iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 Issue: IX Month of publication: September 2021

DOI: https://doi.org/10.22214/ijraset.2021.37945

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue IX Sep 2021- Available at www.ijraset.com

An Advanced Method for Detection of Botnet Using Intrusion Detection System

Alan Saji[1], Milan Sha[2], Raichan Kuriachan[3], Denny P Francis[4]
[1, 2, 3]Dual Degree MCA, Department of Computer Science, De Paul Institute of Science & Technology, Angamaly, MG University
[4]Asst. Professor, Department of Computer Science, De Paul Institute of Science & Technology, Angamaly, MG University

***Abstract:** A botnet, especially with remote-controlled bots that offers a platform for many cyber threats. The powerful measure in opposition to that botnet is supplied by IDS (Intrusion get right of entry to gadget). The IDS frequently monitors and identifies the presence of powerful attacks by way of assessing community site visitor's dangers. The IDS (PI-IDS) check for payload detects energetic tries to test the user's statistics gram protocol (UDP) and transmission manage protocol (TCP) comparisons with acknowledged attacks but the PI-IDS method is destroyed if the package is encrypted. PI-IDS shortages are conquer by using traffic-primarily based IDS (T-IDS), do now not take a look at package load; as a substitute, it exams the packet header to split get entry to, however this manner isn't always appropriate in modern-day global due to the fact network traffic is growing swiftly so looking at the header of every packet isn't always operating nicely and because of this advantage price is also essential. therefore, We endorse a new approach to this paper T-IDS creates an RDPLM (information-readable getting to know model) based totally on the set capabilities, in addition to a feature selection method, simplified sub spacing and multiple randomized meta-mastering techniques .The accuracy of our model is 99.984% and the education time is 21.38 s on a 9aaf3f374c58e8c9dcdd1ebf10256fa5 botnet database. it has been discovered that some mechanical studying fashions resemble a deep neural community, reducing mistakes in pruning the venture of locating a drug in a totally small series, and a random tree.*

***Keywords:** Botnet detection, Intrusion detection, Bots, Botnet traffic.*

I. INTRODUCTION

These days, our reliance on the internet has grown exponentially. as well as the want to protect our complete information to be had thru the net interface along with net passwords, business enterprise secrets, on line financial institution accounts, and social networking debts including Facebook. The emergence of bottles in the on line area over the past decade, and their ever-converting behaviour has created real challenges that cannot be effortlessly remedied.

Consistent with documents, botnet is described as a group of inflamed directors (also called bots or zombies) that perform independently and robotically, controlled via a bot-grasp (bot shepherd) who can integrate his malicious intent using inflamed bots. a number of the maximum risky activities that may be infiltrated via botnets encompass DDoS (dispensed denial-of-carrier), unsolicited mail, touchy identity theft, ransom ware and facts theft. In a DDoS botnet assault, a bot-grasp may additionally order all its bots to assault a selected server (for example: replace.microsoft.com) on a selected day, time and time with a malicious or anonymous proxy used as a hideout for the real command node. In a unsolicited mail campaign, the nodes that make up the bot network are accountable for sending spam behaviourally as unsolicited mail forwarding factors, bringing unsolicited mail emails to a list of cantered email addresses selected with the aid of the bot master. for example: a node this is part of a unsolicited mail botnet can be sent a listing of email addresses to junk mail of the day with the aid of the junk mail upload to be mailed. those unsolicited mail messages can put it on the market pharmaceutical products and can also purpose extra infections As mentioned in many papers (Provos et s thru e-mail hyperlinks or attachments to get greater bots, as is executed with bottles like typhoon and Waledac . it's miles a rip-off to steal touchy statistics that works to behave as internet proxies or web servers to supply hoax content to malicious users in an effort to acquire their e-banking or credit score card credentials. for example, web sites may keep content material that seems like a banking web page asking for login data while a user submits it, may be used by a plant agency to locate legitimate banking sites. eventually finances are transferred to non-forestall bills (Nazario & Holz, 2008).

Storm-like botnets are acknowledged to have inflamed greater than 2 million whilst Conficker has infected extra than nine million consistent with some estimates. As may be visible, the a ways-achieving results of the vicious intent of the bottles and their masters are a actual risk.

II. EXISTING FRAMEWORK

The use of antivirus software and firewall to protect the homeowner isn't always sufficient to prevent its contamination with botnet malware. Further, even supposing we can forestall the C&C server, the infected host (via bot) can be restarted in destiny attacks. In this case, we want a host-primarily based acquisition to complete the bot application at the host. There are various research on host-based strategies [9 - 11]. Huang [10] proposes a sensible solution for locating a bot host primarily based on monitoring community failures within the brief term. This technique is primarily based at the visitor's analyst at the host and not on finding the method. It does not system encrypted packets (command) from the botnet master to bots. in addition, it's miles confined to 1 botnet and does now not work with P2P botnet.

Formerly, botnet detection techniques have been based totally on payload analysis methods that take a look at the content material of TCP and UDP packets for malware signature. Payload analysis techniques eat assets that need processing massive amounts of bundle statistics and are a slow system. further, the new era of botnet uses encryption algorithms and different strategies to encrypt communique visitors and weigh down load loading analytics techniques. Waft-based signals released from network monitoring were alike to net-go with the flow functions like bytes in line with packet, bytes in step with-drift, and bytes in step with second.

III. FRAMEWORK DEMONSTRATE

There are systems that are vulnerable, which are only open to threats, that is. They are only intended for any commercial use. Technology is changing very fast these days. As a result, the banking industry is becoming more and more modern, every day. This creates a deep need for the automatic detection of threats, the machine, the cash register, and the slots on the seller's goods. Many researchers have asked the question, looking at the development of an effective and efficient automatic botnet detection mechanism. In an automated machine that can detect botnets, which is currently widely used in the technical area. Botnet detection technology, which is, in principle, aims to detect and alert the user from the visible to the invisible the characteristics of the technology.

As for the common people, they normally use the computers without high technical knowledge. The botnet detection system helps them to identify that their valuable data are not stolen.

IV. THE PROPOSED SCHEME

A. A general botnet detection technique capable of detecting the three types of botnet (IRC, HTTP, and P2P). For the network traffic analysis, our solution monitors two activities: botnet propagation techniques and network data flow. Botnet propagation detector aims to detect newly infected hosts before this bot starts the communication with the C&C server.

B. Our technique, for the host process analysis, monitors file system creation and registry modification

C. An effective algorithm, HANABot for Host and Network Analyser for Botnet detection, is developed.

In this research, we propose a general hybrid technique capable of detecting botnets in early phase. Early phase means that we try to detect malicious behaviour when the bot tries to propagate the bot malicious code to infect other machines or from the first packets exchanged between the bot and the C&C server. Our technique is deployed at the host level and the network level. The botnet communication traffic that we are interested in includes HTTP, P2P, IRC, and DNS using IP fluxing. Our technique consists of three components: network analyser, host analyser, and detection report:

1) The host analyser observes the process operation in file system and registry.

2) The network analyser observes the network traffic activity of the host process. These activities include botnet propagation operation and botnet communication with command and control server.

3) The detection report component generates a report with infected machines' IP addresses.

To achieve our goal, we develop an algorithm called HANABot (Host and Network Analyser for Botnet detection) to pre-process the data to detect bots based on set of features.

These features have been combined to generate a classification technique capable of differentiating botnet and legitimate flow records with a high degree of accuracy. Although some of these features were previously studied, they are reused and ordered in a different way to improve the accuracy in differentiating legitimate traffic from botnet traffic. In fact, these features are fundamental to achieve high botnet detection accuracy. Moreover, new features are proposed to enhance the botnet detection especially in early stage.

V. FOCAL POINTS

A. IRC Based

IRC based botnets are the preliminary types of botnets which are still effective and usable for attackers. IRC is a text based instant messaging protocol over the Internet. It works on client-server architecture but it is also suitable for distributed environments. In most cases interconnected IRC servers communicate each other and each has own subscribers. Thus, a subscriber on an IRC server may communicate with others if IRC servers are interconnected and are on the same channel. This interconnection between the IRC servers is called multiple IRC (mIRC). IRC-based bots use this infrastructure for malicious purposes by managing access lists, moving malicious files, sharing clients, sharing channel information and so on. A typical IRC based botnet is shown in Fig. 1 Victim machine is the compromised internet host which runs the executable bot triggered by a specific command from IRC server. Once a bot is installed on a victim host, it will make a copy into a configurable directory and let the malicious program to start with the operating system. A secured channel set up by the attacker to manage all the bots is called control channel. IRC server may be a compromised machine or even a legitimate service provider. Attacker is the one controls botnet. As in Fig. 1 attacker opens a private IRC channel on an ordinary IRC server. After spreading malwares on victim computers attacker waits bots to subscribe his own private IRC channel. Then he gives commands and controls the botnet infrastructures for his malicious purposes

B. P2P Botnet

P2P-based bot, Dubbed Sinit appeared. In 2004, bot was using P2P system to send commands to the other compromised hosts. Currently, Storm Worm (Holz, M, & Dahl, 2008) may be the most wide-spread P2P bot over the Internet. Many P2P networks have a central server or a list of peers who can be contacted to add a new peer. Centralized nature of this kind of P2P networks requires a bootstrap procedure which presents a weakness for P2P networks. To overcome this problem authors in (P. Wang, Sparks, & Cou, 2008) presented specific hybrid P2P botnet architecture. Hybrid P2P botnet architecture has servant and client bots who behave as clients and as servers in a traditional P2P file sharing network. Servant bots are connected to each other and form the backbone structure of the botnet. An attacker or bot-master can inject his commands into any hosts of the botnet. Each bot knows only its directed neighbours and transmits the command to its neighbours. If one bot is detected by intrusion detection systems only its neighbours are affected. The hybrid architecture for P2P botnets delivers some new capabilities: (1) it requires no bootstrap procedure; (2) only a limited number of bots nearby the captured one can be exposed; (3) an attacker can easily manage the entire botnet by issuing a single command

C. Http Botnet

Another type of C&C mechanism widely used is http-based botnets. In http-based botnets, bots and C&C centre communicate each other by using http protocol in an encrypted communication channel. In Chiang&Lloyd (2007), an http-based spam bot module in Rustock rootkit is analysed by using a well-known analysis tool IDA Pro to find the encryption key. The paper summarizes that a typical routine for the spam bot to send a spam is as following:

1) The bot asks the controller for local processes/files to kill and delete.
2) The controller sends back system information.
3) The bot asks for SMTP servers.
4) The bot gets failure responses from the SMTP servers.
5) The bot gets spam message
6) The bot gets target email addresses.

VI. CONCLUSION

In this study, we proposed a standard procedure that can detect a new botnet used 1on 3 levels: the level of hosting, the level of the network, or a combining both. Our favourite botnet communication traffic 5contains HTTP, P2P, IRC, and DNS using IP fluxing. Our proposed process 1contains of 3 components: a host analyser, a network analyser, and a discovery report: (i) a network analyser looks at two functions: botnet distribution and botnet communication with a C&C server. The network analyst contains three detectors: distributor, P2P detector, and non-P2P detector. (I i) The host analyst evaluates three functions: registration keys, file system, and the process time over time. The host analyser has three components: behavioural analysis, process integration, and process ethics. (I ii) The acquisition 1report is responsible for making the final score of the points based on the analyst's analysis or network analysis and provides for the report of the infected equipment.

We have developed the HANA Bot algorithm to process hosting traffic data, the performance of hosting processes, and the function of the road 2network to identify bots according to certain rules. All botnet flow records are successfully extracted using specific 1connection process and setting object vectors that differ from the botnet network traffic and the performance of its process. A comparison between the existing methods was provided, focusing on specific features and performance. In our future work, we will apply our solution to real-time separation. In fact, the suggested process uses an offline mode separation algorithm, in which the Internet network tracking is stored in a P.C.A.P file prior to processing them. This method can be developed to detect real-time detection quickly with a high degree of precision. This can be attained by creating the Net flow collector's export time much shorter and by providing Net flow clues sent to instant separation technology, as they arrive. This method can detect botnet activity and, on this basis, the action to be taken. The speed of processing done in real-time phases should be different, depending on a variety of factors, such as the duration of posting and size of the Net flow tracked channels. In addition, this function can be extended, at the hosting level, to bear the needle detection process used by the botnet to fully control the process [3,5].

REFERENCES

[1] M. Sanchez, “The 10 most common security threats explained,” 2017.

[2] http://blogs.cisco.com/smallbusiness/the-10-most-common-security-threats-explained.

[3] Us.norton.com. (n.d.), “Bots 2017, https://us.norton.com/botnet/.

[4] B. Cusack and S. Almutairi, “Listening to botnet communication channels to protect information systems,” in Proceedings of the Australian Digital Forensics Conference, pp. 44–52, Joondalup, Australia, December 2014.

[5] DDoS attacks in Q1, 2018, https://securelist.com/ddos-report-in-q1-2018/85373/.

[6] Kirubavathi and R. Anitha, “Botnet detection via mining of traffic flow characteristics,” Computers & Electrical Engineering, vol. 50, pp. 91–101, 2016.

[7] J. He, Y. Yang, X. Wang, Y. Zeng, and C. Tang, “PeerSorter: classifying generic P2P traffic in real-time,” in Proceedings of the 2014 IEEE 17th International Conference on Computational Science and Engineering, pp. 605–613, Chengdu, China, December 2014.

[8] W. H. Liao and C. C. Chang, “Peer to peer botnet detection using data mining scheme,” in Proceedings of the International Conference on Internet Technology and Applications, pp. 1–4, Wuhan, China, August 2010.