Botnets: From IRC to Android

Dr. Desmond Lobo
Faculty of Science
Naresuan University Thailand
desmondlobo@yahoo.com

Dr. Sarunya Lertputtarak
Graduate School of Commerce
Burapha University Thailand
sarunyalmbabuu@gmail.com

ABSTRACT

This paper outlines the evolution of botnets from IRC to Android. It begins by detailing the two malware that started the botnet ball rolling: the Pretty Park worm and the SubSeven Trojan horse. Having been detected for the first time in 1999, they would listen to and accept malicious commands from an Internet Relay Chat (IRC) channel. There are literally thousands of botnets operating in the world today and FortiGuard Labs is an organization that monitors the activity of these botnets on a global basis, twenty-four hours per day, seven days per week. According to FortiGuard, Vundo, Lethic, Torpig, ZeroAccess and Dorkbot have been five of the most active botnets in the last few years. This paper provides an analysis of incidents involving these five botnets and investigates the potential impact of botnets on Android-based smartphones. To avoid becoming a victim of these botnet attacks, it is recommended that you use an antivirus application that automatically activates whenever the battery is being charged.

KEYWORDS

Computer Security, Malicious Software, Botnets, Android Smartphones, Battery Life

1 INTRODUCTION

We have witnessed the Internet become an integral part of our lives. Web-based computing creates new classes of applications, new methods to interact with people, and provides accessible services. The users are increasingly relying on the Web for their data and computational requirements.

The explosive increase of Internet usage provides tremendous convenience. However, those who use the Internet for business, pleasure or education need to beware of a number of great security challenges. The users should know that most of the attacks on the Internet are dangerous because it is plagued with fraudulent activities. These activities include spam (unwanted emails), phishing (stealing usernames and passwords), click fraud (automated clicks on Web advertisement), etc. There are several types of malware (such as viruses, worms and Trojan horses) that are designed for attacking computer systems and this has led to billions of dollars in financial losses.

Although there has been an increasing awareness of botnets in the last few years, there is a dearth of knowledge about their activities, what attacks are being initiated by them, and what compromised hosts belong to certain botnets. Hench, information about botnets is crucial in order to identify these attacks and safeguard users from botnet activities. This paper provides an analysis of botnets and begins by explaining the differences between viruses, worms and Trojan horses. This is followed by a description of what botnets are and how they have evolved over the years. Finally, an outline of potential Android botnets is given in the concluding section of this paper.

2 VIRUSES, WORMS AND TROJAN HORSES

There are different kinds of computer viruses, ranging from those that are just annoying to dangerous ones that can damage hardware and software. When viruses spread from one computer to another, they attach themselves to a program or an executable file. Usually, viruses exist on computer systems without the user’s knowledge. These viruses cannot infect the computer unless the user runs or opens the malicious file. Human action is necessary for spreading viruses. This can occur by sharing infected files or by sending emails with viruses attached.

The year 2001 was called “the year of the worm” [1]. Since that time, worms, which are fast-moving and self-replicating code, have become the weapon of choice for people who wish to inflict widespread damage on the Internet. Worms have a similar design to viruses and can spread from computer to computer. However, they have the capability to proliferate without any human interaction. Worms take advantage of file or information transport features on computer systems, which is what allows them to travel unaided.

Unlike viruses and worms, Trojan horses neither reproduce by infecting other files nor do they self-replicate. Trojans are known to create backdoors on computer systems that give malicious users access to the systems, possibly allowing confidential or personal information to be compromised. A Trojan horse, at first glance, appears to be useful software, but will actually do damage once installed or run on the computer. Trojan horses usually trick the user into opening them because they appear to be genuine software or files from a legitimate source. When a Trojan is activated on a computer system, the results can vary. Some Trojans are designed to be more annoying than malicious: they may change the desktop or add silly active desktop icons. Other Trojans can cause serious damage by deleting files and destroying information on the system. [2]

3 IRC BOTNETS (1999)

The word botnet was derived by combining the two words robot and network, and refers to a group of computers that have been infected with some malicious software (malware). Once the malware has been installed on these machines, the computers are then essentially mindless zombies that can be remotely controlled by the bot master. Cybercriminals use botnets to generate revenue using several different methods, including distributed denial of service attacks, spamming, and financial fraud. The two pieces of malware that triggered the development of botnets were the Pretty Park worm and the SubSeven Trojan horse. Back in 1999, they would listen to and accept malicious commands from an Internet Relay Chat (IRC) channel [3].

IRC is an open protocol for real-time text messaging and chatting on the Internet or for synchronous conferencing [4]. There were many types of people that joined IRC for different proposes, including hacking. Users on the IRC network used nicknames. The users would send broadcast messages to the channel or private messages to specific nicknames inside that channel.

With the widespread use of public IRC servers, this site became the best tool for botmasters to interact with the bots. At first, botnets used IRC for communication. The bots linked to a single server or a small number of servers to obtain their instructions and then used a centralized command-and-control (C&C) infrastructure. For instance, a botmaster might send messages such as “send me recorded passwords” or “start a DDoS on target X”. In order to avoid detection, bots may encrypt the contents of the messages or use an encrypted connection to the IRC server.

In the last few years, botnets have been used by cyber criminals to create global cooperative networks for launching spam and phishing attacks: Storm is an example of a famous large-scale P2P botnet that was mainly used to send spam. Botnets have also been used to steal sensitive information such as identities, credit card numbers, passwords, or product keys: Kraken is an example of a large botnet that managed to penetrate at least 50 of the Fortune 500 companies.

4 VUNDO BOTNET (2009)

According to FortiGuard Labs, Vundo has been one of the highest ranked botnets in the world in terms of activity. This botnet makes use of a Trojan horse and was first detected in 2004.

In 2009, the Trojan was used to trick users into running a file that appeared to be legitimate software update. In fact, after installation, the Trojan would proceed to encrypt various files, including those with the extension of doc, xls, ppt, pdf, jpg, jpeg, png, mp3, wma, mdb, pst, docx, docm, dotx, dotm, xlsx, xlsm, xltx, xltm, xlsb, xlam, pptx, pptm, potx, potm, ppam, ppsx, and ppsm. These files were located in the victim’s My Documents folder.

When the user attempted to open one of the encrypted files, he or she was presented with the following message: Please register your copy of FileFix Professional 2009 to repair all corrupted files [6]. The FileFix Professional 2009 program did indeed decrypt one file for free. However, if the victim attempted to open more than one file, he or she would need to purchase additional software for a price of $50 in order to decrypt the remaining files.

5 LETHIC BOTNET (2010)

The Lethic botnet was first detected in 2008. The botnet was primarily used for distributing pharmaceutical spam, which accounts for a large chunk of all the spam on the Web. In 2010, approximately 2 out of every 3 spam emails were related to pharmaceutical products and/or companies [7].

In January 2010, the Internet authorities managed to severely disable the Lethic botnet by disabling its command and control servers. Astonishingly, by April of that year, only three months later, the botnet had recovered and was spewing out roughly two billion spam emails per day. [8]

6 TORPIG BOTNET (2011)

In 2011, Stone-Gross et al. [9] managed to take control of the Torpig botnet for a period of ten days. During this period, these researchers determined that this botnet makes use of the Mebroot rootkit to attack its victims. Essentially, the Torpig botnet can take control of the victim’s computer as soon as the Mebroot rootkit replaces the system’s master boot record (MBR).

The Torpig botnet steals personal information such as bank account details and credit card data. It targets approximately 300 different banks and financial institutions. Roughly 49% of the victims live in the United States, 12% in Italy, 8% in Spain, and the remains 31% are scattered among 40 other countries. Every 20 minutes, the stolen information that it collects is uploaded to the botnet’s command and control server.

7 ZEROACCESS BOTNET (2012)

It is estimated that the ZeroAccess botnet has infected a total of 9.5 million computers worldwide, with the majority of these machines being located in the USA. The size of the botnet, as of September 2012, was approximately 1 million computers. [10]

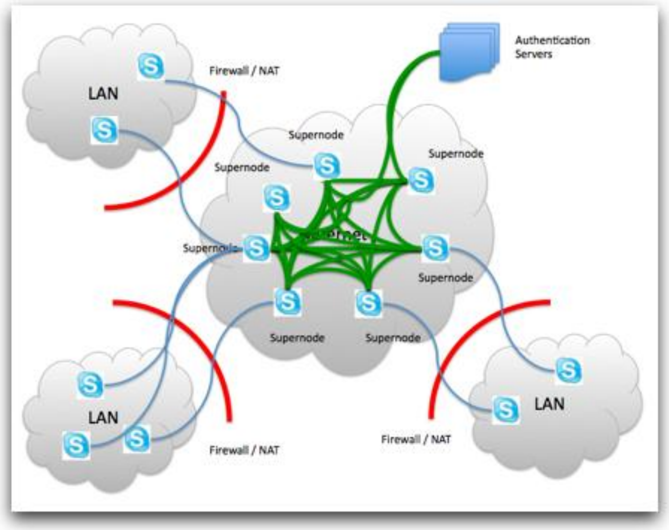

Figure 1: Skype's Infrastructure [20]

The infrastructure of the ZeroAccess botnet is similar to that of Skype. As illustrated in figure 1, the Skype infrastructure consists of both super nodes and normal nodes. Super nodes are those that have a direct connection to the Internet. Many machines within corporate and home networks, however, do not have a direct Internet connection and make use of Network Address Translation (NAT) instead. These computers that are hidden behind NAT firewalls or routers are referred to as normal nodes.

Normal nodes can only contact super nodes and are unable to connect with other normal nodes. Super nodes, on the other hand, have more responsibilities and privileges. In addition to contacting normal nodes, super nodes can also connect with other super nodes, thereby giving rise to a true peer-to-peer network. Obviously, super nodes play an integral part in the operation of the network.

One of Skype’s authentication servers, with links to several super nodes, is clearly visible in figure 1. In terms of ZeroAccess, these servers act as the botnet’s command and control.

8 DORKBOT BOTNET (2013)

The Dorkbot botnet has been circulating around the Web for a decade. It is capable of stealing sensitive information from an infected machine, blocking updates of antivirus software on a system, and launching distributed denial of service (DDoS) attacks. [11]

The very latest variant of Dorkbot has targeted Facebook and was distributed through the chat service. Users are tempted to click on what appears to be a picture file, but the file does in fact contain some malicious code. When this code is executed, the malware would harvest passwords from the victim's browser. [12]

9 CONCLUSION

Several researchers have suggested strategies for combating botnets. Cooke, Jahanain and McPherson [13] described a botnet detection method. Their simple process could be used to identify botnets and involved matching sniffed-IRC traffic against botnet activities. Gu et al. [14] stated that when monitored events match the communication flow model (such as scans, inbound exploits, binary acquisitions, C&C communication, and outbound infections), it is suspected that an infection process is taking place. Binkley and Singh [15] demonstrated a method of detecting the suspicious behavior of botnets by calculating the Transmission Control Protocol (TCP) work weight. The TCP work weight is the ratio of the total amount of TCP control packets to the total number of TCP packets for each IRC host. If the TCP work weight of a host is a high value, the host can be a potential botnet server [16].

Finding countermeasures for tackling botnets should be given high priority because, with the dramatic increase in the adoption rate of smartphones worldwide in the last few years, the issue of botnets is only going to get worse. Future botnets are certainly going to exploit smartphone technologies. As opposed to office computers that are usually only turned on during the daytime on weekdays and home computers that are generally turned on during the evenings and on weekends, smartphones are on ALL the time. This is precisely what bothunters would like to hijack: devices that they can exploit 24 hours per day and 7 days per week.

A second equally important reason revolves around the battery life of smartphones. Personal computers do not have resource constraints; hence, anti-virus software is usually utilized to check for suspicious activity. Smartphone users, on the other hand, are reluctant to use anti-virus software because it can quickly drain the battery [21]. These users would likely disable any type of security software in order to save power. This is playing into the hands of the bothunters: they are looking to take over devices without being detected.

Among the various smartphones, Android-based ones are most likely going to be targeted [17]. Android is the dominant operating system for smartphones, as developers of malware usually targets systems with the highest market penetration. At the end of 2010, the first Android malware with botnet-like characteristics and capabilities had already been identified [18]. A Trojan named Geinimi had the ability to extract personal data from a user's phone and transmit that data to a remote server. It also had the ability to receive commands from that server, which could be used to control the phone. In addition to Geinimi, Pieterse and Oliver [19] have identified other, more recent Android botnets.

Taking all these concerns into consideration, a possible solution might be an antivirus application, designed for Android devices, that automatically activates whenever the smartphone battery is being charged. Ideally, continuously running some antivirus software in the background is the best strategy for ensuring that one does not become a botnet victim. The next best tactic would be to at least scan for viruses, worms, Trojan horses, rootkits and other malware while charging the battery.

10 REFERENCES

1. LEMOS, R. Year of the Worm: Fast-Spreading Code is Weapon of Choice for Net Vandals. 2001. CNET News.com. Retrieved from http://news.cnet.com.
2. WEBOPEDIA. The Difference Between a Computer Virus, Worm and Trojan Horse. 2013. Retrieved from http://www.webopedia.com.
3. FERGUSON, R. The Botnet Chronicles: A Journey to Infamy. 2010. Trend Micro.
4. KALT, C. Internet Relay Chat: Server Protocol, RFC2813 (Informational). 2000. Retrieved from http://www.ietf.org.
5. ANAGNOSTAKIS, K.; SIDIROGLOU, S.; AKRITIDIS, P.; XINIDIS, K.; MARKATOS, E.; KEROMYTIS, A.

Detecting Targeted Attacks using Shadow Honeypots. 2005. Proceedings of the 14th USENIX Security Symposium.
6. DANCHEV, D. Scareware meets ransomware: "Buy our fake product and we'll decrypt the files". 2009. Retrieved from http://www.zdnet.com.
7. WOOD, P. Pharmacy Spam: Pharmaceutical Websites Fall into Two Distinct Operations. 2010. Retrieved from http://www.symantec.com.
8. POMKO, R. Fortinet Threat Landscape Research Finds Surprising Comeback in Lethic Spam Botnet. 2012. Fortinet. Retrieved from http://investor.fortinet.com.
9. STONE-GROSS, B.; GILBERT, R.; KEMMERER, R.; KRUEGEL, C.; VIGNA, G. Analysis of a Botnet Takeover. 2011. IEEE Security and Privacy, January/February 2011.
10. WYKE, J. The ZeroAccess Botnet – Mining and Fraud for Massive Financial Gain. 2012. SophosLabs.
11. MELLO, J. Facebook, Financial Firms Targeted by Online Marauders. 2013. CSO Security and Risk. Retrieved from http://www.csoonline.com.
12. GONSALVES, A. Facebook Attacked with Credential-Harvesting Malware. 2013. CSO Security and Risk. Retrieved from http://www.csoonline.com.
13. COOKE, E.; JAHANIAN, F.; MCPHERSON, D. The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets. 2005. Proceeding of Steps to Reducing Unwanted Traffic on the Internet Workshop. USA.
14. GU, G.; PORRAS, P.; YEGNESWARAN, V.; FROG, M.; LEE, W. Bothunter: Detecting Malware Infections Through IDS-Driven Dialog Correlation. 2007. Proceedings of the 16th USENIX Security Symposium. USA.
15. BINKLEY, J.R.; SINGH, S. An Algorithm for Anomaly-Based Botnet Detection. 2006. Proceedings of Steps to Reducing Unwanted Traffic on the Internet Workshop. USA.
16. JEONG, O.; KIM, C.; KIM, W.; SO, J. Botnets: Threats and Responses. 2011. International Journal of Web Information Systems, 7 (1), PP. 6-17.
17. LOBO, D. In-depth Analysis of Rootkit Attacks on Android-based Smartphones. 2012. Proceedings of the Fourth International Conference on Computer Technology and Development. ASME Press.
18. HULME, G. Geinimi Android Malware has 'Botnet-Like' Capabilities. 2011. CSO Security and Risk. Retrieved from http://www.csoonline.com.
19. PIETERSE, H.; OLIVER, M. Android Botnets on the Rise: Trends and Characteristics. 2012. Proceeding of the Information Security for South Africa Conference. IEEE.
20. YORK, D. Understanding Today's Skype Outage: Explaining Supernodes. 2010. Retrieved from http://www.disruptivetelephony.com.
21. BICKFORD, J.; LAGAR-CAVILLA, H.A.; VARSHASY, A.; GANAPATHY, V.; IFTODE, L. Security Versus Energy Tradeoffs in Host-Based Mobile Malware Detection. 2011. ACM.