took down the Waledec and the Mariposa networks, respectively. The groups that were involved in the operation were able to infiltrate the control structure of the illicit bot networks. In 2010, the Bredolab Botent is takedown and the creator of this botnet Mr. Georg Avanesov was arrested by Dutch Police. [8]

4 Recommendations

- A website's code vulnerabilities can be used to infect it. To minimize the risk of exploitation, regularly update the software updates that are available on your website.
- To prevent unauthorized access to your networks, make sure that all devices are secure. Doing so can include implementing policies such as encrypting web traffic and securing Wi-Fi.
- It's also important to disable autosave for File Transfer Protocol (FTP) clients and accounts. This can help prevent unauthorized individuals from accessing your data. One of the most common ways that hackers can access your accounts is by searching for and extracting the passwords from infected machines.
- Having a backup copy of your website is also important to ensure that it's always safe to use. This can be done by storing a backup of all of your databases and files.
- To avoid re-infection, regularly update the software updates that are available on your website. Doing so can help prevent vulnerabilities from being exploited.
- Using a good antivirus program with up-to-date databases is also recommended.
- A sandbox can be used to analyze and monitor known and unknown attacks. It can also be integrated with a next-generation firewall to enforce multi-factor authentication.

5 Conclusions

After looking into various academic papers and industry reports, I decided to focus on the Bredolab botnet. One of the main features of the operation was its command-and-control center, which made it easier for cybercriminals to manage their malicious content. This feature allowed them to set up multiple redirectors and control their infected computers. Another key feature of the Bredolab operation was its closely repeating cycle, which involved the creation of new zombie networks and the downloading of malicious programs.

6 References

[1] D. D. Graaf, A. F. Shosha, and P. Gladyshev, “BREDOLAB: Shopping in the Cybercrime Underworld.”

[2] “End of the Line for the Bredolab Botnet?” https://securelist.com/end-of-the-line-for-the-bredolab-botnet/36335/ (accessed Aug. 08, 2022).

[3] “BREDOLAB - Threat Encyclopedia.” https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/bredolab (accessed Aug. 08, 2022).

[4] “Bredolab Botnet Crackdown Could Have Wide Impact.” https://threatpost.com/bredolab-botnet-crackdown-could-have-wide-impact-102610/74608/ (accessed Aug. 08, 2022).

[5] “[Malware Review] Trojan.Downloader.Bredolab.CJ,” *Hot for Security*. https://www.bitdefender.com/blog/hotforsecurity/weekly-malware-review-trojan-downloader-bredolab-cj (accessed Aug. 08, 2022).

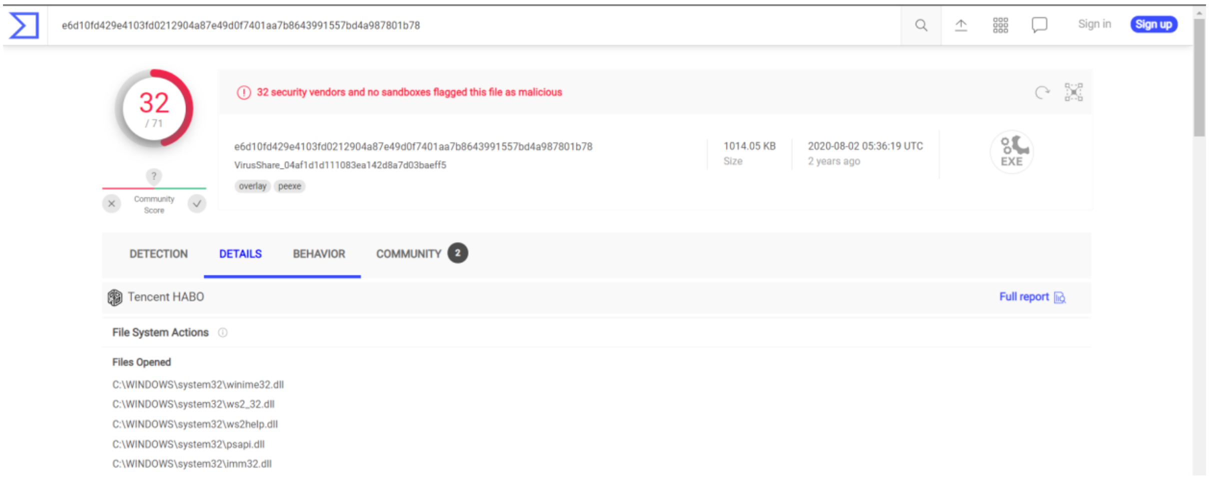
[6] “Dutch police take down Bredolab botnet.” https://www.zdnet.com/article/dutch-police-take-down-bredolab-botnet/ (accessed Aug. 08, 2022).

[7] D. Dittrich, “So You Want to Take Over a Botnet...,” p. 8.

[8] J. Kirk, “Dutch team up with Armenia for Bredolab botnet take down,” *Computerworld*, Oct. 26, 2010. https://www.computerworld.com/article/2513676/dutch-team-up-with-armenia-for-bredolab-botnet-take-down.html (accessed Aug. 08, 2022).

7 Appendix

7.1 Some online analysis reports



e6d10fd429e4103fd0212904a87e49d0f7401aa7b8643991557bd4a987801b78

32 security vendors and no sandboxes flagged this file as malicious

e6d10fd429e4103fd0212904a87e49d0f7401aa7b8643991557bd4a987801b78
VirusShare_04af1d1d111083ea142d8a7d03baeff5
overlay peexe

1014.05 KB
Size

2020-08-02 05:36:19 UTC
2 years ago

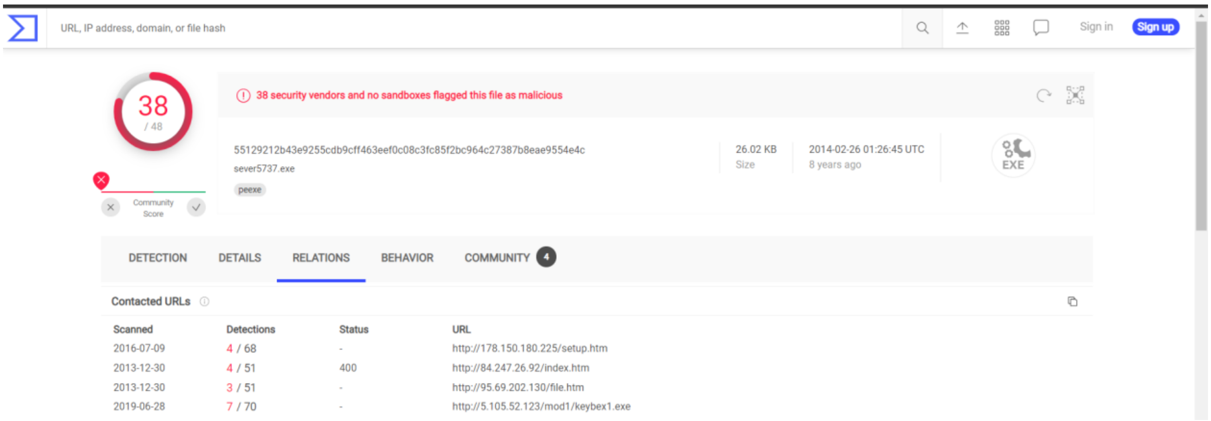
Tencent HABO

File System Actions

Files Opened

C:\WINDOWS\system32\winime32.dll
C:\WINDOWS\system32\ws2_32.dll
C:\WINDOWS\system32\ws2help.dll
C:\WINDOWS\system32\psapi.dll
C:\WINDOWS\system32\imm32.dll

Figure 5 Virustotal report with files affected



38 security vendors and no sandboxes flagged this file as malicious

55129212b43e9255cdb9cff463eef0c08c3fc85f2bc964c27387b8eae9554e4c
sever5737.exe
peexe

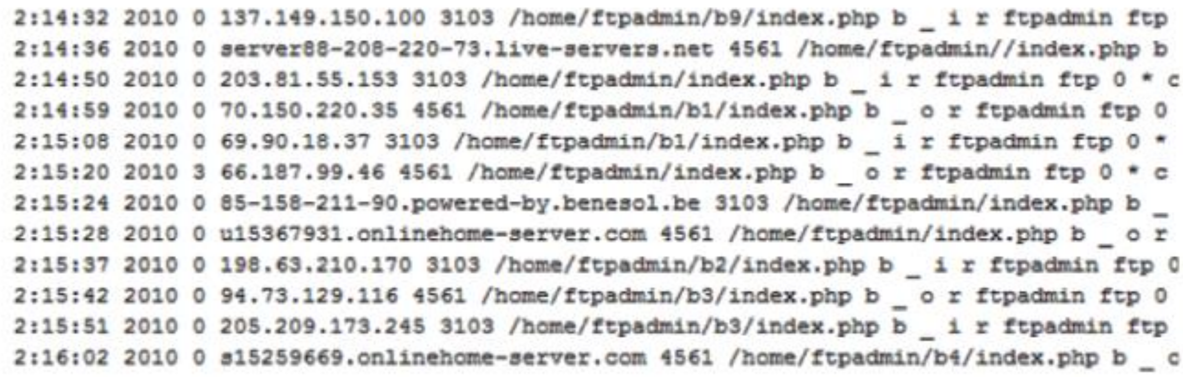
26.02 KB
Size

2014-02-26 01:26:45 UTC
8 years ago

Contacted URLs

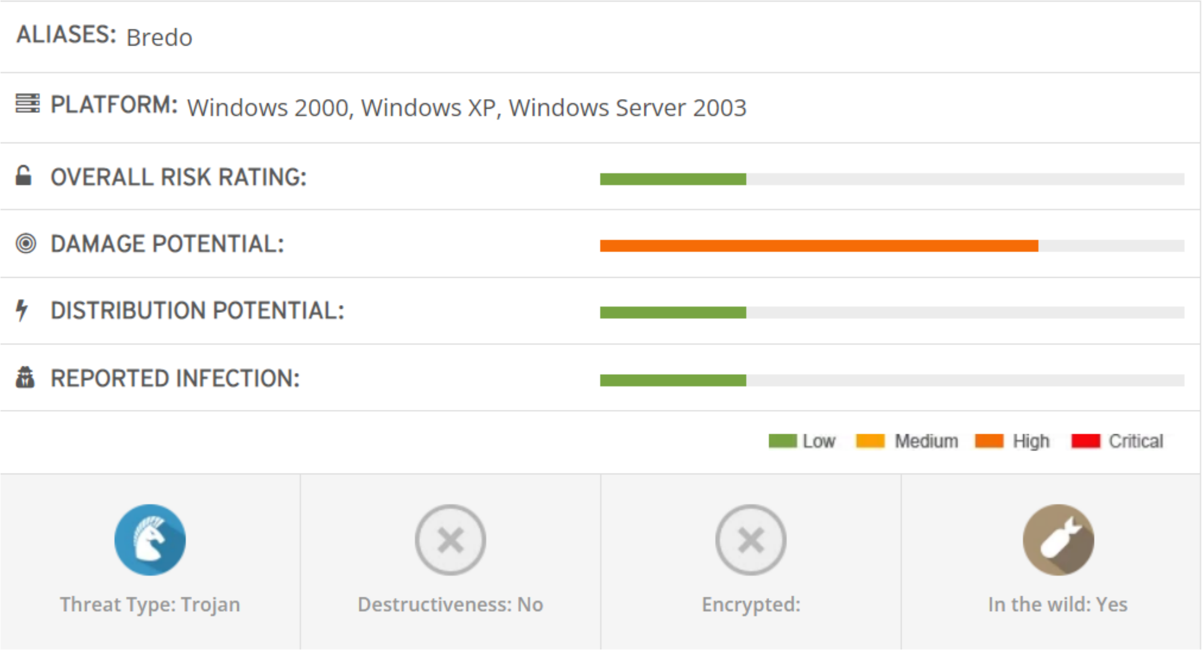
Scanned	Detections	Status	URL
2016-07-09	4 / 68	-	http://178.150.180.225/setup.htm
2013-12-30	4 / 51	400	http://84.247.26.92/index.htm
2013-12-30	3 / 51	-	http://95.69.202.130/file.htm
2019-06-28	7 / 70	-	http://5.105.52.123/mod1/keybex1.exe

Figure 6 Report with some of files embedded in the link



```
2:14:32 2010 0 137.149.150.100 3103 /home/ftpadmin/b9/index.php b _ i r ftpadmin ftp
2:14:36 2010 0 server88-208-220-73.live-servers.net 4561 /home/ftpadmin//index.php b
2:14:50 2010 0 203.81.55.153 3103 /home/ftpadmin/index.php b _ i r ftpadmin ftp 0 * c
2:14:59 2010 0 70.150.220.35 4561 /home/ftpadmin/b1/index.php b _ o r ftpadmin ftp 0
2:15:08 2010 0 69.90.18.37 3103 /home/ftpadmin/b1/index.php b _ i r ftpadmin ftp 0 *
2:15:20 2010 3 66.187.99.46 4561 /home/ftpadmin/index.php b _ o r ftpadmin ftp 0 * c
2:15:24 2010 0 85-158-211-90.powered-by.benesol.be 3103 /home/ftpadmin/index.php b _
2:15:28 2010 0 u15367931.onlinehome-server.com 4561 /home/ftpadmin/index.php b _ o r
2:15:37 2010 0 198.63.210.170 3103 /home/ftpadmin/b2/index.php b _ i r ftpadmin ftp 0
2:15:42 2010 0 94.73.129.116 4561 /home/ftpadmin/b3/index.php b _ o r ftpadmin ftp 0
2:15:51 2010 0 205.209.173.245 3103 /home/ftpadmin/b3/index.php b _ i r ftpadmin ftp
2:16:02 2010 0 s15259669.onlinehome-server.com 4561 /home/ftpadmin/b4/index.php b _ c
```

Figure 7 A fragment of FTP log from Internet



ALIASES: Bredo

PLATFORM: Windows 2000, Windows XP, Windows Server 2003

OVERALL RISK RATING:

DAMAGE POTENTIAL:

DISTRIBUTION POTENTIAL:

REPORTED INFECTION:

🟩 Low 🟨 Medium 🟧 High 🟥 Critical

Threat Type: Trojan

Destructiveness: No

Encrypted:

In the wild: Yes

Figure 8 Threat micro analysis report