INTERNATIONAL JOURNAL OF
TECHNO-ENGINEERING
IJTE

ISSN: 2057-5688

BotDet: A System for Real Time Botnet Command and Control Traffic Detection

KUDUPUDI MADHU SHYAM
PG Scholar, Department of M.C.A,
S.K.B.R P.G College,
Amalapuram, E.G.Dt., A.P, India.
E-Mail: kudupudimadhushyam@gmail.com

Mr. NAGA. SRINIVASA RAO*
Asst. Professor, Dept of M.C.A,
S.K.B.R P.G College,
Amalapuram, E.G.Dt., A.P, India.
E-Mail:naagaasrinu@gmail.com

Abstract

Over the past decade, the digitization of services transformed the healthcare sector leading to a sharp rise in cyber security threats. Poor cyber security in the healthcare sector, coupled with high value of patient records attracted the attention of hackers. Sophisticated advanced persistent threats and malware have significantly contributed to increasing risks to the health sector. Many recent attacks are attributed to the spread of malicious software, e.g., ransom ware or bot malware. Machines infected with bot malware can be used as tools for remote attack or even crypto mining. This paper presents a novel approach, called BotDet, for botnet Command and Control (C&C) traffic detection to defend against malware attacks in critical ultra structure systems. There are two stages in the development of the proposed system: 1) we have developed four detection modules to detect different possible techniques used in botnet C&C communications and 2) we have designed a correlation framework to reduce the rate of false alarms raised by individual detection modules. Evaluation results show that BotDet balances the true positive rate and the false positive rate with 82.3% and 13.6%, respectively. Furthermore, it proves BotDet capability of real time detection.

Keyword: Botnet, Malware, Medical services, Real-time systems, Correlation, Monitoring, Command and control systems

1. INTRODUCTION

1.1 Introduction:

Country's national security, economic vitality and daily life rely on a safe, stable, and resilient cyberspace. This work depends on this vast array of networks to provide healthcare services, transport and communication, power our homes and run our economy [1]. Over the last decade, cyber attacks and intrusions have increased substantially, disrupting critical operations, resulting in business downtime and exposing sensitive personal and business information. Statistics draw a grim picture about the cyber security challenges and digital risks in the healthcare industry.

A report by the US Department of Health and Human Services [2] reveals that the healthcare sector has suffered from approximately four data breaches a week in 2016. To put this into perspective, one in every three American citizens was a victim of a breach in the healthcare sector. One of the primary reasons behind targeting healthcare organizations is that these organizations do not set protecting patient data as a priority, hence they under invest in qualified IT security personnel. The lack of solid information security infrastructure makes healthcare organizations an easy target. For instance, the recent attack on the National Health Service (NHS) in the UK showed that some hospitals and care providers systems were obsolete or has not been patched against well-known vulnerabilities. Additionally, patient records contain a wealth of information that can be used for identifying theft, financial/insurance fraud and even blackmailing. In 2017, 15,000 medical records have been stolen from Beverly Hills plastic surgery clinic to bully several high-profile celebrities. Today, intelligence agencies and governments military are actively preparing for cyber warfare.

Global activities against software, hardware, or data are referred to as cyber attack in the field of computer networks or systems. These activities lead to degrading, disrupting, destroying or denying access to network/system services or resources. Activities that target gathering intelligent are referred to as cyber exploitation [3]. The main objective of these activities is to gain unauthorized access to information and data. Over the last decade, malicious software or malware has increased, particularly in the healthcare industry. They have become one of the main reasons for the majority of the (distributed) denial-of-service (Dos) activities [4], direct and scanning attacks [5]. Noticeably, the motivation from fame seeking and curiosity has been shifted to unlawful financial attainment, which resulted in the sophistication of malicious software. Moreover, the availability of easy to-use toolkits to build malware will probably keep these malwares a threat to individuals, business and governments in the foreseeable future. Generally, there are two classes of malware: (a) malware that targets the general population and (b) customized information-stealing malware that targets particular organizations such as healthcare providers.

Zombies, which refer to those machines infected with bot malware, can be used as tools for remote attack or can be part of a botnet, which is completely controlled by the botnet master. Bots are "enslaved" host computers in botnets (networks formed by bots). One or more botmasters control bots in botnets and the intention is to perform malicious activities. The essential goal of botnets is to control organized crime syndicate, criminal, or group of criminals to use compromised machines for performing illegal activities. Experts mention that about 16–25% of the machines connected to the Internet are parts of botnets. Bots are different from the other malware. They are capable to create Command and Control (C&C) channels. Bots recognize themselves by their C&C channels through which they can be controlled, updated and instructed. The C&C servers are usually machines that have been exploited and sorted in a distributed form to limit traceability.

The detection of botnet C&C traffic is challenging for current Intrusion Detection Systems (IDS) for several reasons: (1) it is a benign traffic and follows normal protocol usage; (2) their volume of traffic is small; (3) the number of bots may be very small in the monitored network; and (4) Bots' communications may be encrypted. This work aims to contribute to IDS research, particularly to botnet C&C traffic detection. The proposed approach, called BotDet, undergoes two main phases. The first phase runs various modules to detect different possible techniques used in botnet C&C communications. The second phase uses a framework for alert correlation to reduce the number of false positives.

1.2 Purpose:

Intelligence agencies and governments military are actively preparing for cyber war fare .Global activities against software, hardware, or data are referred to as cyber attack in the field of computer networks or systems. These activities lead to degrading, disrupting, destroying or denying access to network/system service so sources. Activities that target gathering intelligent are referred to as cyber exploitation. The main objective of these activities is to gain unauthorized access to information and data.

1.3 Scope:

Statistics draw a grim picture about the cyber security challenges and digital risks in the healthcare industry. A report by the US Department of Health and Human Services [2] reveals that the healthcare sector has suffered from approximately four data breaches a week in 2016. To put this into perspective, one in every three American citizens was a victim of a breach in the healthcare sector. One of the primary reasons behind targeting healthcare organizations is that these organizations do not set protecting patient data as a priority, hence they under invest in quailed IT security personnel.

1.4 Motivation:

The motivation from fame seeking and curiosity has been shifted to unlawful financial attainment, which resulted in the sophistication of malicious software [7]. Moreover, the availability of easy to-use toolkits to build malware will probably keep these malwares a threat to individuals, business and governments in the foreseeable future.

1.5 Overview:

An approach for bot-infected machines detection which requires no previous knowledge of the way a bot spreads. It depends on the characteristic behavior of a bot, particularly: (a) receiving commands from the botmaster, and (b) responding to these commands by carrying out some activities. Both commands and responses can be monitored in the network traffic and detection models can be built. The authors ran a bot in a controlled network to record its traffic and then they examine the received commands and responses activities. For this purpose, they proposed techniques to determine points in the network that were involved in the response activity. Afterwards, the traffic had been observed before this response is analyzed to find the corresponding command. By these detection models the network traffic is scanned for similar actions aiming to detect bot-infected machines.

2. RELATED WORKS

In [6], Balram and Wilscy propose a host-based approach for botnet C&C communication detection. This approach analyses suspicious flows produced by filtering out benign traffic from the traffic created by a host. A normal profile of the host traffic is used for the filtering. The behavioral pattern of flows to all destinations is examined in a bid to generate the host profile. This approach achieved a detection rate of 100% and false positives of 8%.

In [7], Fedynyshyn et al. present a host-based detection method able to detect the existence of botnet C&C traffic on the observed machine, and also categorize the type of C&C communication used by the bot, e.g., peer-to-peer (P2P) based, HTTP-based or IRC-based. As it does not examine the packets payloads, their detection method is independent of the content of the C&C messages. Their method for detecting and categorizing botnet C&C connections is based on three hypotheses: (1) it is possible to distinguish between botnet C&C communication and botnet non-C&C communication, (2) it is possible to distinguish between botnet C&C communication and valid communication and (3) there are shared characteristics between different styles of C&C and different botnet families.

An approach for bot-infected machines detection was presented by Wurzinger et al. [8], which require no previous knowledge of the way a bot spreads. It depends on the characteristic behavior of a bot, particularly: (a) receiving commands from the botmaster, and (b) responding to these commands by carrying out some activities. Both commands and responses can be monitored in the network traffic and detection models can be built. The authors ran a bot in a controlled network to record its traffic and then they examine the received commands and responses activities. For this purpose, they proposed techniques to determine points in the network that were involved in the response activity. Afterwards, the traffic had been observed before this response is analyzed to find the corresponding command. By these detection models the network traffic is scanned for similar actions aiming to detect bot-infected machines.

Giroire et al. [9] presented another host-based detection method for botnet C&C traffic detection. This method is based on the fact that the infected machines should stay in contact with C&C severs to be instructed and controlled by the botmaster. It is assumed that those connections are persistent and established regularly. A white-list of benign destinations that the user regularly contacts is built and all the user outbound traffic is monitored. When a connection is persistent enough and the destination is not white-listed, an alert is generated and the user is informed and asked to decide. If the destination is legitimate, the user can easily add it to the white-list; otherwise the connection is deemed as C&C communication and blocked.

A network-based botnet detection system, BotSniffer, was proposed in [10]. This system is based on anomalybased detection algorithms to detect both HTTP and IRC based C&Cs with no previous knowledge of C&C server addresses or signatures. The main goal in BotSniffer is to identify spatial-temporal similarity patterns and correlation in network traffic that are generated between the infected hosts and botnet C&C servers. They study two common styles usually used for botnet control, "push" and "pull". An example for the push style is IRC-based C&C is where the commands are sent or pushed to the infected hosts. In the pull style, the commands are downloaded (or pulled) by the infected hosts, as in HTTP-based C&C. When a set of hosts is found to carry out the same actions in response to similar messages from the same server, it is considered to be part of a botnet

3. EXISTING SYSTEM

There are two main approaches for botnet C&C traffic detection in the existing systems. The first one is based on setting up honey nets in the network. This approach is often used to understand and analyze a botnet technology and characteristics. However, honeynets are not always capable of detecting bot infection. The second approach is based on passive traffic monitoring. These approaches can be classified into signature-based and anomaly-based methods, respectively. Signature-based detection methods make use of known signatures and behavior of existing botnets, therefore it can be used for detecting only known botnets. Anomaly-based detection methods are able to detect unknown botnets as they try to detect botnets based on network traffic anomalies like traffic on unusual ports, high volumes of traffic, unusual system behavior and high network latency.Balram and Wilscy propose a host-based approach for botnet C&C communication detection. Fedynyshyn et al. present a host-based detection method able to detect the existence of botnet C&C traffic on the observed machine, and also categorize the type of C&C communication used by the bot, e.g., peer-to-peer (P2P) based, HTTP-based or IRC-based.

3.1 Disadvantages:

These existing works cannot analyze and detects hidden botnet C&C. Botnet C&C traffic is cannot detect by the observation of direct causes of traffic flows. These works cannot reduce the rate of false alarms raised by individual detection modules.

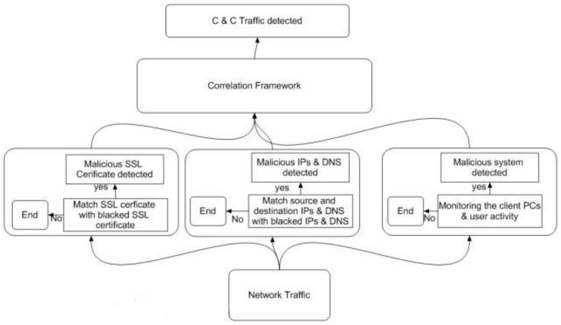
4. PROPOSED SYSTEM

In this project focused on network-based detection and host based detection of bots in Internet-connected networks with regard to the botnet threat and botnet detection. Invisibility is an important factor in botnet survivability; fortunately the invisibility of a botnet has practical limitations. Important causes that limit the invisibility are attack traffic, malware installation, limited resources and other survivability measures. The proposed work based on three major detection methods such as Untrusted Destination by Identifier (UDI), malicious SSL certificate, Traffic Flow Causality (TFC) and it is used to analyze and detect the malicious network traffic in real time.

4.1 Advantages

The framework that analyzes and detects hidden botnet C&C. Botnet C&C traffic is detected by the observation of direct causes of traffic flows. To reduce the rate of false alarms raised by individual detection modules

5. ARCHITECTURE


C & C Traffic detected
Correlation Framework
Malicious SSL Cerificate detected
yes
End
No
Match SSL cerficate with blacked SSL certificate
Malicious IPs & DNS detected
yes
End
No
Match source and destination IPs & DNS with blacked IPs & DNS
Malicious system detected
yes
End
No
Monitoring the client PCs & user activity
Network Traffic

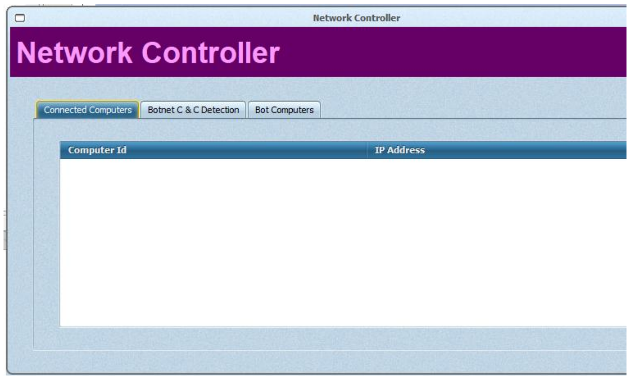
6. Modules Description:

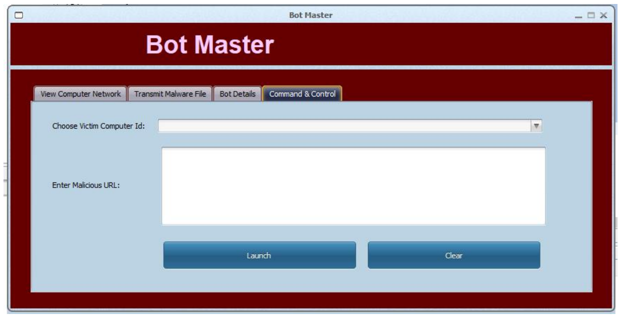
Botnet C & C detection by SSL certificate (https is valid or not). Botnet C & C detection by IP Address.. Botnet C & C detection by DNS. (Detect Malicious URL or not). Botnet C & C detection by causal analysis of traffic flows.

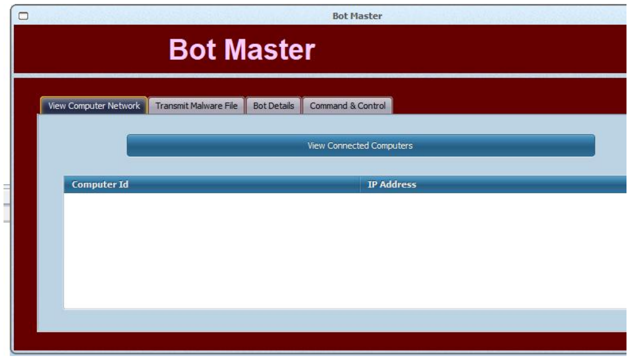
Our proposed approach for botnet C&C traffic detection is outlined. This approach is based on the correlation between the events, which are the outputs of the detection modules. The proposed approach consists of two main phase's communication. To this end, three detection modules have been proposed: Botnet C & C by SSL certificate detection module, Botnet C & C by untrusted destinations detection module and Botnet C & C by causal analysis of traffic flows detection module each detection module is independent of the other modules and aims to detect one technique that can be used in C&C communication. The outputs of these detection modules should be submitted to the second phase where they are correlated to raise an alert and block on botnet C&C traffic detection. In the second phase, the correlation framework takes events (the outputs of our detection modules) as an input and correlates them to raise an alert and block on botnet C&C traffic detection. The correlation method is based on voting between the detection methods to make the final decision about the detection.

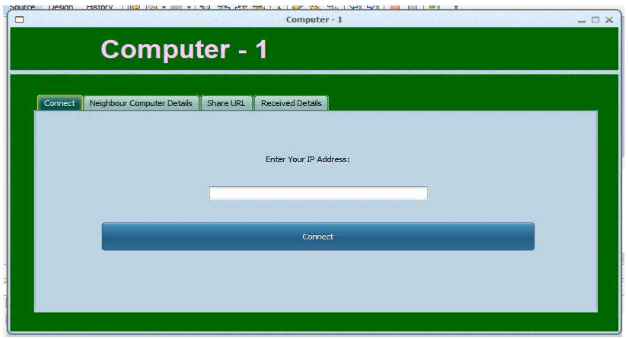
7. SCREEN SHOTS

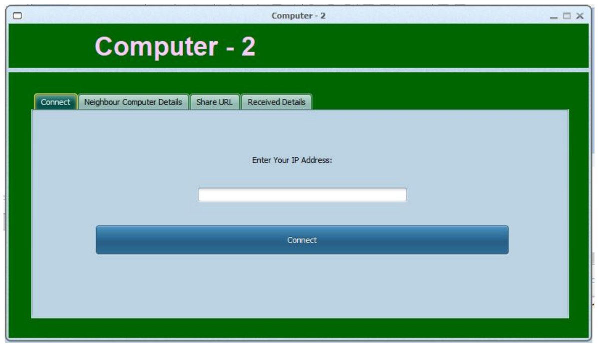
ISSN: 2057-5688

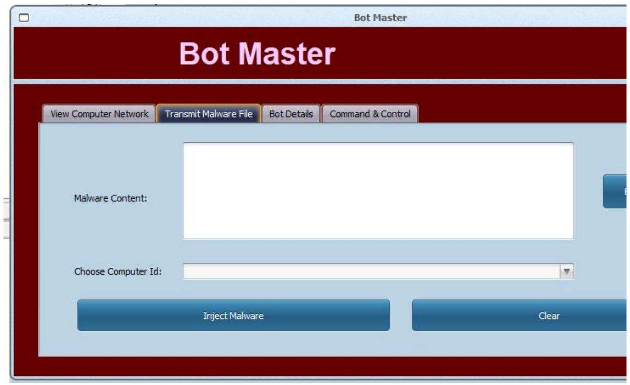


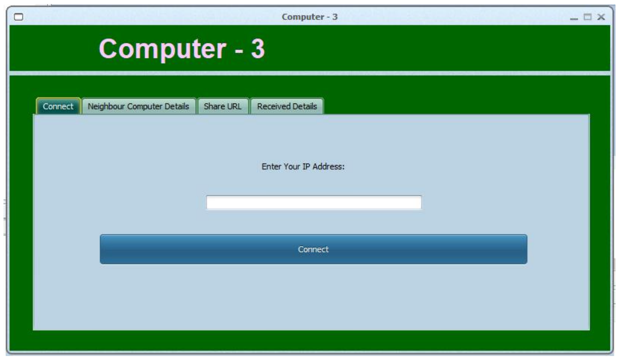












8 CONCLUSION AND FUTURE ENHANCEMENTS

This work presents a novel approach called BotDet for botnet C&C traffic detection. The developed system (BotDet) runs through two main phases, the first one includes developed modules to detect possible techniques used in botnet C&C communications. The second phase uses a framework for alert correlation, based on voting between the detection modules. BotDet achieves detection rate and false alarm of 82:3% and 13:6% respectively. Additionally, the blacklists used in some of the detection modules are automatically updated based on different intelligent feeds, which gives BotDet the capability of real time detection

9. BIBLIOGRAPHY

1. Improving product marketing by predicting early reviewers on E-Commerce websites
S. Kodati, M. Dhasaratham, V. V. S. S. Srikanth, and K. M. Reddy, "Improving product marketing by predicting early reviewers on E-Commerce websites," Deleted Journal, no. 43, pp. 17–25, Apr. 2024, doi: 10.55529/ijrise.43.17.25.

2. Kodati, Dr Sarangam, et al. "Classification of SARS Cov-2 and Non-SARS Cov-2 Pneumonia Using CNN." Journal of Prevention, Diagnosis and Management of Human Diseases (JPDMHD) 2799-1202, vol. 3, no. 06, 23 Nov. 2023, pp. 32–40, journal.hmjournals.com/index.php/JPDMHD/article/view/3406/2798, https://doi.org/10.55529/jpdmhd.36.32.40. Accessed 2 May 2024.

3. V. Srikanth, "CHRONIC KIDNEY DISEASE PREDICTION USING MACHINE LEARNING ALGORITHMS," IJTE, pp. 106–109, Jan. 2023, [Online]. Available: http://ijte.uk/archive/2023/CHRONIC-KIDNEY-DISEASE-PREDICTION-USING-MACHINE-LEARNING-ALGORITHMS.pdf

4. V. SRIKANTH, "DETECTION OF PLAGIARISM USING ARTIFICIAL NEURAL NETWORKS," International Journal of Technology and Engineering, vol. XV, no. I, pp. 201–204, Feb. 2023, [Online]. Available: http://ijte.uk/archive/2023/DETECTION-OF-PLAGIARISM-USING-ARTIFICIAL-NEURAL-NETWORKS.pdf

5. V. SRIKANTH, "A REVIEW ON MODELING AND PREDICTING OF CYBER HACKING BREACHES," IJTE, vol. XV, no. I, pp. 300–302, Mar. 2023, [Online]. Available: http://ijte.uk/archive/2023/A-REVIEW-ON-MODELING-AND-PREDICTING-OF-CYBER-HACKING-BREACHES.pdf

6. S. Kodati, M. Dhasaratham, V. V. S. S. Srikanth, and K. M. Reddy, "Detection of fake currency using machine learning

ISSN: 2057-5688

models," Deleted Journal, no. 41, pp. 31–38, Dec. 2023, doi: 10.55529/ijrise.41.31.38.

7. "Cyberspace and the Law: Cyber Security." IOK STORE, iokstore.inkofknowledge.com/product-page/cyberspace-and-the-law. Accessed 2 May 2024.

8. "Data Structures Laboratory Manual." IOK STORE, www.iokstore.inkofknowledge.com/product-page/data-structures-laboratory-manual. Accessed 2 May 2024.

9. Data Analytics Using R Programming Lab." IOK STORE, www.iokstore.inkofknowledge.com/product-page/data-analytics-using-r-programming-lab. Accessed 2 May 2024.

10. V. Srikanth, Dr. I. Reddy, and Department of Information Technology, Sreenidhi Institute of Science and Technology, Hyderabad, 501301, India, "WIRELESS SECURITY PROTOCOLS (WEP,WPA,WPA2 & WPA3)," journal-article, 2019. [Online]. Available: https://www.jetir.org/papers/JETIRDA06001.pdf

10. V. SRIKANTH, "Secured ranked keyword search over encrypted data on cloud," IJIEMR Transactions, vol. 07, no. 02, pp. 111–119, Feb. 2018, [Online]. Available: https://www.ijiemr.org/public/uploads/paper/1121_approvedpaper.pdf

11. V. SRIKANTH, "A NOVEL METHOD FOR BUG DETECTION TECHNIQUES USING INSTANCE SELECTION AND FEATURE SELECTION," IJIEMR Transactions, vol. 06, no. 12, pp. 337–344, Dec. 2017, [Online]. Available: https://www.ijiemr.org/public/uploads/paper/976_approvedpaper.pdf

12 . SRIKANTH MCA, MTECH, MBA, "ANALYZING THE TWEETS AND DETECT TRAFFIC FROM TWITTER ANALYSIS," Feb. 2017. [Online]. Available: http://ijmtarc.in/Papers/Current%20Papers/IJMTARC-170309.pdf

14 Srikanth, V. 2018. "Secret Sharing Algorithm Implementation on Single to Multi Cloud." International Journal of Research 5 (01): 1036–41. https://journals.pen2print.org/index.php/ijr/article/view/11641/11021.

5. K. Meenendranath Reddy, et al. Design and Implementation of Robotic Arm for Pick and Place by Using Bluetooth Technology. No. 34, 16 June 2023, pp. 16–21, https://doi.org/10.55529/jeet.34.16.21. Accessed 20 Aug. 2023.

16. Babu, Dr P. Sankar, et al. "Intelligents Traffic Light Controller for Ambulance." Journal of Image Processing and Intelligent

Remote Sensing(JIPIRS) ISSN 2815-0953, vol. 3, no. 04, 19 July 2023, pp. 19–26, journal.hmjournals.com/index.php/JIPIRS/article/view/2425/2316, https://doi.org/10.55529/jipirs.34.19.26. Accessed 24 Aug. 2023.

17. S. Maddilety, et al. “Grid Synchronization Failure Detection on Sensing the Frequency and Voltage beyond the Ranges.” Journal of Energy Engineering and Thermodynamics, no. 35, 4 Aug. 2023, pp. 1–7, https://doi.org/10.55529/jeet.35.1.7. Accessed 2 May 2024.

18. K. Meenendranath Reddy, et al. Design and Implementation of Robotic Arm for Pick and Place by Using Bluetooth Technology. No. 34, 16 June 2023, pp. 16–21, https://doi.org/10.55529/jeet.34.16.21. Accessed 20 Aug. 2023