INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

COMPARATIVE STUDY ON BOTNET DETECTION

MISS. ANKITA S. AMBADKAR[1], PROF. H. R. DESHAMUKH[2]

1. Department of Computer Science and Engineering, IBSS College of Engineering, Amravati, Maharashtra, India.
2. Professor, Department of Computer Science and Engineering, IBSS College of Engineering, Amravati, Maharashtra, India.

Accepted Date: 05/03/2015; Published Date: 01/05/2015

Abstract: This paper is a survey of botnet and botnet detection. The survey clarifies botnet phenomenon and discusses botnet detection techniques. Among the various forms of malware, botnets are emerging as the most serious threat against cyber-security as they provide a distributed platform for several illegal activities such as launching distributed denial of service attacks against critical targets, malware dissemination, phishing, and click fraud. The defining characteristic of botnets is the use of command and control channels through which they can be updated and directed. Recently, botnet detection has been an interesting research topic related to cyber-threat and cyber-crime prevention. This survey classifies botnet detection techniques into four classes: signature-based, anomaly-based, DNS-based, and mining-base. It summarizes botnet detection techniques in each class and provides a brief comparison of botnet detection techniques.

Keywords: Botnet; Botnet Detection; Cyber-security;

Corresponding Author: MISS. ANKITA S. AMBADKAR

Access Online On:

www.ijpret.com

How to Cite This Article:

Ankita S. Ambadkar, IJPRET, 2015; Volume 3 (9): 1144-1150

PAPER-QR CODE

INTRODUCTION

According to explanation in [1] malicious botnet is a Botnet; Botnet Detection*;* Cyber-security; network of compromised computers called “Bots” under the remote control of a human operator called “Bot master”. Botnets have become the biggest threats on the Internet and been used for launching attacks and committing fraud. The master computer communicates with its bots by a command and control (C&C) channel, which passes commands from the botmaster to bots, and transmits stolen information from bots to their master. Botnet is a term for a collection of software robots, or bots, which run autonomously and automatically. They run on groups of zombie computers controlled remotely by attackers. A typical bot can be created and maintained in four phases. 1. Initial Infection, 2.Secondary Injection, 3.Malicious Activities, 4. Maintenance and Upgrade. Botnets are always classified according to their command and control architecture. For example, those who use the Internet Relay Chat (IRC) protocol are known as IRC based botnets. In other words, the individual bots are software programs that run on a host computer allowing the bot master to control host actions remotely [1, 2]. Botnets pose a significant and growing threat against cyber-security as they provide a distributed platform for many cyber-crimes such as Distributed Denial of Service (DDoS) attacks against critical targets, malware dissemination, phishing, and click fraud[3,4]. Botnet detection has been a major research topic in recent years. Researchers have proposed several approaches for botnet detection to combat botnet threat against cyber-security. In this survey, botnet phenomenon will be clarified and advances in botnet detection techniques will be discussed. Many researchers focused on how to detect botnets or trace the botnet master. Meanwhile, many surveys reflected what had been done and summarized what future work should be. Feily et al. surveyed botnet mechanisms and botnet detection techniques based on different classes they identified: signature based, anomaly-based, DN S-based, and mining-based. The thesis for our work is that effective network security in the future will be based on detailed understanding of the mechanisms used by malware. While this high level statement does not represent a significant departure from what has been the modus operandi of the IT security industry for some time, unfortunately, data sharing between industry and research to date has not been common. We argue that greater openness and more detailed evaluations of the mechanisms of malware are required across the network security research community.

II. UNDERSTANDING BOTNET

Botnets are emerging as the most significant threat facing online ecosystems and computing assets. Most current research focuses on understanding botnets. There are mainly three types of papers in this area.

• Bot Anatomy: The papers in this category provide extensive analysis of a specific kind of bot for case study. The analysis mainly focuses on its network level behavior, usually involving the use of binary analysis tools. A recent Microsoft survey found more than 43,000 new variants of backdoor Trojans and bots during the first half of 2006 [6].

• Wide-area Measurement Study: The second group of papers provides measurement studies through tracking botnets to reveal different aspects of botnets in the internet, such as botnet size, traffic generated, their usages and dynamics. Currently only IRC-based botnets have been studied.

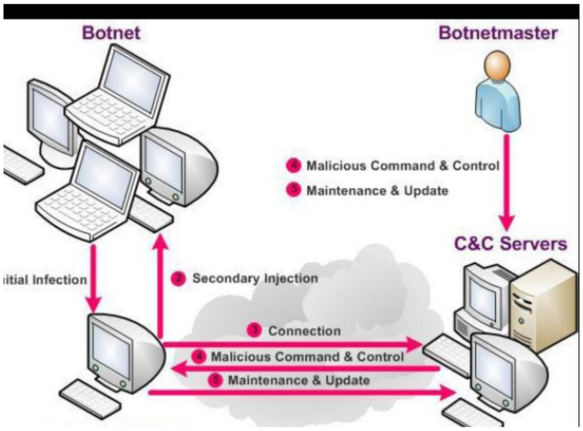
• Botnet Modeling and Future Botnet Prediction: The third group of papers discusses the theoretical modeling of botnets, the possible future evolution of botnets and countermeasures against them.

III. BOTNET CHARACTERISTICS

Bot infection methods are similar to other classes of malware that recruit vulnerable systems by exploiting software vulnerabilities, trojan insertion, as well as social engineering techniques leading to download malicious bot code[2,9,10]. According to measurement studies in [11] modern bots are equipped with several exploit vectors to improve opportunities for exploitation. However, among the other classes of malware, the defining characteristic of botnets is the use of command and control (C&C) channels through which they can be updated and directed. The multi-tier C&C architecture of botnets provides anonymity for the bot master. C&C channels can operate over a wide range of logical network topologies and use different communication protocols. Botnets are usually classified according to their command and control architecture [2, 4, 5, 6,7]. According to their command and control architecture, botnets can be classified as IRC-based, HTTP-based, DNS based or Peer to Peer (P2P) botnets [8]. P2P botnets use the recent P2P protocol to avoid single point of failure. Moreover, P2P botnets are harder to locate, shutdown, monitor, and hijack [9, 10].

IV. BOTNET LIFE-CYCLE

A typical botnet can be created and maintained in five phases including: initial infection, secondary injection, connection, malicious command and control, update and maintenance. This life-cycle is depicted in Fig.1



During the initial infection phase, the attacker, scans a target subnet for known vulnerability, and infects victim machines through different exploitation methods. After initial infection, in secondary injection phase, the infected hosts execute a script known as shell-code. The bot application starts automatically each time the zombie is rebooted. In connection phase, the bot program establishes a command and control (C&C) channel, and connects the zombie to the command and control (C&C) server. After connection phase, the actual botnet command and control activities will be started. Bot programs receive and execute commands sent by bot master. Last phase is to maintain bots lively and updated. In this phase, bots are commanded to download an updated binary. Bot controllers may need to update their botnets for several reasons. For instance, they may need to update the bot binary to evade detection techniques, or they may intend to add new functionality to their bot army. This process is called server migration and it is very useful for bot masters to keep their botnet alive. Bot masters try to keep their botnets invisible and portable by using Dynamic DNS (DDNS) which is a resolution service that facilitates frequent updates and changes in server locations.

V. BOTNET DETECTION

Despite the long presence of malicious botnets, only few formal studies have examined the botnet problem. To date, just very little is known about botnet malicious behavior. The Honeynet project [2] was one of the pioneering informal of the botnet problem Botnet detection and tracking has been a major research topic in recent years. Different solutions have been proposed in academia For instance, solutions in [2] have been initial honeynet-based 6 solutions These techniques can be classified as being signature-based, anomaly-based, DNS-based, and mining-based that will be described and summarized in this section respectively.

A. Signature-based Detection

Knowledge of useful signatures and behavior of existing botnets is useful for botnet detection. For example, Snort is an open source intrusion detection system (IDS) that monitors network traffic to find signs of intrusion. Like most IDS systems, Snort is configured with a set of rules or signatures to log traffic which is deemed suspicioun [7].

B. Anomaly-based Detection

Anomaly-based detection techniques attempt to detect botnets based on several network traffic anomalies such as high network latency, high volumes of traffic, traffic on unusual ports, and unusual system behavior that could indicate presence of malicious bots in the network. Although anomaly detection techniques solve the problem of detecting unknown botnets, problems with anomaly detection can include detection of an IRC network that may be botnet. To solve this, Binkley and Singh [8] proposed an effective algorithm that combines TCP-based anomaly detection with IRC tokenization and IRC message statistics to create a system that can clearly detect client botnets..

C. DNS-based Detection

According to their observation DDNS responses indicating name error (NXDOMAIN) often correspond to botnet C&C servers that have been shut down by authorities. As mentioned in Section II, bots typically initiate connection with C&C server to get commands. In order to access the C&C server bots perform DNS queries to locate the respective C&C server that is typically hosted by a DDNS provider. Thus, it is possible to detect botnet DNS traffic by DNS monitoring and detect DNS traffic anomalies. This technique generates many false positives due to misclassification of legitimate and popular domains that use DNS with short time-to-live (TTL). Simultaneously sent by distributed bots.

VI. CONCLUSION

In this survey botnet detection techniques based on passive network traffic monitoring are classified into four classes including signature-based, anomaly-based, DNS based, and mining-base. Botnets, although quite simple in design, are effective attack tools. Finally, the research on defending against botnet proposes to simply shut down botmaster after they are identified. To better understand the botnet and stop its attack eventually, we provide a survey on existing research on botnets. The survey first discussed botnet formation and exploitation, the lifecycle, and two typical topologies intelligent techniques that rely on behavioral analysis offer the only effective means of detecting and defending against the proliferation of botnets. Those current botnet studies is still in a preliminary stage. Previous analysis shows that majority of botnet traditionally used IRC for their command and control. But we believe the botnets will advance to new communication architectures, for example, P2P-based botnet. And currently the defense against botnet is not very efficient, so much more work needs to be done in this field. Finally future botnet prediction may give us an advanced view of the botnet development. Good model can help people know the properties of botnet and thus control it..

VII. REFERENCES

1. http://en.wikipedia.org/wiki/Botnet.

2. Honeynet Project and Research Alliance. Know your enemy: Tracking Botnets,March2005.Seehttp://www.honeynet.org/papers/bots/.

3. D. Dagon, "Botnet detection and response, the network is the infection," 2005,http://www.caida.org/workshops/dnsoarc/200507/slides/oarc0507Dagon.pdf.

4. Han J. and Kamber M. Data Mining: Concepts and Techniques. Morgan Kaufman Publishers, San Francisco, CA, 2001.

5. D. Dagon, "Botnet Detection and Response, The Network is the Infection," in OARC Workshop, 2005.

6. Microsoft. Microsoft security intelligence report: Julydecember 2006. http://www.microsoft.com/technet/security/default.mspx, May 2007.

7. Snort IDS web page. http://www.snort.org, March 2006/.

8. J. R. Binkley and S. Singh, "An algorithm for anomaly-based botnet detection," in Proc. USENIX Steps to Reducing Unwanted Traffic on the Internet Workshop (SRUTI'06), , 2006, pp 43–48.

9. A. Ramachandran and N. Feamster, "Understanding the network-level behavior of spammers," in *Proc.* ACM SIGCOMM, 2006.

10. E. Cooke, F. Jahanian, and D. McPherson, "The zombie roundup: Understanding, detecting, and disrupting botnets," in Proc. Steps to Reducing Unwanted Traffic on the Internet Workshop (SRUTI'05), 2005, pp. 39-44.

11. M. Rajab, J. Zarfoss, F. Monrose, and A. Terzis, “A multifaceted approach to understanding the botnet phenomenon,” in Proc. 6th ACM SIGCOMM Conference on Internet Measurement (IMC’06), 2006, pp. 41–52.

12. K. K. R. Choo, “Zombies and Botnets,” Trends and issues in crime and criminal justice, no. 333, Australian Institute of Criminology, Canberra, March 2007.