Constructing IoT Botnets Attack Pattern for Host-based and Network-based Platform

Wan Nur Fatihah Wan Mohd Zaki, Raihana Syahirah Abdullah
Warusia Yassin, Faizal M.A, Muhammad Safwan Rosli
Information Security Forensics and Computer Networking (INSFORNET)
Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka (UTeM)
Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia

***Abstract*—Internet of things (IoT) is the things or devices with software, intelligent sensors interconnected via the internet to send and receive data with another device. This capacity makes things, i.e., smartphones, smart homes, intelligent toys, baby monitors, IP cameras, and many more to act as intelligent devices like artificial intelligence (AI) and be utilized in the everyday life-world widely. IoT has enormous expansion potential, and many challenges have been acknowledged but are still open today. The botnet is a collection of bots from IoT devices used to launch extensive network attacks. In addition, rapid growth in technology has led to an incomplete understanding of IoT. The increasing number of IoT devices has led to the spread of malware targeting IoT devices make IoT Botnet behaviors challenging to identify and determine. To detect these IoT Botnets, a preliminary experiment on flow analysis is necessary. This paper is to identify IoT Botnet attack patterns from the IoT Botnet behavior that get from IoT Botnet activities. Therefore, this research is to identify IoT Botnet attack patterns in a host-based and network-based environment. First, this paper contributes to discovering, recognizing, categorizing, and detecting IoT Botnet activities. Next, organizing information to have a better understanding of the IoT botnet's problem and potential solutions. Then, construct the IoT Botnet attack pattern by analyzing the characteristics of the IoT Botnet behavior. This IoT Botnet attack pattern divides into two environments which are host-based and network-based. As a result, this paper aims to inform people about the attack pattern when the IoT device has been infected and become part of the botnet.**

***Keywords*—IoT; botnet; IoT botnet; host-based; network-based**

I. INTRODUCTION

Internet of things (IoT) is the things or devices with software, intelligent sensors interconnected via the internet to send and receive data with another device. This capacity makes things, i.e., smartphones, smart homes, intelligent toys, baby monitors, IP cameras, and many more, act as intelligent devices and widely be utilized in the everyday lifeworld. For instance, a smartphone can be streaming any melody that can be searched from the worldwide song, even though it's not in the storage of that smartphone. Besides smartphones, the intelligent home recently received much attention from the public, such as in [1]–[3] as it has been put into action as IoT devices. Moreover, Botnet is the short form of robot and network as claimed by [4],[5]. In addition, Botnets can compromise any machine system and become bots, automatons, drones, or zombies, from an assortment of computers infected with a malicious program [6]–[8].

This paper is to identify IoT Botnet attack patterns. The paper's goal is to identify IoT Botnet attack patterns in a host-based and network-based environment. Subsequently, the paper title Discovering IoT Botnet Detection Method: A Review [9] proposed placing IoT Botnet attack improved generic taxonomy. To detect these IoT Botnets, a preliminary experiment on flow analysis is necessary. The primary purpose of this experiment is to identify IoT Botnet attack patterns in a host-based and network-based environment. Then, the integration of the integrated analysis approach with static and dynamic analysis approaches has been performed. The integrated analysis will be used in profiling IoT Botnet attacks and characteristics. Then, the findings of both studies resulted in attack pattern identification and integrated analysis are contributed to IoT Botnets' attack patterns.

The flow of this experiment starts with discovering, recognizing, categorizing, and detecting IoT Botnet activities; Second, organizing information to have a better understanding of the IoT botnet's problem and potential solutions. The third step is data collection. The dataset used is IoT-23 since it provides real-world network information and a massive dataset of real-world and categorized IoT Botnet; fourth, analyzing the characteristics of the IoT Botnet behavior. Fifth, construct IoT Botnet attack pattern divides into two platforms which are host-based and network-based. As a result, this paper proposed a general IoT Botnet attack pattern for host-based and network-based platforms.

The expected output is the proposed general IoT Botnet attack pattern for host-based and network-based platforms using a dataset from IoT-23 [10]. From this dataset, the IoT Botnet attack pattern is constructed in two environments which are host-based and network-based. Therefore, even though this paper will face many constraints, but the expected output can be achieved. Crucially, the proposed is for developing the improved IoT botnets detection technique. Furthermore, this IoT Botnet attack pattern is constructed because nowadays, IoT has been used widely, as shown in Fig. 1. The Internet of Things is the decisive technology, as stated by Deloitte Global analysis [11].

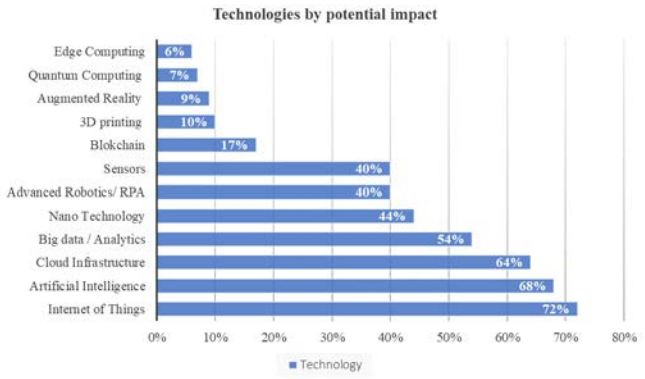

Fig. 1. Static Technology by Potential Impact in Industry 4.0 from Deloitte Global Analysis [11].

This paper has four sections, the Section I is the introduction of this paper consist of background, problem statement, objectives, and improvement of IoT Botnet. Next is Section II, which discusses the related work from previous research based on IoT devices infected by malware. Then, in Section III, discuss the methodology and implementation of this paper consist of the analysis process, data preparation, IoT Botnet experimental approach, IoT Botnet behavior for host-based and network-based platform, and present the proposed general IoT Botnet attack pattern for host-based and network-based platform. Lastly, section IV discusses the conclusion of this paper, limitations, and further work of this research.

II. Related Work

The Internet of Things is the things that are being connected with the internet. When something is connected with the internet, that implies it can send data, get data, or in both conditions. This capacity to send and receive data makes things brilliant such as a smartphone for instance. A smartphone can tune any melody that can be searched from the worldwide song, even though it's not in the storage of that smartphone. Yet, your telephone can send data by requesting the tune and afterward get data and streaming that tune on the telephone.

The next example is IoT of the home, which is a smart home; there are numerous studies and articles on the smart home. One of all these is the Implementation of IoT in a smart home [1]–[3] in this paper makes two systems, the first system is energy efficiency systems and the second is security systems. It links all devices to a device known as an intelligent central controller. For each device, this device is linked to a switch module. Then, connect to the router to access the Internet to communicate with the user, if necessary, if a license is needed. Smart Homes are just a network of devices that are used in daily life and other sensors which help to make life easy [1]. Devices communicate with each other but in reality, all devices communicate information to the smart central controller which then due to triggers and other programmed modifications the setting of other devices.

According to Table I, IoT devices include [12] IP cameras, motion sensors, smart bulbs, smart switches, and smart plugs. Next, [13] using this IoT device Danmini, Ennio, Ecobee, Philips B120N/10, Provision PT-737E, Provision PT-838, Simple Home XCS7-1002-WHT, Simple Home XCS7-1003-WHT, and Samsung SNH 1011N. Next, type of IoT device is used in toys, such as Hello Barbie, Furby Connect, Toy-Fi Teddy, and I-Que Intelligent Robot [14], [15] state that surveillance cameras are used in the experiment while [16] used Central hub, Lightbulb, Power switch, Motion sensor, Security cam for the testbed. In this journal [14], using toys that can be connected to the internet. The toys can be attacked by malware, it is because the toys using the open port to update information on the internet. These toys don't have login and passwords just need an internet connection to use. These toys also can be dangerous because they can take personal information by asking, listen and talk to the children with the basic information. This toy can talk with each other as a two-way connection. It contains sensors such as speakers, a microphone, and a camera. So, it can be easy for the hacker to attack when the device is not actively protected.

Furthermore, the Philips B120N/10 baby monitor from [13] has been reported for eavesdropping and espionage against other devices with a microphone or camera. This device can collect the data and samples from the user devices to harm the user in multiple ways. From this paper [12], [13], [15], [16], the device that recently been attack is Ip Camera and Security Camera. There are many reasons for Ip Camera can be easily attacked by malware. The first reason is the IoT devices have no security update because the developers take low priority in security. Next, the processing power and memory are expensive for implementing conventional cryptography. Furthermore, [12] state that IoT devices have weak login because the manufacture provides it for the users and using the default login. Some IoT devices leave open ports to support remotely. Lastly, Users often connect the device without going through the firewall. Therefore, this paper proposes to identify IoT Botnet attack improved generic taxonomy. Crucially, the proposed is developing the improved IoT Botnet detection technique.

TABLE I. Related Work

Author, years	IoT device
Kumar & Lim, 2020 [12]	IP cameras (D-Link) Motion sensors (D-Link) Smart bulbs (Philips Hue) Smart switches (WeMo) Smart plugs (TPLink)
Tzagkarakis, Petroulakis, & Ioannidis, 2019 [13]	Smart Doorbell Face Recognition (Danmini) Smart Door Phone (Ennio) Smart Home (Ecobee) Smart Baby Monitor (Philips B120N/10) IP Camera (Provision PT-737E) IP Camera (Provision PT-838) Security Camera (Simple Home XCS7-1002-WHT) Security Camera (Simple Home XCS7-1003-WHT) Smart Webcam (Samsung SNH 1011N)
Viding, 2019 [14]	Smart Toys (Hello Barbie) Smart Toys (Furby Connect) Smart Toys (Toy-Fi Teddy) Smart Toys (I-Que Intelligent Robot)
Shouran, Ashari, & Kuntoro, 2019 [15]	Surveillance cameras
Sun, Gong, Shea, & Liu, 2018 [16]	Central hub Lightbulb Power switch Motion sensor Security cam

III. Methodology and Implementation

Based on Fig. 2, the experiment's flow begins with the use of recording methods that are used in data collection processes. Before the malware samples are executed, both tools will begin capturing network traffic. Following malware execution, the data analysis process will begin by examining data from both tool-based results. The Wireshark tool will generate a large number of packets capture call as PCAP files, while the Process Monitor tool from the testing environment will generate a massive data log to reduce the studying workload for raw data and processed data, each of the data will be studies using a filter provided by the tools.

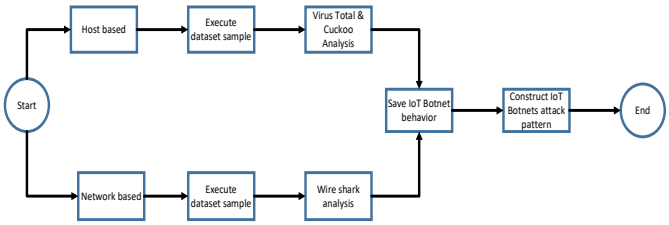

Fig. 2. Flowchart of the Analysis Process.

Fig. 2 depicts the overall analysis process, which begins with the analysis of each IoT Botnet infected folder. There were two levels of analysis approach which are host-based and network-based. The approach analyses network packet captured and on every single host log to control whether the payloads are spam or malicious. But if it corresponded follows unusual conventions or to a remote check for vulnerabilities not follow to standard IoT Botnet options. The integrated analyzer, as shown in Fig. 2, works by taking two perspectives into account: the host-based level and the network-based level. The host logs were examined at the host level using the file system monitoring, registry monitoring, and log monitoring characteristics. As an alternative, the characteristics of the full-payload from a network packet have been investigated at the network level as refer to MIT Lincoln Lab [6].

To detect these IoT Botnets, a preliminary experiment on flow analysis is necessary. The primary purpose of this experiment is to identify IoT Botnet attack patterns in a host-based and network-based environment. Then, the integration of the integrated analysis approach with static and dynamic analysis approaches has been performed. Static analysis function as examines the application or internet structure as compared to functional testing. Besides, the dynamic analysis is performed when the application programmed is running refer to MIT Lincoln Lab [6]. The integrated analysis will be used in profiling IoT Botnet attacks and characteristics. Then, the findings of both studies resulted in attack pattern identification and integrated analysis are contributed to IoT Botnets' attack patterns.

The methodology of overall analysis process is illustrated in Fig. 3 started by preparing dataset. Stratosphere Laboratory [10] is a dataset used in this study and labeled dataset of malicious IoT network traffic. Next step is overview of IoT Botnet experimental approach. This research analyzes the IoT Botnet attack pattern based on host and network environment. Then, the general approach used in the experiment, hardware, and software used, and datasets used for both analyses is discussed. In addition, the third step is IoT Botnet analysis flow. Technically, the analysis is divided into two parts: attacking pattern analysis and integrated approach analysis. The next following segment discusses the analysis of IoT Botnet attack pattern host-based and network-based platform that have been evaluating and generalized in detail. Lastly, proposed general IoT Botnets relationship model for host-based and network-based platform. Therefore, the goal of this research is to identify IoT Botnet attacks pattern and improved generic taxonomy.

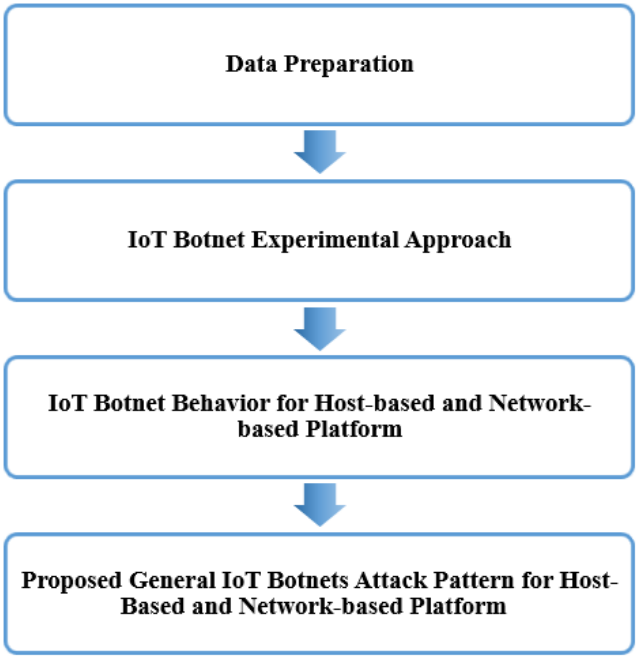

Fig. 3. Methodology.

A. Data Preparation

The data consists of real IoT malware infections as well as benign IoT traffic. Stratosphere Laboratory [10] is a dataset used in this study and labeled dataset of malicious IoT network traffic. This study makes use of seven data points from this dataset. In each situation, an exact or real malware was executed in a Raspberry Pi, which was used to make various actions and various protocols. Table II summarizes the characteristics of each scenario, and the malware used to infect the device. The details of a table can be seen in Table II. The dataset used is IoT-23 since it provides real-world network information and a massive dataset of real-world and categorized IoT Botnet. This dataset uses the updated IoT device, the duration of the experiment is 8 to 24 hours, and the dataset use the real IoT Botnet malware.

The dataset IoT Botnet network traffic is shown in Table II. The actual IoT network traffic is collected on two levels: host and network. The host-based level was selected based on the monitoring attack performed on its host as well as the actions that occurred within a suspicious activity for that host. Meanwhile, one important reason to choose network-level capture is that monitor network traffic for specific network devices to detect suspicious activity that studies network and protocol. To detect bots accurately, host-level and network-

level analyses had to be developed. These two types of analyses balance individually in detecting malevolent activity in the IoT Botnet network. As a result, the network packets captured in this study originate in both a host and a network environment.

TABLE II. IOT BOTNETS DATASETS SUMMARY

Name of Dataset	Duration (hrs)	#packets	#zeekFlows	Pcap size	IoT Botnet type
CTU-IoT-Malware-34	24	233000	23146	121MB	Mirai
CTU-IoT-Malware-44	2	1309000	238	1.7GB	Mirai
CTU-IoT-Malware-49	8	18000000	5410562	1.3GB	Mirai
CTU-IoT-Malware-48	24	13000000	3394	1.2GB	Mirai
CTU-IoT-Malware-9	24	6437000	6378294	472MB	Linux. Hajime
CTU-IoT-Malware-42	8	24000	4427	2.8MB	Mirai
CTU-IoT-Malware-35	24	46000000	10447796	3.6G	Mirai

Clarification of the experimental method and each dataset is used in the study. Based on Table II, the network traffic capture is from these three types of IoT devices to get real network which are the Amazon Echo that uses as a home intelligent private assistant for the owner's home, a Somfy which is a smart door lock that automated, and Philips HUE which is the smart lamp. It is significant to note that the three Internet of Things devices is actual devices of hardware, not simulations. The use of real devices of IoT tolerates for the capture analysis of real network attacks from simulated traffic. The malicious scenarios, like any other genuine IoT device, operate in a controlled network environment with unrestricted internet access. By running a specific piece of malware on a Raspberry Pi, the malicious scenarios were created. Mirai and Hajime traffic are included in this dataset. Malware captures are carried out over extended periods.

B. IoT Botnet Experimental Approach

This research analyzes the IoT Botnet attack pattern based on host and network environment. Existing IoT Botnet detection techniques were classified and profiled based on their technique, criterion, platform analyses, and previous framework. In this section, Fig. 4 shows the illustration of the IoT Botnet testbed in detail to collect the sample malware. This IoT Botnet testbed has three steps to setup the testbed.

The first section of the IoT Botnet testbed is the network configuration used in this experiment refers to the network simulation and formally has been modified using Linux and Windows 7 to suit the testbed experiment of this research. The experimental testbed lab is used to monitor the activities of the IoT Botnet. This testbed was carried out in a controlled setting. The network design depicted in Fig. 4 illustrates the network testbed proposal used in this research, which is comparable to [8], [17], [18]. This research replicates their design of experiment due to the success achieved. As a result, the testbed design consists of 1 router, 2 switches, 4 personal peers or computers with new installations of Windows and Linux, 1 server to complete the packet capture method and one NTP server. Several software specifications are essential to help make the project succeed.

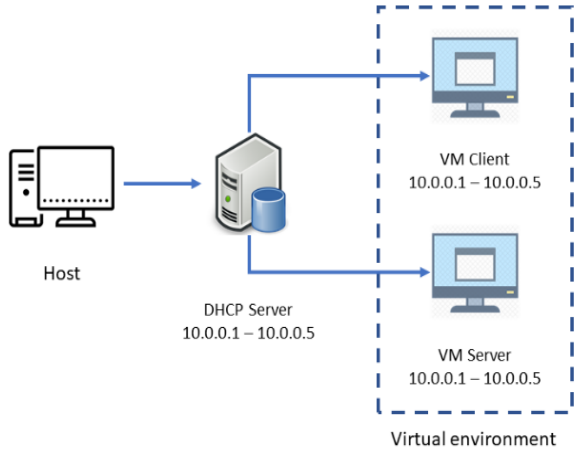

Fig. 4. IoT Botnet Testbed.

There are four softwares that are used in this experiment. The first software is Cuckoo Sandbox, an open-source security program for suspicious file security. Moreover, it uses custom components that track malicious process activity when operating in an isolated environment. The second software is Virus Total, an online system that provides antivirus engines and website scanners to analyze files and URLs to detect viruses, worms, trojans, and other types of malicious content. This can also be used to spot false positives. Last software is Wireshark, a packet analyzer for networks. An analyzer of network packets provides as much information as possible about the captured packet data. Thus, the overview of the IoT Botnet Experimental Approach for this research to identify IoT Botnet attacks pattern and improved generic taxonomy.

C. IoT Botnet Behavior for Host-based and Network-based Platform

This section discusses the IoT Botnet behavior for host-based and network-based platform. In a host-based approach, [17], [19] monitoring behaviors are carried out in a single host, and events for suspicious activity occur within that host. The data is simulated from Virus Total for the file system. The network-based analyzed the full payload packet data framework using Wireshark. This tool is the effective network analyzer for the network based. This section identifies C&C servers and infected hosts in the network. Data is collected at each peer and throughout the traffic. Each peer produces a security log, a system log, and an application log. The service generates network traffic using tcpdump. Wireshark and tcpdump are used to verify traffic between specific hosts at the network level. There are seven datasets which are CTU-IoT-

Malware-34, CTU-IoT-Malware-44, CTU-IoT-Malware-49, CTU-IoT-Malware-48, CTU-IoT-Malware-9, CTU-IoT-Malware-42, and CTU-IoT-Malware-35. The Host-based data can be simulated from Virus Total while the network-based is simulated from the Wireshark. Therefore, this section discusses IoT Botnet behavior for host-based and network-based platform.

1) Host-based: In a host-based approach, [17], [19] monitoring behaviors are carried out in a single host, and events for suspicious activity occur within that host. The overall system behavior continuously records each host monitor. All host been observed by the log monitoring. All abnormal behaviors and characteristics will be identified in every single activity that occurred in the host. The Host-based data can be simulated from Virus Total. From the seven dataset CTU-IoT-Malware-44 are the best datasets that illustrate the attack pattern for host-based platform as shown in Table III.

TABLE III. IOT BOTNET BEHAVIOR FOR HOST-BASED DATASET

IoT Botnet data	Filed open	File written	File copied	File dropper
CTU-IoT-Malware-44 (Mirai)	locale.alias	.dat.nosync100c.Y3KZqJ	.dat.nosync100c.Y3KZqJ	/System/Library/CoreServices/pbs
	en_US.UTF-8	mdsDirectory.db_	mdsObject.db_	
	en_US.utf8	.dat.nosync0fa1.JacR1I	.dat.nosync0fa1.JacR1I	
	en_US	mdsObject.db_	mdsDirectory.db_	
	en.UTF-8	com.apple.smb.server.plist-lock	A66DD831-8DB9-49C7-85C6-87F3F660A041.perfd.events.XXXXXX.stats	
	en.utf8	supportedCountriesTraffic-5.plist	networkDefaults.plist	
	en	default-shields-index-extralarge-70.shieldindex	ResourceManifest.pbd	
	.CFUserTextEncoding	ResourceManifest.pbd	default-16637.styl	
	com.apple.nsservicescache.plist	hybrid-1426.styl	default-search-3806@2x.styl	
	AppleInternal	default-genericshields-extralarge-6.genericshieldstyles	globe-default-1522.styl	
	com.apple.NSServicesRestrictions.plist	default-shields-index-large-88@2x.shieldindex	hybrid-1425@2x.styl	

The Experiment data was tabulated as Table III and classified into four columns that are FileOpen, FileWritten, FileCopied, and FileDropper. The data from Table III simulated from Virus Total for the file system. FileOpen is a function that opens a file named and flagged with the given name and flag. The IoT Botnet samples are injected into the FileOpen, which initiates the creation of an IRC channel for infected clients to join. When opening a FileOpen encrypted document in Adobe Acrobat or Adobe Reader, the FileOpen plugin is only available. It contains no spyware or malware, leaves nothing running on the machine, and makes no changes to the Windows registry or system files. The FileWritten function is designed to write data information into a CSV folder automatically. The character "rn" will be shown at the end line, after writing into the file. The message is either a string expression or a number that contains the text that is written to the file. The following function, FileCopied, copies the first file which is the original file from a local or shared folder to a different file. FileCopy.exe is an executable file included in the IObit Advanced SystemCare Ultimate 8 programmed. The software is typically 498.97 KB in size. Finally, FileDropper is a type of Mirai (Trojan) that some type of malware designed to install such as backdoor and virus; on a target device system.

Based on the result of this research, the IoT Botnet attack sample showed similarity and unique behavior during the experiment. In the lifecycle of IoT Botnet, typical IoT Botnet showed the process that will be downloaded by using one of the methods which are file dropper, mail attachment, or drive-by download before execution of the malware. Since the IoT Botnet samples are already downloaded from infected devices after the experiment was launched, IoT Botnet's initial lifecycle behavior for this experiment may be negligible. The bots can contact the infected machines by IP address. The data product form and rundown of known bots to reach the bots' answer. The bot will remove the record and refresh if one of the bots' forms is lower. Thus, the rundown of each bot for the infected devices will develop and updates itself immediately into single known bot. As IoT botnets keep on developing, being utilized dispatch DDoS assaults. Since IoT gadgets are Linux and Unix-based frameworks, they frequently are focuses on executable and linkable arrangement format ELF binaries, a typical record design found in inserted frameworks' firmware. The malware conveyance strategy regularly targets SSH or Telnet network conventions by misusing default, hardcoded accreditations. Once undermined, the malware payload is conveyed to the gadget for enlistment into the botnet. Thus, the existing IoT Botnet detections based on host-based techniques were classified in terms of are FileOpen, FileWritten, FileCopied, and FileDropper.

2) Network-based: The network-based analyzed the full payload packet data framework using Wireshark. This tool is the effective network analyzer for the network based. This section identifies C&C servers and infected hosts in the network. This section of the analysis focuses on defining the unique communications to form IoT Botnet malware, IP address, Port number and protocol over a suspicious port. The detecting any indication of malevolent activity attack that

attempts the network, and identifying which IoT botnets are on the infected network host. From the seven dataset CTU-IoT-Malware-34 are the best datasets that illustrate the attack pattern for network-based platform as shown in Table IV.

TABLE IV. IOT BOTNET BEHAVIOR FOR NETWORK-BASED DATASET

Dataset	IoT botnet	IP Address	Port Number	Protocol
CTU-IoT-Malware-34	Mirai	185.244.25.235	6667	IRC
	script bots	192.168.1.195	48986	IRC
	amplified attacks			
	netblocks			
	Spoof			
	AmpAttacks	66.67.61.168	63798	TCP
	Tragedy	1.1.1.1	1	TCP
	bot-master AmpAttacks	50.50.50.53	53	TCP
	tripsit.me	192.223.29.150	62351	TCP
			80	HTTP
	Bot Master Spoof	71.61.66.148	65279	TCP
	Bad packets (Mirai like Botnet host)	116.220.1.247	-	TCP
	bot-master shadoh	123.59.209.185	80	TCP
	STD Dos	74.91.117.248	5376	UDP

The network-based pattern is extracted from full payload network traffic that captured the whole activity of IoT Botnets. The pattern is studied in the protocol used, suspicious port, suspicious IP address, and attack that have been launched. The IoT Botnets attack pattern at the network level is summarized in Table IV. The summary then has been discussed in this section. The dynamic analysis, for the first phase the controlled environment has been implemented known as IoT Botnet testbed environment. The static analysis had been done in reviewing the real codes of infected files to reveal and study their true characteristics. In the dynamic approach, the capabilities are highly concerned with the detection of malicious activities during or after program files execution. The IoT Botnets' activities are captured through the event host logs and whole network traffic.

Subsequently, the dynamic analysis is performed on the event host log and network traffic datasets. The IoT Botnet test bed setup applied by controlled environment where the datasets were collected. Process monitors and process explorer capture the event host log to gather information on the localhost. Meanwhile, the tcpdump service has captured the overall network traffic. Through this dataset, the IoT Botnets' attack and characteristics are fully observed to ensure the interaction on the botnet's server and the effect on each of the infected files to a real environment. After that, the integration of analysis results on static and dynamic analysis will be correlated together to construct the basic and general attack model of IoT Botnets. This research analyzes the IoT Botnet attack pattern for host-based and network-based platform. Thus, the existing IoT Botnet detections methods were classified and profiled in terms of analyzing IP address, port number, and Protocol.

D. Proposed General IoT Botnets Attack Pattern for Host-based and Network-based Platform

This section proposed general IoT Botnets attack pattern for host-based and network-based platform. This proposed based on these seven datasets which are CTU-IoT-Malware-34, CTU-IoT-Malware-44, CTU-IoT-Malware-49, CTU-IoT-Malware-48, CTU-IoT-Malware-9, CTU-IoT-Malware-42, and CTU-IoT-Malware-35. The proposed general IoT Botnets attack pattern for host-based platform consists of FileOpen, FileWritten, FileCopied, and FileDropper, it considered as risky event process that happens to allow the attacker in operating systems, replace the original files. Next, the proposed general IoT Botnets relationship model for network-based platform consist of IoT Botnet malware, IP address, port number, and protocol. Therefore, this section discusses the proposed general IoT Botnets attack pattern for host-based and network-based platform.

1) Proposed general IoT botnets attack pattern for host-based platform: The generic IoT Botnets attack pattern and integrated approach as described in the earlier section are utilized to construct the IoT Botnets attack pattern. For the finest of information, there is no published study has been found that performs the IoT Botnets attack pattern model based on the file system for the host-based. As a result, this study implemented the IoT Botnets attack pattern model following the proposed IoT botnets attack pattern for the host-based based on a file system. The following section describes the details Fig. 5.

Fig. 5. Proposed General IoT Botnets Attack Pattern for Host-Based Platform.

The static analysis began with isolating the experimental setup in a controlled environment. The ability to detect malicious activities by static analysis before the execution of programmed files and then implement the data in Virus Total. The operation processes involved in all IoT Botnets infected files have been created as its main process start. The information of IoT Botnets infected files has been discovered in four main components. The proposed model consists of FileOpen, FileWritten, FileCopied, and FileDropper for the host-based as shown in Fig. 5, are considered as risky event process that happens to allow the attacker in operating systems, replace the original files. Here, malicious activity attempts to exploit the victim host to create an.exe file and remove essential files in the system directory. Otherwise, the frequent changes in the registry had been noticed as a high possibility of

malicious activity has arisen. The specifics are as follows: The IoT Botnet samples enter the FileOpen, which creates an IRC channel for infected clients to join. The FileWritten function is designed to write data information into a CSV folder automatically. The character "rn" will be shown at the end line, after writing into the file. The following function, FileCopied, copies the first file which is the original file from a local or shared folder to a different file. Finally, FileDropper is a type of Mirai for Trojan that some type of malware designed to install such as backdoor and virus; on a target device system.

2) Proposed general IoT botnets attack pattern for network-based platform: The network-level pattern is extracted from full payload network traffic that captured the whole activity of IoT Botnets. The pattern is studied in a protocol used, suspicious port, suspicious IP address, and attack that have been launched. Generally, on a network level, the scanning activity is mainly concerned with a protocol. Both suspicious port and suspicious IP addresses can be found in exploit and C&C connection attack steps. The generalized attributes designed for exploit activity are concern with protocol and, destination port. The C&C connection considers the detection of IoT botnets and the C&C website as the attribute. Moreover, the generalized attributes for impact or effect steps allowed the attacker to launch an attack on a remote address attack. As a summarization of the generalized IoT Botnets attack patterns, the findings are relatively depicted in Fig. 6 based on the discussion in analysis of generalized IoT Botnets from a network-level perspective.

Fig. 6. Proposed General IoT Botnets Attack Pattern for Network-Based Platform.

The generic IoT Botnets attack pattern and integrated approach as described in the previous section are utilized to construct the IoT botnets attack pattern. For the finest of information, there is no published study has been found that performs the IoT botnets attack model. As a result, this study implemented the IoT Botnets attack pattern model following the proposed IoT botnets attack pattern for the network-based based on IoT Botnet malware, IP address, port number, and protocol. This research analyzes the IoT Botnet attack pattern for host-based and network-based platform. The existing IoT Botnet detections methods were classified and profiled in terms of analyzing IP address, port number, and Protocol.

Based on the proposed pattern, show the general IoT Botnet attack pattern analysis. From the finding have been referred to develop new IoT Botnet attack pattern. This IoT Botnet attack pattern has been designed for host-based and network-based. The host-based attack pattern provides explanation for the IoT Botnet attacks aims and strategies in protecting from the attack. Practically, the attack pattern provided by researchers to identified the bot server and botmasters. While the network-based pattern is used to identify the method of network attack by the Botmaster. Overall, this paper was effective in recognizing the characteristics and behavior of IoT Botnet for host-based and network-based. The result was improved outcomes to researchers to create a new IoT Botnet attack pattern.

IV. Conclusion and Further Work

In conclusion, the researchers have studied the host logs data and network traffic data to determine the attack pattern from host-based and network-based perspectives. The attack pattern serves as a guide for administrators in determining who the true attacker is behind the scenes. The analysis's output is proposed as the general IoT Botnets attack pattern on the host and the general IoT Botnets attack pattern on the network. Furthermore, this paper also presents the integrated approach to studies and classify the whole IoT Botnets activities and events to recognize the attack pattern and characteristics of IoT Botnet. This study combines static and dynamic analysis approaches to gain a better understanding of how IoT Botnets behaved in a real-world IoT network environment. The attack pattern and integrated analysis result are inherited to construct the basic and general IoT Botnets attack, pattern model.

This paper contributes to discovering, recognizing, categorizing, and detecting IoT Botnet activities. Next, organizing information have a better understanding of the IoT botnet's problem and potential solutions. Then, construct the IoT Botnet attack pattern by analyzing the characteristics of the IoT Botnet behavior. This IoT Botnet attack pattern divides into two environments which are host-based and network-based. As a result, this paper aims construct the attack pattern when the IoT device has been infected and become part of the botnet. The limitation of this research is the dataset from IoT-23 is bigger, and need more space to run the dataset. Therefore, the result for this paper has been accomplished and the aim objective has been complete. This is ongoing research in finding an effective technique to make the detection on IoT Botnets attack pattern. The further work for this research is developing the IoT Botnet attack pattern in graph degree theory. The graph degree theory will visualize the attack pattern of the IoT Botnet.

Acknowledgment

This publication has been supported by Center of Research and Innovation Management (CRIM), Universiti Teknikal Malysia Melaka (UTeM). The authors would like to thank UTeM and INSFORNET research group members for their supports.

References

[1] M. El Beqqal and M. Aziz, "Taxonomy on IoT Technologies for Designing Smart Systems," Int. J. Interact. Mob. Technol., vol. 12, no. 5, p. 182, 2018.

[2] P. Gokhale, O. Bhat, and S. Bhat, "(PDF) Introduction to IOT," Int. Adv. Res. J. Sci. Eng. Technol., vol. 5, no. 1, pp. 41–44, 2018.

[3] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, "Internet of Things (IoT): Taxonomy of security attacks," 2016 3rd Int. Conf. Electron. Des. ICED 2016, pp. 321–326, 2017.

[4] D. Plohmann, E. Gerhards-Padilla, and F. Leder, "Botnets: Detection, Measurement, Disinfection & Defence," Inf. Secur., 2011.

[5] C. Hung and H. Sun, "A Botnet Detection System Based on Machine-Learning using Flow-Based Features," Securware, vol. The Twelft, no. c, pp. 122–127, 2018.

[6] R. S. Abdullah, "Preliminary Study of Host and Network-Based Analysis on P2P Botnet Detection," pp. 105–109, 2013.

[7] E. Alomari, S. Manickam, B. B. Gupta, S. Karuppayah, and R. Alfaris, "Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art," Int. J. Comput. Appl., vol. 49, no. 7, pp. 24–32, 2012.

[8] R. S. Abdullah, M. F. Abdollah, Z. Azri, M. Noh, M. Zaki, and S. R. Selamat, "Revealing the Criterion on Botnet Detection Technique," vol. 10, no. 2, pp. 208–215, 2013.

[9] W. Nur et al., "Discovering IoT Botnet Detection Method : A Review."

[10] Sebastian Garcia, Agustin Parmisano, and Maria Jose Erquiaga, "IoT-23 Dataset: A labeled dataset of Malware and Benign IoT Traffic. — Stratosphere IPS," IoT-23: A labeled dataset with malicious and benign IoT network traffic, 2020. [Online]. Available: https://www.stratosphereips.org/datasets-iot23. [Accessed: 28-Jun-2021].

[11] S. Goswami, M. Bagchi, A. Sain, and V. Tyagi, "Internet of Things (IoT)," 2020.

[12] A. Kumar and T. J. Lim, "Early detection of mirai-like IoT bots in large-scale networks through sub-sampled packet traffic analysis," Lect. Notes Networks Syst., vol. 70, pp. 847–867, 2020.

[13] C. Tzagkarakis, N. Petroulakis, and S. Ioannidis, "Botnet Attack Detection at the IoT Edge Based on Sparse Representation," pp. 1–6, 2019.

[14] E. Viding, "Does Your TV Spy on You ? The security , privacy and safety issues with IoT," no. May, 2019.

[15] Z. Shouran, A. Ashari, and T. Kuntoro, "Internet of Things (IoT) of Smart Home: Privacy and Security," Int. J. Comput. Appl., vol. 182, no. 39, pp. 3–8, 2019.

[16] A. Sun, W. Gong, R. Shea, and J. Liu, "A Castle of Glass: Leaky IoT Appliances in Modern Smart Homes," IEEE Wirel. Commun., vol. 25, no. 6, pp. 32–37, 2018.

[17] R. S. Abdullah, "Tracing the P2P Botnets Behaviours via Hybrid Analysis Approach," vol. 118, no. 1, pp. 75–85, 2014.

[18] R. S. Abdullah, M. Zaki, M. F. Abdollah, S. Sahib, and R. Yusof, "Recognizing P2P Botnets Characteristic Through TCP Distinctive Behaviour," vol. 9, no. 12, pp. 12–16, 2011.

[19] A. Movaghar, "Intrusion Detection : A Survey Chapter 2 Intrusion Detection : A Survey," no. January 2008, 2014.