IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

DETECTION OF STEALTHY P2P BOT COMPROMISED HOSTS IN A NETWORK

Raveesha H H

[*] **(Student)** Department of ISE, BMSCE, Bengaluru, India

DOI: 10.5281/zenodo.56028

ABSTRACT

Peer-to-peer (P2P) botnets have recently been adopted by botmasters for their resiliency against take-down efforts. Besides being harder to take down, modern botnets tend to be stealthier in the way they perform malicious activities, making current detection approaches ineffective. In addition, the rapidly growing volume of network traffic calls for high scalability of detection systems. In this paper, we propose a novel scalable botnet detection system capable of detecting stealthy P2P botnets. Our system first identifies all hosts that are likely engaged in P2P communications. It then derives statistical fingerprints to profile P2P traffic and further distinguish between P2P botnet traffic and legitimate P2P traffic. The parallelized computation with bounded complexity makes scalability a built-in feature of our system. Extensive evaluation has demonstrated both high detection accuracy and great scalability of the proposed system.

KEYWORDS: P2P traffic, botnet, stealthy, legitimate, bot compromised host .

INTRODUCTION

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority.

Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password**.**

A botnet is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks. This can be as mundane as keeping control of an Internet Relay Chat (IRC) channel, or it could be used to send spam email or participate in distributed denial-of-service attacks. The word botnet is a combination of the words robot and network. The term is usually used with a negative or malicious connotation.

Existing system

A few approaches capable of detecting P2P botnets have been proposed, Compared with the existing methods, the design goals of our approach are different in that: our approach does not assume that malicious activities are observable, unlike ; our approach does not require any botnet specific information to make the detection, unlike our approach needs to detect the compromised hosts that run both P2P bot and other legitimate P2P applications at the same time, unlike; Other methods use machine learning for detection, which require labeled P2P botnet data to train a statistical classifier.

Disadvantages

- A bot-compromised host may exhibit mixed patterns of both legitimate and botnet P2P traffic due to the coexistence of a file-sharing P2P application and a P2P bot on the same host.
- Modern botnets tend to use increasingly stealthy ways to perform malicious activities that are extremely hard to be observed in the network traffic. BotMiner identifies a group of hosts as bots belonging to the same botnet if they share similar communication patterns and meanwhile perform similar malicious activities, such as scanning, spamming, exploiting, etc.
- Unfortunately, the malicious activities may be stealthy and non-observable, thereby making BotMiner ineffective.

Proposed system

In Proposed system, aim at detecting all hosts within the monitored network that engage in P2P communications. And also we analyze raw traffic collected at the edge of the monitored network and apply a pre-filtering step to discard network flows that are unlikely to be generated by P2P applications. We first apply a flow clustering process. The distance between two flows is subsequently defined as the Euclidean distance of their two corresponding vectors. Two P2P bots in the same botnet should have small distance and thus are connected at lower level (forming a dense cluster). In contrast, legitimate P2P applications tend to have large distances and consequently are connected at the upper level.

Advantages

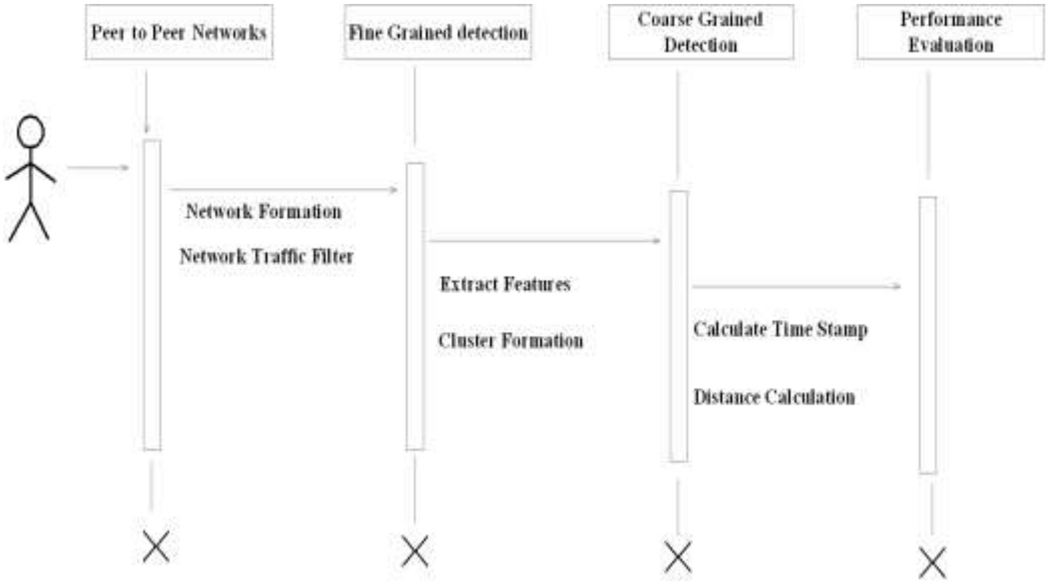
- In proposed System our system analyzes the traffic generated by the P2P clients and classifies them into either legitimate P2P clients or P2Pbots.
- It identify the performance bottleneck of our system and optimize its scalability.
- Our proposed system accomplishes high accuracy on detecting stealthy P2P bots and great scalability.
- It provides both high detection accuracy and great scalability of the proposed system.

MODULES AND METHODS

MODULES

- Network traffic filter
- Fine Grained Detection of P2P Clients
- Coarse Grained P2P Bots Detection
- Fine Grained Detection of P2P Bots
- Performance Evaluation

Figure:



Sequential flow representation of botnet detection

MODULES DESCRIPTION

Network traffic filter

The Traffic Filter component aims at filtering out network traffic that is unlikely to be related to P2Pcommunications. P2P clients usually contact their peers directly by looking up IPs from a routing table for the overlay network, rather than resolving a domain name. This is accomplished by passively analyzing DNS traffic. And also identifying network flows whose destination IP addresses were previously resolved in DNS responses .

Fine Grained Detection of P2P Clients

This component is responsible for detecting P2P clients by analyzing the remaining network flows after the Traffic Filter. We consider as successful those TCP connections with a completed SYN, SYN/ACK, ACK handshake, and those UDP (virtual) connections for which there was at least one "request" packet and a consequent response packet. The distance between two flows is subsequently defined as the euclidean distance of their two corresponding vectors. We then apply a clustering algorithm to partition the set of flows into a number of clusters .

Coarse Grained P2P Bots Detection

Bots are malicious programs used to perform profitable malicious activities, they represent valuable assets for the bot master, who will intuitively try to maximize utilization of bots. This is particularly true for P2P bots because in order to have a functional overlay network (the botnet), a sufficient number of peers needs to be always online. P2P applications is determined by users, which is likely to be transient. It is worth noting that some users may run certain legitimate P2P applications for as long as their machine is on.

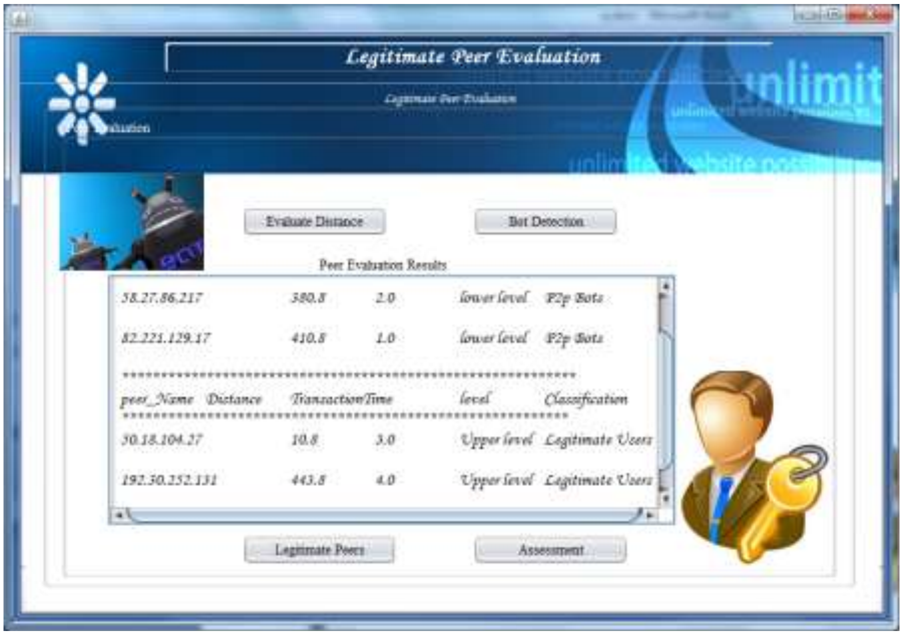
Fine Grained Detection of P2P Bots:

The objective of this component is to identify P2P bots from all persistent P2Pclients (i.e., set P). We leverage one feature: the overlap of peers contacted by two P2P bots belonging to the same P2Pbotnet is much larger than that contacted by two clients in the same legitimate P2P network. Two P2P bots in the same botnet should have small distance and thus are connected at lower level (forming a densecluster). In contrast, legitimate P2P applications tend to have large distances and consequently are connected at the upper level.

RESULTS

Analyzing the network traffic by appying the steps one by one, the peers are classified into p2p bots and legitimate users. The bot compromised peers in the botnet have small distance and thus are connected at lower level (forming a densecluster) and vice versa. The below figure shows that hosts are classified into bots and legitimated users after applying all methods as shown in section Modules and Methods.

Figure:



```
58.27.86.217      380.8    2.0      lower level   P2p Bots

82.221.129.17     410.8    1.0      lower level   P2p Bots

************************************************************
peer_Name  Distance  TransactionTime   level     Classification
************************************************************
50.18.104.27      10.8     3.0      Upper level  Legitimate Users

192.50.252.131    443.8    4.0      Upper level  Legitimate Users
```

Legitimate peer evaluation

CONCLUSION

This project presented a novel botnet detection system that is able to identify stealthy P2P botnets, whose malicious activities may not be observable. To accomplish this task, it derive statistical features of the P2P communications to first detect P2P clients and further distinguish between those that are part of legitimate P2P networks.

A centralized Fine-Grained P2P Bot Detection Component can perform detection based on all fingerprint clusters. As programmable network devices (e.g., switches) gain popularity, such improvements become practically feasible and also identify the performance bottleneck of the proposed system and optimize its scalability.

ACKNOWLEDGEMENTS

I would like to take this opportunity to express my profound gratitude and deep regard to my project guide Dr.M.Dakshayini, for their exemplary guidance, valuable feedback and constant encouragement throughout the duration of the project. Their valuable suggestions were of immense help throughout my project work. Their perceptive criticism kept me working to make this project in a much better way. Working under their was an extremely knowledgeable experience for me.

I would also like to give my sincere gratitude to all the friends and colleagues who filled in the survey, without which this research would be incomplete.

REFERENCES

[1] G. Gu, R. Perdisci, J. Zhang, and W. Lee, “Botminer: Clustering analysis of network traffic for protocol-and structure-independent botnet detection,” inProc. USENIX Security, 2008, pp. 139–154. T.-F

[2] Yen and M. K. Reiter, “Are your hosts trading or plotting? Telling P2P file-sharing and bots apart,” inProc. ICDCS, Jun. 2010, pp. 241–252.

[3] S. Nagaraja, P. Mittal, C.-Y. Hong, M. Caesar, and N. Borisov, “BotGrep: Finding P2P bots with structured graph analysis,” inProc. USENIX Security, 2010, pp. 1–16.

[4] S. Saad, I. Traore, A. Ghorbani, B. Sayed, D. Zhao, W. Lu, et al., “Detecting p2p botnets through network behavior analysis and machine learning,” in Proc. 9thAnnu. Int. Conf. PST, Jul. 2011, pp. 174-180.

[5] D. Liu, Y. Li, Y. Hu, and Z. Liang, “A P2P-botnet detection model and algorithms based on network streams analysis,” in *Proc. IEEE FITME*, Oct. 2010, pp. 55–58.

[6] W. Liao and C. Chang, “Peer to peer botnet detection using data mining scheme,” in *Proc. IEEE Int. Conf. ITA*, Aug. 2010, pp. 1–4.

[7] en.wikipedia.org/wiki/Botnet.