Botnets: Zeus Botnet Detection and Its Removal

Sobia Arshad¹ Lecturer University of Engineering & Technology Taxila Shahid Mehmood² Lecturer COMSATS Institute of Information Technology Islamabad Nida Yasir³Maria Arshad⁴ Lecturer^{3, 4} The University of Lahore^{3, 4} Lahore

ABSTRACT

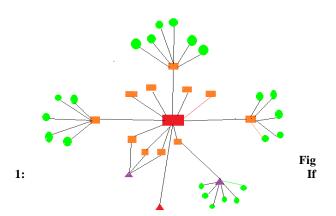
Today's Internet is widely spreading in every part of the world. As the number of internet users increasing, the number of people with bad desires increasing. Botnet is such a group of infected nodes on worldwide network. Bot master spread viruses and utilizes the network resources of the nodes, which have been contaminated or infected by Bot herder. Effect of this is to slow down the internet speed and illegal utilization of personal documents of bots. As the size of Botnet becomes large, it will be difficult to trace out the Bot herder. This research will hand out a preface to the Botnets, its major type Zeus Botnet and its sound effects on the network security. We also propose some ways to detect as well as remove the effect of Zeus Botnet to personal computers.

Keywords

Botnets, Zeus Botnet, Bot master, Bot herder, Bot Net Detection, Bot Net Removal

1. INTRODUCTION

Much of the computer criminal technology is based on Botnets. Virus was infrequent in the 1980's and 1990's. User error was the simple case. Now a days, viruses and spywares can be found almost in every website. Incorrect request for visiting the wrong website at the incorrect time of the day and you could get a new toolbar or new icon on your existing browser toolbar installed automatically. Sometimes by downloading an attractive image like wallpapers, screen savers and playing online games you getting involved in building a giant Botnet or you may somehow helping in constructing a Botnet. Now your installed operating system is no safer and not helps you anymore against attack of any kind of virus or spywares. And unluckily many innocent users' especially home users don't install any good anti-virus and usually they have turned off firewalls in their systems. With twenty thousand or more computers are common in one Botnet [1]. Botnet is a group of Bot, where Bot is an affected computer that can be used to hack other computers or it can be used to steal other computer's password, personal information or important documents. Botnet is such a network of affected computers running on an Internet Relay Chat (IRC) network that has been created with a Trojan [2]. The common goals of Botnets are spam relays, Denial of Service attacks and adware installs. Sometimes these are directed to play with "click for money" ads. This work is totally performed on the code provided by the Bot master or Bot herder.



necessary, Botnets with its bots. Bot herder (Bottom purple triangles) logs into Command and control server (central red rectangle).After the entering of him into the control server, he train or teach his army to look into for fresh victims. At once he hit upon a fresh victim and contaminates it.

Above figure shows a small Botnet with a central command and control server and with herder. As soon as Bot herder logs into command and control server, it instructs his commanders to scan for new victims. Bot herders continuously scan and infect new PCs. In the same way, infected nodes can scan for new victims and so on. It is grows up to big and bigger Botnet.

The Botnet "masters" or "Bot herder" are the only ones whom have all the information about the bots what they are doing. Bots are innocent infected nodes, that either doesn't know how to use computer safely or who that don't have any good antivirus. Bot herder knows all those activities that are performed by Bots i.e. which website he visits, which page he opens, to which person he talk online, what are his account passwords and many more.

In this paper, we outline one of Botnets major type i.e. Zeus Botnet. This research paper has been divided as follows. Firstly, a brief introduction of Zeus Botnets that includes how it works and grows up. Then, a brief discussion about how it affects computers and user's personal life. Finally, it is discussed how to detect Zeus Botnet and how to remove it.

2. ZEUS BOTNETS

Millions of compromised computers are estimated to include in present Zeus' Botnet e.g. 3.5 million in U.S.A. [3]. On Face book Zeus has sent out almost 1.5 million phishing messages till October of 2009.

The foremost big size attack by Zeus was against Outlook. It was a corporate attack, indicating Z-bot's latest strategy.

The Zeus Botnet malware is commonly used by attackers to steal banking information from infected computers. Zeus is primarily an information stealing Trojan, and the bot software itself is generated using a toolkit that is sold online. It is highly configurable with regard to the information it can obtain from an infected PC. At any given time, there are thousands of known individual Zeus Botnets in existence [4]. Zeus, also known as Bot, is one of the biggest malware threats currently circulating on the internet. Zeus is the name of awful (bad) program that infects your PC by steal your bank account details. This is one of the most spyware/virus in the world used today by the hackers.

Cyber criminals use the Zeus Builder Toolkit to configure and rebuild this virus the way they want, with the functions they want to perform by. PRG and WSNPoem are the other names of Zeus Botnet.

The Zeus Botnet found on your system due to spam emails. By clicking on those emails you will connected to various compromised websites. During download any web file by providing personal information to these websites, many users install one of the variant of the Zeus Botnet in their system.

Some of them are infected due to one of these variants by visiting social websites. These variants send messages to install new updates in your system. This variant is nothing, just a virus i.e. Zeus Botnet trying to trap you.

Once Zeus Botnet traps your system, it will pass the time for internet connection. The virus will spread further to obtain a bank account detail file from the net only to steal your personal information.

3. EFFECTS OF ZEUS BOTNETS

The Zeus Botnet is a dangerous virus that affects our personal life as well as slows down the performance and speed of computer. Therefore we should wipe our computer of everything i.e. Programs, spyware, junk and other things. To solve this issue we should updated our computer with a good antivirus solution and should deep scan our computer system regularly.

4. DETECTION OF ZEUS BOTNETS

If your system is trapped by a Botnet then it is not very much easy to detect it. Once you found that your system is not working properly and perhaps it may be doing functions or tasks slowly, then it can shows a symbol that your system is affected by virus i.e. Zeus Botnet. To prevent your system from these dangerous and risky viruses, you must install a fine and updated antivirus in your system. These anti-virus and anti-spyware software should detect these viruses, take care of your system from unsafe measures, or prevent the problem.

Even using up-to-date antivirus software, Zeus virus is very difficult to detect. This is also the main cause of being the Zeus Botnet as the largest Botnet on the internet. About 3.5 million computers are contaminated alone in the U.S. It is often advised through Security experts that training should continue to teach users to avoid them from clicking unfriendly or doubtful links in spams or on the websites with regularly updated antivirus. Bots can be detected and removed by many good anti-viruses through different safety measures [5]. But it remains unclear if modern antivirus software is effective at preventing all of its variants from taking root.

5. ZEUS BOTNETS REMOVAL

When you clean and wash your system by removing that virus i.e. Zeus Botnet, then you supposed to be alert or watchful while doing it in such a manner. You must consider two things when trying to clean manually your system from that virus:

- to stop its process
- to delete its main file

You can get rid of this virus i.e. Zeus Botnet by installing updated anti viruses in your system .You must try to update your system regularly by antivirus. You must scan your system as early as possible.

088709. exe process is use in the removal of Zeus Botnet. This process will most likely be unique to your installation. Therefore you can either bring up the Task Manager or see if you have a similar process running or use a well-known security client like Spyware Doctor with Antivirus to scan for the threat. Next, remove the **088709.exe** file from your hard disk. Now your computer is safe from Zeus Botnet.

Different antivirus are used to remove that virus i.e.; Zeus Botnet from your system. These are:

- Spyware Doctor with Antivirus
- Norton
- Kaspersky
- AVG
- Avira Antivirus

6. CONCLUSION

We conclude this research by this that security should be provided to home computer systems as well as for office computers. Secure your passwords for accounts and for bank account for being saved from the world of hackers. Moreover security can be achieved by installing a good antivirus.

7. FUTURE WORK

While the description of Zeus Botnet state over is an admirable start-up for achieving a gigantic representation seem to be at the Botnet underground.

To enhanced filter and state the facts numerous other steps must be taken account. Moreover, further research and study and work related to Zeus Botnet can be processed.

Zeus Botnet removal in somewhat different ways can be more explored.

8. ACKNOWLEDGEMENT

We are in depth of gratitude to Engr. Maryam for her guidance and support. Our wholehearted gratitude is to our Computer Engineering Department faculty for their support and courage. University of Engineering & Technology (UET) Taxila has supported us in financial assistance to complete this research.

9. REFERENCES

- [1] Nicholas Albright, Security Researcher, "Researching Botnets".
- [2] Jivesh Govil, Jivika Govil "Criminology of Botnets and their Detection and Defense Methods" IEEE EIT 2007 Proceedings.
- [3] "UAB computer forensics links internet postcards to virus", http://www.hindu.com/thehindu/holnus/00820090727132 1.htm
- [4] "IBM Internet Security System Ahead of the threats",2007 http://www.ibm.com/jm/download/IBM_ISS_Overview. pdf
- [5] "Trojan.Zbot",http://www.symantec.com/security_respon se/writeup.jsp?docid=2010-011016-3514-99.