KING OF TROJANS - ZEUS

MIS 513 – Web Computing and Analytics

CYBER ANALYTICS PROJECT
A detailed research on banking Trojan Zeus, using data from Hacker Web and Shodan and analytics tools.

Geethu Babu, Shayan Parhite, Jaiteerth Patil, Rajesh S Gill
Introduction

Zeus named as the king of botnet, has been a nightmare in the banking world for years. Zeus is a toolkit that provides a malware creator all of the tools required to build and manage a botnet. A Control Panel application is used to maintain/update the botnet, and to retrieve/organize recovered information. A configurable Builder tool allows to create the executables that will be used to infect victim's computers. These executables are usually detected as ZBot by anti-virus software. There is no single Zeus botnet. The toolkit is a commercial product that is sold to many different users, and distributed freely. Each of them can create one or more botnets of their own, so the number of Zeus botnets is likely quite large.

- The latest version of the toolkit typically sells for about 3000 USD to trusted buyers, with the bot source code possibly available for a much larger sum.
- Additional modules, which can cost as much as $10,000, are available for specific tasks. After a few months the new toolkit version is released as a free “public” version, which is probably meant to serve as a promotion for the commercial version.
- Modified versions of the public toolkit have also been offered for sale at lower prices by third party developers, sometimes known as "modders".

Because a Trojan built with a Zeus toolkit is so adaptable, variations of Zeus Trojans are often missed by anti-virus software applications. According to a report by security vendor Trusteer, 77% of the PCs infected with Zeus Trojans have up-to-date anti-virus software.

Literature Review

Zbot, also called as Zeus, is a Trojan horse is used to steal confidential information from computers that are compromised using various methods. Zbot distribute itself through spam campaigns and downloads. Email messages are sent to users purporting to be from organizations such as MySpace, Facebook, or Microsoft. In some cases, the message body warns the user of a problem with their financial information or online account, or software and suggests they visit a hyperlink provided in the email. As soon as the user clicks the hyperlink, the computer is compromised, if it is not protected.

Zeus is designed to steal information related to the system it compromises, login credentials and details related to banks. Recent versions of this botnet can be used to collect information of any possible kind. The configuration files are modified and installed by the hacker. Later on, the attacker can tailor the file to get any data the attacker needs. The functionality of the Zeus Trojan is:

- Confidential information is gathered through multiple methods. Upon execution the Trojan automatically gathers any Internet Explorer, FTP, or POP3 passwords that are contained within protected Storage (PStore).
- Its most effective method for gathering information is by monitoring Web sites included in the configuration file, sometimes intercepting the legitimate Web pages and inserting extra fields (e.g. adding a date of birth field to a banking Web page that originally only requested a user name and password).
- Trojan.Zbot contacts a command-and-control (C&C) server and makes itself available to perform additional functions. This allows a remote attacker to command the Trojan to download and execute further files, shutdown or reboot the computer, or even delete system files, rendering the computer unusable without reinstalling the operating system.
Research Questions

Our four research questions are related to Zeus Trojan. The data was collected from HackerWeb and Shodan related to Zeus. The data was analyzed using various mining and visualization tools such as Rapid Miner, Tableau, Excel and Semantria.

1. Even after 8 years of origin, how widely is Zeus used and how prevalent it is in different parts of the world?

2. SpyEye and Gameover Zeus came out as variants of Zeus but now has emerged as Zeus’ major competitors. But have these really taken over Zeus?

3. How Trojans, Botnets and malware evolved over time, from being experimental self-replicating programs to money making business?

4. Zeus targets FTP servers to collect sensitive data. How secure are FTP servers worldwide? The security threats of Zeus and FTP are clustered around United States mainly?
Research Design

- **Collection Methods**

1. **Hacker web**: Most of the information was collected through Hacker web. With the use of Java code in Eclipse, we were able to run queries against cyber analytics database. The data was distributed across 6 tables – anonposts, elitehackposts, hackhoundposts, cnhonkerarmyposts, unpackposts and vctoolposts. The java code can automatically collect data from hacker web and give us the required output such as number of threads, views, popular posts and so on.

   ```sql
   select * from (select v.threadID, v.title, v.numOfView, v.numOfPosts, p.postID, p.flatContent, CONCAT(mid(replace(replace(replace(p.postDate,'(',''),')',''),' ', '-',2,20),' ', rtrim(p.postTime)) postTimeStamp, p.postrank, p.subforum, va.authorName, va.reputationscore from vctoolthread v, vctoolposts p, vctoolauthor va where v.threadid = p.threadid and va.authorID = p.authorID and (lower(p.flatContent) like '%spyeye%' or lower(p.flatContent) like '%zues%' or lower(p.flatContent) like '%zeus%' or lower(p.flatContent) like '%zbot%' or lower(p.flatContent) like '%botnet%' or lower(p.flatContent) like '%bot%')) x where lower(x.flatContent) like '%purchase%' or lower(x.flatContent) like '%buy%' or lower(x.flatContent) like '%sell%' or lower(x.flatContent) like '%money%' or lower(x.flatContent) like '%cost%';
   ```

2. **Shodan API**: Shodan is a search engine that has a collection of specific devices such as computers, routers, mobiles using a set of filters. The search engine lets you find devices with various vulnerabilities. We have used shodan to expose the FTP servers around the globe that has anonymous access granted. These servers have their FTP access granted to any user and thus has the vulnerability of letting anyone access their data. Python code was used to query Shodan and extract data. The keyword used in Shodan is: “Anonymous access granted”.

![Java code snippet](image-url)
3. **Twitter API**: The third collection method for data we have used is Twitter API to collect relevant tweets on our research topics. Twitter gives a realistic view of how relevant the topic is in the current scenario and helps us gauge the popularity of a hack or a threat. Zeus -- one of our research topics, has extensively used Twitter to defame multi-nationals, news channels including Barrack Obama’s account. The tweets were collected using Java code run in Eclipse using Twitter API “twitter4j”. Maximum of 100 tweets can be extracted, it gives us useful information such as screenname, text of the tweet associated with the keyword, number of re-tweets, favoured tweets and geo-location. Search keyword: “Zeus”.
Analytics Method

1. **Microsoft Excel**: The primary source of analytics is using Excel-pivot tables. This is mainly for the data collected from Hacker web. Pivoting is used on measures such as number of posts, number of views, postRank for the posts and threads. These pivot tables are used to plot various graphs in order to achieve visualization for the data plotted.

2. **Tableau**: The data collected from Shodan was first put through a manual process of ETL. The code in python was written in a way to extract data as comma separated values. This data was then stored as CSV file, cleansed to remove extra characters and then transformed into a format that can be analyzed by Tableau – a data mining and data visualization tool. The data from Shodan was collected with Latitude, Longitude, City, Country Name, IP Address and Hostname. Latitude and Longitude were used in Tableau to plot the locations of the servers across worldwide.

3. **Rapid Miner**: Rapid Miner is a text mining software that we have used to mine tweets collected on research topics Zeus and its competitor, Spyeye. The Rapid Miner software was used to read data from multiple documents and then perform word frequency counts. This gave us an idea of the popularity of the topic and how relevant it is in the current scenario.

Findings and Discussions

1. **Even after 8 years of origin, how widely is Zeus used and how prevalent it is in different parts of the world?**

The below bar graph shows the number of posts mapped against year collected over Hacker Web.

- Close to 14,000 posts contained discussions around Zeus in year 2011 and 2012.
- The number of posts reduced in year 2013. This is because the variants of Zeus have become so prevalent that now Zeus has to share the market place with Gameover Zeus and SpyEye mainly.
- After analysis and scanning on other data showed that it is still being widely used for various hacking activities.
- New techniques have been adopted by Zeus to hack data from personal computers. The latest extension used by Zeus is .enc.

![Figure 1 - Number of posts on Zeus per year](image-url)
After plotting the number of Zeus hosts files world-wide, it can be seen the most number of Zeus hosts are present in United States. United States has an alarming number of 112 Zeus hosts.

![Figure 2 – Number of Zeus hosts files in top ten Countries](image)

2. SpyEye and Gameover Zeus came out as variants of Zeus but now has emerged as a competitor. But have these really taken over Zeus?

Over the years Zeus has been so widely used in the hacking world that, multiple variants of Zeus was released in the market. Two variants of Zeus that emerged as competitors are Gameover Zeus and SpyEye. As per 2013 data, Zeus and Gameover Zeus was responsible for more than half of known banking malware last year. The graph below shows how the variants have taken over the discussions on forum of HackerWeb. They have gained popularity over the years taking over a lot of Zeus market. But graphs clearly indicate that Zeus retains the status of “King of Trojans” as of 2013. They continue to remain a threat to the security world.

![Figure 3 – Number of posts on Gameover and SpyEye per year](image)
Tweets with #Zeus and #SpyEye were collected and subjected to text mining in RapidMiner. The analysis conveys the message that Zeus is still more popular than SpyEye.

![Tweet analysis of Zeus and SpyEye](image)

**Figure 4– Tweet analysis of Zeus and SpyEye**

3. **How Trojans, Botnets and malware evolved over time, from being experimental self-replicating programs to money making business?**

In 1971, the Creeper system which was an experimental self-replicating program that infected computers running the TENEX operating system. It gained access via the ARPANET and copied itself to the remote system where the message, ”I’m the creeper, catch me if you can!” was displayed. Another program (Reaper) was later created to delete Creeper.

However the past decade, botnets have evolved from small networks of a PCs controlled from a single command and control center (C&C) into sophisticated distributed systems which comprise of millions of computers with decentralized control. Main motive behind all the efforts can be summed up in a single word i.e. money. Below are the major sources of income:

- Theft of confidential information
- Phishing / Spam / Search engine spam
- Adware and malware installation
- Click fraud
- Leasing and selling botnets
We have analyzed the data from Hacker web forum and created below graph which shows the number of posts in HackerWeb that had discussions related to botnets especially Zeus botnet (zbot) and spyeye which is another variant. In addition to that, we have identified the posts/threads where authors are discussion about money making, revenue, selling and purchasing of botnets. The graph clearly shows how the number of posts were increasing over the years till 2013.

![Graph showing the number of posts on botnets that are revenue related.](image)

**Figure 5 – Number of posts on botnets that are revenue related**

The data collected from Hacker Web was text mined in Rapid Miner to find the frequency of occurrences of words related to revenue generation i.e Sellers, Selling, Sells, Money and so on. The result clearly showed that this was a topic of discussion for many authors on HackerWeb.

![Table showing revenue related words analysis on Zeus data from HackerWeb.](image)

**Figure 6 – Revenue related words analysis on Zeus data from HackerWeb**

8
4. **Zeus targets FTP servers to collect data. How secure are FTP servers worldwide? The security threats of Zeus and FTP are clustered around United States mainly?**

File Transfer Protocol servers are critical for any organization as sensitive information as stored in files and transferred using this protocol. Hence it is important for organizations to keep their FTP servers secure. Zeus Trojan takes advantage of this vulnerability to hack into FTP servers and take confidential data. In 2009, Zeus was responsible for hacking into more than 75,000 FTP servers. Hence we thought it is necessary to perform an analysis of vulnerable FTP servers across the globe. Coincidently, we could see that most of vulnerable FTP servers are clustered around United States.

This was similar to what we found for Zeus host files across the globe. The data of vulnerable FTP servers with “Anonymous access granted” was collected from Shodan with the Latitude and Longitude information. These coordinates were plotted in Tableau software for their location.

![Figure 6 – Plot of location of unsecure FTP servers worldwide](image)

**Conclusion**

It is a known fact that Zeus has been the most popular banking Trojan of all times. But it was difficult to gauge the extent of the reach of Zeus, after 8 years of origin. One would think with the latest advancements in technology, Zeus should have been wiped out the Cyber Security world by now. But our analysis on data collected from Hacker Web, Shodan and Twitter helped us to understand that Zeus continues to be a nightmare in the banking world. The trends do not indicate Zeus going to extinction anytime in the coming years. Gameover Zeus and SpyEye are the highest competitors of Zeus which were originally developed as variants of Zeus. Also, FTP servers across the world needs to be more secure in terms of access in order to prevent any vulnerabilities from Trojans such as Zeus.
References


