Detecting Command and Control Traffic Using Botnet Correlator Module

Justin David Pineda, Jacqueline Cajefe, Japhet Eliel Marcos, Ronald Christianne David and Allan Dave Perez

School of Computer Science and Information Technology
Asia Pacific College
3 Humabon Place, Magallanes, Makati City 1232 PH

justinp@apc.edu.ph, jbcajefe@student.apc.edu.ph, japhmarcos@gmail.com, rddavid@student.apc.edu.ph, asperez@student.apc.edu.ph

Abstract. The proliferation of malicious Command and Control (C&C) servers or botnets is a very big security issue in the Internet today. Triggering malware can be found in most known, popular and visited websites. Any user who is tricked in clicking something interesting (usually an advertisement) is redirected to a malicious website or unknowingly forced to install a malware that makes them a victim (also known as zombie). When a lot of users have been victimized, malware is stored in their computers in stealth mode. When thousands or millions of computers are infected, the leader can order all infected machines to do something malicious like attacking servers to cause Distributed Denial of Service (DDOS) and other attacks on confidentiality. Only in 2013, the FBI discovered millions of machines were infected by a botnet called Citadel. The agency was able to shutdown the server leaving the victims still infected. Anti-virus and firewall solutions are defenseless in this type of attacks because botnets cannot be prevented using rule-based and signature-based solutions. The Botnet Correlator Module (BCM) is a mobile and powerful tool used to determine presence of active C&C activities in a Local Area Network (LAN) topology. It is capable of reading the most updated C&C knowledgebase from reputable sources and correlating it with Intrusion Detection System (IDS) rules as a detective control. The module loads the C&C information to the firewall as primary preventive control and consolidates traffic for further analysis and incident response.

Keywords: botnet, bots, zombie tracker, botnet detection

INTRODUCTION

People today live in an age where information is so ubiquitous and can be easily retrieved with just a few key strokes or screen taps. With all the recent technological advancements, anyone can be connected to the Internet in just a matter of seconds. They may opt to freely browse hundreds, or even thousands, of websites, and even build several communities with the power of social networking. However, what a lot of users usually overlook is that the Internet is not always a safe place. In reality, several threats are present that need to be given proper attention and response.
One of the biggest threats in the Internet is botnets. Botnets are Internet-connected computers infected by malicious content or malware that is usually unknowingly downloaded to the user’s computer. Any computer that falls to this scheme is called a “zombie.” These compromised computers can be used by a Master Computer, also referred to as a Mothership, to forward transmissions to other computers which usually involves performing Distributed Denial-of-Service attacks (DDoS), spreading viruses, or even disseminate spam [9].

**FIGURE 1.** Typical Botnet Setup

Botnets that attack through DDoS are increasing in number and volume. This may be a result of the trend that is leaning towards shorter duration with bigger packet volume per attack. According to a study conducted by Prolexic, during the fourth quarter of 2011, there has been a 45% increase in the number of DDoS attacks compared to the same quarter in 2010, and twice the rate of number of attacks during the third quarter of the same year [7]. As per IncapsulaDDoS Center, about 40% of respondents of a survey had experienced an attack that exceeded 1Gbps in 2011 and about 13% of those had at least one that had exceeded 10Gbps in bandwidth. It has been found that financial motivation is a common motivator for DDoS attacks [7].

**PROBLEM STATEMENT**

The “mothership” or botmaster in a master-slave relationship acts as the controller of the zombies. Facilitators of botnet activities usually let others, who pay them, rent these bots and let them do unscrupulous activities. Some cybercriminals even sell the list or database on his infected zombies to others [10].
About Online Tips enlisted the types of attacks that the “mothership” can do [1]:

1. Distributed Denial-of-Service Attacks (DDoS)
2. Spamming
3. Sniffing Traffic & Keylogging
4. Infecting New Hosts
5. Identity Theft
6. Attacking Chat Networks
7. Hosting of Illegal Software
8. Google AdSense Abuse & Advertisement Add-ons
9. Manipulating online polls

All these attacks enable the controller to get the bot’s personal information such as credit card numbers, bank account details and passwords. Once gathered, the said information can be sold to what they called the black marketplace or a forum of underground hackers and cyber criminals [6].

With all these cyber-attacks, one may be wondering how these bots are able to hide on the network and prevent themselves from being scanned by known anti-viruses. The botnet is very hard to track and crack because law enforcers need to find the master server that controls all other victims. Attackers also use a system named “Tor” which was originally designed to hide information and to prevent trace back of source [4]. According to Cisco Systems Inc. on the other hand, a major contributor to this dilemma is that botnet hosts and controllers are functioning with the use of captured resources. It makes botnets dynamic and ephemeral, and difficult to overthrow [2].

There were about 17 million bots according to the activity report from Japan’s Cyber Clean program. Japan has started to launch a system in their country to defend users against illegal acts of botnets and they were successful enough to inform half a million users to download and use a cleaning software and 32.3 percent responded [8].

Banks are also one of the critical and usual targets of botnets. According to Dell SecureWorks, “Attackers used financial trojans to target more than 900 financial institutions in more than 65 countries, and there was an increase in attacks and in the number of targeted organizations located in the Middle East, Africa, and Asia” [5][8].

![FIGURE 2. Typical Botnet Setup](image)
In addition, over $54 billion have been estimated to be the cost of fraud and identity theft in the U.S. for the past three years [3]. One maybe wondering why they and other countries haven’t done a big step to support and fight against botnets as one of the biggest threats in the online industry. Protection against these kinds of attacks may vary from different levels of users and devices, but a simple preventive act is to refrain from going to malicious websites.

RESULTS AND DISCUSSION

![Architectural Design of the Botnet Correlator Module](image)

The Botnet Correlator Module (BCM) is a system designed to avert the user from going to such botnet-infected websites based on reputable knowledgebase engines. The module can be loaded both to a firewall and an Intrusion Detection System (IDS) so that proper rules and policies can be set.

The BCM starts when the hostnames in the Botnet Source database are read. The Botnet Source database is a dynamic list that contains the source of the botnet sources. The following trackers are set by default in the Botnet Source:

2. Palevo Tracker (Website: [https://palevotracker.abuse.ch/blocklists.php](https://palevotracker.abuse.ch/blocklists.php))
3. Feodo Tracker (Website: [https://feodotracker.abuse.ch/blocklist/](https://feodotracker.abuse.ch/blocklist/))
FIGURE 4. Sample bad domains from https://zeustracker.abuse.ch/

The administrator can add and modify the contents of the Botnet Source. However, it is advised that the entries in this database must be scrutinized comprehensively to ensure proper security and performance in the network.

The Consolidation Timer allows the administrator to determine how often, in hours, the feeds from the Botnet Source are refreshed. The sources in the Botnet Source database can be classified based on severity. For example, the external Zeus tracker source has daily updates and the Bad Hostname list for Zeus must be updated every 24-hours. On the other hand, the SpyEye tracker (Website: https://spyeyetracker.abuse.ch/goodbye.html), which is not anymore updated frequently, maybe set to be refreshed every month or 730 hours. It may even be set not to be refreshed at all by setting to 0 hours.

The Hostname Consolidator is an interface where the administrator inputs or modifies Botnet Source contents. It is also responsible for reading feeds from the Botnet Source and storing the contents in the Bad Hostname database. It also processes and
associates the time set in the Consolidation Timer and the contents of the Botnet Source list.

The Bad Hostname database contains all hostnames determined in the Botnet Source feeds. The hostnames may either be IP addresses or URL’s. The contents of the Bad Hostname database differs from time to time based on the contents of the Botnet Source feeds and the refresh time set.

The Firewall Rule Generator and the IDS Rule Generator both read the Bad Hostname database and create a set of rules for the installed firewall and IDS devices. The firewall places a block policy for the blacklisted hostname to prevent users from accessing the infected website. The IDS acts as a detective control and notifies the administrator when an access to an infected website is detected. The reason why the bad hostname is placed both in the firewall and IDS is for defense-in-depth. There may be overlapping top-down policies in the firewall that allows a website even if it is listed as malicious later on. There may be some companies that only have either a firewall or an IDS. In either case, the BCM can be applied to any device.

The Alert Manager is the reporting and logging console of the BCM. It alerts the administrator if a Botnet traffic is blocked (firewall-initiated) or detected (IDS-initiated). The administrator can immediately check on the workstation that is accessing the malicious website and conduct a thorough investigation.

CONCLUSION AND RECOMMENDATION

Botnets are prevalent in any network environment and stealthy, making it hard to detect. Although many Anti-Virus companies are doing its effort to create ways and means to detect malware in the host level, the botnet variants increase exponentially daily. Creating a consolidated module that can be placed in any device like the BCM is very helpful and cost-efficient. Since most infected computers don’t know that they’re infected, it is crucial to be able to determine that they are communicating to the master site or infected site. This communication gives a hint that the computer is infected and
needs proper incident response. These issues are resolved by the features of the BCM.

By continuously adding more reputable feeds in the Botnet Source, the contents of the Bad Hostname are more comprehensive. Alerting the administrator in a real-time manner is very important as well. Over-all, the BCM is a handy yet robust tool that can be used in any network setting.

Some improvements or future research that can be done to improve BCM include:

1. Dynamically search for reputable feeds to be entered in the Botnet Source. If an algorithm to search for similar trackers like Zeus and Palevo is created, the administrator no longer needs to search for sources manually. This improvement may need to look for patterns in the trackers used.
2. Study the historical content of the Bad Hostname list and determine which hostnames are true alerts and false positives. This improvement may lessen very noisy but false alerts.
3. Research and create behavior-based alerts aside from signature-based ones. This improvement helps determining how the particular C&C activity works. Most botnets have an automated activity like reporting in particular time of the day or sending a repetitive similar packet daily etc. This can be added as a rule that can help determine the presence of a botnet activity without the need of a hostname.

REFERENCES

http://arstechnica.com/security/2013/04/a-beginners-guide-to-building-botnets-with-
little-assembly-required/


8. Lasar, M. (2010, October 21). Japan has national botnet warriors; why don’t we?
Retrieved May 14, 2014, from Ars Technica: http://www.arstechnica.com/tech-
policy/2010/10/japan-has-a-national-botnet-fighter-where-ours/

Search Security: http://searchsecurity.techtarget.com/definition/botnet