International Journal of Information Technology and Business Management

29th October 2012. Vol.6 No.1

ISSN 2304-0777 www.jitbm.com

Detection of Zeus Botnet in Computers Networks and Internet

Dr.Laheeb M. Ibrahim
Assistant Professor

Karam Hatim Thanoon
Assistant Lecturer/ PhD. Student

Dept. of Software Engineering, College of Computer Sciences and Mathematical, University of Mosul

Abstract

Huge spread use of internet with wide scale spread of E-commerce processes becomes a great motivation for the attackers to move their goals from fun to finical profits.

Attackers tend to use botnets which is a group of computers managed by botmaster to perform malicious activities which are criminal jobs. One of the most popular botnet is Zeus, which its main objective is to steal banking accounts for finical profit, so it is called "king of botnet".

In this research infection process of Zeus botnet is implemented on computer networks and internet, in this research, the main objective is to design and implement a system has the ability to detect Zeus bot in user's computers. Future work focus into design a system has the ability to prevent Zeus botnet from infect and penetrate computers networks and internet.

Keywords: Botnet, zeus, detection, financial, malware, Zbot.

1. Introduction

Botnets are nowadays one of the most serious threats to cyber security. The term botnet is used to define a network of infected machines, called bots, which are under the control of a human operator commonly known as botmaster. Bots are used to carry out a wide variety of malicious and harmful actions against systems and services such as DoS attacks, spam distribution, phishing and click fraud, among others. As an example of the relevance of botnets deployment, the FBI (Federal Bureau of Investigation) has recently uncovered more than $20 million in economic losses in the USA. In one case, a victim confirmed damages of nearly $20,000 due to denial of service attacks committed from botnets [5].

Zeus is perhaps the most commonly encountered and easily accessible botnet DIY construction kit. It is used for an incredibly broad range of crimes – ranging from banking credential theft to back-dooring new equipment and long-term infiltration of industrial systems[3].

Zeus is known by many names (ZBOT due to its botnet capabilities, WSNPoem , PRG, and others—but its use has been particularly criminal [7].

Zeus is the name of a toolkit used to create a particular strain of information stealing Trojans. The bots created by the kit run silently in the background on compromised computers, harvesting information and sending it back to the botherder. The main focus is to steal online banking details and other login credentials but the range of different types of data theft is extremely broad [10]. The Zeus-based botnet led the Top 10 – dominating 19% of botnet infections for the year. For the first quarter of 2010, the Zeus-based botnet persisted, Zeus-based botnet which attained third position in our 2010 Top 10 largest botnets and still until now the top ten of botnet list. [3]

Zeus uses some rootkit techniques to evade detection and removal. Zeus is the #1 botnet, with 3.6 million PCs infected in the US alone

International Journal of Information Technology and Business Management

29th October 2012. Vol.6 No.1

ISSN 2304-0777 www.jitbm.com

(approximately 1% of the PCs in the US. As can be seen in figure 1 which explain financial malware relative distribution [8].

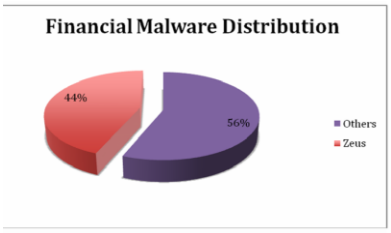


Figure 1: Financial Malware distribution[8]

In this research an automated system is designed to detect a zeus botnet, after study carefully the zeus bot life cycle , and study the infection process and implement it and work and implement a software that has the ability to detect zeus bot in computer networks and internet.

2. Zeus History

Zeus is a Trojan horse that steals banking information by keystroke logging and Form Grabbing. Zeus is spread mainly through drive-by downloads and phishing schemes. First identified in July 2007 when it was used to steal information from the United States Department of Transportation, it became more widespread in March 2009. In June 2009, security company Prevx discovered that Zeus had compromised over 74,000 FTP accounts on websites of such companies as the Bank of America, NASA, Monster, ABC, Oracle, Play.com, Cisco, Amazon, and BusinessWeek [9].

It was still active in 2010. On July 14, 2010, security firm Trusteer filed a report, which says that the credit cards of more than 15 unnamed US banks have been compromised. On October 1, 2010, FBI announced it had discovered a major international cybercrime network which had used Zeus to hack into US computers and steal around $70m. More than 90 suspected members of the ring were arrested in the US, and arrests were also made in UK and Ukraine. In May 2011, the then-current version of Zeus's source code was leaked.[9]

3. What is Zeus and Why Zeus?

Zeus is primarily a crimeware kit designed to steal users' online banking login credentials, among other things. It is the handiwork of Eastern European organized criminals that has now entered the underground cybercriminal market as a commodity. The principal perpetrators behind the Zeus botnet are in Eastern Europe, particularly in the Ukraine and Russia. However, the recent availability of the Zeus Builder toolkit in the open market has muddied the waters on attributing crimes to any one individual or group. That said, there is definitively a difference between "professional" criminals and "amateurs." The professional, organized crime syndicates also have other business connections, which they leverage to perpetrate their crimes and move their money.[7]

In short, Zeus is two things:

• From a technical perspective, it is a crimeware tool primarily used to steal money.

• From another perspective, it signals a new wave in online criminal business enterprise wherein many different organizations cooperate with one another to perpetrate outright online theft and fraud, figure 2 shows how a typical Zeus infection takes place[7].

29th October 2012. Vol.6 No.1

ISSN 2304-0777 www.jitbm.com

Figure 2: Zeus infection process[7]

Zeus has become the most popular crimeware kit in the criminal underground for wholesale monetary theft. In fact, the sophistication cybercriminal operations use can be seen in their ability to also recruit money mules to move their stolen money around through bogus work-from-home scams. The cybercriminals know that given the current economic situation in the United States—with millions of people out of work—they will have a high success rate in recruiting unwitting accomplices [7].

Antivirus industry see huge numbers of Zbot samples that seem to bear no relation to each other, as each botnet owner packs and obfuscates their samples in different ways. Some of these self-contained botnets have been hugely successful with stories in the press of some operations managing to steal hundreds of millions of dollars [10].

When talking about why Zeus?, The answer found in Damballa which is a US company that protects, detects and removes botnets for enterprise businesses. They have published the ten top botnets that they have encountered in 2009 as shown in Figure 3 [6].

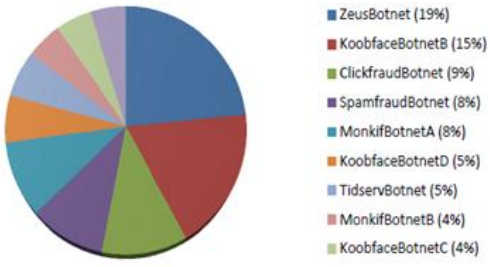


Figure 3: top botnet in 2009 [6]

4. Zeus life cycle

The general lifecycle of a bot can be split into 4 different operations or weeks. In the first week infection of the computer is attempted. Its main goal is to gather all the information it can from the computer; information such as passwords for websites including email, banking and social networking. It uses various means for collecting information such as redirecting to phishing websites. In Week 2, the bot will gather information about a local network such as a corporate network. In Week 3, the bot attempts to spread by, for example, sending spam email to the users' address book, messages via Instant Messaging (IM) or through social networking websites. In week 4, the bot will integrate into the main botnet and will receive commands to perform Denial of Service attacks and mass spamming. [6]

When a victim visits a targeted site, the bot steals the credentials that are entered by the victim. Afterward, it posts the encrypted information to a drop location that is meant to store the bot update reports. This server decrypts the stolen information and stores it into a database.[2]

5. Zeus functions

The main purpose of Zeus is to steal online credentials as specified by the hacker. Zeus performs four main actions:

- Gathering system information.
- Stealing protected storage information, FTP passwords, and POP3 passwords.
- Stealing online credential information as specified by a configuration file.
- Contacting the command and control server for additional tasks to perform.[4]

In very general terms Zeus performs the following actions:

- Copy itself to another location, execute the copy, delete the original.
- Lower browser security settings by changing IE registry entries.
- Injects code into other processes, main process exits.
- Injected code hooks apis in each process.
- Steals several different type of credential found on the system.
- Downloads config file and processes it
- Uses api hooks to steal data.

International Journal of Information Technology and Business Management

29th October 2012. Vol.6 No.1

ISSN 2304-0777 www.jitbm.com

- Sends data back to C&C. [10]

6. Components of Zeus

The Zeus crimeware toolkit is a set of programs which have been designed to setup a botnet over a high-scaled networked infrastructure. Generally, the Zeus botnet aims to make machines behave as spying agents with the intent of getting financial benefits. The Zeus malware has the ability to log inputs that are entered by the user as well as to capture and alter data that are displayed into web-pages. Stolen data can contain email addresses, passwords, online banking accounts, credit card numbers, and transaction authentication numbers.The overall structure of the Zeus crimeware toolkit consists of five components:[2]

1) A control panel which contains a set of PHP scripts that are used to monitor the botnet and collect the stolen information into MySQL database and then display it to the botmaster. It also allows the botmaster to monitor, control, and manage bots that are registered within the botnet.

2) Configuration files that are used to customize the botnet parameters. It involves two files: the configuration file config.txt that lists the basic information, and the web injects file webinjects.txt that identifies the targeted websites and defines the content injection rules.

3) A generated encrypted configuration file config.bin, which holds an encrypted version of the configuration parameters of the botnet.

4) A generated malware binary file bot.exe, which is considered as the bot binary file that infects the victims' machines.

5) A builder program that generate two files: the encrypted configuration file (config.bin) and the malware (actual bot) binary file bot.exe. [2]

7. Zeus Detection and removal

Zeus is very difficult to detect even with up-to-date antivirus software. This is the primary reason why its malware family is considered the largest botnet on the internet: Some 3.6 million PCs are said to be infected in the U.S. alone. Security experts are advising that businesses continue to offer training to users to prevent them from clicking hostile or suspicious links in emails or on the web while also keeping up with antivirus updates. Symantec claims its Symantec Browser Protection can prevent "some infection attempts", but it remains unclear if modern antivirus software is effective at preventing all of its variants from taking root[9].

Removal of the Zeus rootkit was confirmed by rebooting and performing subsequent scans of corroborating tools, as well as observing the lack of certain behaviors, such as the hiding of the System32/lowsec directory and the lack of the backdoor TCP port associated with Winlogon.exe or Svchost.exe.[1]

8. Our work

In this section explanation of infection process are done step by step, then detection process are explained. In this research Zeus builder is used to generate a binary file of Zeus Bot (bot.exe) which will be used to penetrate other computers on the internet, figure 4 show Zeus builder.

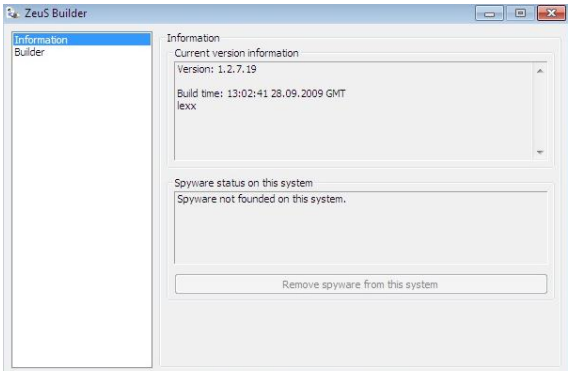
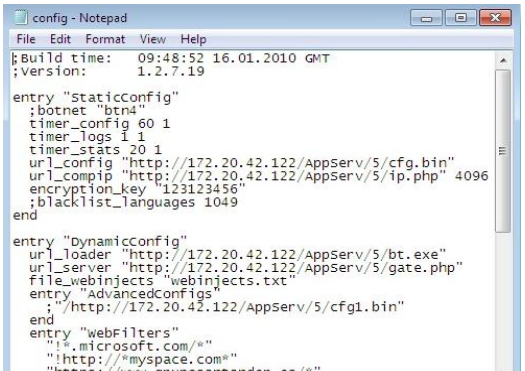


Figure 4: Zeus Builder toolkit

A suitable modification on the configuration file also made to create encrypted configuration file (.bin) which contain all configuration must be send by the botmaster after Zeus bot execute on the victim computer. figure 5 explain contents of configuration file.



International Journal of Information Technology and Business Management

29th October 2012. Vol.6 No.1

ISSN 2304-0777 www.jitbm.com

Figure 5: Zeus configuration file

Xampplite program also used which enable us to make our computer as a server, that is because Zeus botnet used client-Server approach, and Xampplite provide an environment to run and execute (.php) files where it is the extension of the server of Zeus botnet.

By using Spam Email which it one of the infection methods used by Zeus botnet to infect victim computer ,the penetration operation are successful and we have the ability to get any account information typed on victim computer such as Banking accounts, So that is main objective of Zeus Botnet. Figure 6 show the window of command and control server used by botmaster.

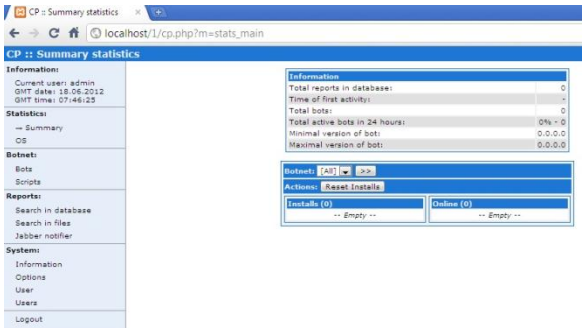


Figure 6: command and control server window

This implementation gives the ability to obtain other account info such as yahoo mail account information, Google mail account information and Facebook account information; here accounts mean user name and passwords typed on victim computer not passwords only.

A database of Zeus botnet are created which contain many information provided to botmaster such as operating system of victim computer and version of this operating system and country of victim computer and recent websites that the user uses with all accounts and keylogging information of these websites.

A software for detect zeus bot are programmed using visual c# programming language, the main idea of this software is to search and find (detect) zeus bot after it infect computers, really the detection process are made after check zeus bot on a honeypot and learn the files and the locations and the processes which zeus bot deal with such as Winlogon.exe and some registry files and keys which it infect. Our program has the ability to detect zeus bot in any computer has this software, only you press on the button named "find zeus bot" you will find a text on the screen explain that your operating system is free of zeus bot or not as shown in the figure 7.

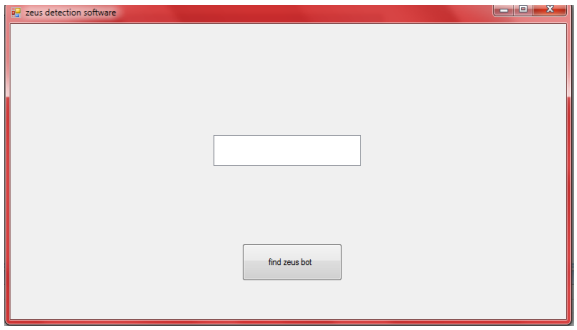


Figure 7:Zeus detection windows

9. Conclusion and future work

Zeus bot and it's botnet are most common in last two or three years, because of their wide scale spread in computer networks and internet. This paper interest in design and implement a "Host Botnet detection system" which have the ability to detect Zeus botnet in user's computers whose use the internet. But in this research implementation of infection process are made to understand how zeus work precisely ,then implementation of detection process are successfully made. future work is to design and

ISSN 2304-0777 www.jitbm.com

implement a "Host botnet prevention system " which prevent zeus bot from infect personal computer due to it's large dangerous because it the largest finical botnet over the world in our days until now.

10. References

1. Arnold T. M. , " A comparative analysis of rootkit detection techniques", 2011,thesis at the university of houston-clear lake.

2. Binsalleeh H., Ormerod T.," On the Analysis of the Zeus Botnet Crimeware Toolkit", 2010,IEEE, Computer Security Laboratory, Concordia University Montreal, Quebec, Canada.

3. Damballa ," Top 10 Botnet Threat Report – 2010", 2011, http://www.damballa.com

4. Falliere N.,Chien E.," Zeus: King of the Bots",2009, Symantec Corporation.

5. Rodr´ıguez-G´omez R.A.," Analysis of botnets through life-cycle ",2011, International Conference on Security and Cryptography, supported by Spanish MCIN under project TEC2008-06663-C03-02.

6. Shaikh A., "Botnet Analysis and Detection System",2010,thesis at Edinburgh Napier University, Matriculation No: 06015008.

7. Threat Research Team," ZeuS: A Persistent Criminal Enterprise",2010, Trend Micro, Incorporated.

8. Truster ,"Measuring the in-the-wild effectiveness of Antivirus against Zeus",2009, Trusteer, Inc. 142 Wooster St. New York, ww.trusteer.com.

9. Wikipedia, the free encyclopedia," Zeus (trojan horse)",2011, Text is available under the Creative Commons Attribution-ShareAlike License.

10. Wyke J.," What is Zeus?", 2011, Threat Researcher, SophosLabs UK.