A proposal of metrics for botnet detection based on its cooperative behavior

Mitsuaki Akiyama, Takanori Kawamoto, Masayoshi Shimamura,
Teruaki Yokoyama, Youki Kadobayashi, Suguru Yamaguchi
Nara Institute of Science and Technology
Internet Engineering Laboratory
Takayama 8916–5, Ikoma, Nara, Japan.
{mitsua-a, takan-ka, masayo-s, terua-yo, youki-k, suguru}@is.naist.jp

Abstract

In this paper, we propose three metrics for detecting botnets through analyzing their behavior. Our social infrastructure (i.e., the Internet) is currently experiencing the danger of bots' malicious activities as the scale of botnets increases. Although it is imperative to detect botnet to help protect computers from attacks, effective metrics for botnet detection have not been adequately researched. In this work we measure enormous amounts of traffic passing through the Asian Internet Interconnection Initiatives (AIII) infrastructure. To validate the effectiveness of our proposed metrics, we analyze measured traffic in three experiments. The experimental results reveal that our metrics are applicable for detecting botnets, but further research is needed to refine their performance.

1. INTRODUCTION

Recent times have seen the rapid spread of "bot" across the Internet. A bot is malicious software that compromises computers, and malicious people called "bot-masters" can control these computers with control packets. By receiving certain commands, bots can perform vulnerability scans, distributed denial-of-service attacks (DDoS attacks), and send enormous amounts of spam email. Since our social foundation (i.e., the Internet) is vulnerable to the danger of bots, it is imperative that we detect their activity.

A large number of bots forms a group called a "botnet," and they combine over the Internet to conduct malicious activities. Botnets have two main characteristics. First, all the components of a botnet are widely scattered across the Internet. We cannot comprehend the activity of botnets even if we observe one local network because the scale of botnets has been growing so rapidly. This means massive numbers of bots in infected computers assigned to valid IP addresses can send HTTP requests across the Web very quickly. Although a network administrator can observe this activity, he or she cannot determine whether the activity is malicious because the request sent by a bot is the same as a normal HTTP request.

In this paper, we propose three metrics to determine the behavior of botnets: relationship, response, and synchronization. To clarify the behavior of botnets, we measure a variety of traffic on a large actual network. This is necessary because the bots are generally distributed across a wide area network. In this work we adopted the Asian Internet Interconnection Initiatives[1] (AIII), which covers a broad swathe of Asia. We could easily observe all the traffic because its satellite network has a narrow bandwidth.

The reminder of this paper is organized as follows. Section 2 describes the features of a botnet. In Sect. 3, we discuss three proposed metrics in terms of the behavior of botnets. To validate the effectiveness of our metrics, in Sect. 4, we analyze the entire traffic volume of a botnet in AIII.

2. FEATURES OF BOTNETS

Before we discuss the metrics of botnets, we introduce the following typical functions of botnets: command and control (C&C), propagation, and self-updating. A "bot" is a program controlled by a "bot-master," and it performs malicious activities [3]. We call a malicious platform comprising large numbers of interconnected infected a "botnet."

A bot-master can operate bots via command and control (C&C). Here, we define C&C as a control platform for transmitting the commands of a bot-master and the activity reports of all bots in the network. Many existing service platforms are utilized for C&C. Above all, a bot-master takes advantage of Internet Relay Chat (IRC) because this makes it easy to operate C&C.

A bot-master implements a self-updating function into a bot. All bots in the botnet can periodically update themselves to extend functions and fix bugs enabling them to

Proceedings of the 2007 International Symposium
on Applications and the Internet Workshops (SAINTW'07)
0-7695-2757-4/07 $20.00 © 2007 IEEE

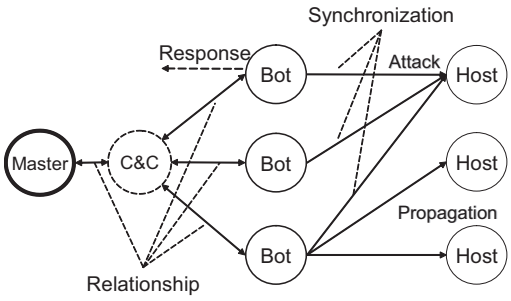


Figure 1. Behavior of a botnet: relationship, response, and synchronization

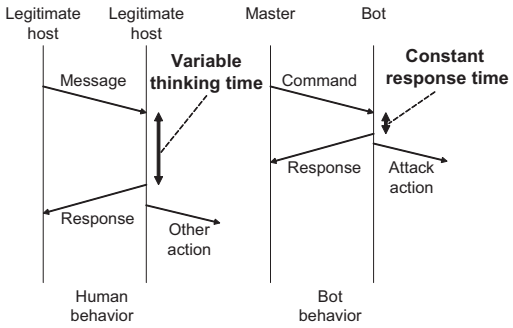


Figure 2. Comparison of response time between humans and bots

change their malicious acts under the complete control of the bot-master.

For instance, a malicious customer may rent a botnet to send spam, attack target sites, or commit click fraud. In this context, a bot-master customizes a botnet and sets function of the botnet to meet the customer's request.

Methods of IRC-based detection are exiting such as finding botnet commands in payload strings at unusual port [4] [2], these methods have high false positive rate. Defense based on CAPTCHA [5] use reverse Turing test to determine whether or not to the user is human.

3 METRICS FOR DETECTION

As mentioned in Sect. 2, all bots commit malicious activities according to the bot-master's commands. Here we propose three metrics derived from the behavior of botnet, assuming that the behavior of a botnet has the following three regularities: relationship, response, and synchronization. Figure 1 depicts the behavior of a botnet. A bot-master correlates the activities of all bots in the botnet through C&C. After the bots receive the master's command, they immediately and accurately respond and simultaneously conduct malicious activities at a set time.

3.1 Relationship

A botnet has a one-to-many relationship between the bot-master and bots. Here, we define that "relationship" as representing the connection with them over one protocol. Even if they have no direct connection over the transport layer, they may have a relationship over an upper layer such as overlay networks.

We assume that a botnet forms a dense topology in their relationship where a bot-master is centrally located. Since we focus on the structure of the relationship in order to detect a botnet, it is important to extract relationships in a botnet from measured traffic and identify suspicious groups that may be botnets.

3.2 Response

A botnet has another characteristic in terms of response. After bots receive commands from their master, they respond immediately and accurately. Figure 2 shows a comparison of response time between humans and bots. Regarding human behavior, when a legitimate host receives a message, it responds or performs an action from a wide variety of possibilities after a variable thinking time. On the other hand, when a bot receives a command from its master, it performs preprogrammed activities with a constant response time. Therefore, we assume that the response may be one of metrics for botnet detection. In the context of countermeasures against DDoS, this method has been applicable for distinguishing between normal and malicious hosts [7].

3.3 Synchronization

A bot basically carries out preprogrammed activities based on the bot-master's commands. We assume that all bots may be synchronized with each other, and that they simultaneously take the following actions: DDoS attack, reporting their activities, sharing information, or receiving commands. Therefore, we suppose that we can detect homogeneous and suspicious groups of bots by observing the amount of traffic or their actions.

4 EXPERIMENT

In this section, we analyze measured traffic to validate the effectiveness of our proposed metrics described in Sect. 3. We utilize a data set of traffic in AIII through a

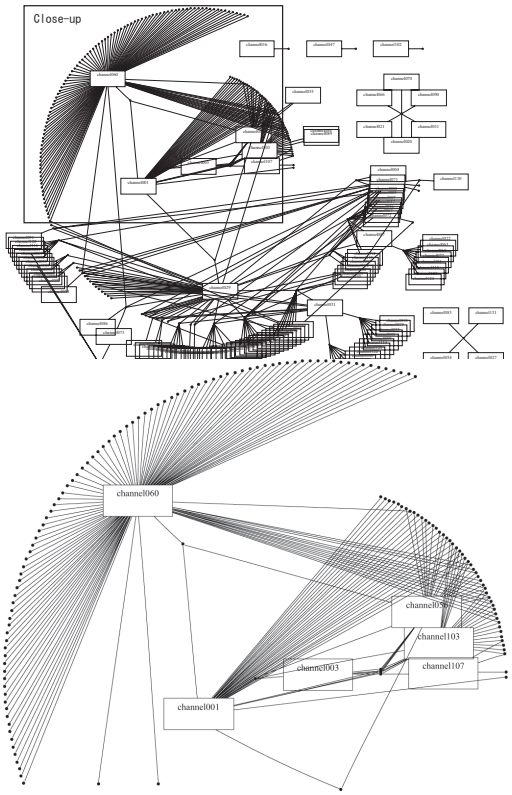
Proceedings of the 2007 International Symposium
on Applications and the Internet Workshops (SAINTW'07)
0-7695-2757-4/07 $20.00 © 2007 IEEE

satellite network. Traffic through the satellite network features the following two advantages: (1) link-shared media; and (2) narrow bandwidth. Therefore, we can measure all the traffic without packet sampling at the traffic aggregation point. The measurement time is 24 hour.

4.1 Anomalous structure

To find the relationship among bots as described in Sect. 3.1, we analyzed measured traffic on an IRC. In the measured traffic, we found many variants of bots to parse IRC traffic. To group an enormous number of IRC clients, we bound IP addresses to a tuple comprising nicknames and channels. Here, we focused on the topology of the application layer to observe the relationship among bots, because they may have no connection in the transport layer.

Figure 3 (a) depicts the Structure of IRC clients on an IRC channel, and Fig. 3 (b) represents a close-up of Fig. 3 (a). A point represents an IRC client, and a box indicates an IRC channel. In Fig. 3 (a), we observe that various numbers of clients joined each channel. Figure 3 (b) represents a group of malicious bots. The groups of bots are dense (the maximum number of these bots is 120), while groups of legitimate clients are loosely spaced. In comparison to the density of legitimate users, those of bots have an anomalous structure, indicating that a high-density structure of hosts is related to the relationship among bots.



(b) Enlarged view

Figure 3. Structure of IRC clients on an IRC channel

4.2 Response time

Next, we analyze the difference of response time between humans and bots to prove our assumption in terms of their response. We obtained response times of bots through measuring PRIVMSG messages exchanged between a botmaster and bots on an IRC. Similarly, we focused on PRIVMSG messages among legitimate clients as response times of humans. Figure 4 displays the distribution of response times. The results reveal the total number of responses for bots and legitimate users to be 173 and 1535 respectively. The x-axis represents the time in seconds, and the y-axis indicates the rate of distribution with respect to response time. The response times of humans vary in all ranges. In contrast with human behavior, however, the response times of bots is distributed across a very short time ranges. Therefore, we conclude that the response must be a significant factor in detecting botnets.

4.3 Synchronized traffic

Finally, we analyze measured traffic to observe synchronization among bots. As described in Sect. 4.1, many bots joined same the IRC channel because of their relationship. Therefore, we focused on "channel060" in Fig. 3 (b), which was compromised by 120 bots belonging to the same botnet.

Figure 5 (a) and (b) represents the measured IRC traffic of bots and legitimate hosts, respectively. In comparison with Fig. 5 (b), we observed synchronized traffic of bots in Fig. 5 (a). From time 10 to 11, all bots simultaneously conduct their respective activities. We observed that bots comunicate each other for malicious activities over C&C.Through this experiment, we conclude that the dynamics of the measured traffic is a component of the synchronization of bots.

4.4 Discussion

In this section we discuss what is remarkable about our metrics. First, we present the problem of proposed metrics, and then suggest a countermeasure to the problem.

Regarding the relationship metric, we found a relationship among bots to group all hosts. However, we note that the relationship among bots cannot be derived from only this metric because the connection of a massive number of

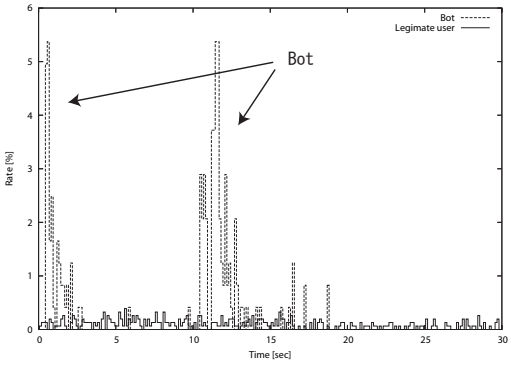


Figure 4. Distribution of response times

clients may converge to a legitimate one such as a Web service. As for the response metric, a bot-master can intentionally adjust the response time of bots to camouflage the similarity of their responses. Furthermore, regarding the synchronization metric, we could not easily detect synchronized bot traffic if we measured the traffic of random or all hosts. From the view point of synchronization, the traffic of multi-player online games [6] or some P2P application may have similar characteristic of client behavior. Moreover, sophisticated C&Cs using proxy or P2P network are reported consistently. Therefore, we must utilize a combination of all proposed metrics to achieve effective botnet detection. That is, it is necessary to measure the responses and dynamics of traffic after focusing on suspicious traffic based on the relationship in question.

5 CONCLUSION

In this paper, we proposed three metrics for botnet detection and experimentally evaluated the effectiveness of our metrics. Following that, we discussed a problem with our metrics and suggested a countermeasure to it. Overall, we conclude that the three metrics are applicable to detecting typical botnets. The future direction of this study will be to design a detection algorithm for various C&Cs based on an appropriate combination of our proposed metrics.

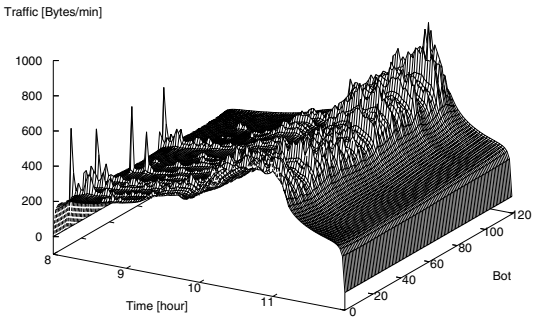
Acknowledgements

This work was supported in part by the 21st Century Center of Execellence (COE) Program.

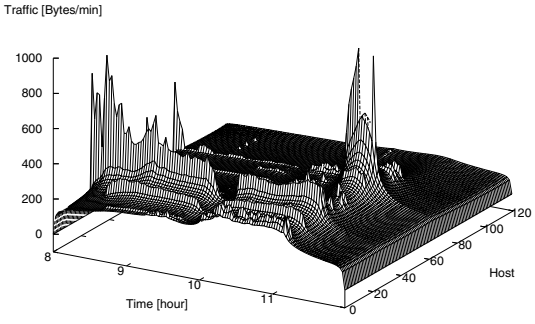
References

[1] Asian Internet Internetconnection Initiatives Project (AIII). `http://www.ai3.net/`.

[2] Bleeding edge threats. `http://www.bleedingthreats.net/`.



(a) Measured IRC traffic of bots



(b) Measured IRC traffic of legitimate hosts

Figure 5. Amount of traffic on each host

[3] The honeynet project, know your enemy: Tracking botnets. `http://honeynet.org/papers/bots/`.

[4] E. Cooke, F. Jahanian, and D. Mcpherson. The zombie roundup: Understanding, detecting, and disrupting botnets. pages 39–44, June 2005.

[5] S. Kandula, D. Katabi, M. Jacob, and A. Berger. Botz-4-sale: Surviving organized ddos attacks that mimic flash crowds. In *Proceedings of the 2nd USENIX Symposium on Networked Systems Design and Implementation (NSDI '05)*, Boston, MA, USA, May 2005.

[6] J. Kim, J. Choi, D. Chang, T. Kwon, Y. Choi, and E. Yuk. Traffic characteristics of a massively multi-player online role playing game. In *NetGames '05: Proceedings of 4th ACM SIGCOMM workshop on Network and system support for games*, pages 1–8, New York, NY, USA, 2005. ACM Press.

[7] S. Ranjan, R. Swaminathan, M. Uysal, and E. Knightly. DDoS-resilient scheduling to counter application layer attacks under imperfect detection. In *proceedings of INFOCOM 2006*, 2006.