Sri Lanka Institute of Information Technology

Zeus Bot

Individual Assignment

IE2022 – Introduction to Cyber Security

Submitted by:

Student Registration Number	Student Name
IT20627928	H. M. T. D. Herath

Date of Submission - 2021.11.04

Table of Contents

Abstract

We live in a world where nothing is really safe. Spontaneous cyber-attacks have become a larger concern during the previous decade. The days of a bunch of guys barging into a bank with weapons and knives and robbing bank are long gone. Humans have become intelligent, brilliant they can steal our money secretly by using web. To view what is happening in real time and preserve that information for later use, a flexible network monitoring system is required. If nothing is done now to combat cybercrime, one can only speculate on what world may become in the future.

Zeus, called as Zbot,it is widely-used for stealing information.It can also consider as the king of the botnets in the modern world.It is mainly focused on stealing financial information. It's quality has resulted to the loss of billions worldwide(4). As a result of that, the reputations of respected firms have been ruined. A large spread The widespread usage of the internet, along with the widespread use of E-commerce procedures, provides a powerful incentive for attackers to shift their aims from amusement to financial gain. We will explore the various components of the Zeus botnet like its functions, components, setup, detection and removal of zeus and future

work in the zeus world. The goal of this study project is to reverse engineering hackers techniques by discovering vulnerabilities to understand how we can better defend our systems from cyber threats today.

Introduction to the topic

In the modern world with the development of the technology banks now allow customers to access their accounts over the Internet. Online services decrease the need of costly retail stores and paper transactions. Mobile platforms have created new apps for online banking, but this means that financial services are now vulnerable to new types of online attacks. Today's battleground is cyberspace. People are terrified because they have seen the impact of cyber warfare and are much more afraid of what it has the potential to do in the future. Hackers have found that the majority of the money they're chasing isn't kept in steel vaults, but rather on the internet.

Botnets are currently one of the most severe cyber security concerns. The word "botnet" refers to a network of infected devices, which are coordinated for malicious purposes, control by the human operator called botmaster.Every computer in a botnet is known as a bot. Bots are used to spread malware and spam, as well as to conduct attacks against systems and devices. DoS attacks, spam distribution, phishing, and click fraud are just a few examples. Botnets of today include functionalities like P2P architecture and encrypted traffic. Botnets utilize a variety of protocols, stealth methods, and social networking websites to propagate.3ve,Mirai,methbot,mariposa ,pushdo, kraken, grum, cutwail storm, srizbi, earthlink spammer, conficker and zeus are some botnets on the world.(1)

ZeuS is one of the most well-known botnet nowadays, with the primary goal of gaining financial benefit. Zeus is started in Russia or Eastern Europe and now become a commodity in the cybercriminal world. Zeus is also named as Zbot, Gorhax ,PRG, Kneber and WSNpoem. Zeus mainly affect Microsoft Windows XP (SP2/SP3) computers. infected Windows Vista PCs have also been found. Zeus use Techniques such as keystroke recording, snapshot capturing.When computer system affected by this trojan ,keys that press on keyboard will be captured and

recorded. Also capable of doing web injects, which is inserting additional html codes into web sites in order to instructed the user into providing their sensitive information , which are not normally needed by the website. Zeus also can set a variety of online adds when we browsing the internet.so then it can redirect web browser to fake websites. So this is very dangerous because cyber criminals can use zeus steal bank login credentials, bank card numbers, usernames, passwords, and other sensitive data. The primary goal is to steal online banking information as well as other login credentials. However various kind of data theft by this.

Zeus includes a control panel that is used to keep track and update fixes to the botnet, it is created using mysql and php.It also includes a tool known as a builder, which enables for the development of executables that are used to corrupt user systems(4). Zeus collects a wide range of system data, as well as passwords and encryption certificates and These are sent to a command and control server. Then A configuration file can be sent from the server to the bot stating a set of tasks to be completed. The zeus virus mainly infected user systems using two methods. they are spam messages and drive-by downloads. Zeus Trojan transmitted via malicious email attachments or downloads hidden in free games, apps, movies, or greeting cards.

The cyber criminals sent the emails to a large number of people while concealing their identity by using well-known aliases like organizations such as banks and social networking sites. As a result of seeing that popular names, people are more likely to open these emails. Then they're informed that there's a big issue with their account. Users are guided to click on the link included in the email to resolve the problem. When click on the link, the Zeus infection is started. After infiltrating victim computer, the Zeus malware employs stealth tactics to conceal itself. so that our normal antivirus software doesn't recognize it up. Now it begins to operate according to the configuration file that the botmaster has entered. Maker instructed it to what type of data should be captured. It is entirely up to the maker's decision if they want your personal and system details or your bank login information. So zeus can consider as a generic back door that gives full administration to outsider. Because of the impact of this zeus victim computer will often slow down.

A Trojan scanner is one of best method to find out whether you've been infected. Bugat, Neutrino, Ice IX, Torpig, Panda banker, Gameover Carberp, , Shylock, Citadel, Atmos, Sphinx, and SpyEye are some of the Zeus based Trojans. Users can purchase Zeus as a commercial

product from underground marketplaces and simply set up their own botnet. It is estimated that the best versions will cost over $600.Botnets based on Zeus are still in the top ten botnet list.

Evolution of the topic

ZeuS was created by Hamza Bendelladj, he is called as Bx1 online.

- In july 2007, it was first founded when it was stole data from the US Department of Transportation.
- In March 2009, it grew increasingly prevalent.
- According to the data report of the security organization called ‘prevx’,in june 2009,zeus has hijacked over 73,000 FTP accounts on the websites of organizationes including nasa , abc, oracle, play.com, cisco, bank of America and amazon.
- The Zeus trojan infected approximately 154,000 computers in the USA, with Japan, Canada, England, Australia, Netherland , Germany, Russia, India and Italy again in 2009.
- Zeus was affiliated with the "Rock Phish" cyber-threat organization, which targets financial institutions all around the world.(12)
- To propagate ZeuS, about 1.5 million phishing messages were posted on Facebook on October 28, 2009.
- On July 14, 2010, the security company Trusteer released a report claiming that more than 15 unidentified US banks' credit cards had been hacked because ot this Trojan.
- On October 1, 2010,the FBI reported a large international criminal network that had utilized Zeus to break US systems and steal nearly $70 million.
- Floki bot malware is designed using the source code of the Zeus trojan, according to a study released by Flashpoint and Cisco Talos. The code of floki bot was leaked in May 2011. So then researchers could find about the inner workings of one of the most contemporary botnets of current time. This allowing hackers to utilize the methods employed by ZeuS and create new bots.
- Kaspersky Labs discovered five new versions of the zeus trojan affecting Blackberry and Android phones in 2012.

- The Citadel virus was created using Zeus code in 2013.
- In 2016, researchers identified the Atmos virus, which targeted France banks, and discovered that it is a component of the Zeus trojan.
- Trojan.Bolik.1used zeus web injection to steal bank credentials of Russian banks in June 2016.
- In June 2016, users' credentials were targeted by a phishing effort disguised as a FedEx delivery notice. Malicious PDF attachments were included in the phishing emails. When the infected attachment was opened, Fareit malware and the Zeus trojan were activated.
- In 2016, a new Zeus malware version known as ‘Panda Banker' was discovered, which attacking online financial services in Netherland, North America, the United Kingdom, Canada, Europe, Poland, Germany, and the United States. Digital wallets, card payments, internet gambling accounts, and other services are targeted by Zeus Panda.
- Panda began attacking Brazilian banks and other online financial systems of boleto July 2016. Local police websites, computer security hardware suppliers, and Brazilian e-commerce rewards programs and transactions were also attacked.
- A phishing effort that posing as a tax notice from the canada tax office targeted users' banking credentials in October 2016. A malicious MSG file attachment was included in the phishing emails, it install the Terdot downloader, which release the Zeus virus to the user systems.
- In may 2017 users get web notice that informed "The HoeflerText font was not found" and need to keep latest update of the "Mozilla Font bundle." The Zeus malware is launched when click the ‘Update' option appears on the screen to update the Mozzila font bundle.
- Another version of Zeus, called ‘Neutrino,' was discovered in July 2017 stealing credit card details of Point-of-Sale networks. Downloading data, capturing screenshots, finding processes by names, altering register branches, searching for items by infected host names, and executing proxy commands are only some of Zeus Neutrino's features.(16)
- During the 2017 Christmas period, Zeus Panda attacked online stores for credit card details.
- Analyzers noticed Zeus Panda's three activities in May 2018. The initial effort was aimed at bitcoin exchanges.

- Amazon, Facebook, Twitter, Instagram, MSN, Bing.com, YouTube, Flickr, Microsoft, Gmail, Yahoo, and Japanese pornographic sites were targeted in the second effort. Wells Fargo and CitiBank were the financial institutions targeted in the third effort, which took place in the United States and Canada.(18)
- In november 2018 zeus panda was spread through the Emotet financial malware distribution network, targeting systems in the japan, Canada, and united states. Its main aim was steal credit card information, bank account details, and ewallet credentials.
- The greatest Trojan of all time, Zbot, was named malware of the month in November 2019.

Components of zeus malware tool

The Zeus malware toolkit is a collection of programs for building up a botnet on a large-scale networked infrastructure. The Zeus botnet's primary goal is to making systems act like spies with the goal of gaining financial advantages. Zeus is a virus that has the capability to logging user inputs as well as capturing and storing data and change the data that is shown on web sites.

The Zeus crimeware toolset is made up with five parts.

1. Control panel (server)

   Includes a group of php scripts for monitoring the botnet, gather stolen data into a mysql database, and delivering it to the botmaster.Also it enables the botmaster to keep in touch of controls, and manage bots that are part of the botnet.The Zeus Server is also very easy to set up. A cybercriminal just copies the Web server data to his or her computer and

searches for setup and fills in some very basic parameters. This server will gather all of information that zeus steal once it is set up. It also includes a number of additional capabilities, like counting how many infected systems there are (depending on Operating system, geographic area, and other factors) and executing programs on infected computers.

2. Configuration file

   used to tweak the botnet's settings It consists of two files,config.txt,that contains the basic data, and webinjects.txt, which identifies the attacked webpages and specifies the content injection principles. A very flexible, all around configuration file is used to build all of the Zeus botnets. This file includes information such as the name of the botnet, the times when stolen data will be sent back, and the server that virus should infect. It includes a list of banks that Zeus should attack. Zeus can not collect all of the banking login usernames and passwords that users input, but it can inject additional form sections straight into the users' banking webpage screen.

3. Encrypted config file

   config.bin, which includes an encrypted version of the botnet's configuration settings. All Zeus bots must contact home and obtain the encrypted configuration file to check whether new orders have arrived, which making security analysts' work more complex. Encrypted configuration file tells nothing if the researcher cannot obtain the encryption key from the associated Zeus binary file.

   Criminals that use Zeus currently gain the encrypted configuration file as well as the Zeus binary file they generated with Zeus Builder and keep those on a Web server. Zeus enables every component to be put on detached Web servers or to be put on the same Web server.

4. Binary file

bot.exe,the bot binary file that infects the target computer. When the binary infects a user's machine, it will update its configuration settings and start capturing the user's personally identifying details. The “Build loader” key can be used to create the executable. Before packaging the Zbot binary with its own proprietary run-time packer, the Builder will insert the data required to access and decrypt the configuration file.

5. Zeus builder

   One of the most important components of the Zeus toolkit is Zeus Builder. Generate the botnet's binary file and also the configuration file that contains all of the botnet's parameters. When a criminal launches Zeus Builder for the first time, open a window that displays details about the Zeus version they bought. Also scans, machine is already infected by the Zeus virus, and then giving option to remove it.

How create a Zeus Trojan Botnet

- First both of the web server and database server must be installed. Install xampp on Windows computer because we need it to set up the Zeus botnet. Then ensure that the MySQL services and xampp apache are up and working.

- Then type http://localhost/phpmyadmin in the address bar of the web browser. Insert the login details, root is the username by default, don’t type a password keep it empty. Then create a new database and give a name to it as you like, I name it as Zeus. The remote administration tool will be installed using that database name.

- Now download and unpack the remote administration tool zip file, which has three folders: builder, other, and server[php].inside C:\xampp\htdocs ,make a new folder & name it as you like, I name it as zeus. then transfer the content of server[php] to the created folder, C:\xampp\htdocs\zeus (9)

- Return to web browser and type http://localhost/zeus/install in the url bar. Fill all required details with accurate data.

Mysql's host address is set with database server's ip address. It should be ip address if we are using xampp.

The database should contains with details about the database name we established in second step.

Fill the encryption key with any digits ranging in length from 1 to 255.

To begin the installation process, click Install.

Error – failed connect to mysql server.host 'myusername' is not allowed to connect to this mysql server. If you receive a error like this, you must complete the steps below.

Click the Privileges tab in PHPMyAdmin (http://localhost/phpmyadmin). To change the root user's rights, click the edit button.

Scroll down to the login details area on the edit user page. Press the Go button after switching the Host from localhost to Any host.

- Now zeus administration tool installed correctly.

- Then we need to zeus bot client configuration and creation. Go to the config.txt configuration file in the builder folder. According to your setting Customize the url server, url loader, and url config configurations.

- Then open zeus builder exe and build the botnet configuration and bot executable.

- config.bin and bot.exe files are now available. These two files should be placed into the htdocs folder. Mine was located at C:\xampp\htdocs\zeus.

- Now if we transmit the bot.exe to the target We can scan our attacker server once the target executes the file. Type http://localhost/bot/cp.php in your browser and enter your login details.

- Now In the graphical interface, we can see the infected target and snapshot of the target's desktop.

- Now we successfully setup a zeus botnet. Because this program behave as a key logger and capture the login details, the attacker can collect a lot of details from the target, such as all online activities and website login details.

How it works

The bot is performed, the following events take place(5)

- It copies itself to sdra64.exe in the system32 folder.

- It changes earlier path to hkey local machine\software\Microsoft\Windowsnt\winlogon\userinit because of that winlogon.exe starts the process at begining.

- It searches for winlogon.exe, elevates its capabilities, inserts its code and a string table into the process, and establishes a thread to run the code.

- The primary bot executable terminates.

- Additional code is injected into svchost.exe by the injected code in winlogon.

- It also makes a subdirectory called %system% lowsec, which contains two files, local.ds and user.ds.

- The most recent dynamic configuration file obtained from the server is Local.ds.

- User.ds is a file that includes stolen credentials and other data that has to be sent to the server.

- The svchost code is in charge of network communication and third-party process injection, which is required to connect Intemet-related APIs in order to insert or get data from banking sites.

- Mutexes and pipes called AVIRA u,u is a number (e.g., u=1850 in winlogon.exe, u=1849 in svchost.exe), are used to communicate between the various injected components.

- When Zeus is launched with a user account that does not have Administrator rights, code is injected into explorer.exe,but it is not injected in to winlogon.exe. Also, instead of copying itself to the %System% folder. the bot will copy itself to %User Profile%\Application Data\sdra64.exe and make the folder %User Profile%\Application Data\lowsec.

- At last, the bot will generate a load point HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"userinit"="%UserProfile%\Application Data\sdra64.exe" in the registry.

Zeus functions

The bot will collect data from a local network, such as a company network. Zeus carry out four main operations.

1. First Its primary aim is to collect all of the data from the computer, including passwords of websites including email, financial, and social media. It gathers data via a variety of methods, including redirection

2. The bot will be integrated into the major botnet and will be given instructions to carry out DoS and mass spam attacks.

3. When a target visits a attacked website, the bot takes the target's login information. After that, it sends the encrypted data to a drop destination where the bot update records are kept, called C&C server. The stolen details is decrypted and stored into database by this server.

4. to phishing websites

Impact of the zeus

It's tough to find, we have been infected with the Zeus virus. It operates invisibly. To detect the Zeus malware, keep a careful eye on the computer(10).

- Users may sometimes see text boxes on the start screen that are not usually visible.
- The Zeus malware redirect you to harmful websites.
- personal email and social media accounts and bank accounts can be hacked.
- By adding additional text fields to the start screen, it gathers private details.
- for example, it can provide an additional field for you to input your birth date when login, something the bank did not ask for.
- The attacker has complete control over victims computer, including the ability to download and destroy victim data.

- Zeus may cause your computer to restart or shut down, as well as damage the operating system.
- Can see new softwares and applications with out installing them.
- Overloaded hard disk.
- With out doing many tasks, but the fan produces a noise and show that working hard.
- Received many emails from unknown users and sites.
- Web browsers responding getting very slow and also redirect to many sites that don’t request.
- Antivirus software or firewalls aren't working properly.
- Softwares will not working.
- Lost of internet connection.

Zeus Detection and removal

Even using latest update antivirus software, zeus is very tough to recognize. Because of this factor Zeus malware family is regarded as the internet's biggest botnet. Security professionals provide coaching to individuals and companies to protect the system from clicking on malicious email links on the internet & how we can mitigate this Trojan malware. There are several practical actions to protect computers from Zeus. If you sense your machine has been infected, attempt the methods below to remove the Trojan from computer.(20)

- Start the computer in safe mode.

  Remove the system's connection to the Internet. Zeus will not operate in Safe Mode, so this will restrict Zeus from spreading over the files. Continue pressing the F8 button until display the 'Advanced Boot Options' 'Safe Mode with Networking' should be selected. Then Press the Enter key.

- Clear the cache and temporary files.

Before starting a virus scan, delete all temporary data and storage cache. This will boost the checking speed, free up memory space, and in certain cases, remove viruses. To utilize the 'Disk Cleanup' app, go to search bar and type disk cleanup(11). Then you can open Disk Cleanup tool and clear cache files. using %temp% , temp , prefetch commands we can delete hidden temporary files. This action isn't necessary, but it is beneficial.

- Download and run best virus guard.
- Troubleshoot web browser,

Virus may change your browser's configuration and show pop-ups and ads in order to reinfect machine. Before you start your browser, check the connection and homepage configurations. Click 'Control Panel' from the Start menu, then select Internet Options. Before you start your browser, check the connection and homepage settings. Click 'Control Panel' from the Start menu, then select 'Internet Options.' Ensure that the 'Home Page' configuration is set to a website you are familiar with. Select the 'LAN Settings' box from the 'Connections' menu. Also Select 'Automatically Detect Settings' from the drop-down menu. Keep the browser updated.

- Keep the real time protection on.
- Spam emails should note be followed.
- Examine the Trustworthiness of Confidential Login Pages
- Don't go to websites that aren't trustworthy.

By doing these actions we can successfully remove Zeus from victim system.

Future developments in the area

Zeus is now using Adobe Reader features to conduct malicious assaults. Zeus 1.6, the most recent version on the market, is designed to target Firefox Web browser. Zeus is now utilizing

social media websites to carry out its phishing messages to people, as a result of the global growth of social networking. It sent almost 1.5 million emails to Facebook users last year. If a person clicked on the link in the mail, a Trojan would be installed on their computer.

concentrate on designing a solution that can prevent the Zeus botnet from infecting and infiltrating computer networks and the internet. These methods aren't set in stone for future bots, because new advancements in Internet and IT technology, make botnet creation more successful and spread quicker and simpler than ever before.

For example, social media platforms like Facebook, Twitter, and others have allowed botnet creators greater leeway in terms of improvements and quicker botnet propagation.

In today's fast-paced IT world, mobile devices such as HTC, iPhones, and Blackberry are being used to access the Internet. As a result, more people are using the Internet, and more operating systems are being utilized. Botnets have so far targeted the Windows operating system, taking use of the operating system's flaws. The use of additional operating systems has given a large number of options for identifying the flaws in various operating systems. As a result, future botnets will operate on a variety of operating systems and mobile phones using superb techniques.

Conclusion

In modern world, network security is a rising issue. The Zeus bot and its botnets have been more popular in the past two or three years, and their widespread distribution in computer networks and the internet makes them very hazardous, now it is the world's biggest financial botnet in the world. Cybercriminals are using Zeus to steal financial details and even people's personal data. Because Zeus is so simple to use, even a novice hacker can quickly steal online banking and other information for financial gain. This is due to the large number of toolkit versions that are easily accessible, as well as the capabilities that it has to resist antivirus programs.

We can protect our systems if the necessary controls are in place. Zeus's strength can be thwarted. Zeus can beatable, and many users are taking actions to prevent and not been infected. The success of Zeus demonstrates that this kind of malware, whether in the form of Zeus or its rivals, is only going to grow in popularity. Clearly, there is a huge demand for simple to use data stealing Trojans, and as long as there is a need, someone will be ready to provide it.

End!

References

(1) "Zeus (malware) from Wikipedia, the free encyclopedia" [online] , https://en.wikipedia.org/wiki/Zeus_(malware)

(2) "Zeus virus" [online] , https://usa.kaspersky.com/resource-center/threats/zeus-virus

(3) "The life and death of the ZeuS Trojan" [online] , https://blog.malwarebytes.com/101/2021/07/the-life-and-death-of-the-zeus-trojan/

(4) "Zeus Trojan – What it is & How to Prevent it | Digital Defense" [online] , https://www.digitaldefense.com/blog/zeus-trojan-what-it-is-how-to-prevent-it-digital-defense/

(5) "The Zeus Trojan: What it is , How it Works , and How to Stay Safe" [online] , https://www.avast.com/c-zeus

(6) "Zeus Banking Trojan Report" [online] , https://www.secureworks.com/research/zeus

(7) "Zeus Trojan (Zbot)" [online] , https://www.hypr.com/zeus-trojan-zbot/

(8) "Zeus Trojan Analysis Published by Alex Kirk" [online] , https://talosintelligence.com/zeus_trojan

(9) "Zeus_2.1.0.1" Trojan tool , https://mega.nz/folder/1ccgAYbB#p1IAycx0GgNcGjzCfIIYpA

(10) "Threat Spotlight: ZeuS (aka Zbot) Infostealer Trojan" [online ,]https://blogs.blackberry.com/en/2020/04/threat-spotlight-zeus-infostealer-trojan

(11) "What is Zeus Trojan Malware By Comodo" [online] , https://enterprise.comodo.com/blog/what-is-zeus-malware/

(12) "Zeus Malware: Variants,Methods and History" [online] , https://www.cynet.com/network-attacks/zeus-malware-variants-methods-and-history/

(13) "Trojan – Spy:W32/zbot" [online] , https://www.f-secure.com/v-descs/trojan-spy_w32_zbot.shtml

(14) "Zeus/Zbot" [online] , https://community.jisc.ac.uk/library/janet-services-documentation/zeuszbot

(15) "Zeus Trojan Remover" [online] , https://www.bullguard.com/zh-tw/bullguard-security-center/pc-security/computer-security-resources/zeus_trojan_removal.aspx

(16) "Zeus Botnet Eurograbber Steals $47 Million" [online] , https://www.darkreading.com/attacks-breaches/zeus-botnet-eurograbber-steals-47-million

(17) "Botnets Unearthed – The ZEUS BOT" [online] , https://resources.infosecinstitute.com/topic/botnets-unearthed-the-zeus-bot/

(18) "Zeus Botnet News" [online] , https://www.wired.com/2010/10/zeus-botnet-news/

(19) "Zeus botnet Trojan horse is back" [online] , https://en.wikinews.org/wiki/Zeus_botnet_trojan_horse_is_back

(20) "Zeus Malware (and modern variants) what it is and how to prevent it" [online] , https://www.ryadel.com/en/zeus-malware-what-how-prevent/