INTERNET OF THINGS BOTNET (MIRAI): A SYSTEMATIC REVIEW

[1]*Burair Saad Hameed, [2]Selvakumar Manickam, [3]Kamal Alieyan
National Advanced IPv6 Centre (IPv6)
[1,2,3]Universiti Sains Malaysia, 11800 Gelugor, Penang, Malaysia.
*Correspondence: brersaad@student.usm.my

ABSTRACT:*The Internet of Things (IoT) came into being as the consequence of new and rapid advancements in connectivity and technology. The research focuses on the effects of Botnet in relation to IoT by systematically reviewing 49 peer-reviewed scholarly journal articles. The study of these articles brings to light varying degrees of problems discussed therein and the different stages and procedures adapted to attain the maximum position to solve the problems presented. While investigating the databases of SCOPUS and GOOGLE SCHOLAR, this research will examine such problems.*

Keywords: IoT, Mirai Botnet, Cyber Attacks, Detection, Review

INTRODUCTION

The technological world is recently plagued with increasing rates of security breach using IoT. The IoT is an essential tool for hackers to conduct their cyber attacks, as they serve as the weak entry point to infiltrate a chain of modern computer networks. The IoT is very numerous, even though its computational capabilities are limited. One major feature of the IoT is that they are connected to the internet always and therefore, constitute several flaws/weaknesses, which is mostly as a result of non-standard security configurations. As such, they serve as easy target for hackers. The IoT is popular for its negative activity on the internet and how people use it negatively to their advantage. One of such people includes the perpetrators of cyber attacks known as Distributed Denial-of-Service (DDoS) attacks.

The white-hat research group titled “Malware Must Die”[1] discovered Mirai Botnet, a famous example of DDoS in August of 2016. The word Mirai stands for “the future” in Japanese. This IoT device is characterized by several variants and imitators and has successfully driven some of the most treacherous attacks in the history of cyberattacks. Brian Krebs, a computer security consultant, witnessed one of such attacks in September of 2016 when his website was attacked with as much as 620 Gbps of traffic. According to Krebs on Security[2], this represents much more than is usually required in order of magnitude to send several sites offline, under normal circumstances.

The DDoS attack of French webhost and cloud provider, OVH Goodin [3] using Mirai Malware is even bigger. It went as high as 1.1 Tbps and occurred within the same period as that of Krebs. Furthermore, the creator of Mirai botnet publicly made the source code of the aforementioned DDoS available, allowing hackers to use Mirai botnet even for rental, such that at the same time, as it can connect to several different devices, up to 400,000 [4]. The internet kept suffering from different attacks from Mirai botnet, but one of the most important of such cyber attacks occurred against service provider Dyn, in October 2016 where it successfully disrupted thousands of sites including popular ones such as Twitter, Netflix, Reddit, and Github, for several hours[5].

The main mode of operation of Mirai is that it attacks digital devices such as routers, DVRs and webcams that have in them some version of BusyBox (busybox.net), it infects such devices and then spread thus. Using a small dictionary of possible or common pairs of usernames and passwords, it comes up with the administrative credentials of other IoT devices by brute force. These mutations are generated every day, and they continue to infect and disrupt others’ activities in seriously damaging ways. Surprisingly, they still employ the same methods of infiltration as the original malware. This goes a long way to show that IoT device vendors are careless by neglecting to implement even the basics of security practices. Instead, IoT botnets receive even more attention from researchers [6, 7]. However, there is a possibility of the creation of even more chronic attacks which will disrupt different web activities and could even affect the infrastructural settings of the internet itself. This can be avoided if the security personnel respond proactively by coming up with entirely new defence methods, and by reacting swiftly to situations.

LITERATURE REVIEW

In launching attacks against servers, Mirai brings about a DDoS against chosen sets of target servers by continuously spreading to IoT devices whose configuration are not secured enough. For a Mirai botnet to function properly, it constitutes four (4) components; the bot, the command and control (C&C) server, the Tor network, and the report server.

1. The Bot: This part of Mirai comprises the malware which infects devices. A bot master usually controls it. The bot works in two ways. First, it spreads its infection to weakly configured devices, thereby disrupting their normal activities. Secondly, upon receiving a command from the botmaster, the bot attacks the target server.
2. The Command and Control (C&C) Server: This component of Mirai is charged with the duty of making sure that the botmaster has a centralised management interface, which they use to launch new DDoS cyber-attacks and to check the condition of the botnet.
3. The Tor Network: The Tor network has the responsibility of handling communication between the different parts of the infrastructure. One of its significant features is its anonymity. Using the Tor network, the botmaster communicates directly with new victims to ensure that practical targets from different platforms out of the 18 available ones are adequately spread out. Some of the platforms include HRM, MIPS and x86.
4. The Report Server: The primary function of this component of the bot is the control and organisation of all the detailed information about the devices in the botnet. It transacts directly with all newly infected devices.

In the beginning, transactions and methods of operation of botnet included scanning public IP address systems randomly using TCP ports 23 or 2323. It, however, boycotts some public servers such as the Department of Defense, the U.S Postal Service, General Electric, the Internet Assigned Numbers Authority, the Hewlett – Packard, among others. This is a crucial tactic to prevent the government from having any suspicions [8, 9]. The major stages in botnet transactions (operation and communication) is illustrated in Figure 1 below. Below are the methods employed by the bot in attacking servers, in stages.

- Step 1. Using 62 probable pairs of matching usernames and passwords, the bot identifies the presence of weakly configured IoT devices to find out their default credentials and infiltrate their system in a brute force attack.
- Step 2. The bot acquires a shell (a command-line or graphical user interface) as soon as it has successfully recognised adequate and suitable credentials.
- Step 3. Using the Tor network, the botmaster interacts with the report server continuously to establish the botnet's current level/status while at the same time continually searching for potential target victims.
- Step 4. The botmaster conducts the infecting process after identifying victim servers which are vulnerable enough to infect, by issuing an infect command in the loader which is made up of all the necessary details of the victim. Such details involve hardware architecture and IP addresses.
- Step 5. Here, the download occurs with the loader logging into the target device and commanding it to download and execute the malware's corresponding binary version. This uploading is usually conducted using the GNU Wget (www.gnu.org/softwareWgnet/manual/w.get.html). It also uses the Trivial File Transport Protocol. It is important to note that the malware immediately shuts down its own weak entry points including Secure Shell (SSH) services and Telnet in a bid to protect itself from other malware after successfully infiltrating others. The newly recruited bot instance then starts to interact (communicate) and receive attack commands from the C&C) server at this point. However, it does not use a static IP address in doing so. Instead, it resolves a domain name hardcoded in the executable (by default, the value of this entry is cnc.changeme.com in Mirai's source code). Therefore, the IP address can be altered in time without having to change the binary and without any extra flow of data.
- Step 6. After the botmaster has ensured its own protection, it commands all the several bots under its command to begin an attack against a chosen server. It does so by using the C&C server to give a simple order. It also takes into consideration associating factors which include the type of attack, the duration of the attack, the IP addresses of the different bot instances, and even the target server.
- Step 7. The attacks come in varieties, up to ten of them, including Generic Routing Encapsulation (GRE), TCP, and HTTP flooding attacks. At this stage, the bot instances employ some or all of the attack variations in attacking the target server.

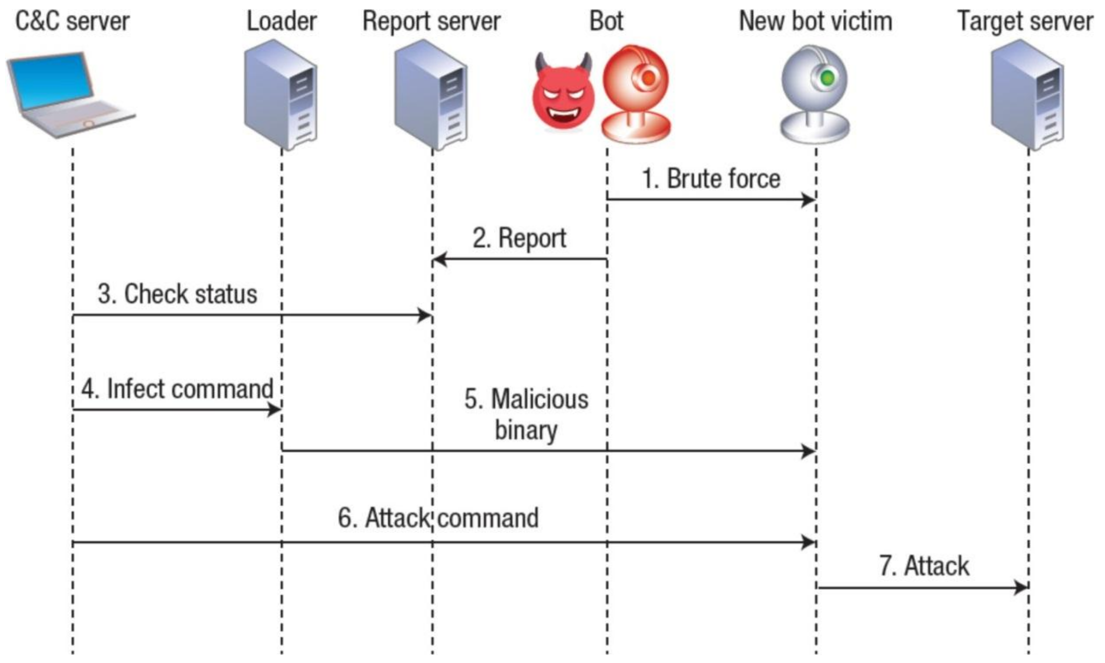

Figure 1: Mirai botnet operation and communication. Mirai results in a distributed denial of service (DDoS) to a set of target servers by consistently propagating to vulnerable configured Internet of Things (IoT) devices.

Mirai signatures Compared to other similar malware[10]. The Mirai botnet is a bold one because it is evident wherever it is present. It does not attempt to hide; rather, it leaves clearly recognisable evidence or footprint at almost all steps of infection. The Mirai botnet can be identified using basic network analysis. Some Mirai signatures are outlined below as follows:

1. Numerical or sequential testing of particular credentials in particular ports.
2. Sending reports that bring about specific patterns.
3. Downloading a distinct type of binary code.
4. Exchange of keep-alive messages.
5. Receiving specifically structured attack commands.
6. Using a relatively small number of random elements in generating traffic attack.

Figure 2 portrays the possible distinctions that exist between different botnets. It expresses some standard interaction patterns between Mirai's loader component and other IOT infected devices that have not commenced any form of attacking. The time of interaction or communication of Mirai botnet on devices are different. Notwithstanding, Mirai's infection is easily identified via the following features or message type, sizes of their packets, sequence of messages etc. These features make the Mirai malware infection distinctive from others.

The Mirai bot is noisy and readily available compared to other bots, especially since its source code is public knowledge. The ease of accessing Mirai's source code led to several assertions. One of such assertions is that it will become easily and effectively detectable while devices will prepare adequate defence mechanisms against it. However, even with the release of its source code, the quantity of Mirai bot instances increased rapidly from 213,000 to 493,000 in a period of just two months since the release of the source code [11]. Additionally, several varieties of it in other forms emerged. A surprising issue is how Mirai bots successfully keep on using similarly weak security configurations, in infecting the same types of IoT devices, as they have been using since almost four (4) years ago when the malware was discovered. Most Mirai infections are done using TCP ports 23 and 2323. However, in November 2016, it was discovered that it employs other TCP ports for its use in commandeering devices. Such ports include port 7547. This port is used by ISPs to manage customers' broadband routers locally. According to Krebs [2] close to a million Deutsche Telekom offline subscribers were disrupted by a particular Mirai bot instance, still in November 2016.

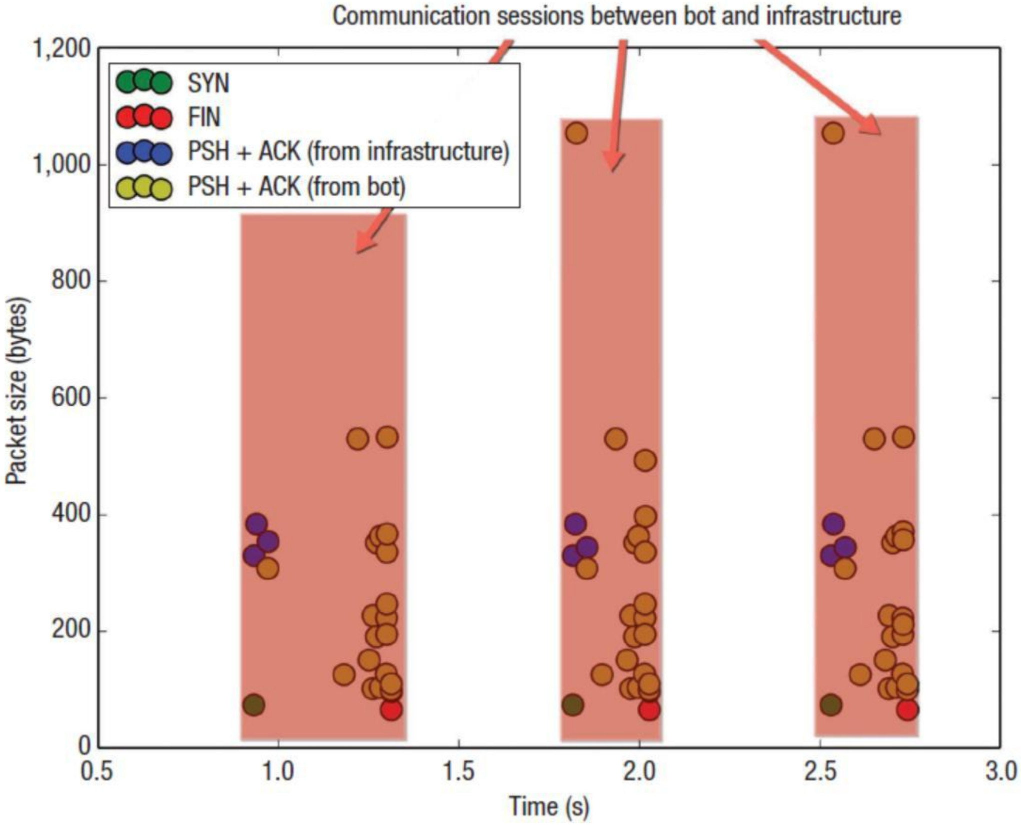

Figure 2: Specific Patterns of Communication between an infected IoT device and Mirai's Loader Component. The meanings of abbreviations used, and which are referred to as standard TCP packet types are as follows:

SYN – synchronise
FIN – Finish
PSH – Push
ACK – Acknowledge

Below are some outstanding attacks by Mirai botnet. One of the variants of Mirai attacked a U.S college [12] launching a DDoS attack that lasted for 54 hours in March 2017. Another new variation was identified with bitcoin miner functionality. However, there is much pessimism as to how compromising IoT devices will succeed in producing any important revenue [13]. The Trend Micro researchers discovered another famous IoT botnet known as Persirai. The name Persirai derives from a mix of Persia (because it is suspected to be of Iranian origin) and Mirai (because it shares the same code base as Mirai). This botnet uses TCP port 81 to try and gain access into the interface of webcams of particular servers. If it succeeds in gaining access, it then enters the router of its victim via universal plug and play (UPnP) vulnerability. Once inside, it downloads the victims' malicious binaries. One significant difference between Mirai botnet and Persirai botnet is that while Mirai botnets leave traces of its existence in its victim, the Persirai deletes all traces of its presence after executing its attack.

Furthermore, Persirai does not employ the use of brute force attack to deduce webcam credentials; rather, it exploited a documented zero-day flaw by infiltrating its victim. This allows hackers direct access to the password file. User Datagram Protocol Flooding attacks form one of the armory of the DDoS. It is estimated that Persirai has made vulnerable about 120,000 devices out there.

RESEARCH METHODOLOGY

The study of IoT botnet forms the basis of this research by reviewing different literature. The researcher employs the use of the PRISMA style review. This review style is a systematic literature review which involves systemic researches for articles on a particular topic by searching through the database of various libraries or other sources. It evaluates full texts for eligibility by screening the article for appropriateness and also by conducting quantitative and qualitative analysis [14]. For Moher, *et. al.*, [14] "this methodology uses systematic and explicit measures to select, identify and critically evaluate important research, and to gather and evaluate data from the researches that are included in the review". While Pickering and Byrne [15] suggest that "it is designed to be comprehensive and reproducible, in contrast to the more subjective narrative review process".

Initially, this methodology was developed for use in the healthcare sector for healthcare reviews and meta-analyses [14] However, its systematic aspects are useful for different fields in the natural and social sciences and information systems. The 49 articles used in this research were gotten using SCOPUS, a very important database. The researcher searched SCOPUS on the 26th of April, 2019 for articles containing the keyword "Botnet" in the title and the expression IOT in any parts of the papers. Using the same process, the database of Google Scholar was searched coming up with 159 articles. 42 out of the 159 articles were the same as those already found on SCOPUS, making the total articles for study, 166.

RESULTS AND DISCUSSION

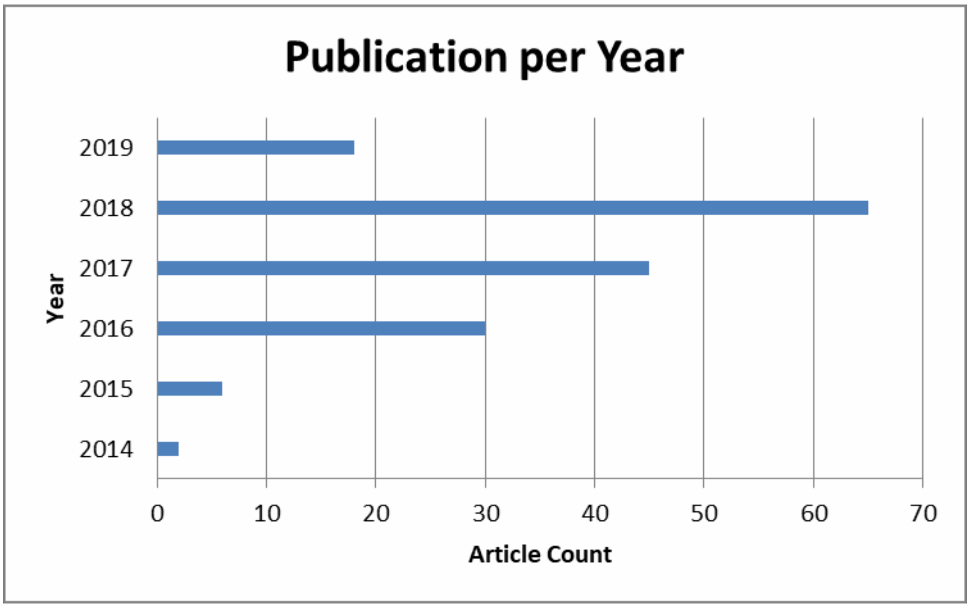

Figure 3: Publications through the years

Table 1: The selected articles from both databases "Scopus & Google Scholar."

No.	Cites	Authors	Title	Year	Data
1	128	C. Kolias	Ddos in the IoT: mirai and other botnets	2017	Scopus
2	19	J. Jerkins	Motivating a market or regulatory solution to IoT insecurity with the mirai botnet code	2017	Scopus
3	11	G. Kambourakis	The Mirai botnet and the IoT zombie armies	2017	Scopus
4	4	Y. Meidan	N-baIoTnetwork-based detection of IoT botnet attacks using deep Autoencoders	2018	Scopus
5	3	M. Paquet-Clouston	Can we trust social media data? Social network manipulation by an IoT botnet	2017	Scopus
6	2	H. Joshi	Collaborative botnet detection with partial communication graph Information	2017	Scopus
7	2	C. Putman	The business model of a botnet	2018	Scopus
8	2	C. Mcdermott	Botnet detection in the internet of things using deep learning Approaches	2018	Scopus
9	2	T. Oh	Android botnet categorization and family detection based on behavioural and signature data	2015	Scopus
10	2	A. Prokofiev	A method to detect internet of things botnets	2018	Scopus
11	1	C. Mcdermott	Towards situational awareness of botnet activity in the internet of Things	2018	Scopus
12	1	N. KoronIoTis	Towards developing network forensic mechanism for botnet activities in the IoT based on machine learning techniques	2018	Scopus
13	1	Y. Ji	The study on the botnet and its prevention policies in the internet of Things	2018	Scopus

14	1	A. Marzano	The evolution of bashlite and Mirai IoT botnets	2018	Scopus
15	1	H. Bahsi	Dimensionality reduction for machine learning-based IoT botnet Detection	2018	Scopus
16	1	S. Homayoun	Botshark: a deep learning approach for botnet traffic detection	2018	Scopus
17	1	X. Li	Botnet detection technology based on DNS	2017	Scopus
18	1	I. Ghafir	Botnet: a system for real-time botnet command and control traffic Detection	2018	Scopus
19	1	J. Margolis	An in-depth analysis of the Mirai botnet	2018	Scopus
20	0	B. Heydari	Utilizing features of aggregated flows to identify botnet network Traffic	2018	Scopus
21	0	S. Nomm	Unsupervised anomaly-based botnet detection in IoT networks	2019	Scopus
22	0	S. Sajjad	Ucam: usage, communication and access monitoring based detection system for IoT botnets	2018	Scopus
23	0	X. Li	Traffic detection of transmission of botnet threat using bp neural Network	2018	Scopus
24	0	S. Haria	The growth of the hide and seek botnet	2019	Scopus
25	0	A. Oliveri	Sagishi: an undercover software agent for infiltrating IoT botnets	2019	Scopus
26	0	Y. Balasubramanian	Quantum IDS for mitigation of DDoS attacks by Mirai botnets	2018	Scopus
27	0	J. Dev	On the imminent advent of botnet powered cracking	2017	Scopus
28	0	S. Chawathe	Monitoring IoT networks for botnet activity	2018	Scopus
29	0	D. Acarali	Modelling the spread of botnet malware in IoT-based wireless sensor Networks	2019	Scopus
30	0	D. Acarali	Modelling botnet propagation in networks with layered defences	2018	Scopus
31	0	C. Dietz	IoT-botnet detection and isolation by access routers	2018	Scopus
32	0	H. Nguyen	IoT botnet detection approach based on psi graph and DGCNN classifier	2018	Scopus
33	0	J. Ceron	Improving IoT botnet investigation using an adaptive network layer	2019	Scopus
34	0	Y. Wang	Gleer: a novel gini-based energy balancing scheme for mobile botnet retopology	2018	Scopus
35	0	M. Wielogorska	Dns traffic analysis for botnet detection	2017	Scopus
36	0	A. Schmitt	Capability analysis of internet of things (IoT) devices in botnets and implications for cybersecurity risk assessment processes	2018	Scopus
37	0	M. Anagnostopoulos	Botnet command and control architectures revisited: tor hidden services and fluxing	2017	Scopus
38	0	H. Dhayal	Botnet and p2p botnet detection strategies: a review	2018	Scopus
39	0	B. Qi	Botcensor: detecting dga-based botnet using two-stage anomaly Detection	2018	Scopus
40	0	D. Wu	Bot catcher: botnet detection system based on deep learning	2018	Scopus
41	0	G. Sagirlar	Autobotcatcher: blockchain-based p2p botnet detection for the internet of things	2018	Scopus
42	0	M. Erquiaga	Analysis of botnet behavior as a distributed system	2018	Scopus
43	0	B. Hammi	An empirical investigation of botnet as a service for cyberattacks	2019	Scopus
44	0	J. Divita	An approach to botnet malware detection using nonparametric bayesian methods	2017	Scopus
45	0	A. Kumar	A secure contained testbed for analyzing IoT botnets	2019	Scopus
46	0	H. Yağci	A parallel cyber universe: botnet implementations over tor-like Networks	2017	Scopus
47	0	M. Moodi	A new method for assigning appropriate labels to create a 28 standard android botnet dataset (28-sabd)	2018	Scopus
48	0	O. Hachinyan	A game-theoretic technique for securing IoT devices against mirai Botnet	2018	Scopus
49	0	A. Bansal	A comparative analysis of machine learning techniques for botnet Detection	2017	Scopus
50	223	M Antonakakis, T April, M Bailey, M Bernhard…	Understanding the mirai botnet	2017	G.scholar
51	51	J Kwon, J Lee, H Lee, A Perrig	Psybog: a scalable botnet detection method for large-scale dns Traffic	2016	G.scholar
52	48	B Herzberg, D Bekerman, I	Breaking down mirai: an IoT ddos botnet analysis	2016	G.scholar

		Zeifman			
53	43	Oy Al-Jarrah, O Alhussein, Pd Yoo…	Data randomization and cluster-based partitioning for botnet intrusion detection	2016	G.scholar
54	25	R Dobbins, S Bjarnason	Mirai IoT botnet description and ddos attack mitigation	2016	G.scholar
55	16	B Krebs	Source code for IoT botnet 'mirai'released	2016	G.scholar
56	16	Kc Lin, Sy Chen, Jc Hung	Botnet detection using support vector machines with artificial fish swarm algorithm	2014	G.scholar
57	16	D Tran, H Mac, V Tong, Ha Tran, Lg Nguyen	A lstm based framework for handling multiclass imbalance in dga botnet detection	2018	G.scholar
58	13	S Soltan, P Mittal, Hv Poor	BlackIoT: IoT botnet of high wattage devices can disrupt the power grid	2018	G.scholar
60	9	I Ghafir, V Prenosil, M Hammoudeh	Botnet command and control traffic detection challenges: a correlation-based solution	2015	G.scholar
61	9	G Bottazzi, G Me	The botnet revenue model	2014	G.scholar
62	8	R Graham	Mirai and IoT botnet analysis	2017	G.scholar
63	7	S Ragan	Here are the 61 passwords that powered the mirai IoT botnet	2016	G.scholar
64	7	N Goodman	A survey of advances in botnet technologies	2017	G.scholar
65	6	A Greenberg	The reaper IoT botnet has already infected a million networks	2017	G.scholar
66	6	Bd Mirai	An IoT ddos botnet analysis	2017	G.scholar
67	6	N Pantic, Mi Husain	Covert botnet command and control using twitter	2015	G.scholar
68	5	T Yeh, D Chiu, K Lu	Persirai: new internet of things (IoT) botnet targets ip cameras	2017	G.scholar
69	4	C Xiao, C Zheng, Y Jia	New IoT/linux malware targets dvrs, forms botnet	2017	G.scholar
70	4	D Mcmillen, M Alvarez	Mirai IoT botnet: mining for bitcoins	2017	G.scholar
71	4	F Jelic	Analysis: record ddos attacks by mirai, IoT botnet	2016	G.scholar
72	4	S Khandelwal	New IoT botnet malware discovered; infecting more devices Worldwide	2016	G.scholar
73	4	Db Cid	IoT home router botnet leveraged in large ddos attack	2016	G.scholar
74	4	I Letteri, M Del Rosso, P Caianiello, D Cassioli	Performance of botnet detection by neural networks in software-defined networks.	2018	G.scholar
75	3	J Slay	Towards developing network forensic mechanism for botnet activities in the IoT based on machine learning techniques	2018	G.scholar
76	3	N Mims	The botnet problem	2017	G.scholar
77	3	M Kan	IoT botnet highlights the dangers of default passwords,”	2016	G.scholar
78	3	L Paul	New reaper IoT botnet leaves 378 million IoT devices potentially vulnerable to hacking	2017	G.scholar
79	3	B Krebs	Mirai IoT botnet co-authors plead guilty-krebs on security	2017	G.scholar
80	3	M Mimoso, C Brook, T Spring	New IoT botnet malware borrows from mirai	2016	G.scholar
81	3	P Loshin	Details emerging on dyn dns ddos attack, mirai IoT botnet	2016	G.scholar
82	3	S Weagle	IoT-driven botnet attacks us university	2017	G.scholar
83	3	M Yusof, Mm Saudi, F Ridzuan	A new mobile botnet classification based on permission and api Calls	2017	G.scholar
84	3	A Arora, Sk Yadav, K Sharma	Denial-of-service (dos) attack and botnet: network analysis, research tactics, and mitigation	2018	G.scholar
85	3	T Lee, H Cho, H Park, J Kwak	Detection of malware propagation in sensor node and botnet group clustering based on e-mail spam analysis	2015	G.scholar
86	2	P Moriuchi, S Chohan	Mirai-variant IoT botnet used to target financial sector in january 2018	2018	G.scholar
87	2	G Falco, C Li, P Fedorov, C	Neuromesh: IoT security enabled by a blockchain powered botnet vaccine	2019	G.scholar

		Caldera…			
88	2	D Fleck, A Stavrou, G Kesidis…	Moving-target defense against botnet reconnaissance and an adversarial coupon-collection model	2018	G.scholar
89	2	R Chinn	Botnet detection: honeypots and the internet of things	2015	G.scholar
90	2	M Graham, A Winckles…	Practical experiences of building an ipfix based open source botnet Detector	2016	G.scholar
91	2	T Seals	Leet IoT botnet bursts on the scene with massive ddos a ack. H ps	2017	G.scholar
92	2	P Dean	Largest ddos attack ever delivered by botnet of hijacked IoT devices	2016	G.scholar
93	2	P Paganini	The linux remaiten malware is building a botnet of IoT device	2016	G.scholar
94	2	S Khandelwal	IoT botnet–25,000 cctv cameras hacked to launch ddos attack	2016	G.scholar
95	2	W Ray	IoT botnet launching massive ddos attacks on websites-bestvpn. Com	2016	G.scholar
96	2	M Kan	An IoT botnet was partly behind friday's massive ddos attack	2016	G.scholar
97	2	M Mimoso	Mirai-fueled IoT botnet behind ddos attacks on dns providers	2016	G.scholar
98	2	C Cimpanu	There'sa 120,000-strong IoT ddos botnet lurking around	2016	G.scholar
99	2	C Beek	Mirai botnet creates army of IoT orcs	2017	G.scholar
100	2	P Paganini	The hosting provider ovh continues to face massive ddos attacks launched by a botnet composed at least of 150000 IoT devices	2016	G.scholar
101	2	G Cluley	These 60 dumb passwords can hijack over 500,000 IoT devices into the mirai botnet	2016	G.scholar
102	2	Ki Sgouras, An Kyriakidis, ...	Short-term risk assessment of botnet attacks on advanced metering Infrastructure	2017	G.scholar
103	1	Mj Farooq, Q Zhu	Modeling, analysis, and mitigation of dynamic botnet formation in wireless IoT networks	2019	G.scholar
104	1	S Amina, R Vera, T Dargahi, ...	A bibliometric analysis of botnet detection techniques	2019	G.scholar
105	1	B Thakar, C Parekh	Reverse engineering of botnet (apt)	2017	G.scholar
106	1	L Sebastian, J Yong, I Katsuyoshi	Detection and control of dns-based botnet communications by using sdn-ryu solution	2016	G.scholar
107	1	B Krebs	Source code for IoT botnet 'mirai'released, 2016	2018	G.scholar
108	1	M Smith	IoT botnet: 25,513 cctv cameras used in crushing ddos attacks	2016	G.scholar
109	1	Mzbina Aziz, K Okamura	An analysis of botnet attack for smtp server using software define network (sdn)	2016	G.scholar
110	1	E Stalmans, B Irwin	Spatial statistics as a metric for detecting botnet c2 servers	2016	G.scholar
111	1	Tb Waghela, Kt Devi	Botnet: switching c&c servers using raspberrypi	2016	G.scholar
112	1	S Herwig, K Harvey, G Hughey, R Roberts, D Levin	Measurement and analysis of hajime, a peer-to-peer IoT botnet	2019	G.scholar
113	1	S Ryu, B Yang	A comparative study of machine learning algorithms and their ensembles for botnet detection	2018	G.scholar
114	1	D Santana, S Suthaharan, S Mohanty	What we learn from learning-understanding capabilities and limitations of machine learning in botnet attacks	2018	G.scholar
115	1	S Ding	Machine learning for cybersecurity: network-based botnet detection using time-limited flows	2017	G.scholar
116	1	E Masum, R Samet	Mobil botnet ile ddos saldırısı	2018	G.scholar
117	1	J Van Roosmalen	The feasibility of deep learning approaches for p2p-botnet detection	2017	G.scholar
118	0	M Nur, W Bin	Analysis on IoT botnet and ddos attack	2017	G.scholar
119	0	A Rezaei	Identifying botnet on IoT and cloud by using machine learning techniques	2018	G.scholar
120	0	Cd Mcdermott, Jp Isaacs, Av Petrovski	Evaluating awareness and perception of botnet activity within consumer internet-of-things (IoT) networks	2019	G.scholar
121	0	N KoronIoTis, N Moustafa, E	Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: bot-IoT dataset	2018	G.scholar

		Sitnikova, ...			
122	0	D Kennefick	Can a strictly defined security configuration for IoT devices mitigate the risk of exploitation by botnet malware?	2017	G.scholar
123	0	Ak Bediya, R Kumar	Review of security and privacy of internet of things from botnet attack: challenges and solutions	2018	G.scholar
124	0	Q Shafi, A Basit	Ddos botnet prevention using blockchain in software defined internet of things	2019	G.scholar
125	0	T Tyagi	Botnet of things: menace to internet of things	2018	G.scholar
126	0	P Wainwright, H Kettani	An analysis of botnet models	2019	G.scholar
127	0	B Nassi, M Sror, I Lavi, Y Meidan, A Shabtai, ...	Piping botnet-turning green technology into a water disaster	2018	G.scholar
128	0	R Marinho, R Holanda	Exploring a p2p transient botnet-from discovery to enumeration	2017	G.scholar
129	0	R Mckay, B Pendleton, J Britt, ...	Machine learning algorithms on botnet traffic: ensemble and simple Algorithms	2019	G.scholar
130	0	Kf Xylogiannopoulos, P Karampelas, ...	Detecting ddos attacks on multiple network hosts: advanced pattern detection method for the identification of intelligent botnet attacks	2019	G.scholar
131	0	S Baruah	Botnet detection: analysis of various techniques	2019	G.scholar
132	0	D Acarali, M Rajarajan	Botnet-based attacks and defence mechanisms	2018	G.scholar
133	0	Z Wang, M Qin, M Chen, C Jia, Y Ma	A learning evasive email-based p2p-like botnet	2018	G.scholar
134	0	M Graham	A botnet needle in a virtual haystack	2017	G.scholar
135	0	S Taheri, M Salem, Js Yuan	Leveraging image representation of network traffic data and transfer learning in botnet detection	2018	G.scholar
136	0	J Wang, Y Chen	Botnet detection method based on survival analysis	2017	G.scholar
137	0	A Muneer	A framework to mitigate propagation of IoT based botnet by patching intermediary nodes	2018	G.scholar
138	0	R Upadhyay	Chatbot platform as command & control channel in botnet	2017	G.scholar
139	0	Mc Riegel	An analysis of the mirai botnet and its impact on the future of embedded systems	2017	G.scholar
140	0	Jh Shin, Yk Cho, Sb Eun, Ys Yun, Jm Jung	Robust android botnet c&c over gtalk service	2015	G.scholar
141	0	M Riegel	Tracking mirai: an in-depth analysis of an IoT botnet	2017	G.scholar
142	0	F Ke, Z Deng, Y Zhang	… in hierarchical wireless sensor networksanalysis of dns txt record usage and consideration of botnet communication detectionnonlinear shannon …	2018	G.scholar
143	0	X Meng	An integrated networkbased mobile botnet detection system	2018	G.scholar
144	0	P Kaur, A Gupta	A study on botnet detection in cloud network	2017	G.scholar
145	0	G Kesidis, Y Shan, D Fleck, A Stavrou, ...	An adversarial coupon-collector model of asynchronous moving-target defense against botnet reconnaissance*	2018	G.scholar
146	0	Vg Siloa, B Soniva	Data stream clustering for botnet detection	2018	G.scholar
147	0	P Barthakur	Development of a real-time machine-learning based botnet detection mechanism	2016	G.scholar
148	0	Y Park, Nnv Kengalahalli, Sy Chang	Distributed security network functions against botnet attacks in software-defined networks	2019	G.scholar
149	0	P Thakur, J Rajan, M Poojari, N Jha, K Nair	Comparative analysis of botnet ids based on classification and clustering techniques	2018	G.scholar
150	0	A Georgescu	Pandora's botnet–cybercrime as a persistent systemic threat	2018	G.scholar

151	0	M Nogueira	Anticipating moves to prevent botnet generated ddos flooding Attacks	2016	G.scholar
152	0	Nq Sunaidi, Aa Ahmed	Back propagation algorithm-based intelligent model for botnet Detection	2018	G.scholar
153	0	Rc Joshi, Es Pilli	Botnet forensics	2016	G.scholar
154	0	C Ardi, J Heidemann	Leveraging controlled information sharing for botnet activity Detection	2018	G.scholar
155	0	R Perrotta, F Hao	Botnet in the browser	2018	G.scholar
156	0	Tf Fladby	Adaptive network flow parameters for stealthy botnet behavior	2018	G.scholar
157	0	Z Wang, M Tian, C Jia	An active and dynamic botnet detection approach to track hidden concept drift	2017	G.scholar
158	0	J Olorunmaiye	Hybrid intrusion detection systems adoption in cloud (iaas) platform to mitigate botnet threats	2018	G.scholar
159	0	P Vardhamane	Detecting botnet traffic using machine learning	2017	G.scholar
160	0	D Barrett, A Arora, M Gannon	Morning session 2-botnet detection and prevention	2017	G.scholar
161	0	Xg Li, Jf Wang	Traffic detection of transmission of botnet threat using bp neural Network	2018	G.scholar
162	0	R Perrotta, F Hao	Botnet in the browser: understanding threats caused by malicious browser extensions	2018	G.scholar
163	0	Ma Prado	Análise experimental da botnet IoT mirai.	2018	G.scholar
164	0	K Pucyński	Botnet detection and analysis: a tool for improving IoT security	2017	G.scholar
165	0	Y Benahmed, M Yargui, A Boukerram	Machine learning pour la détection des botnet dans les réseaux informatique.	2018	G.scholar
166	0	Nd Tai, Dn Thanh, B Duy, Nt Hieu, Nt Duong	Internet of things security: mirai botnet in-depth analysis and countermeasurements	2017	G.scholar
167	0	A Gc	Analysis of botnet classification and detection based on c&c Channel	2018	G.scholar

Systematic Analysis

These 167 articles are going to be systematically inspected to answer the following questions:

1. What are the types of the infected devices studied?
2. What are the techniques of infections (exploited and vulnerabilities)?
3. What is the population size?
4. What is C&C communication Portal used?
5. What are the Types of attacks?

Examining the previous studies for a focused approach specific to the IoT provides several new avenues of research that can be examined in the future. Given the limitations of the broad nature of this study, areas of future research could be better served by focusing on more specific categories for the Internet of Things. A deeper examination of IoT protocols and devices themselves and how are they specifically compromised, the emergence of malware on IoT devices not reliant on paired communications, and the effectiveness of security policy designed specifically for IoT devices and networks.

As the research has shown from this review IoT devices do have inherent flaws that can be compromised, but the majority of the compromises have occurred due to insecurity in communications and protocols between the IoT device and a second host providing control [16] Limited research is being identified that compromises the IoT device directly. To identify the true vulnerability of these devices, studies should move beyond the compromise through a Bluetooth channel or other form of communication and examine vulnerabilities to the device OS As IoT devices use operating systems similar to other hosts, the vulnerabilities could mirror what is currently seen by security researchers. However as many devices are running leaner, more optimized versions of OS code, their security platforms may not be as robust. This could allow for compromise from exploits that were previously believed to be mitigated by the OS version. Additionally, research could validate the potential of compromise through secured communications from a remote host. This review can also cover a wider range of devices, from emerging healthcare monitors to smart car operating systems, or electronic locks.

Malware has been and continues to be one of the largest security concerns for any device operating on the Internet. There are multiple security firms and companies that are dedicated to researching the design, function, and impacts of malware and as this study has shown, the IoT is not immune to the effects. The current trends for malware against IoT devices are currently seen attacking smart phone devices through a software store or attacking hosts that control IoT functionality.

The development and implementation of security controls and policies have progressed along an iterative process since the beginnings of the Internet. While the controls have been developed from a set of international standards to ensure communications and a baseline of security, the policies to enforce those controls have always been up to the discretion of local administrators. To date the development of security controls and policy for the Internet of Things has proven to be no different, often emerging as an addition or separate branch of current policies already in place to govern IT networks.

As the spread of IoT devices increases, and the capabilities and use cases are further developed, controls and policies should be developed to address the specific nuances of IoT networks. Smart cars and healthcare devices will require security that can protect patients and vehicles while operating at speeds that cannot afford the reduced latency that packet inspection firewalls could introduce. Communications need to be secure to prevent interception and change, but without the processing overhead that could be required from current encryption standards. The policies in place currently for defense in depth work well for IT networks, but as the IoT develops further into mesh networks, how can policy address a protocol that is not secured or a lone device that does not nest easily inside of a security perimeter.

CONCLUSION

In this work, we used bibliometric analysis to examine botnet detection techniques during the period from 2014 to April 2019, which allowed us to expose global tendencies related to bibliography production of botnet detection techniques. In this investigation, we offered additional five (5) systematic analysis criteria including types of the infected devices studied, the techniques of infections (exploited and vulnerabilities), the population size, C&C communication Portal used, and Types of attacks.

REFERENCES

[1] MalwareMustDie. (2016). MMD-0056-2016 - Linux/Mirai, how an old ELF malcode is recycled.

[2] Krebs, B. (2016). New Mirai worm knocks 900k Germans offline. *Krebs on Security*. KrebsOnSecurity. (2016). KrebsOnSecurity Hit with Record DDoS.

[3] Goodin, D. (2016). Record-breaking DDoS reportedly delivered by> 145k hacked cameras. *Ars Technica*, *28*.

[4] Cimpanu, C. (2016). You Can Now Rent a Mirai Botnet of 400,000 Bots. *BleepingComputer. com*, *24*.

[5] Williams, C. (2016). Today the Web Was Broken by Countless Hacked Devices—Your 60-Second Summary. *The Register*, *21*.

[6] Angrishi, K. (2017). Turning internet of things (IoT) into internet of vulnerabilities (iov): IoT botnets.*arXiv preprint arXiv:1702.03681*.

[7] Bertino, E., & Islam, N. (2017). Botnets and internet of things security. *Computer*(2), 76-79.

[8] Herzberg, B., Bekerman, D., & Zeifman, I. (2016). Breaking down mirai: An IoT DDoS botnet analysis. *Incapsula Blog, Bots and DDoS, Security*.

[9] Silva, S. S., Silva, R. M., Pinto, R. C., & Salles, R. M. (2013). Botnets: A survey. *Computer Networks*, *57*(2), 378-403.

[10] Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets.*Computer*, *50*(7), 80-84.

[11] D. Bekerman, ”. (2017). New Mirai Variant Launches 54 Hour DDoS Attack against US College. Gamblin, J. (2016). Mirai-Source-Code. In: GitHub.

[12] McMillen, D., & Alvarez, M. (2017). Mirai IoT Botnet: Mining for Bitcoins. *SecurityIntelligence (April 2017)*.

[13] Yeh, T., Chiu, D., & Lu, K. (2017). Persirai: New Internet of Things (IoT) Botnet Targets IP Cameras.*blog*, *Trend-Labs*, *9*.

[14] Moher D, Liberati A, Tetzlaff J, Altman DG, The PRISMA Group (2009) Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. PLoS Med 6(7): e1000097. https://doi.org/10.1371/journal.pmed.1000097

[15] Pickering,C.M.andByrne,J.(2013- online).The benefits of publishing systematic quantitative literature reviews for PhD candidates and other earlycareer researchers.Higher Education Research and Development.http://dx.doi.org/10.1080/07294360.2013.841651

[16] Chen, T., & Abu-Nimah, S. (2011, April). Lessons from Stuxnet. IEEE Computer Society, 91-93. Retrieved from IEEE : http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5742014&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5742014