Journal of Theoretical and Applied Information Technology
15th October 2020. Vol.98. No 19

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A COMPREHENSIVE STUDY OF BOTNETS ON INTERNET OF THINGS AND MOBILE DEVICES : DETECTION AND MITIGATION TECHNIQUES

SHWETARANI[1], NAWAB MUHAMMAD FASEEH QURESHI[2], DONG RYEOL SHIN[3]

[1] Department of Electrical & Computer Engineering, Sungkyunkwan University, South Korea

[2] Department of Computer Education, Sungkyunkwan University, South Korea

[3] Department of Electrical & Computer Engineering, Sungkyunkwan University, South Korea

E-mail: shwetamora@skku.edu[1], faseeh@skku.edu[2], drshin@skku.edu[3]

Corresponding Author : Nawab Muhammad Faseeh Qureshi

ABSTRACT

Network formed by a group of internet-connected compromised devices is known as Botnet, which may include personal computers, servers, internet of things and mobile devices. The botnet has been one of the most common network security threat. Botnets have been used for stealing data, sending spam, and allows attackers to access the device for collecting personal information of the users and for conducting distributed denial of service attacks (DDoS attacks). Increasing popularity and recent advances in the Internet of Things (IoT) and mobile devices have made IoT devices and mobile devices an easy and alluring target for attackers. Various studies have proposed many sophisticated mechanisms for understanding and identifying botnets and how they creating security threats for IoT devices and Mobile devices. This survey work presents a comprehensive review that discusses about IoT and mobile botnets propagation, detection, and mitigation. In this work, we focus on various types of IoT and mobile botnets propagation, attack methodology, and how they exploited in DDoS attacks along with various technologies used to detect IoT and Mobile botnets. Also we introduce the structure and characteristics of basic botnets.

Keywords: *Botnets, Internet of Things (IoT), IoT botnets, Mobile botnets, DDoS attacks, cybersecurity*

1. INTRODUCTION

Botnets have become the source for most of the security issues on the internet[1]. Botnets continuously change their structure, protocols, and attack methods. The problems caused by botnets have motivated many researchers to create sophisticated detection and mitigation techniques. To understand Botnet and distinct Botnet from other kinds of malware it is important to know what is a bot and botmaster [2]. Bot is a short form of the robot also known as a zombie, which is a type of malware[3]. Botmaster or bot herder install this malware into compromised devices and control using a command & control system (c & c).

So the "Botnet" word is formed by combining two words Robot&Network (Robot + Network = BotNet) Botnet is an intelligent network formed using bots or zombies. These bots are remotely handled by a hacker who is called as BotMaster or BotHerder. BotMaster controls the botnet using the c&c system. BotMaster/Hacker, c&c system, and bot/zombie are three major components of a botnet.

Based on the communication methods, botnets are classified into direct, centralized, peer-to-peer, or decentralized (P2P) and hybrid as shown in figure 1 to figure. 4 [4].

1.1 Direct

In this architecture botmaster can recruit and control bots directly. Only the botmaster knows all the bots in the botnet as bots do not have any forms of interactions with each other.

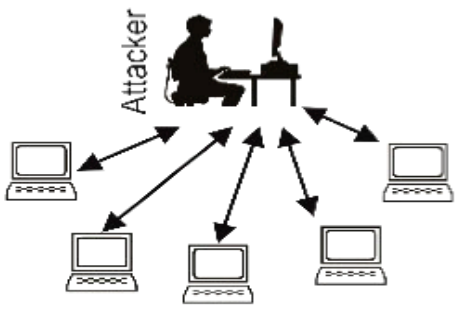


Figure 1. *Direct C&C Architecture*

1.2 Centralized

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

This botnet is simple to set up and manage. For communication HTTP or IRC protocols can be used. Centralized botnet generally have a c&c system to which all the zombies are connected. If someone manages to detect this c&c system, the entire botnet will collapse. Hence the drawback of a centralized botnet is single-point failure [5].

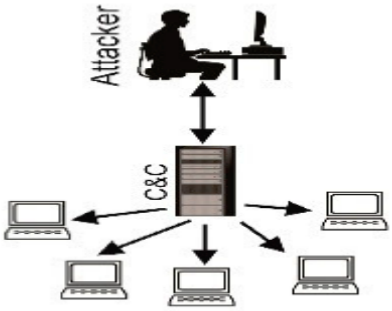


Figure 2. Centralized C&C Architecture

1.3 P2P or decentralized

In P2P botnets c&c system is Peer-To-Peer based means no central c&c system, all zombie plays the role of both server and client. There is no single c&c system that makes P2P botnets very resilient, so it is very hard to detect and prevent P2P botnets [5,6].

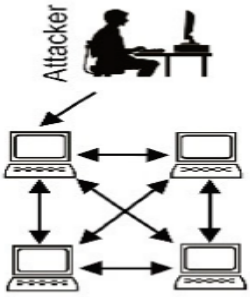


Figure 3. P2P or decentralized C&C Architecture

1.4 Hybrid

Centralized and P2P architectures are combined to form a more resilient hybrid architecture. The implementation methods are explained in [7]. Most modern botnets that have been a threat to the internet are discovered to use the hybrid method.

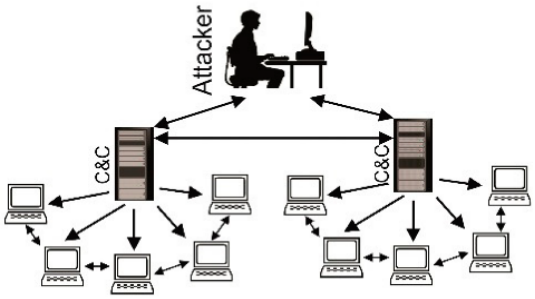


Figure 4. Hybrid C&C Architecture

Further in section II and Section III we will discuss IoT botnet and mobile botnet characteristics, operations, and some of the IoT botnet attacks and mobile botnets attacks. Section IV and V gives information about IoT botnets and mobile botnet detection and mitigation techniques respectively. Section VI explains about DDoS attacks. Finally, section VII presents the conclusions.

2. IoT BOTNETS

In 1999 Kevin Ashton, used the word internet-of-things (IoTs) for a project [49]. This got advanced and the electronic world and the internet are brought together. IoT is a group of interconnected computing, digital & mechanical devices. These devices communicate via the internet and also sends and receives data via the internet. Sensors used in these and their processing power made these adaptable in many environments [8]. IoT is used for applications like home automation, smart city, smart grids, health care appliances, smart retails, autonomous car and industrial automation, and many other fields as shown in figure.5 [50].

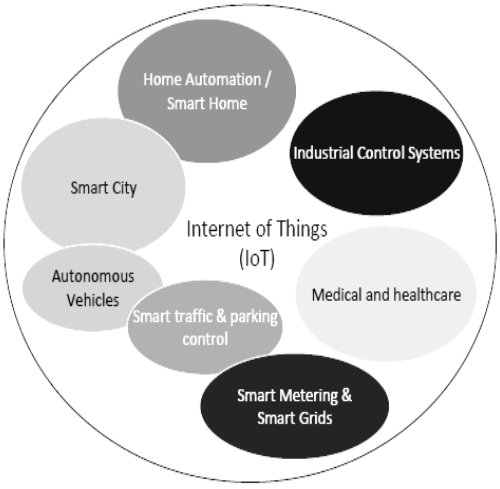


Figure 5. Internet of Things

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The absence of the human role made IoTs different from traditional internet. IoTs are capable of creating and analyzing an individual's information and to take actions according to those analyzed information [9]. The increasing popularity and recent growth of IoTs, made them an easy target for attackers. Most of the IoT devices use default passwords, which makes bots to get access easily. Because IoT includes a variety of an ever-growing array of networked systems, which constantly connects to the internet and many use default passwords which allows for easy access, an attacker can build and use to spam mailing, bitcoins and DDoS, etc. within minutes. A group of malware-infected IoT devices is called as "IoT Botnet" [10]. IoT botnet attacks classified into four groups as physical attack, network attack, software attack, and encryption attack [11].

2.1 Physical attack

These types of attacks are possible only for near distance. Physical attacks, mainly targets hardware parts of the IoT systems. Physical attacks may include Node tampering, RFID's, malicious code injection, sleep deprivation attacks etc.

2.2 Network attack

Able to manipulate the networks of internet-of-things to cause damage. Focused on the IoT system network. Sybil attacks, DoSs, routing information attacks, RFID cloning, RFID unauthorized access, and Sinkhole attack types may occur under network attacks.

2.3 Software attacks

These type of attacks are possible when the IoT application exhibit some security vulnerabilities. The biggest threat to the security issues of any digitized system. Software attacks may include DoS, Malicious codes, Phishing attacks and virus, worms, trojan, spyware.

2.4 Encryption attacks

These are conducted through cryptanalysis, Side-channels, etc. A new way of IoT botnet attack classification is introduced in [12].

2.5 Some IoT botnet attacks are listed below

2.5.1 Linux.Hydra

Is the first noticed malicious activity, which targeted IoTs. This is an open-source botnet framework released in 2008 [52]. It features both a spreading and DDoS functionality. Once the device compromised, get involved in internet relay chat network. It can conduct SYN and UDP flood attacks[53]. Linux.Hydra is simple malware but has become the base of many malicious activities on MIPS processors.

2.5.2 Linux.Darlloz

Symantec researchers discovered in November 2013. It uses web server-based security issues to infect the internet of things. [13]. Linux.Darlloz supports various architecture including x86, ARM, MIPSEL, PPC architectures. After infection it makes legitimate clients stop accessing the compromised system. Linux.Dralloz has infected more than 31000 devices by 2014 February. An advanced version of Linux.Darlloz, utilizes compromised systems for crypto mining [51]. Linux.Darlloz malware can damage LightAidra malware [50].

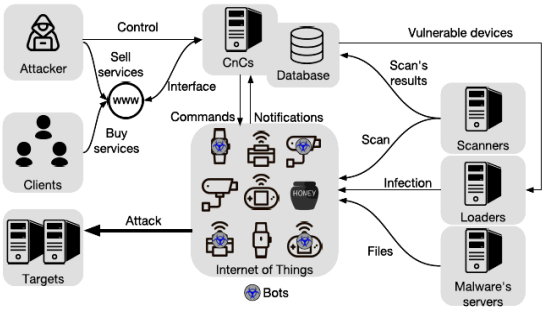
2.5.3 Linux.Aidra

Is also known as Linux.LightAidra, discovered in 2012 by security researchers at ATMA.ES. It is a IRCTelnet based attacks on IoT devices. Linux.Aidra is a very composite malware which can run on various processors. But still it can perform only simple malicious activities [14] [54]. Linux.Darlloz malware can delete Linux.Aidra files and stop its communication process.

2.5.4 Bashlite

In 2014 Level 3 Threat Research Labs spotted this malware [56]. It has different names like Gayfgt, Qbot, Lizkebab, and Torlus. In 2015 Bashlite malware code along various versions has been made available publically. Few versions of Bashlite has compromised more than 100,000 IoTs. Mirai and Bashlite belongs to the same family of malware. These two malware have many common features. These two botnets can infect IoT devices using default user information. In figure 6 we can see the outline of an environment in which Bashlite and Mirai malware can function [55]. This bot code consists of both server and client codes where server code must be running on at least one c&c server, using this one active server Botmaster will be able to handle other malicious programs on a client. For communication these use IRC. It has the predefined pair of user names and passwords using this information it will try to access unsafe systems [58].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195



Figgure 6. IoT Botnet Overview

2.5.5 Mirai

In 2016 Malware Must Die company detected this botnet. Mirai affected many companies like Krebs, OVH, Netflix, Reddit, GitHub & Dyn [15]. Mirai compromised many IOT devices like IP cameras, DVRs, and routers. Mirai formed nearly 1Tbps of network traffic. Mirai has the ability to scans the internet to find unprotected IoT devices [60]. Mirai employs default username and passwords and infects the detected unprotected IoT devices [59]. Mirai uses a brute-force attack to scan the default usernames and passwords of home devices[63]. Mirai was Minecraft. The creator of Mirai was just trying to get the advantage of a computer game, their intention was not to conduct such a big DDoS attack [61]. Mirai malware has highly sophisticated features, it has the ability of killing other malware in the compromised IoT devices [62].

2.5.6 Hajime

Is malware similar to Wifatch malware(open source piece of malware, which has not been used for malicious actions but attempting to secure devices from other malware). Hajime is a Japanese word which means " beginning". Discovered as early as October 2016 [57]. Hajime has different design and operation procedures compared to Mirai malware but still able to target most of the same devices like Mirai botnet. Hajime is more advanced than Mirai botnet, but not launched any attacks. Till today Hajime is used only for self propagate. But Hajime is worth to study because its design and operation makes researchers to learn more about vulnerable IoT devices. Hajime tries to be more resilient by adding new devices. Its c&c system is a P2P system [48].

2.5.7 Linux/IRCTelnet

This IoT botnet targets routers, DVRs and IP cameras. Discovered in 2016 by malware must die. It is a Linux based attacking Telnet ports of the IoT devices [63]. It affects the OS of the device and adds a botnet network. It is controlled IRC and malware is written in c++ [64]. It borrows code from several existing malicious IoT applications. It uses all the sections of the Aidra malware's source code. It also borrows Telnet scanning logic from Bashlight botnet [65].

3. MOBILE BOTNETS

Mobile botnet has become the critical problem of cybersecurity. Mobile botnets can cause simple personal threats to serious financial threats also. Sets of malware-infected mobile devices, controlled by botherders are called Mobile botnets. Basic mobile botnet architecture is shown in figure.7 [66]. Many of the Mobile malware use short messaging service (SMS) as a c&c system for recruiting and controlling the infected mobile devices [16]. Due to financial intention, ease of exploit and functionality botnets are shifted to mobile devices that to Android has become an easy target [17]. In addition to the basic botnet architectures, mechanisms based on SMS, Bluetooth, and multimedia messaging system (MMS) also has been used as a c&c system [18]. Mobile botnets in smartphones are classified in accordance with API calls [17].

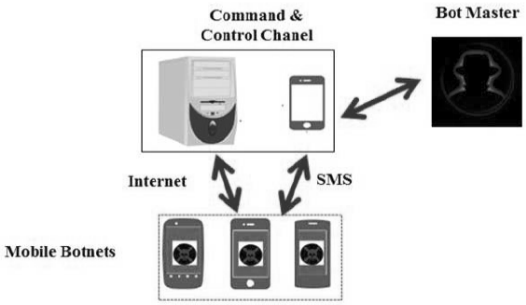


Figure 7. Basic mobile botnet architecture

In 2004 first mobile malware was found, named as Cabir [35]. Symbian Phones were most affected by the Cabir mobile malware because Cabir is specially made for Symbian Operating system based phones. Cabir mobile malware can affect the nearby phones. It uses wireless Bluetooth for finding and affecting the nearby devices. Few mobile bots and their malicious activity are explained here,

3.1 SymbOS.Yxes

Mobile botnet targets Symbian operating system phones and exploits a simple HTTP- based C&C system[36]. SymbOS/Yxe is the first malware to target Symbian S60 third edition phones [68]. SymbOS.Yxes mobile botnet can reach the contact

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

numbers of a bot in the botnet. These contact numbers will be the ones who sent or received messages from the mobile bot of the botnet. SymbOS.Yxes mobile malware collects the personal credentials of the bot devices and also it tries to kill the applications in the bot devices by searching bot devices application manager [68].

3.2 Zeus

Mobile botnet is a package of trojan malware. Other names of Zeus mobile malware are ZeuS/Zbot [70]. Zeus malicious code originally is made for computers. Zeus first observed in the USA. It compromised more than 3.5 million computers in the USA [69]. Zeus also affected banking services through mobile banking as it is a commonly used service by most of the mobile users [19]. Zeus uses social malware and false web site address to send the message to new targets. This false web site makes clients to install malicious code. [20]. Zeus can collect the information about the mobile bot device [21]. Malicious code used by Zeus can support various operating system based mobile devices. Zeus spreads to other mobile devices by making clients to install false web sites and spoofing attacks. Zeus utilizes man in the browser keystroke, grabbing and crypto locker ransomware to get the banking information of the true users. Zeus sends the pop-up to victim's devices to trick them as if they have the malware in their devices but they may have and may not and makes them pay for it.

3.3 DroidDream

Mobile botnet, appeared in 2011 also known as myournet, Pjapps, Lotoor, and DroidRooter [71]. Droid.Dream can get root access to Android mobile operating systems. After getting access, it makes users to download applications for the further malicious activities to conduct. This mobile bot is activated when the users are asleep. It distributes in conjunction with legitimate applications including games, ring tones,etc. The second application sends sensitive information to the C&C server including the device model, SDK version,and user's country and it prevents DroidDream removal [22]. DroidDream is configured within AndroidManifest.xml to run along with the application's legitimate code. By reviewing the Android Manifest file of an infected application provides much information immediately. Infected applications commonly include com.android.root. Visible when viewing data from an APK, extracted, converted into a JAR, and then viewed within JD-GUI.

3.4 AnserverBot

Detected on September 19, 2011 by NetQin Security research group. This mobile botnet has well-advanced techniques [72]. It can detect the safety system on the bot devices and tries to destroy them so that it can carry out malicious activities. This is possible by using its two-layer c&c system [23]. As a Trojan program this bot piggybacks on legitimate applications. At a high level it repackages into the host application with two hidden applications those are anservera.db and anserverb.db. These two applications have the same package name. The below figure.8 shows the high-level relationship of Host app, Payload A and Payload B [72].

3.5 Ikee.B

First noticed in 2009 by iPhone version jailbroken client from Dutch. This client noticed a blackmailing pop up on their phone. Which clearly tells that phone is hacked. Then this client is forced to a hacker's site and asked to pay for removing the bot [73]. Clients Personal data can also be stored by this mobile botnet. Ikee.B mobile botnet showed that mobile devices have the same level of vulnerabilities like computers and mobile botnets have the same level of ability as computer malware [24]. This mobile botnet's c&c server is found in Lithuania [25]. Ikee.B adds more bots to its network by scanning IP addresses and self-propagation methods. It can spread overseas through self-propagation and it can also share clients private data to its c&c server

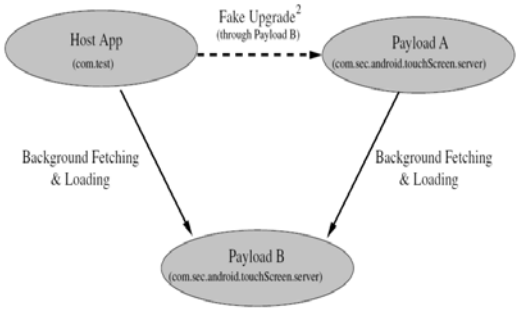


Figure 8. A high-level overview of three related applications in AnserverBot

3.6 TigerBot

Detected by two research groups worked together, those are NQ mobile security research center and researchers group from North Caroline State University [74]. This botnet is not controlled by the internet, it only uses SMS service for

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

controlling the botnet. These SMSs are not visible to the legitimate clients [26]. Symantec research lab reports tell that this mobile botnet is made for spying. Through which it gets the users personal data, records voice calls, and nearby sounds [27]. It has a receiver for receiving botmaster's instructions, through this receiver it can notice SMS on any bot prior to a legitimate user. It can send messages, record calls, upload GPS location, reboot, change network settings and kill running processes.

3.7 Android.Bmaster

Mobile botnet found by Saxon Jiang. Android.Bmaster have the high level control on the bots of the botnet. It can make users pay for videos, make calls and send messages [75]. This botnet is limited to China [28].

4. IoT BOTNET DETECTION AND MITIGATION TECHNIQUES

IoT botnets have become the largest security issue for cybersecurity. IoT malware use high-speed networks, are scalable and diverse. More research work needs for developing sophisticated methods to detect IoT botnets. Many researchers proposed sophisticated methods using different technologies for detecting IoT botnets and to understand their characteristics. This section will explain various IoT botnets detection methods built using machine learning, deep learning, neural networks, convolutional neural network etc. In[29], the authors proposed Deep autoencoder based method for detecting IoT botnets. In their method authors trained Deep autoencoders using statistical features of benign traffic data. The authors followed the steps of collecting data, extracting features, training anomaly detectors, and continuous monitoring. In[30], the authors proposed a new method using Deep learning technique for detecting IoT botnets. Author's deep learning-based method uses recurrent neural network and bidirectional long short term memory. In [31], the authors introduced a new model that detects botnets in Linux based IoT device. Author's new method combines PSI graph and convolutional neural network classifier techniques. With this new method authors achieved 92% of accuracy. In [32], the author's method is based on the network behaviors of IoT devices. Understanding network behaviors helps in feature selection which gives high accuracy to detect IoT based DDoS attacks. For this method authors employed machine learning and neural network techniques. In [33], the authors proposed and implemented a solution for flash crowd attacks of IoT botnets. In their work they have implemented an adaptive filter for reducing IoT based DDoS attacks. They achieved 99.69% of accuracy for detecting IoT botnets. They used Amazon public cloud platform for testing the proposed method. Authors succeeded in reducing the illegal requests from botnets like FBot, APEP, ARIS, and EXIENDO. In [34], the authors proposed a deep learning model using convolutional neural network. This proposed model is made up of a data processing module and eight layers of convolutional neural networks. As most of the IoT devices use software-defined networking (SDN) in place of traditional networks, it makes IoT botnet detection tough. In [76] authors proposed a method for detecting IoT botnets. Their proposed method uses techniques of deep learning. SDN specific data set is used by authors for testing their proposed method and they achieved nearly 97% of accuracy. The authors used Keras and Tensor flow frameworks in their algorithm. Automatically scanning for unsafe IoT devices and disconnecting those devices from the internet can be a way of blocking IoT botnets. In [77], the authors presented one such method for detecting and isolating infected IoT devices. Their method detects IoT botnets before accessing routers which helps IoT devices to become more attack resilient. In [78], Introduced a method for detecting IoT botnet attacks using unsupervised learning techniques. Authors used grey wolf optimization algorithm and one-class support vector machine. In [79], the authors proposed an IoT botnet detection method using Honeynets and network flow & classification techniques. Honeynet provides information about login activities and network traffic for obtaining traffic flow. They used local Honeynets for the implementation of their technique. Datasets obtained from these local Honeynets are exploited for the detection of botnets, using supervised machine learning classification techniques. In [80], the authors proposed a method based on IoT botnet features and used decision tree for classification purpose. Their goal is to minimize the number of features need for detecting IoT botnets. To achieve this they used feature selection techniques. They showed that with less number of features high accuracy can be achieved. In [81], the authors introduced a new methodology based on features for detecting IoT botnets. Authors have adopted both machine learning and deep learning techniques. They formed a PSI rooted subgraph using features. They have achieved 97% of accuracy. In [82], the authors

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

introduced a method to detect botnets in the application layer. In the application layer particularly for the services provided by domain name system (DNS). The authors collected the information about the DNS. Later authors classified domains as normal and abnormal, using deep learning architecture based domain generation algorithm. They used two data sets to test their method. In [83], the authors introduced a technique named AutoBotCatcher main thought behind this technique is, authors, thinking that in a botnet all bots often try to communicate with each other and also make groups. They targeting P2P based IoT botnets. They used network traffic flow and a blockchain technique called as Byzantine fault tolerant (BFT). In [84], the authors Technique using logistic regression for detecting infected IoT devices. Using this technique authors trying to find the probability of a device being infected. This technique is best suited for finding botnets those trying to enter illegally. For this they used brute force technique. Authors achieved 97.30% of accuracy. In [85], the authors proposed technique is based on Anomaly method, related to feature selection. The author intends to achieve high accuracy with less features using unsupervised learning. They also intended to make a general model that can be suitable for any type of IoT device. In [86], the authors proposed a method for detecting IoT botnets at IoT edge. For this purpose they used network traffic and classified network traffic as benign and infected at the IoT edge. The authors used a small-sized network traffic data of legitimate IoT devices. In [87], the authors introduced a technique based on usage, communication, and access monitoring, named as UCAM. This method has three parts namely Descriptor for defining policies, Monitor for having the information about present state and comparator to detect unusual activities. With this method authors been able to find Mirai botnet. In [88], the authors presented a method for detecting and mitigating botnets in home routers. Authors named their method as BoDMitM. This method employed manufacture usage description (MUD) for limiting entry to IoT devices. With this method authors achieved 99% of accuracy

5. MOBILE BOTNET DETECTION AND MITIGATION TECHNIQUES

The use of mobile devices is increasing day by day. Mobile devices may be smartphones, tablets, smartwatches, and notebooks. Most of these devices use the internet. Applications running on these devices are usually provided by the third party application developers. Operating system in these devices are open source, which makes mobile devices easy target for attacks. In [37], authors proposed a method for the classification of mobile applications as benign or malign, this helps in finding mobile applications which can allow botnets. For this method authors used background services along with broadcast receivers, MD5, and permissions. They used machine learning techniques for classifying mobile applications. They used UNB ISCX data set for testing this method. According to their results Naïve Bayes gives good results compared to other machine learning techniques. In [38], the authors proposed a method based on communication patterns to detect Peer-to-Peer botnets in mobile devices. For developing this method they used Graphlet graph representation for catching normal patterns. Their method don't affect the client's privacy. This method can be applied to encrypted traffic. For evaluating authors used principal component analysis method. They have also used machine learning in this work. In [39], the authors presented a new technique for the classification of android application as infected and legitimate applications. For this work authors used convolutional neural network and android permissions. They also presented applications in image form and used these images to train the CNN classifier. For this work authors used 5450 android applications. Using this proposed technique authors achieved 97.2% accuracy. In [40], the authors presented a technique for detecting HTTP based mobile botnets. In this technique authors used neural network and random interval concepts. Authors considered botnets having random intervals and which are free from commands content, packet payload, and encryption complexity. In [41], the authors introduced a method using unsupervised learning for detecting SMS based mobile malware. Used messages in this method, are classified into four classes. For this classification process authors used clustering algorithms. In this method, they also used behavioral-based evaluation and rule base correlation. SMS are marked as benign or malign using rule-based correlations. In[42], authors Introduced a new method for detecting android applications containing botnets with c&c abilities. Authors used machine learning techniques to develop static and dynamic mixed approach for detecting malicious Android applications. The authors achieved 97.48% accuracy, with random forest giving the best results. In[43], the authors presented a method for detecting mobile botnets

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

based on log analysis. Authors named their model as Logdog. Authors developed their model by deploying logcat command login system on android devices. In[44], the authors introduced a new method for detecting SMS based mobile botnets using textual and behavioral-based anomaly detection methods. They named it as SMSBotHunter. In this method authors classified SMS mobile malware as SMS stealer, SMS spammer,and Info stealer using botnets characteristics. In [89], authors trying to find robust classifier and best fitting network traffic features for detecting mobile malware. For this purpose authors selected multilayer perceptron, Support Vector Machine, Naïve Bayes, k-nearest neighbor, and decision tree machine learning techniques. And TCP size, Connection duration, and number of get/post parameters for selecting the best fitting traffic feature. Their evaluation results show that among five classifiers k-nearest neighbor provides high accuracy. In [90], the author's main intention is to find mobile malware using VPN. To achieve this authors Presented a network-based method for detecting pull style c&c channels in mobile botnets. In this method, the authors analyzed suspicious network flow from c&c traffic which will be traveling via VPN. In [91], the author intends to study the characteristics of botnets to find the best suitable character for detecting mobile malware. They named this method as DeDroid. Authors analyzed bot operations of some popular botnets with c&c character. In this work Drebin data set is been used. In [92], researchers introduced a method for detecting HTTP based mobile malware. This is based on the examination of network operations. Authors presented three metrics considering HTTP based mobile malware community functions. And they successfully grouped communication patterns based on periodicity. In [93], a method has been introduced to detect mobile botnets in network traffic which is named as MBotCS. For this purpose a trained model has been developed exploiting machine learning methods. For this work android devices with benign and malware apps have been used. In [94], Authors introduced a new method for detecting mobile botnets by analyzing off device behaviors, this method is named as SMARTbot. Based on these analyses a model is formed to learn about mobile botnets. For developing this model authors adopted artificial neural network backpropagation techniques. This model is tested with various machine learning techniques, among all logistic regression gives high accuracy. In [95], the authors proposed a mobile botnet detection method using Neural Network. They have created a neural network training set using mobile malware features. In [96], the authors proposed a method for detecting mobile botnets in mobile ad-hoc networks (MANETs). For developing this method authors used a defense system based on artificial immune system (AIS). The authors showed fuzzy related security approaches give better security. In [97], the authors proposed a method for finding spamming botnets in android phones. For developing this method authors used artificial immune system. In [98], the authors proposed a technique for preventing SMS based mobile botnets using real-time signature based detection methods. For messages, incoming as well as outgoing authors used pattern matching detection method and for classifying unknown messages as benign and malicious messages, rule based methods are used. Using this method nearly 12000 messages and achieved 100% accuracy. In [99], the author's goal is to produce network-based security solutions for finding and reducing attacks and abnormalities in mobile networks. For this authors deployed analytical modeling, learning, simulation along with control plane data and billing. In [100], the authors proposed a technique for detecting malicious applications in Android applications. They named it as Android Botnet Identification System (ABIS). To develop this method authors made their proposed model to learn properties of all android botnet families. The authors identified a suitable machine learning method along with the best suitable features by inspecting Android APK files. With this method authors achieved 96.9% accuracy.

6. DDOS ATTACKS

Increasing popularity, very common and unsafe usage of the IoT and Mobile devices made them a way for strongly emerging security issues and attracts various malicious activities like spam mailing, bitcoins, pay per video, phishing and DDoS attacks etc. Among all malicious activies DDoS attacks using IoT and mobile devices is bigest threat . DDoS attacks are extended varsions of denial-of-service attacks (DoS attacks). In DDoS attacks, botmasters intended to increase their botnet size as much as possible by adding more and more bots. Basic classification of DDoS attacktypes is shown in figure.9[45]. Network device level targets routers using secutity defects in routers . Defects in operating systems are used by OS level attacks. Using port scan method application level attacks identifies security issues in applications . intention of Data flood type attacks is making services

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

unavilable for its clients by flooding with fake requests. Protocol feature level exploits the protocol's vulnerability.

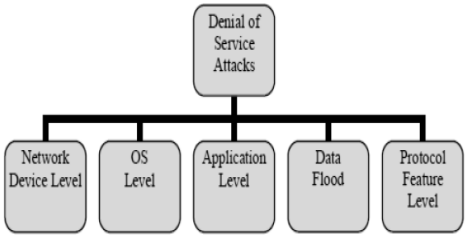


Figure 9. Classification of DDoS Attack Types

Based on the working method of botnets used for conducting DDoS attacks, the architecture of DDoS attacks are divided as Centralized and Decentralized [104]. Bots in the centralized architecture based attacks doesn't communicate with each other but all zombies are connected to common c&c system. IRC & web based along with agent handler stages need to be completed to form a centralized architecture attack. A P2P network is used to form a botnet for conducting decentralized architecture based DDoS attacks. Botmaster gives instructions to few bots in the botnet to control the botnet, using the P2P network these received instructions will be redirected to all the bots in the network. Centralized and decentralized DDoS attack architectures are shown in figure.10 & figure.11 [101]. Using these two types of architecture it is possible to create many other hybrid types of architectures for conducting DDoS attacks. When we see DDoS attack history, Mirai botnet has become the biggest IoT based DDoS attack in recent years. Malware Must Die research group detected Mirai malware in 2016, August. Mirai is a Japanese word which means "the future". Mirai botnet working method is showed in figure.12 [46]. In step 1, Bots tries to find new devices by scanning common IP addresses via 23 or 2323 TCP ports. After finding an unsafe device, it performs brute force attack to find that device access information.

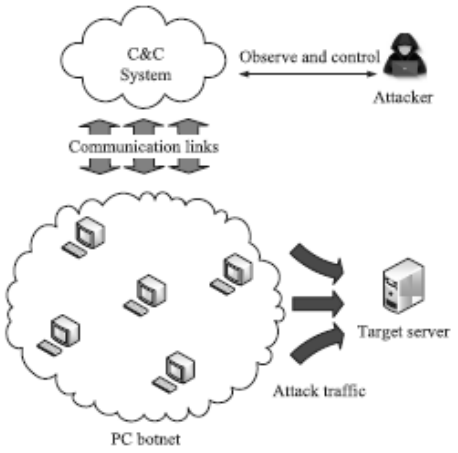


Figure 10. Architecture For Centralized Ddos Attack

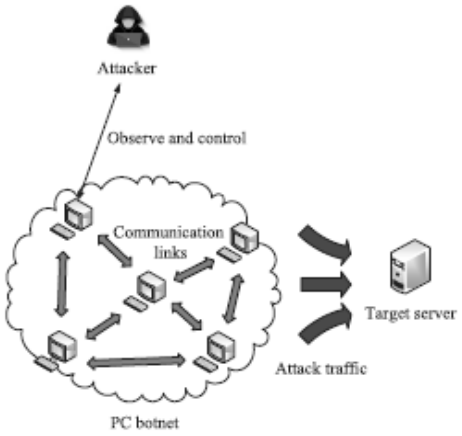


Figure 11. Architecture For Decentralized Ddos Attack

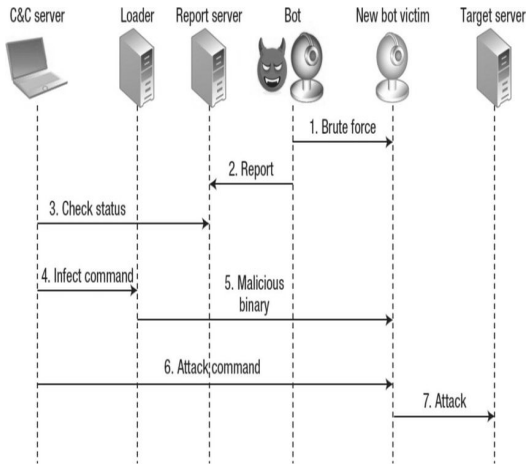


Figure 12. Working Method Of Mirai

In step2, after collecting the compromised device access information along with a shell such as GUI, several features about the compromised device are sent back to the Report server. In step3, the botmaster keeps checking for new devices for

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

compromising, via the c&c server. Also, the botmaster gets the present status of the botnet through report server. In step4, the botmaster decides the next device to be infected and sends infect command with the required information to the loader. Next in step5, loader makes targeted device is to download and install the malicious code. In step6, via c&c server attack command is sent to all the compromised devices by botmaster to conduct an attack. In the final step, the targeted server gets attacked by all bots in the botnet. In [101,115,116], the authors intended to explain a less costing method for performing DDoS attacks using IoT devices. For this purpose authors presented a new architecture with benefits of easy controlling with zero cost, hard to find, and powerful. This method is good for attacks with fewer sources. Attacker, target server, and botnet are the three main parts of the presented model those are shown in fig.13. Here authors wrote a onetime malicious code that can be applied for all targets.

Figure 13. Low-Cost Ddos Attack Architecture

Today's mobile devices can be equally as powerful as personal computers based on their working features. Mobile devices consists of highly performing processors, different connection modules along with large memory drives. A simple mobile device based DDoS attack is shown in Figure.14 [103].

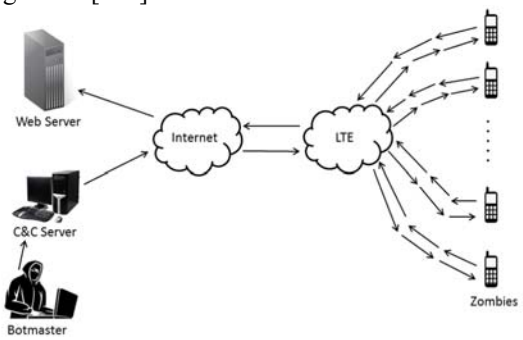


Figure 14. Ddos Attack Model Of Mobile Botnets

In [47], authors have shown a possibility in which mobile devices are used to conduct denial-of-service attacks. The authors presented a new system using mobile botnets to conduct a DoS attack. The authors evaluated their presented model by comparing it with a system called Low Orbit Ion Cannon (LOIC). In [102,105,106,107,108,109,110,111,112,113,114], Based on self-organization and adoption nature and dynamics of mobile botnets authors proposed a method for conducting DDoS attacks. Based on the server's activity reinforcement and fading rules can be combined using bot's cooperation. Also authors showed the effects of massive attacks on servers. An increase in botnet attacks showed the importance of identifying the security threats caused on the internet of things and mobile devices. The effect of DDoS attack is more dangerous than the DoS attack, in terms of available resources for the attack. Which makes DDoS attacks detection and mitigation challenging. Many studies have been conducted to develop a robust method to detect and mitigate botnets activities. But still growing capacities of botnets creates the need for more suitable, quick responding and sophisticated methods to develop.

7. CONCLUSIONS

Finally, we conclude that the various types of IoT and Mobile device botnets and defensive solutions for them. This survey explains the variety of IoT and mobile device botnets along with propagation and detection techniques. Also explains about DDoS attacks, how IOT and Mobile device making DDoS attacks easy to commence. We explained the large-scale DDoS attack, Mirai botnet working, and communication process. We hope that this survey may guide beginner researchers with the same area of interest.

ACKNOWLEDGMENT

This paper was supported by Samsung Research Fund, Sungkyunkwan University, 2018.

REFERENCES

[1] McCarty, "Botnets: big and bigger," in IEEE Security & Privacy, vol. 1, no. 4, pp. 87-90, July-Aug. 2003.

[2] H. R. Zeidanloo and A. A. Manaf, "Botnet Command and Control Mechanisms," 2009 Second International Conference on Computer and Electrical Engineering, Dubai, pp.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

564-568. 2009.

[3] Barford P., Yegneswaran V. "An Inside Look at Botnets". In: Christodorescu M., Jha S., Maughan D., Song D., Wang C. (eds) Malware Detection. Advances in Information Security, vol 27. Springer, Boston, MA, 2007.

[4] Emmanuel C. Ogu, Olusegun A. Ojesanmi, Oludele Awodele and Shade Kuyoro, "A Botnets Circumspection: The Current Threat Landscape, and What We Know So Far," in Information 2019, 10(11), 337, October 30, 2019. https://doi.org/10.3390/info10110337

[5] Sangita Baruah, "Botnet Detection: Analysis of Various Techniques", International Journal of Computational Intelligence & IoT, Vol. 2, No. 2, 2019. https://ssrn.com/abstract=3355519

[6] M. Feily, A. Shahrestani, and S. Ramadass, "A Survey of Botnet and Botnet Detection," 2009 Third International Conference on Emerging Security Information, Systems and Technologies, Athens, Glyfada, pp. 268-273, 2009.

[7] G. Vormayr, T. Zseby, and J. Fabini, "Botnet Communication Patterns, " in IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2768-2796, Fourthquarter 2017.

[8] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things, " in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250-1258, Oct. 2017.

[9] Irfan Saif and Sean Peasley and Arun Perinkolam, "Safeguarding the internet of things: Being secure, vigilant, and resilient in the connected age," https://dupress.deloitte.com/dup-us-en/deloittereview/issue-17/internet-of-things-data-security-and-privacy.html, 2015.

[10] "A Quick History of IoT Botnets" https://blog.radware.com/uncategorized/2018/03/history-of-iot-botnets/

[11] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, pp. 180-187, 2015.

[12] E. Ronen and A. Shamir, "Extended Functionality Attacks on IoT Devices: The Case of Smart Lights," 2016 IEEE European Symposium on Security and Privacy (EuroS&P), Saarbrucken, pp. 3-12, 2016.

[13] https://drive.google.com/file/d/1uNZr8PEyKv1B2LelnomKQaY4IgGv29O_/view

[14] https://www.cyber.nj.gov/threat-profiles/botnet-variants/aidra-botnet

[15] Antonakakis, Manos, et al. "Understanding the Mirai botnet." 26th {USENIX} Security Symposium ({USENIX} Security 17). 2017.

[16] Faghani, Mohammad R., and Uyen T. Nguyen. "Mobile botnets meet social networks: design and analysis of a new type of botnet." International Journal of Information Security 18.4 (2019): 423-449.

[17] Yusof, Muhammad, Madihah Mohd Saudi, and Farida Ridzuan. "A new mobile botnet classification based on permission and API calls." 2017 Seventh International Conference on Emerging Security Technologies (EST). IEEE, 2017.

[18] Karim, Ahmad, et al. "Mobile botnet attacks–An emerging threat: Classification, review and open issues." KSII Transactions on Internet and Information Systems (TIIS) 9.4 (2015): 1471-1492.

[19] Eslahi, Meisam, Rosli Salleh, and Nor Badrul Anuar. "MoBots: A new generation of botnets on mobile devices and networks." 2012 International Symposium on Computer Applications and Industrial Electronics (ISCAIE). IEEE, 2012.

[20] D. Maslennikov. (2011). ZeuS in the Mobile – Facts and Theories. Available: http://www.securelist.com/en/analysis/204792194/

[21] https://www.mobeyforum.org/wp-content/uploads/2015/09/Zeus-in-the-Mobile_20110801.pdf

[22] S. Perez. More DroidDream Details Emerge: It was Building a Mobile Botnet (2011). http://www.readwriteweb.com/

[23] Zhou, Yajin, and Xuxian Jiang. "Dissecting android malware: Characterization and evolution." 2012 IEEE symposium on security and privacy. IEEE, 2012.

[24] Porras, Phillip, Hassen Saidi, and Vinod Yegneswaran. "An analysis of the ikee. b iphone botnet." International Conference on Security and Privacy in Mobile Information and Communication Systems. Springer, Berlin, Heidelberg, 2010.

[25] M. Postman. (2012). iPhone Viruses: Ikee.b Worm. http://www.letsunlockiphone.com/ios-viruses-iphone-ikee-b-worm

[26] X. Jiang. (2012). New TigerBot Malware Found in Alternative Android Markets. http://www.csc.ncsu.edu/faculty/jiang/

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

TigerBot/
[27] A. Yamamoto. (2012). Android.Tigerbot. http://www.symantec.com/security_response/print_writeup.jsp?docid=2012-041010-2221-99
[28] ThreatPost. (2012). Researchers Discover Android Mobile Botnet 100k Strong. http://threatpost.com/en_us/blogs/researchers-discover-android-mobile-botnet-100k-strong-021012
[29] Meidan Yair, et al. "N-baiot—network-based detection of iot botnet attacks using deep autoencoders." IEEE Pervasive Computing 17.3 (2018): 12-22.
[30] McDermott, Christopher D., Farzan Majdani, and Andrei V. Petrovski. "Botnet detection in the internet of things using deep learning approaches." In 2018 international joint conference on neural networks (IJCNN), pp. 1-8. IEEE, 2018.
[31] Nguyen, Huy-Trung, Quoc-Dung Ngo, and Van-Hoang Le. "IoT botnet detection approach based on PSI graph and DGCNN classifier." In 2018 IEEE International Conference on Information Communication and Signal Processing (ICICSP), pp. 118-122. IEEE, 2018.
[32] Doshi, Rohan, Noah Apthorpe, and Nick Feamster. "Machine learning ddos detection for consumer internet of things devices." In 2018 IEEE Security and Privacy Workshops (SPW), pp. 29-35. IEEE, 2018.
[33] Kumar, CU Om, and Ponsy RK Sathia Bhama. "Detecting and confronting flash attacks from IoT botnets." The Journal of Supercomputing 75.12 (2019): 8312-8338.
[34] Jung, Woosub, et al. "IoT botnet detection via power consumption modeling." Smart Health 15 (2020): 100103.
[35] Xiang, Cui, Fang Binxing, Yin Lihua, Liu Xiaoyi, and Zang Tianning. "Andbot: towards advanced mobile botnets." In Proceedings of the 4th USENIX conference on Large-scale exploits and emergent threats, pp. 11-11. USENIX Association, 2011.
[36] Apvrille, Axelle. "Symbian worm Yxes: Towards mobile botnets?." Journal in Computer Virology 8.4 (2012): 117-131.
[37] Anwar, Shahid, Jasni Mohamad Zain, Zakira Inayat, Riaz Ul Haq, Ahmad Karim, and Aws Naser Jabir. "A static approach towards mobile botnet detection." In 2016 3rd International Conference on Electronic Design (ICED), pp. 563-567. IEEE, 2016.
[38] Mongkolluksamee, Sophon, Vasaka Visoottiviseth, and Kensuke Fukuda. "Robust Peer to Peer Mobile Botnet Detection by Using Communication Patterns." In Proceedings of the Asian Internet Engineering Conference, pp. 38-45. 2018.
[39] Hojjatinia, Sina, Sajad Hamzenejadi, and Hadis Mohseni. "Android Botnet Detection using Convolutional Neural Networks." arXiv preprint arXiv:1911.12457 (2019).
[40] Eslahi, Meisam, et al. "Mobile botnet detection model based on retrospective pattern recognition." International Journal of Security and Its Applications 10.9 (2016): 39-44.
[41] Alzahrani, Abdullah J., and Ali A. Ghorbani. "Sms-based mobile botnet detection module." In 2016 6th International Conference on IT Convergence and Security (ICITCS), pp. 1-7. IEEE, 2016.
[42] Qamar, Attia, Ahmad Karim, and Shahab Shamshirband. "Hybrid Machine Learning Techniques Applied in Real Engineering Applications." (2019).
[43] Girei, Daifur Abubakar, Munam Ali Shah, and Muhammad Bilal Shahid. "An enhanced botnet detection technique for mobile devices using log analysis." In 2016 22nd International Conference on Automation and Computing (ICAC), pp. 450-455. IEEE, 2016.
[44] F. Faghihi, M. Abadi, and A. Tajoddin, "SMSBotHunter: A Novel Anomaly Detection Technique to Detect SMS Botnets," 2018 15th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC), Tehran, pp. 1-6, 2018.
[45] Aamir, Muhammad & Arif, Muhammad. (2013). "Study and Performance Evaluation on Recent DDoS Trends of Attack & Defense," International Journal of Information Technology and Computer Science. 5. 54-65. 10.5815/ijitcs.2013.08.06.
[46] Kolias, Constantinos, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. "DDoS in the IoT: Mirai and other botnets." Computer 50, no. 7 (2017): 80-84.
[47] P. Farina, E. Cambiaso, G. Papaleo, and M. Aiello, "Understanding DDoS Attacks from Mobile Devices," 2015 3rd International Conference on Future Internet of Things and Cloud, Rome, 2015, pp. 614-619.
[48] Herwig, Stephen, Katura Harvey, George Hughey, Richard Roberts, and Dave Levin. "Measurement and Analysis of Hajime, a Peer-to-peer IoT Botnet." In NDSS. 2019.
[49] Ashton K. That 'internet of things' thing.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

RFID journal. 22(7):97-114. 2009 Jun 22;

[50] Angrishi, Kishore. "Turning internet of things (iot) into internet of vulnerabilities (iov): Iot botnets." arXiv preprint arXiv:1702.03681 (2017).

[51] Hayashi, Kaoru. "IoT worm used to mine cryptocurrency." SymantecSecurity Response (2014).Source: https://herrymorison.tistory.com/entry/IoT-Worm-Used-to-Mine-Cryptocurrency?category=540332?category=540332

[52] De Donno, Michele, et al. "DDoS-capable IoT malwares: Comparative analysis and Mirai investigation." Security and Communication Networks 2018 (2018).

[53] http://insecurety.net/hydra-irc-bot-the-25-minute-overview-of-the-kit/

[54] Zelika Zorz, "Linux/IRCTelnet creates new, powerful IoT DDoS botnets". Source https://www.helpnetsecurity.com/2016/11/02/linuxirctelnet-iot-ddos-botnet/

[55] A. Marzano et al., "The Evolution of Bashlite and Mirai IoT Botnets," 2018 IEEE Symposium on Computers and Communications (ISCC), Natal, 2018, pp. 00813-00818,doi:10.1109/ISCC.2018.8538636.

[56] https://securityintelligence.com/news/bashlite-malware-uses-iot-for-ddos-attacks/

[57] Jornt van der Wiel, Vincente Diaz, yury Namestnikov, Konstantin Zykov, " Hajime the Mysterious evolving botnet", April 25, 2017. Source: https://securelist.com/hajime-the-mysterious-evolving-botnet/78160/

[58] Shobana, M., and S. Rathi. "IOT Malware: An Analysis of IOT Device Hijacking." 2018.

[59] Sinanović, Hamdija, and Sasa Mrdovic. "Analysis of Mirai malicious software." In 2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), pp. 1-5. IEEE, 2017.

[60] "what is the Mirai Botnet ? " source: https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/

[61] "How a Dorm Room Minecraft Scam Brought Down the Internet". source https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/

[62] Scott Sr, James, and Winter Summit. "Rise of the Machines: The Dyn Attack Was Just a Practice Run" December 2016.

[63] Singh, Jai Puneet, and Akashdeep Chauhan. "Detection and prevention of non-PC botnets." 2018.

[64] Swati Khandelwal "The Hackers News". source :https://thehackernews.com/2016/10/linux-irc-iot-botnet.html

[65] https://arstechnica.com/information-technology/2016/11/new-iot-botnet-that-borrows-from-notorious-mirai-infects-3500-devices/

[66] Abdullah, Zubaile, Madihah Mohd Saudi, and Nor Badrul Anuar. "Mobile botnet detection: Proof of concept." In 2014 IEEE 5th control and system graduate research colloquium, pp. 257-262. IEEE, 2014.

[67] https://www.f-secure.com/v-descs/worm_symbos_yxe.shtml#manual

[68] Alvaro Rocha, Ana Maria Correia, Felix.B Tan,Karl. A Stroetmann, "New Perspective in Information Systems and Technologies" Springer science & Business Media. 159, Mar 19, 2014.

[69] H. Binsalleeh et al., "On the analysis of the Zeus botnet crimeware toolkit," 2010 Eighth International Conference on Privacy, Security and Trust, Ottawa, ON, 2010, pp. 31-38, doi: 10.1109/PST.2010.5593240.

[70] GoldSparrow, "Zeus(Zbot)Botnet Targets Financial Institutions & Bypasses Most Anti-virus programs". https://www.enigmasoftware.com/zeus-zbot-botnet-targets-financial-institutions/

[71] Foremost, J. "DroidDream mobile malware." https://www.virusbulletin.com/virusbulletin/2012/03/droiddream-mobile-malware

[72] Zhou, Yajin, and Xuxian Jiang. "An analysis of the anserverbot trojan." Tech. Rep., 9 (2011).

[73] Javox.com "Secure your jailbroken iphone from ssh hacking with mobile terminal app", 2009. http://jaxov.com/2009/11/secure-your-jailbroked-iphone-from-ssh-hacking-with-mobileterminal-app/

[74] Jeff Goldman, " New TigerBot Android Malware Found", 2012. https://www.esecurityplanet.com/mobile-security/new-tigerbot-android-malware-found.html

[75] Dan Kaplan "World's biggest Android botnets spotted",Feb 15, 2012. https://www.crn.com.au/news/worlds-biggest-android-botnets-spotted-290379

[76] Letteri, Ivan, Giuseppe Della Penna, and Giovanni De Gasperis. "Security in the internet of things: botnet detection in software-defined networks by deep learning techniques." International Journal of High Performance Computing and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Networking 15.3-4 (2019): 170-182.

[77] C. Dietz et al., "IoT-Botnet Detection and Isolation by Access Routers," 2018 9th International Conference on the Network of the Future (NOF), Poznan, 2018, pp. 88-95, doi: 10.1109/NOF.2018.8598138.

[78] Al Shorman, Amaal, Hossam Faris, and Ibrahim Aljarah. "Unsupervised intelligent system based on one class support vector machine and Grey Wolf optimization for IoT botnet detection." Journal of Ambient Intelligence and Humanized Computing, 1-17 (2019).

[79] Banerjee, Mahesh, and S. D. Samantaray. "Network Traffic Analysis Based IoT Botnet Detection Using Honeynet Data Applying Classification Techniques." International Journal of Computer Science and Information Security (IJCSIS) 17.8 (2019).

[80] H. Bahşi, S. Nõmm and F. B. La Torre, "Dimensionality Reduction for Machine Learning Based IoT Botnet Detection," 2018 15th International Conference on Control, Automation, Robotics and Vision (ICARCV), Singapore, 2018, pp. 1857-1862, doi: 10.1109/ICARCV.2018.8581205.

[81] Nguyen, Huy-Trung, Doan-Hieu Nguyen, Quoc-Dung Ngo, Vu-Hai Tran, and Van-Hoang Le. "Towards a rooted subgraph classifier for IoT botnet detection." In Proceedings of the 2019 7th International Conference on Computer and Communications Management, pp. 247-251. 2019.

[82] Vinayakumar, R., Mamoun Alazab, Sriram Srinivasan, Quoc-Viet Pham, Soman Kotti Padannayil, and K. Simran. "A Visualized Botnet Detection System based Deep Learning for the Internet of Things Networks of Smart Cities." IEEE Transactions on Industry Applications (2020).

[83] Sagirlar, Gokhan, Barbara Carminati, and Elena Ferrari. "AutoBotCatcher: blockchain-based P2P botnet detection for the Internet of things." In 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC), pp. 1-8. IEEE, 2018.

[84] Prokofiev, Anton O., Yulia S. Smirnova, and Vasiliy A. Surov. "A method to detect Internet of Things botnets." In 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), pp. 105-108. IEEE, 2018.

[85] Nõmm, Sven, and Hayretdin Bahşi. "Unsupervised anomaly based botnet detection in IoT networks." In 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA), pp. 1048-1053. IEEE, 2018.

[86] Tzagkarakis, Christos, Nikolaos Petroulakis, and Sotiris Ioannidis. "Botnet Attack Detection at the IoT Edge Based on Sparse Representation." In 2019 Global IoT Summit (GIoTS), pp. 1-6. IEEE, 2019.

[87] Sajjad, Syed Muhammad, and Muhammad Yousaf. "UCAM: usage, communication and access monitoring based detection system for IoT botnets." In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pp. 1547-1550. IEEE, 2018.

[88] Hadi, Hassan Jalil, Syed Muhammad Sajjad, and Khaleeq un Nisa. "BoDMitM: Botnet Detection and Mitigation System for Home Router Base on MUD." In 2019 International Conference on Frontiers of Information Technology (FIT), pp. 139-1394. IEEE, 2019.

[89] Feizollah, Ali, Nor Badrul Anuar, Rosli Salleh, Fairuz Amalina, and Shahaboddin Shamshirband. "A study of machine learning classifiers for anomaly-based mobile botnet detection." Malaysian Journal of Computer Science 26, no. 4 (2013): 251-265.

[90] Choi, Byungha, Sung-Kyo Choi, and Kyungsan Cho. "Detection of mobile botnet using VPN." In 2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 142-148. IEEE, 2013.

[91] Karim, Ahmad, Rosli Salleh, and Syed Adeel Ali Shah. "DeDroid: a mobile botnet detection approach based on static analysis." In 2015 IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom), pp. 1327-1332. IEEE, 2015.

[92] Eslahi, Meisam, Moslem Yousefi, Maryam Var Naseri, Y. M. Yussof, N. M. Tahir, and H. Hashim. "Cooperative network behaviour analysis model for mobile Botnet detection." In 2016 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), pp. 107-112. IEEE, 2016.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[93] Meng, Xin, and George Spanoudakis. "MBotCS: A mobile botnet detection system based on machine learning." In International Conference on Risks and Security of Internet and Systems, pp. 274-291. Springer, Cham, 2015.

[94] Karim, Ahmad, Rosli Salleh, and Muhammad Khurram Khan. "SMARTbot: A behavioral analysis framework augmented with machine learning to identify mobile botnet applications." PloS one 11, no. 3 (2016).

[95] Oulehla, Milan, Zuzana Komínková Oplatková, and David Malanik. "Detection of mobile botnets using neural networks." In 2016 Future Technologies Conference (FTC), pp. 1324-1326. IEEE, 2016.

[96] Hanafy, Ibrahim Mohamed, A. A. Salama, M. Abdelfattah, and Y. M. Wazery. "AIS Model for botnet detection in MANET using fuzzy function." International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC) 3, no. 1 (2013): 95-102.

[97] Vural, Ickin, and Hein Venter. "Detecting mobile spam botnets using artificial immune systems." In IFIP International Conference on Digital Forensics, pp. 183-192. Springer, Berlin, Heidelberg, 2011.

[98] Alzahrani, Abdullah J., and Ali A. Ghorbani. "Real-time signature-based detection approach for SMS botnet." In 2015 13th Annual Conference on Privacy, Security and Trust (PST), pp. 157-164. IEEE, 2015.

[99] Abdelrahman, Omer H., Erol Gelenbe, Gökçe Görbil, and Boris Oklander. "Mobile network anomaly detection and mitigation: The NEMESYS approach." In Information Sciences and Systems 2013, pp. 429-438. Springer, Cham, 2013.

[100] Tansettanakorn, Chanin, Supachai Thongprasit, Siritam Thamkongka, and Vasaka Visoottiviseth. "ABIS: a prototype of android botnet identification system." In 2016 Fifth ICT International Student Project Conference (ICT-ISPC), pp. 1-5. IEEE, 2016.

[101] Huang, Kaifan, Lu-Xing Yang, Xiaofan Yang, Yong Xiang, and Yuan Yan Tang. "A Low-Cost Distributed Denial-of-Service Attack Architecture." IEEE Access 8 (2020): 42111-42119.

[102] Santos, Augusto Almeida, Michele Nogueira, and José MF Moura. "A stochastic adaptive model to explore mobile botnet dynamics." IEEE Communications Letters 21, no. 4 (2016): 753-756.

[103] Kitana, Asem, Issa Traore, and Isaac Woungang. "Impact Study of a Mobile Botnet over LTE Networks." J. Internet Serv. Inf. Secur. 6, no. 2 (2016): 1-22.

[104] Silva, Sérgio SC, Rodrigo MP Silva, Raquel CG Pinto, and Ronaldo M. Salles. "Botnets: A survey." Computer Networks 57, no. 2 (2013): 378-403.

[105] Abbas, A., Siddiqui, I. F., Lee, S. U. J., Bashir, A. K., Ejaz, W., & Qureshi, N. M. F. (2018). Multiobjective optimum solutions for IoT-based feature models of software product line. IEEE Access, 6, 12228–12239.

[106] Choi, H. W., Qureshi, N. M. F. & Shin, D. R. (2019) Comparative analysis of electricity consumption at home through a Silhouette-score prospective. In 2019 21st International conference on advanced communication technology (ICACT) (pp. 589–591). IEEE.

[107] Qureshi, N. M. F., Siddiqui, I. F., Abbas, A., Bashir, A. K., Choi, K., Kim, J., & Shin, D. R. (2019). Dynamic container-based resource management framework of spark ecosystem. In 2019 21st International conference on advanced communication technology (ICACT) (pp. 522–526). IEEE.

[108] Qureshi, N. M. F., Siddiqui, I. F., Abbas, A., Bashir, A. K., Nam, C. S., Chowdhry, B. S., et al. (2020). Stream-based authentication strategy using IoT sensor data in multi-homing sub-aqueous big data network. Wireless Personal Communications, 1–13.

[109] Siddiqui, I. F., Qureshi, N. M. F., Chowdhry, B. S., & Uqaili, M. A. (2020). Pseudo-cache-based IoT small files management framework in HDFS cluster. Wireless Personal Communications.

[110] Qureshi, N. M. F., Bashir, A. K., Siddiqui, I. F., Abbas, A., Choi, K. & Shin, D. R. (2018). A knowledge-based path optimization technique for cognitive nodes in smart grid. In 2018 IEEE global communications conference (GLOBECOM) (pp. 1–6). IEEE.

[111] Siddiqui, I. F., Qureshi, N. M. F., Shaikh, M. A., Chowdhry, B. S., Abbas, A., Bashir, A. K., et al. (2019). Stuck-at fault analytics of IoT devices using knowledge-based data processing strategy in smart grid. Wireless Personal Communications, 106(4), 1969–1983.

[112] Qureshi, N. M. F., Shin, D. R., Siddiqui, I. F., & Chowdhry, B. S. (2017). Storage-tag-aware scheduler for hadoop cluster. IEEE Access, 5, 13742–13755.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[113] Faseeh Qureshi, N. M., Shin, D. R., & Siddiqui, I. F. (2017). Key exchange authentication protocol for NFS enabled HDFS client. Journal of Theoretical & Applied Information Technology, 95(7).

[114] Siddiqui, F. I., et al. (2019). Edge-node-aware adaptive data processing framework for smart grid. Wireless Personal Communications, 106(1), 179–189.

[115] Qureshi, F. N. M., & Shin, D. R. (2016). RDP: A storage-tier-aware Robust Data Placement strategy for Hadoop in a cloud-based heterogeneous environment. TIIS, 10(9), 4063–4086.

[116] Qureshi, F. N. M., et al. (2019) An aggregate mapreduce data block placement strategy for wireless IoT edge nodes in smart grid. Wireless Personal Communications, 106(4), 2225–2236.