ASH1925022M

by Iftekhar Efat

Submission date: 13-Mar-2022 01:32AM (UTC-0500)
Submission ID: 1782988537
File name: ASH1925022M.pdf (276.27K)
Word count: 2048
Character count: 10808

Bot Detection using Network Traffic Analysis

Sourov Debnath
ASH1925022M

March 13, 2022

Report submitted for **CSE2205: Information Security** under BSc. in Software Engineering Program, Institute of Information Technology (IIT), Noakhali Science and Technology University

Project Area: **Information Security .....**
Project Supervisor: **MD. IFTEKHARUL ALAM EFAT**
Assistant Professor
Institute of Information Technology (IIT)
Noakhali Science and Technology University

Abstract

Recently, botnet becomes a social problem due to the expansion of bot infection. Ideally, all the vulnerable computers should be fortified to counteract laying malware. Accordingly, it is important to implement an information system which detects bot-infected computers and alerts them.

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.

In this paper, we focused on bots using IRC to communicate, and examined the behavior of such bots when they connected to an IRC server. We observed the actual traffic of some ports which were often used by IRC protocol. As a result, we confirmed that bots tried to reconnect to an IRC server at certain intervals when the server refused the connection from the bot. Moreover, we examined the distribution of the intervals and confirmed that the communication from other IP addresses showed similar behavior.

1 Introduction

Currently, computers and the Internet are indispensable for our life. Computers have spread explosively from their convenience, and the Internet has infiltrated the ordinary family by low price and large capacity. However, the number of users who connect the Internet with low consideration to the computer security and insufficient knowledge has been increased. Currently, computers are infected with malicious program such as computer viruses at little time if we connect computers to network without adopting defense methods to threats.Malicious software called bot has been a global problem in such a situation.

Once the bots have been configured with suitable malware, they are commanded by a series of bot controllers located around the Internet. These controllers generally utilize some familiar protocol such as Internet Relay Chat (IRC) simply for convenience, although they could certainly use any sort of communication protocol to interact with their bots. The idea is that the controller commands the bots to perform an attack task aimed at a target predetermined by the botnet operator. This works to the advantage of the attacker, because the bots are generally distributed across a broad geographic spectrum, and their bandwidth capacity might be substantive when viewed as a collective capability.
A botnet uses home-based PCs to distribute an attack.

This paper aims to discover new features by monitoring and analyzing operations of bots. Bots need to connect with a server that passes on instructions when instructions are received from the attacker. Then, we monitored operations when clients connected it with a server. In the result, we observed common operations to doubtful clients. In addition, we investigated intervals of the time that the client communicated with the server, and observed similar patterns.

2 Background

2.1 Botnets

A infected computer with bots is controlled by outside person. Botnets are network composed of two or more these computers[2]. Bots wait for instructions from the attacker when bots infect a computer. For example, those instructions are DDoS attack, sending spam mail, etc.

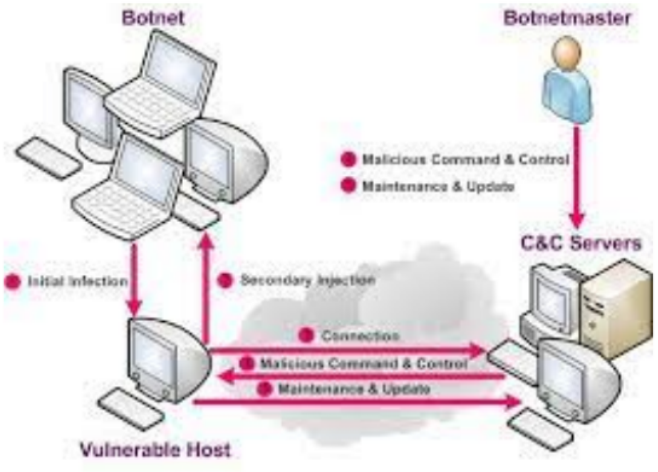

Figure 1: A Typical Botnet Life-cycle

Infected computers with bots connect with an instruction server. The instruction server relays instructions from the attacker to infected computers with bots. The server that becomes the center of this control is called a CC (Command and Control) server. The attacker's instructions reach infected computers with bots by relaying of instruction servers. Bots which receive instructions from the attacker act according to the instructions. It is infected computers with bots that actually take actions according to the attacker's instructions like this. Thus, it becomes one of assailants of the crimes of DDoS attack and sending spam mail, etc while victims can not notice.[1]

2.2 IRC(Internet Relay Chat)

When an attacker passes the instructions onto bots, IRC is generally used as a way of communications[3]. IRC is a talking system that exchanges the client's messages for text data on the TCP/IP protocol through servers. It is possible to send instructions to many bots by utilizing the multicast delivery mechanism of IRC. It is a reason why attackers use IRC to transmit instructions to bots.

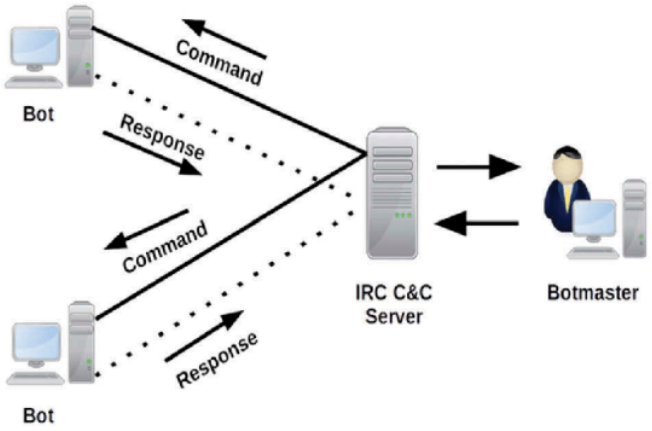

Figure 2: IRC based attack

When computers are infected with bots, they try to connect to an IRC server. The computer that connects with IRC participates in a specified channel, and waits for instructions. Instructions are communicated by attackers' messages. Bots execute instructions after bots are received them. The IRC server might be infected with bots and might be controlled. We can not stop an entire botnet if we can stop one IRC server. Therefore, it is difficult to ascertain the attacker.[2]

---

3 Detection Methods

3.1 Signature-based Detection

Signatures mentioned here are features information on the packets. Features information on the packets of bots is registered beforehand, and corresponding packets to the signatures are detected. The process of this method is easy because this compares simple byte sequences. Moreover, it is certainly possible to detect the defined illegal packets.

However, it is not possible to correspond to unknown bots because it is necessary to make definition files beforehand. Moreover, there is a problem that the expansion of a database of signatures happens because it always needs the registration of new signatures. That problem causes lower performance and higher management cost. Another shortcoming of this method is the time difference making the definition file to it after new bots are discovered, too.[2]

3.2 DNS-based Detection

DNS-based detection techniques are based on particular DNS information generated by a botnet. DNS-based detection techniques are similar to anomaly detection techniques as similar anomaly detection algorithms are applied on DNS traffic. As mentioned in Section II, bots typically initiate connection with CC server to get commands. In order to access the CC server bots perform DNS queries to locate the respective CC 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.

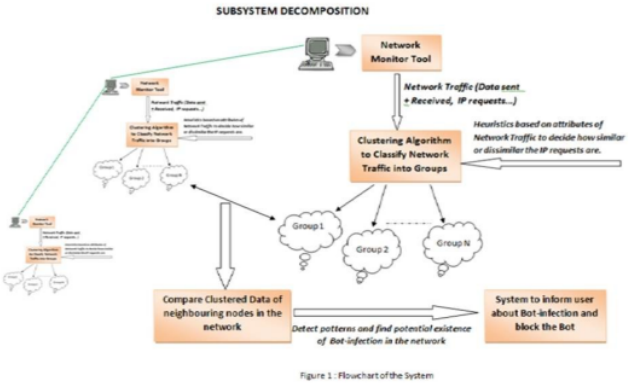

Figure 3: DNS-based Botnet detection techniques

3.3 Detection utilizing features of IRC client

Now, the attacker of botnets often uses IRC for the control. Then, there is a technique for detecting botnets by using features of IRC.

An IRC client is an interface for users to do messages exchanging, and it is operated interactively by users. On the other hand, IRC clients that exchange messages automatically like bots appear, too. In these two kinds of clients, we sure that the behaviors of interactive commands and the messages exchanging with IRC servers are different. Then, we pay attention to the behaviors of IRC clients to which operations are decided by the program.

Moreover, certain kind of features is seen in the commands used with IRC. The computer that seems that it is bot tend to scratch for information in the large range. For example, the bandwidth is measured and host's information is transmitted to other servers. When IRC is used by the chat purpose, this information and the commands to obtain such information are not needed.[2]

4 Proposed Methods

4.1 Overview

We aimed to observe new features of IRC-based bots in this research. Firstly, we monitored the port which generally used by IRC. As the result, we observed that clients with specific IP address are different from other clients in terms of flow of connection to IRC server.

4.2 Actions and features while connection to server

When an IRC client uses an IRC server, it is necessary to connect it with the IRC server. The procedure of connection is provided. A IRC client transmits the command of NICK and USER to the server. The IRC server registers the client after receiving both commands. The connection of the client and the server establishes by being processed these commands. Secondly, the client transmits the JOIN command to participate in the channel. The client can exchange messages mutually by participating in the channel. The PRIVMSG command or the NOTICE command are used for it.
Generally communication like this is following flows.

- NICK → USER → JOIN → PRIVMSG(or NOTICE) → ...

However, clients with specific IP addresses are refused to connect to the IRC server. IRC servers refuse the connection by the clients with suspicious behaviors in order to prevent the nickname duplication, the overload to the server and the connection by doubtful clients. Such clients repeat transmitting NICK and USER until the connection succeeds.
Thus, the flow of the clients is follows.

- NICK → (ERROR) → NICK → (ERROR) → ...
- NICK → USER → (ERROR) → NICK → USER → (ERROR) → ...

5 Consideration

In this chapter, we presumed that there are differences between IRC client by user and bots, and we examined traffic port used by an IRC server generally. We indicated that how much time the communication intervals between a client and an IRC server. As a result, we observed common features of clients traffic guessed to be bot. We confirmed that there is a bias of intervals of communication to the server in any traffic. In addition, there are differences of the distributions bias and the number of time in common features

6 Conclusion

In this paper, we aimed to examine new features on bot detection methods based on features of bot behaviors.

Firstly, we consider the features of behaviors of bots based on IRC. Secondly, we captured the traffic of port used by IRC, and examined in what patterns the feature was seen. As a result, we observed that clients guessed to be bot take different communication patterns compared with clients guessed not to be bot.

8

We consider that there are various advantages by making traffic visible like these.

- Judgments of kind of bots more than past viruses
- Automation of detection of bots by machine studies Future works are as follows.
- Investigations of more objects(problem of verification and generality)
- Considerations of detection by concrete visible
- Measures against bots that does not use IRC

References

[1] Maryam Feily, Alireza Shahrestani, and Sureswaran Ramadass. A survey of botnet and botnet detection. In *2009 Third International Conference on Emerging Security Information, Systems and Technologies*, pages 268–273. IEEE, 2009.

[2] Yuji Kugisaki, Yoshiaki Kasahara, Yoshiaki Hori, and Kouichi Sakurai. Bot detection based on traffic analysis. In *The 2007 International Conference on Intelligent Pervasive Computing (IPC 2007)*, pages 303–306. IEEE, 2007.

Notes: A critical component of the work is the list of references. We have discussed their use earlier – here I simply make some notes on their presentation.

This is one of the hardest parts to get just right. BibTeX can help a great deal, but you need to put a good deal of care in to make sure that

- the references are in a consistent format;
- all information is correct; and
- the information included is in the correct style for the intended audience.

Details *really* matter in this section. It's easy to lose marks in this section.

ASH1925022M

ORIGINALITY REPORT

89%	61%	78%	23%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Yuji Kugisaki, Yoshiaki Kasahara, Yoshiaki Hori, Kouichi Sakurai. "Bot Detection Based on Traffic Analysis", The 2007 International Conference on Intelligent Pervasive Computing (IPC 2007), 2007 Publication	61%
2	v1.overleaf.com Internet Source	9%
3	Edward G. Amoroso. "Correlation", Cyber Attacks, 2011 Publication	6%
4	www.ijert.org Internet Source	5%
5	Submitted to University of Missouri, Kansas City Student Paper	4%
6	ieeexplore.ieee.org Internet Source	2%
7	www.simonsfoundation.org Internet Source	2%

8	www.ijraset.com Internet Source	1 %
9	www.coursehero.com Internet Source	1 %

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

ASH1925022M

PAGE 1

Article Error You may need to use an article before this word. Consider using the article **the**.

PAGE 2

Proper Noun If this word is a proper noun, you need to capitalize it.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

PAGE 3

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Prep. You may be using the wrong preposition.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

Missing "," You may need to place a comma after this word.

PAGE 4

Confused You have a spelling mistake near the word **A** that makes **A** appear to be a confused-word error.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Article Error You may need to use an article before this word.

Article Error You may need to remove this article.

Article Error You may need to use an article before this word. Consider using the article **the**.

PAGE 5

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Prep. You may be using the wrong preposition.

PAGE 6

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Wrong Article You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.

Wrong Article You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Article Error You may need to remove this article.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Article Error You may need to remove this article.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Article Error You may need to use an article before this word. Consider using the article **a**.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Prep. You may be using the wrong preposition.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

PAGE 7

Confused You have a spelling mistake near the word **A** that makes **A** appear to be a confused-word error.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Possessive You may need to use an apostrophe to show possession.

PAGE 8

Missing "," You may need to place a comma after this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

PAGE 9

PAGE 10