Peer-to-Peer Networking and Applications (2023) 16:1380–1431
https://doi.org/10.1007/s12083-023-01478-w

IoT malware: An attribute-based taxonomy, detection mechanisms and challenges

Princy Victor[1] · Arash Habibi Lashkari[2] · Rongxing Lu[1] · Tinshu Sasi[1] · Pulei Xiong[3] · Shahrear Iqbal[4]

Received: 24 November 2022 / Accepted: 10 March 2023 / Published online: 10 May 2023

Abstract

During the past decade, the Internet of Things (IoT) has paved the way for the ongoing digitization of society in unique ways. Its penetration into enterprise and day-to-day lives improved the supply chain in numerous ways. Unfortunately, the profuse diversity of IoT devices has become an attractive target for malware authors who take advantage of its vulnerabilities. Accordingly, enhancing the security of IoT devices has become the primary objective of industrialists and researchers. However, most present studies lack a deep understanding of IoT malware and its various aspects. As understanding IoT malware is the preliminary base of research, in this work, we present an IoT malware taxonomy with 100 attributes based on the IoT malware categories, attack types, attack surfaces, malware distribution architecture, victim devices, victim device architecture, IoT malware characteristics, access mechanisms, programming languages, and protocols. In addition, we have mapped these categories into 77 IoT Malwares identified between 2008 and 2022. Furthermore, To provide insight into the challenges in IoT malware research for future researchers, our study also reviews the existing IoT malware detection works.

Keywords Internet of Things · Malware · Taxonomy · Challenges of malware detection methods

1 Introduction

Internet-of-Things (IoT) refers to an extensive network of smart interconnected devices such as home appliances, sensors, and actuators that transfer data without human intervention [1]. Over the years, Internet of Things (IoT) devices have expanded drastically, hovering at 27 billion by 2025. According to IoT analytic experts, devices are growing at a rate of 9% despite Covid-19's influence on the supply chain [2]. However, the rapid growth of IoT and its lack of security mechanisms make them a valuable target for attackers, including malware authors.

As the nefarious activities in IoT devices are surging, researchers, industrialists, and security personnel are concerned about consumers' security. According to ZScaler telemetry reports, the IoT malware attacks during the Covid-19 pandemic have increased dramatically, [3], and the malware modifications have been raised by three-fold compared to that during 2018. These IoT devices, ranging from smartphones to underwater sensors [4], are vulnerable to several privacy and security issues. Among the different attacks, the most famous one is the Mirai attack that ensued in 2016 [5], where the malware authors launched a DDoS attack, which brought down Brian Krebs' website and famous Domain

✉ Rongxing Lu
rlu1@unb.ca

Princy Victor
pvictor@unb.ca

Arash Habibi Lashkari
ahabibil@yorku.ca

Tinshu Sasi
tsasi@unb.ca

Pulei Xiong
pulei.xiong@nrc-cnrc.gc.ca

Shahrear Iqbal
shahrear.iqbal@nrc-cnrc.gc.ca

[1] Faculty of Computer Science, University of New Brunswick, Fredericton NB E3B 5A3, Canada

[2] School of Information Technology, York University, Toronto ON M3J 1P3, Canada

[3] National Research Council Canada, Ottawa ON K1A 0R6, Canada

[4] National Research Council Canada, Fredericton NB E3B 9W4, Canada

service provider Dyn. After the attack, the authors published the malware source code, which paved the way for creating diverse malware like Okiru, Satori, etc.

In 2015, Hewlett Packard conducted a study on IoT devices and identified that 90% of the devices capture at least one personal information, 80% display privacy issues, and 70% exhibit vulnerable user interfaces. Besides, they also realized the main reasons as the absence of transport encryption, inadequate authorization and authentication, insecure software, web interface, and firmware [6]. The hazards due to these devices affect the IoT system security and the whole network, servers, websites, social networks, and applications. This risk of a single component that ultimately affects the networking system [7] results in the new acronym of IoT as the Internet of Troubles rather than the Internet of Things [8]. Under these circumstances, even though the manufacturers considered security the primary objective before developing an IoT device, increasing production costs made them feel security was insignificant.

Security practices for IoT devices include protection by developing secure devices or techniques to detect and prevent IoT malwares. Many researchers in enterprises and academia focused on IoT security by considering these aspects and preventing the devices from threats. However, most of the current works focus on machine learning-based or deep learning-based detection algorithms [1, 9, 10] rather than understanding the IoT malware that builds such an extensive network of infected devices. Consequently, reviews are required to analyze existing research conducted on the topic. Meanwhile, some works like [11–15] discussed IoT malware, their different attacks, features and so on.

As a plethora of IoT malware is available, its expeditious evolution and mismatched explanations in different sources make the studies on IoT security more complex. Furthermore, it is interesting that the malware once used for personal computers is also advancing, affecting IoT devices. One example is Emotet which improved their Trojan and compromised IoT devices [16]. Similarly, ransomware-categorized malware, once prevalent in mobile devices, has already compromised IoT devices [17]. This highlights a real need to face the IoT security issue seriously. Moreover, we believe that the scarcity of an organized and in-depth study obstructs the malware prevention and protection of the devices. Because of this, extensive research is needed in IoT malware that considers both technical aspects and existing solutions to solve security issues.

Considering the above facts, 100 attributes of IoT malware based on IoT malware categories, attack types, attack surfaces, malware distribution architectures, victim devices, victim device architectures, characteristics, access mechanisms, programming languages, and protocols are discussed in this paper. As each malware behaves differently, the attributes selected in the study help in analyzing the overall aspect of each IoT malware family. Overall, the selected attributes offer a panoramic view of IoT malware that can create possibilities for a robust defensive and preventive solution.

As attributes alone cannot help in a deeper understanding, a mapping was also needed so that each malware could be studied extensively. Hence, 77 IoT malware families that appeared between 2008 and 2022 are identified from different sources and mapped to these attributes. Interestingly, it was recognized that most of the attributes are not family-specific and can be exhibited in other families as well. This might be due to the release of novel malware by enhancing publicly available malware source codes. The main objective of the mapping was to help future research in this field, especially attribute-specific or family-specific studies.

To get a complete picture of IoT malware, existing detection mechanisms need to be studied by focusing on their challenges. Therefore, we have reviewed the various IoT malware detection articles and categorized them based on traditional and learning-based detection algorithms. Moreover, we were able to identify the 12 challenges in IoT malware research, which can help create novel detection methods. Furthermore, each challenge was then concluded with the future scope so that researchers could focus on the keywords provided for attaining the same. To the best of our knowledge, this is the foremost study that comprehensively investigates IoT malwares, illustrates a taxonomy, and studies the existing IoT malware detection mechanisms.

Overall, the contributions of the paper include the following:

- A comprehensive taxonomy of IoT malwares with 100 attributes based on IoT malware categories, attack types, attack surfaces, malware distribution architecture, victim devices, victim device architecture, characteristics, access mechanisms, programming languages, and protocols.
- A detailed analysis of 77 IoT malwares between 2008 and 2022 based on the abovementioned categories.
- A study on works related to IoT malware case studies, surveys, and detection methods.
- Presents the existing challenges and future research scopes in IoT malware.

The overall objective of the paper is to offer a comprehensive reference to the IoT research community for understanding the growth of IoT malwares and its consequences. The remainder of the paper is structured as follows. Section 2 gives the background of IoT malware, and Section 3 describes the methodology used for writing this paper. Section 4 discusses the related taxonomies from past studies, and Section 5 presents the IoT malware categories and their attributes. In Section 6 we discuss 77 IoT Malwares identified between 2008 and 2022, and Section 7 deals with the detection methods. Finally, Section 8 discusses the research challenges, conclusion, and future work in Section 9.

2 Background of IoT malware

This section addresses the background of IoT malware in a lucid manner. Malware is malicious software created for exploiting or attacking the devices, either into their hardware or software [18]. There are different categories for malware, such as Virus, Trojan, Rootkit, Backdoor, etc. During the 1980s, the malware was just file infectors or boot sectors that were transferred through floppy disks inserted into the system [19]. However, as the devices and technologies became more standardized, malware has been advanced to attack those devices. One such new technology being exploited by malware is IoT, which is a group of devices connected to the Internet without human intervention [20, 21]. Unlike traditional malware, IoT malware scans the Internet for vulnerable devices and hosts their initial payload, which is a stager script, in the devices for downloading the architecture-specific binary sample. Once it is downloaded, the script executes the sample, which communicates with the C&C server. Some scanner modules exist in the binary, so it infects more devices by distributing the sample. Most malware like Gamut, Necurs, and Skeeyah that used to attack Personal computers started attacking IoT devices by advancing their capabilities. Following are some of the common IoT vulnerabilities which make IoT devices attracted towards malware authors [22]:

1. *Weak/default passwords*: Lack of robust password recovery mechanism; Weak or default password; Lack of enforcement of stronger password rules; Inability to modify the default username and password.
2. *Poor security awareness in users*: Lack of granular permissions models in IoT devices, collection of excessive user data, and inability to distinguish administrators from users.
3. *Lack of Encryption*: Transmission of unencrypted data and credentials; Lack of integrity verification.
4. *Firmware issues*: Hardcoded credentials; files uploaded are not encrypted or verified.
5. *Missing updates*: Lack of software and security update mechanisms.
6. *Insecure network*: Connecting devices over insecure public networks; No login or screening mechanism to log in to the network; networks with weak/no password policies.

Among all these shortcomings, weak/default passwords are identified to be the primary reason for the attacks on IoT devices. To access the device easily, users skip changing the passwords or update poor passwords that Brute Force attacks can crack. Once the device is accessed, the attackers perform further infection based on their objective. Even though IoT malware is used for different attacks, it is mainly used for DDoS attacks, making the resources unavailable for the users. However, the malware attacks can be prevented by specific mechanisms, including [23]:

1. *Anti-virus and Anti-spyware software*: Installing and routinely updating your security software and any virus being uncovered must be removed immediately. Files should be examined for errors, missing data, and illegal/authorized changes.
2. *Secure Authentication*: Securing IoT devices with Multi-Factor Authentication mechanism (MFA).
3. *Least privilege principle*: Give users the bare minimum of system features, services, and information needed to do their tasks.
4. *Email and Spam Filtering*: Putting spam and email security procedures in place, every receiving email should have its attachments checked for malwares. Spam filter rules should be applied to reduce unwanted emails, and users should be blocked from accessing unauthorized emails, links and messages.
5. *File exchanging or downloading*: Files should be exchanged or downloaded from trusted sources/websites only.

3 Methodology

This section presents the methodology of selecting relevant articles, different data sources, search criteria, research questions, taxonomy creation, and the scope of this work. In this paper, we have proposed a taxonomy, and it is developed based on the study of a vast amount of research articles and resources on IoT malware. To have meaningful research, we limited the scope of the paper to the last five years, with most of the papers selected from various databases, including IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, and Google Scholar. On each database, search keywords like “IoT malware”, “Mirai”, “Smart Home attack”, “IoT attack”, “IoT malware detection”, “IoT malware survey”, “IoT malware machine learning”, and “IoT malware review” were considered which led to finding relevant papers. Moreover, we have included a backward approach for finding new articles and identifying new ones based on the list of references in the article under study. Furthermore, we narrowed the analysis by considering the following questions:

1. What is the current research state of IoT malware as new attacks are emerging daily?

2. What are the different aspects of IoT malware?
3. Which techniques are used to perform IoT malware detection?
4. How can the research gaps identified in the existing IoT malware detection studies be filled?

All articles on Automotive IoT were excluded, including IoT malware papers from non-English journals or conferences.

Following the abovementioned criteria, we have selected articles and identified different aspects of IoT malware. On identifying each attribute, we briefly described one or two related works on that attribute. These associated works are considered from online resources like Medium, Bleeping computer, Malwarebytes, etc.

4 Related works

Although numerous surveys were conducted on IoT Malware, there is no single complete literature on IoT malware taxonomy. Therefore, we are proposing a new taxonomy in this section presents the works that analyze the existing taxonomies. A comparison of the current works with our proposed work is shown in Table 1.

In [11], a taxonomy of IoT malware DDoS attacks is discussed based on literature from 2008. This taxonomy classifies DDoS attacks into subcategories based on architecture model, exploited vulnerabilities, protocol level, degree of automation, scanning strategy, propagation mechanism, impact on the victim, attack rate, source address validity, attack traffic distribution, resources involved, victim type. Moreover, this work compares malware based on characteristics such as source code, agent CPU, architecture model, and attacks. This work also explains different DDoS attack phases: recruitment, exploitation, infection, communication, and the attack.

The taxonomy [12] considers the IoT and IIoT environments along with their vulnerabilities, attack vectors, and eight different IoT malware families. Moreover, the taxonomy of DDoS attacks introduced in the work was from [24], and vulnerabilities were from the top 10 OWASP threats.

Shobana and Rathi [13] discusses the nine most widespread IoT malware between 2013 and 2017 and the IoT environment's vulnerable points. This work explains the IoT malware and the comparison based on the target devices, architecture, attack, number of devices, communication protocol, and language. Based on the study, the authors identified the most attacked devices, architectures, communication protocols, etc.

The work [14] investigates the evolution of the 16 most widespread IoT malware between 2008 and 2018 by comparing various characteristic features such as DoS capabilities, Data Stealing, Endpoint Exploit, Industrial Spying, Exploit, Target Architecture, Scanning methods, Botnet architecture, Anti-detection Features, Efficiency Enhancing Features, DGA Algorithm, Code Modularity, Victim Scan, Virtualization Evasion, and Crypto Mining. Besides, this work considers a phylogenic malware classification and a feature propagation multi-graph that depicts how each malware influenced the successors and how the feature spreads in the malware pool. The authors identify the challenges IoT devices face and their solutions through this work.

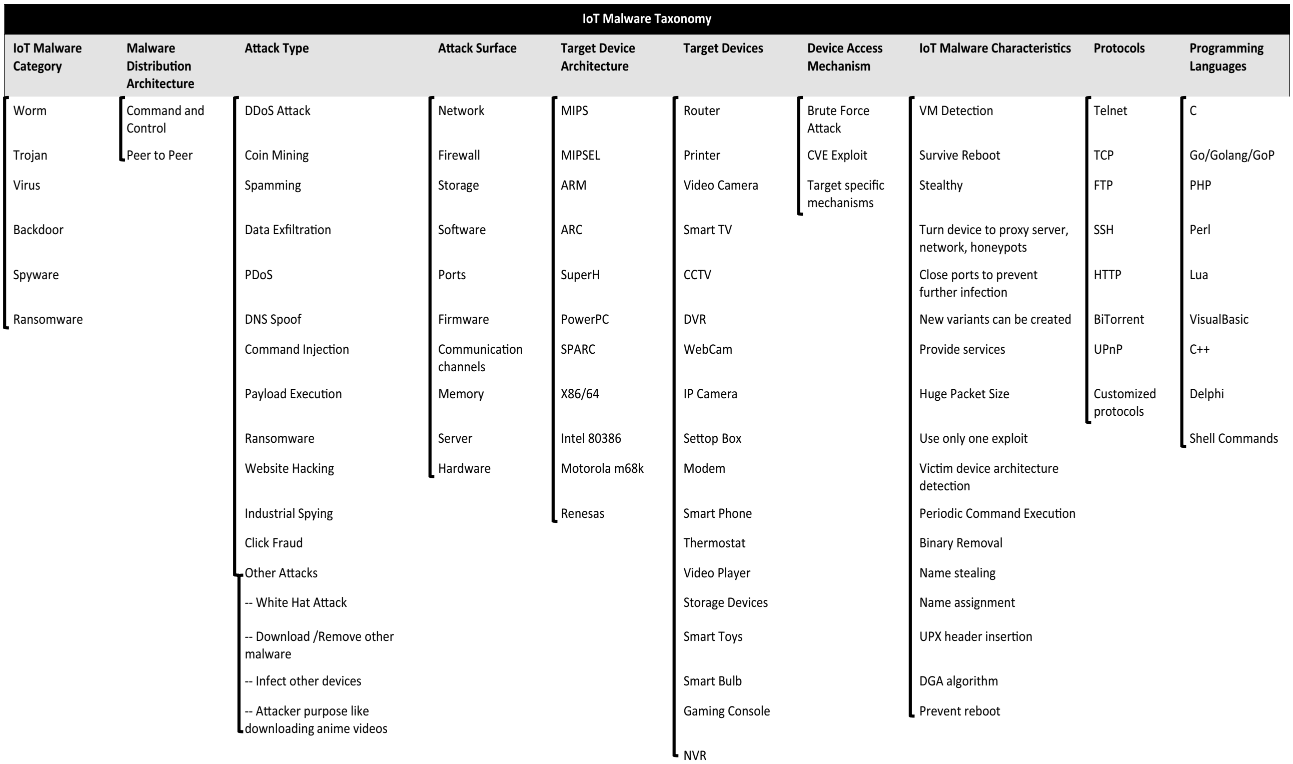
In their next work [15], 28 IoT malware from 2008 to 2019 is considered in taxonomy with 77 taxa. Besides that, the authors could predict the future evolution of IoT botnets using their simulation tool.

5 IoT malware categories and families

This section discusses a new taxonomy with 100 attributes based on IoT malware categories, attack types, attack surfaces, malware distribution architecture, victim devices,

Table 1 Comparison with existing works

Year	Title	# Malware discussed	# Attributes	Taxonomy	Malware Mapping	Detection methods	Challenges in Detection methods
2017	Analysis of ddos-capable IoT malwares [11]	13	45	Yes	Yes	No	Yes
2017	IoDDoS-the internet of distributed denial of sevice attacks [12]	8	4	Yes	No	No	Yes
2018	IoT malware: An analysis of IoT device hijacking [13]	9	39	No	Yes	No	Yes
2019	10 years of IoT malware: A feature-based taxonomy [14]	16	46	Yes	Yes	No	Yes
2021	The evolution of IoT malwares, from 2008 to 2019: Survey, taxonomy, process simulator and perspectives [15]	28	77	Yes	Yes	No	Yes
––	Proposed survey	77	100	Yes	Yes	Yes	Yes



IoT Malware Taxonomy									
IoT Malware Category	Malware Distribution Architecture	Attack Type	Attack Surface	Target Device Architecture	Target Devices	Device Access Mechanism	IoT Malware Characteristics	Protocols	Programming Languages
Worm	Command and Control	DDoS Attack	Network	MIPS	Router	Brute Force Attack	VM Detection	Telnet	C
Trojan	Peer to Peer	Coin Mining	Firewall	MIPSEL	Printer	CVE Exploit	Survive Reboot	TCP	Go/Golang/GoP
Virus		Spamming	Storage	ARM	Video Camera	Target specific mechanisms	Stealthy	FTP	PHP
Backdoor		Data Exfiltration	Software	ARC	Smart TV		Turn device to proxy server, network, honeypots	SSH	Perl
Spyware		PDoS	Ports	SuperH	CCTV		Close ports to prevent further infection	HTTP	Lua
Ransomware		DNS Spoof	Firmware	PowerPC	DVR		New variants can be created	BiTorrent	VisualBasic
		Command Injection	Communication channels	SPARC	WebCam		Provide services	UPnP	C++
		Payload Execution	Memory	X86/64	IP Camera		Huge Packet Size	Customized protocols	Delphi
		Ransomware	Server	Intel 80386	Settop Box		Use only one exploit		Shell Commands
		Website Hacking	Hardware	Motorola m68k	Modem		Victim device architecture detection		
		Industrial Spying		Renesas	Smart Phone		Periodic Command Execution		
		Click Fraud			Thermostat		Binary Removal		
		Other Attacks			Video Player		Name stealing		
		-- White Hat Attack			Storage Devices		Name assignment		
		-- Download /Remove other malware			Smart Toys		UPX header insertion		
		-- Infect other devices			Smart Bulb		DGA algorithm		
		-- Attacker purpose like downloading anime videos			Gaming Console		Prevent reboot		
					NVR				

Fig. 1 IoT Malware Taxonomy

victim device architecture, characteristics, access mechanisms, programming languages, and protocols., as shown in Fig. 1. Furthermore, this work better understands 77 IoT malware families between 2008 and 2022 by mapping them to each taxon based on the information gathered from various reliable sources.

Table 2 summarizes the references used to create different attributes in the proposed taxonomy.

5.1 Categories

Over the years, malware has evolved in functionality complexity and caused a significant impact on nearly all devices. Various malware categories exist based on their functionality, like Worms, Trojans, Viruses, Spyware, Ransomware, Rootkits, and backdoors. The exciting fact about IoT malware is that even though they belong to different categories,

Table 2 IoT Malware Taxonomy Summary

Attribute Category	Academic Source	Other references
IoT Malware Category	[26, 27, 29, 31, 33–35, 37, 38]	[25, 28, 30, 32, 36]
IoT Botnet Architecture	[11, 13–15, 39–41]	[42]
Attack Type	[11, 13–15, 22, 43–57]	[14, 14, 26, 36, 58, 59, 59–67, 67–84]
Attack Surface	[11, 13–15, 49, 50, 85–92]	[25, 76, 93–98]
Target Device Architectures	[1, 1, 1, 11, 13–15, 99, 100, 100–102]	[103–112]
Target Devices	[11, 13–15, 34, 37, 46, 48, 92, 113]	[114–118]
Device Access Mechanisms	[11, 13–15, 45, 92, 119, 120]	[14, 59, 121–126]
Characteristics	[11, 13–15, 15, 26, 27, 31, 127, 128]	[14, 129–139]
Port/Protocols	[11, 13–15, 26, 27, 91]	[140–142, 142–145, 145, 146, 146–156]
Programming Language	[11, 13]	[157–164]

the nature of all malware is bot-based, which uses botnet as a technique for malware distribution, execution, command, and control. This section explains the IoT malware categories based on their functionality.

1. *Worm*: This category of IoT malware spreads and propagates itself in IoT devices in an automated fashion. Due to this propagation method, Juniper Threat [25] considers the worm as an annoying malware. Mirai, Darlloz, Brickerbot, and Gitpaste-12 are some of the worms in IoT devices. However, some situations exist where certain malware is better for the systems.

   One such IoT malware is Hajime which acts as a white-hat malware that secures the devices from other IoT malware. Various IoT malware analysis works were also conducted to identify these types of malware behaviour. One such work is done by [26] in which a lifespan is introduced to the Hajime worm using the PN^2 method. The outcome of the work proved that the model is a safe mitigation technique that reduces the infection ratio of Mirai. Similarly, using several existing artefacts, forensic analysis is done on the Mirai botnet server in [27]. The work uses various tools, including LiME, Volatility, DD8.3, Autopsy, WireShark, Bulk Extractor, and Ghidra.
2. *Trojan*: A Trojan, also known as Trojan Horse or Trojan Virus, is another IoT malware category where the malware appears benign to the users even though it has a hidden malicious functionality [28]. Indeed, the functionality of Virus and Trojan is entirely different as the Trojan cannot replicate itself, and the Virus can replicate [28]. An IoT malware, ProxyM, is a Trojan that performs email spamming in addition to DDoS attacks.

   [29] discusses Trojan malware and various types of attacks and vulnerabilities in IoT. Moreover, the challenges in IoT are also presented following Confidentiality, Integrity, and Availability.
3. *Virus*: Although the Virus is a common term in computer science, the Virus in IoT devices seems confusing. IoT virus works similarly to the normal virus category except that IoT virus attacks IoT devices by self-replicating malicious programs [30]. Due to this reason, the Virus is hard to clean, and it attacks the device in a complex way. For example, Silex is an IoT virus that logs into the device and attacks it by bricking it, also known as a Permanent DoS attack.

   Various toolchains exist to create this IoT malware for architectures like ARC, ARM, MIPS, PowerPC, etc. Work was done by [31] for identifying the toolchains used for IoT malware like Silex, Tsunami, Mirai, Gafgyt, etc. For each toolchain available on the web, the authors have generated patterns of library functions and identified the library functions in the IoT malware by pattern matching using YARA. Based on the results, the authors could identify that each IoT malware sample used in the study was built using 13 building tools available on the web. Moreover, it was revealed that most of the samples used Firmware Linux 0.9.6 toolchain because of the description given in the Mirai installation guide.
4. *Spyware*: The IoT malware category Spyware permits the attackers to eavesdrop or spy the data on a target using the infected device [32]. Spybot, Skeeyah, and HNS are some IoT malware that spy on users. As IoT devices' usage increases, attacks caused by this malware are rising drastically.

   A spyware category Context-Aware Adaptation-based Spyware, SpyCon, was introduced in [33] where the daily behaviour of users is tracked from Smart Home and mobile phones. Integrating this spyware identified that it can spy on various human behaviours, including average home-to-work commuting time, working hours, and weekend behaviour, with an accuracy of 90.3%. As system behaviour and code signature-based, traditional detection approaches could not detect Spycon; an information-based detection engine was also proposed.
5. *Ransomware*: IoT Ransomware is a malware category that holds the IoT devices and demands a ransom from the victim to exchange the device [30]. Once the device is infected, the attacker encrypts the files and restricts the user from accessing them. After getting the ransom, the attacker gives the decryption key and releases the device. Necurs is an IoT malware that launches a ransomware attack and various other digital extortions.

   Various Ransomware attacks in IoT, including Frantic Locker, attacks on Thermostats, Smart TVs, and Smart Bulb, were presented in [34] along with their methodologies and preventive solutions. Furthermore, the authors delivered the frightening hazards that can occur due to Ransomware with the help of some real-life examples. However, the work could not cover the IoT malware families responsible for these attacks. Unlike other works, a descriptive survey was done in [35] where the homeowners with IoT experience were interviewed and given questionnaires to find the security threats, including Ransomware in IoT. Nevertheless, an in-depth analysis was not performed to identify the challenges.
6. *Backdoor*: Backdoor, an IoT malware category, is a type of malware where manufacturers make several hidden access mechanisms [30]. Although these mechanisms make the customer fulfil requirements, these pave the way for making the device poor in security aspects. As a result, backdoors are also known as the front door of attackers [36]. Tsunami and Bashlite are backdoor IoT malware with a few resources that address them as Trojans.

   The work [37] gave an overview of backdoors in IoT and discussed different types of attacks, including simple attacks, complicated attacks, IoT-initiated attacks, internal attacks, and accomplice attacks that can occur in IoT devices. Moreover, the work introduced an IoT-enabled network infrastructure that monitors incoming and outgoing packets in IoT devices and matches the pre-defined pattern for finding attacks. As part of this work, backdoor scripts were used on Raspberry Pi devices. However, the work is not applicable for unordered packet patterns and exhibits an overfitting problem when considering actual IoT attacks like session hijacking.

A work [38] investigated a smart controller and a smart meter to identify their security vulnerabilities and promote the creation of IoT security methods that are less expensive. The study found that these devices can be attacked even with simple backdoors and could lead to hijacking functionality, damaging property, deploying rogue services, disrupting operations, and so on.

5.2 Malware distribution architecture

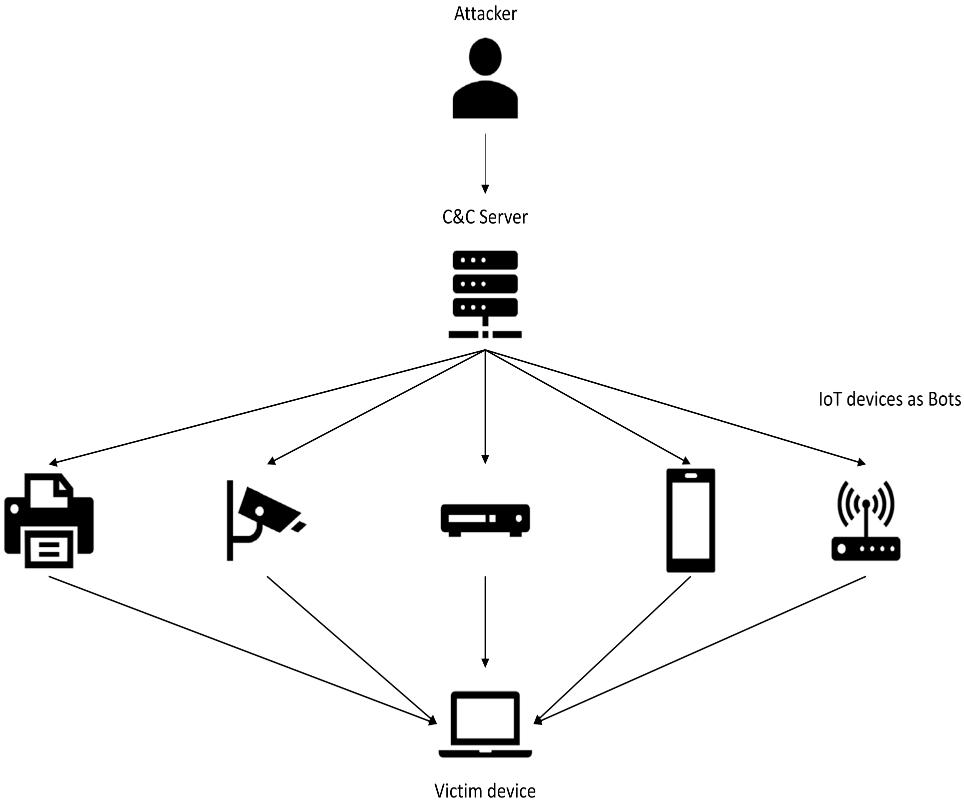
As mentioned in the section 5.1, all IoT malware categories can use infected devices within the botnet to propagate malware further to uninfected devices. The attributes in this section discuss the most commonly used two kinds of architectures used for malware distribution.

1. *Command and Control*: Command-and-Control (C&C) is a centralized architecture that sends commands to the bots using various communication protocols, including Internet Relay Chat or Hypertext Transfer Protocol. This is the broadly used botnet architecture due to its simplicity. Nevertheless, it is easy to remove the server when discovered as it has a centralized server [42] as shown in Fig. 2. Mirai, Aidra, and Okane are some IoT Malware with C&C architecture.

   Malware authors use several techniques to avoid the tracking of the C&C server. One such method, fast-flux, is discussed in [39], where the botnet uses various IP addresses and domain names to hide the C&C server. In this work, botnet domain name characteristics are analyzed and detected to filter out the same and stop communication. To achieve this, the Rustock botnet, which uses a.cn top-level domain server, was studied, and the log data from the server was collected. Moreover, 32 botnet domain name features, such as Meaningful length ratio, queries per recursive server, queries per hour, etc., were estimated for the malicious domain name detection model. However, the model considers a small imbalanced dataset and is considered in future work.

   A Threshold Random Walk (TRW) based IoT botnet detection approach, ConnSpoiler, is proposed in [41] by investigating the random NXDOMAINs generated by the DGA(Domain Generation Algorithm) schemes. In

Fig. 2 C&C Botnet Architecture



this model, a finite-state machine is used to handle the system by identifying the malicious attempts and alerting the system, which prevents the device's connection to C&C. Moreover, as it needs fewer system resources, this is well-suited for resource-constrained IoT devices. Unlike other works, in this model, real-world DNS traffic is collected from two large ISPs, and results proved that the proposed model could detect the unknown IoT botnets that create domains never reported earlier.

2. *Peer to Peer*: Peer-to-Peer (P2P) architecture is a decentralized architecture that considers each bot as both server and client [42] as shown in Fig. 3. Due to this characteristic, unlike C&C architecture, it is hard to take down the network. However, it is not widely used. Hajime, a worm, is one IoT malware that follows P2P architecture.

   A work [40] also briefly discusses the advantages of P2P architecture over C&C architecture. Moreover, the phases of the product development life cycle CRIME are explained by giving a lucid explanation of Conception, Recruiting, Interaction, Marketing, and Execution. In addition to that, different botnet models, including Epidemiological Models, Machine Learning Models, Stochastic Models, Game Theory Models, Non-parametric Bayesian Models, Graph Models, and Economic Models, are also studied in this work. However, the paper did not deal with the simulations and presented the same as future work to compare the effectiveness.

Table 3 Comparison on C&C and P2P Architecture

C&C Architecture	P2P Architecture
Easy to take down once discovered	Hard to take down
Must contain the list of all bots in the network	Contains the list of neighboring peers only
Easy to discover malicious traffic due to the unusual traffic size	Hard to distinguish malicious and legitimate traffic

A comparison of C&C and P2P Architecture is illustrated in Table 3, and mapping of IoT malware to the architecture is depicted in Table 4.

5.3 Attack types

Attributes under attack types discuss the various ways in which the IoT malware attacks IoT devices.

1. *DDoS Attack (A1)*: DDoS is an attack where the attacker prevents the users from accessing the resources by making them unavailable [68]. DDoS

Fig. 3 P2P Botnet Architecture

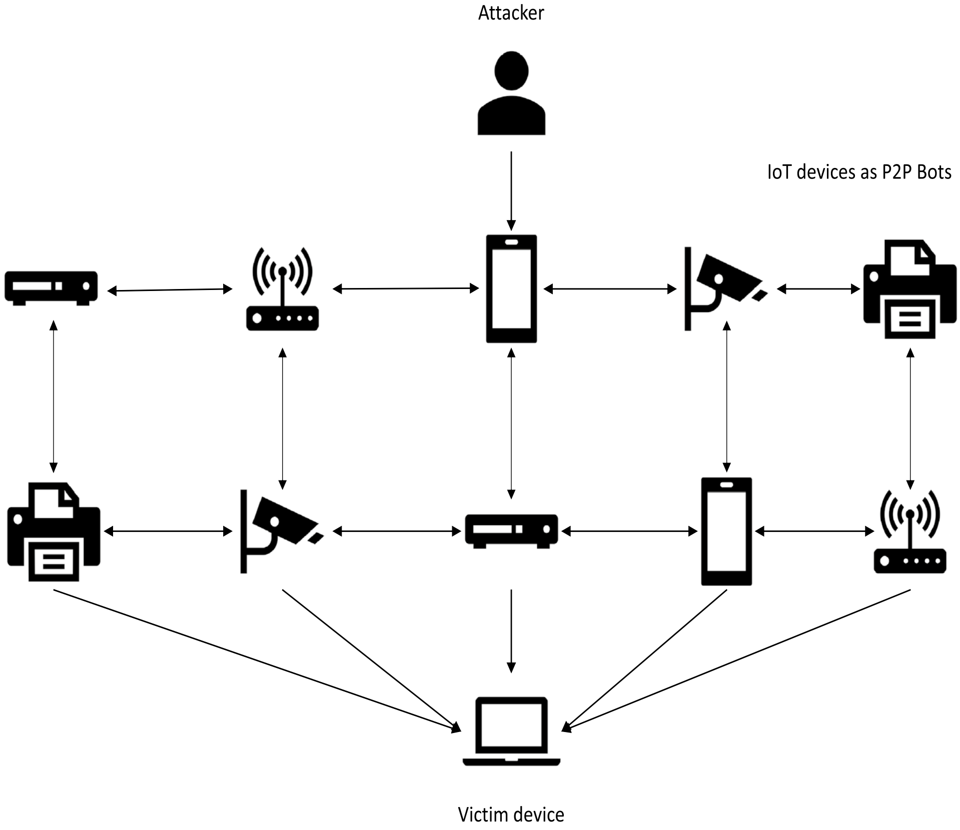


Table 4 Malware Distribution Architecture

Category	Malware	Year	Architecture	
			C&C	P2P
Worm	Mirai	2016	X	
	Hajime	2016		X
	Aidra	2012	X	
	Darlloz/Zollard	2013	X	
	Satori	2017	X	
	Sefa	2018	X	
	Okane	2018	X	
	Okiru	2018	X	
	ZHtrap	2021	X	
	Persirai	2017	X	
	Gitpaste-12	2020	X	
	Moose	2015	X	
	Shishiga	2017	X	
	Mozi	2019		X
	Carna	2012	X	
	Echobot	2019	X	
	Wicked	2018	X	
	Masuta	2018	X	
	Tori	2018	X	
	Bushido	2018	X	
	JenX	2018	X	
	Miori	2018	X	
	Sora	2018	X	
	Omni	2018	X	
	Fritzfrog	2020		X
	TheMoon	2014	X	
	Yowai	2019	X	
	OMG	2018	X	
	Owari	2018	X	
	Ouija	2017	X	
Spyware	VPNFilter	2018	X	
	Psybot	2009	X	
	Gamut	2013	X	
	Hide and Seek	2018		X
	Xarcen/XORDDoS	2015	X	
	Spybot	2005	X	
	Skeeyah	2015	X	
Ransomware	Necurs	2016		X
	Cr1ptT0r	2019	X	
	Hades	2020	X	
	Razor	2019	X	
	Lulz	2017	X	
	Muhstik	2017	X	
Backdoor	Bashlite	2014	X	
	Kaiji	2020	X	
	Tsunami	2010	X	
	IRCflu	2020	X	
	Brickerbot	2017	X	
	IoTReaper/IoTroop	2017	X	
	Elknot/BillGates/Mayday	2015	X	
	Gr1n	2017	X	
	Setag	2014	X	
	Karu	2019	X	
	InterPlanetaryStorm	2020		X
Trojan	Blueborne	2017	X	
	ProxyM	2017	X	
	Luabot	2016	X	
	Emotet	2014	X	
	AirDropBot/Cloudbot	2019	X	
	Leet	2016	X	
	Pnscan	2016	X	
	dark_nexus	2020	X	
	Hydra	2008	X	
	Demonbot	2018	X	
	APEP	2018	X	
	Ares	2019	X	
	Kluh	2015	X	
	Qbot	2008	X	
Virus	Silex	2019	X	
	Amnesia	2017	X	
	Wifatch	2014		X
	Joker	2017	X	
	Cereal	2012	X	
	HEH	2020		X

attacks in IoT devices have rapidly increased in the past few years, putting the IoT world in a hazardous situation. Due to this reason, it is one of the top attacks caused by IoT malware. Even though this attack can occur from multiple categories of IoT Malware, the worm is the most widely used category. According to [83], Mirai, which belongs to the Worm category, and Kaiji [60], which belongs to the Backdoor category, are some of the IoT malware that performs DDoS attacks.

IoT DDoS attack is clearly explained in [51] by mentioning the IoT device vulnerabilities, protocols, and the working of the attack in each layer. In addition, malware, including Mirai, Reaper, and Torii, that causes DDoS attacks on IoT devices are also discussed, along with different detection methods. [49] presents an IoT DoS and DDoS attacks detection method by converting network traffic data into an image using OpenCV, from which the patterns are identified using a residual network model ResNet. Results proved that the model achieved 87% accuracy, more than the state-of-the-art methods. Another machine learning-based DDoS attack detection model is introduced in [47] that consists of three layers of defence; the first defence layer prevents the access of blacklisted devices by authenticating ZigBee and Bluetooth devices. The second defence layer detects the DDoS attack using a decision tree in preprocessed data, and the third defence layer is where the blacklisted devices are prevented from access.

2. *Coin Mining (A2)*: Coin mining attacks mine various types of cryptocurrencies such as XMR, bitcoins, and dogecoins by hijacking IoT devices [73]. As some of the existing IoT malware evolves with new features, coin mining is an evolving threat not limited to any particular coin. Fritzfrog [65], Satori, and Sefa from the Worm category, and Dofloo and Ayedz from the Backdoor category are some of the IoT malware performs coin mining in IoT devices.

   Coin mining is also discussed in [55], which presents a hybrid IoT honeypot, IoTCMal, that records 8 IoT malware families of 11 infection patterns with different capabilities for DDoS and coin mining attacks. On successful implementation, 8 IoT malware families are captured with 11 infection patterns and named each pattern according to the character strings in the samples. The malicious samples were captured using two components, and corresponding logs and patterns were recorded. Likewise, another article [22] also discusses the DDoS and coin mining attacks in IoT devices in addition to the vulnerabilities, security measures, and different aspects of IoT botnets.

3. *Spamming (A3)*: Spam attacks or spamming is one of the quotidian attacks where innumerable messages are sent to people in an unauthorized way using any digital systems like a social network, mobile phones, etc. [81]. ProxyM that belongs to the Trojan category is one of the IoT malware spams, and the device that is infected receives an SMTP server address, credentials to access the server, an email address list and an email template for sending numerous emails to the mail addresses provided [62].

   A work [53] was proposed to address the QR-based web spamming in IoT using digital signature-embedded QR codes. This work generates a digitally signed QR code with original content, and a digital signature is generated using an Elliptic Curve private-public key pair and the content creator's public key. The digital certificates are placed at the URL if the content is a website link. Once the QR code is generated, a mobile application is used to verify the QR code by retrieving the original content, signed version, and public key of the content creator. This application ensured the QR code's integrity and opened the referred website. For this experiment, the author used spammer and actual links and identified the hits on each website.

4. *Data Exfiltration (A4)*: Data exfiltration, also known as data extrusion or data theft, is the unauthorized data transfer from the IoT device either manually or using malware attack [72]. This includes data compression and disassembling it into short undetectable chunks. A variant Mozi of worm category evolved from the IoT malware Gafgyt, IoT Reaper, and Mirai focuses on data exfiltration and other attacks such as command injection and payload execution [61]. In addition, malware like HNS from Spyware, Razor, and Lulz from Ransomware is also known for data exfiltration in IoT devices.

   A data exfiltration attack is performed in [46] using a smart light bulb in a secure environment where people have limitations in accessing the data. This is done using a chromium-based web browser and the Bluetooth web API. The web application does not need any internet connection, administration rights, or software installation and can be used in air-gapped networks. In this data exfiltration attack, the attacker inside the network performs data encoding in Bluetooth commands with a javascript script to be accessed within 25 m from the smart bulb. Two techniques are used for the script deployment; the inside attacker can take the QR-code with embedded script on paper, or a minified version of the script is rewritten inside the protected area. Once the script is opened in a Chromium-based web browser, it is executed, and data is encoded using steganography. The data thus encoded is sniffed from the receptor side utilizing a computer, BLE sniffer, WireShark, and Python script. Results proved that the data could be exfiltrated, and the smart bulb colour could be adjusted without notifying the owner. In future work, Javascript scripts can be used for optical channel attacks when Bluetooth connections cannot be sniffed.

5. *PDoS Attack (A5)*: PDoS, also known as Permanent Denial of Service, is an attack type similar to a DoS attack except for the fact that the hardware is destructed or sabotaged instead of the resources [76]. Brickerbot malware, which belongs to the Backdoor category, performs a group of Linux commands after gaining access to the device and aims to damage the hardware permanently. Unlike other attacks, rebooting cannot remove the infection from the device and IoT malware. Spyware is another category known for PDoS attacks using IoT malware like Skeeyah and VPNFilter.

   Permanent DoS attacks were concisely described in work [50], which identifies the different IoT attacks in IoT wireless protocols such as BLE, LoRaWAN, Z-Wave, and ZigBee along with their vulnerabilities. PDoS and several other attacks like DDoS and Coin-mining were also discussed in [44], which detects these attacks using FastGRNN, which offers faster detection with less complexity. As it does not require additional equipment, it is considered an independent module with less training time. Moreover, the work also compares other deep learning algorithms using two datasets.

6. *DNS Spoof (A6)*: Domain Name System (DNS) is an Internet phone book that helps in resolving the domain names to find the corresponding Internet Protocol address [79]. However, DNS records can be altered by malware attacks that result in traffic redirection to a malicious website that causes theft of credentials or related attacks [82]. Tsunami from the Backdoor category is an IoT malware that performs DNS spoofing in IoT devices, where the user credentials are stolen by providing them with a fake website. Ttint and Wroba from the Trojan category also perform DNS spoofing in IoT devices.

   DNS Spoofing is one of the several attacks used for testing the IISR router proposed in [48], using different penetration testing tools in Kali Linux. However, results found that except for DNS Spoofing, Malware Injection, and Firmware Vulnerability attacks, all attacks were detected by the proposed router. DNS-related attack like DDoS, Spoofing is also discussed in [52], with examples like Dyn and a target-specific university attack. Even though DNS-based attack is common, recognizing the same is crucial to the model. This article also discussed the solutions to prevent the same, like building a standard for IoT devices.

7. *Command Injection Attack (A7)*: Command injection in IoT is an attack that executes arbitrary commands on the host device through vulnerable web interfaces or applications [69]. Although code injection and command injection appear similar, code injection is an attack where the attacker adds code to the application. In contrast, command injection executes commands without injection of code [84]. Mozi, an IoT Malware from the worm category, is known for different attacks, including command injection, payload execution, and data exfiltration.

   A Command injection attack is focused in [57] where the PLC register values are identified and altered for the malfunctioning of two pumps in an Industrial IoT testbed. Furthermore, the work also identifies the challenges of IIoT-ML integration as the effect of imbalanced datasets in detection models. The authors have used an ANN-based anomaly detection model with an imbalance ratio to prove the same. Instead of standard performance measures, MCC, also known as Matthews Correlation Coefficient, is used for the performance evaluation.

8. *Payload Execution (A8)*: Payload execution in IoT is an attack type where the malicious payload is downloaded to the device and remains in a dormant phase until it is executed [78]. Once executed, it takes over the IoT device and follows various other attacks. Mozi from the Worm category, Luabot, and Wroba from the Trojan category do payload execution in IoT devices in addition to their different attack types. As mentioned in the above section, Mozi is known for several attacks on IoT devices.

   An interesting fact about the payload is discussed in [36], where the malware is the secondary payload once downloaded. It will perform other attacks related to that particular malware.

9. *Ransomware (A9)*: This attack holds the device by encrypting the files inside them and demands a ransom in exchange for the decryption key. Unlike other malware, Ransomware is both an attack type and a malware category. Even though ransomware is a typical attack on ordinary devices, it severely impacts IoT devices, according to the latest reports by [67]. Necurs, a malware that appeared in 2012, is known for its capability to perform ransomware attacks in both IoT and ordinary devices [75].

   IoT ransomware attacks during the two years are reviewed in [56] to understand the increase in IoT ransomware attacks. In addition, a Cryptowall ransomware attack detection model is also presented in this work, where the TCP/IP header is extracted from the traffic, and C&C is used for the blacklisting. However, the model could not address new or unknown C&C servers, and in the future, new ransomware families and attack nature in different operating system platforms need to be studied.

10. *Industrial Spying (A10)*: Industrial Spying is an attack where IoT malware targets industries to spy on their movements and control operations. This IoT malware often attacks SCADA systems known for capturing data from turbines in the industry [14]. VPNFilter, spyware, is one such IoT malware that targets Ukrainian hosts and makes the industry activities slow down using a C&C server specific for this specific country [59]. In addition, spyware like Skeeyah and worms like Omni and Themoon also perform industrial Spying in IoT areas.

    Spying, along with different attacks like data type probing, is detected in [45], using a three-stage machine learning-based detection model. Stage one includes the dataset preparation and assortment. The data is then passed through the preprocessing phase involving data cleaning, visualization, feature engineering, and vectorization. Once the preprocessing is done, sampling is performed, and the dataset is divided into training and testing sets. The training set is then applied with machine learning algorithms such as Logistic Regression, SVM, ANN, Decision tree, and Random Forest.

11. *Website Hacking (A11)*: This attack access website in an unauthorized way for performing various activities like information theft, content modification, and at times, adding malware to the device that views the website [66]. ProxyM of the Trojan category is one such IoT Malware attackers use to perform website hacks [74]. This malware's proxy server hacks websites via different techniques, including SQL injections, XSS, and Local File Inclusion. Worms like Omni and Themoon also perform website hacking in IoT devices.

    Website hacking is discussed in [54], with different vulnerabilities such as code execution, command execution, buffer overflow, etc. Moreover, the paper addressed a crawler model that identifies the vulnerability trends or patterns using a four-step process: Building a functional crawler using the dark web, classifying vulnerabilities based on keywords, storing results in a database, and visualization all vulnerabilities using a python script that executes in a website. The model proved that vulnerability trends could be identified quickly based on the results.

    Another work [43] introduced two web-based attacks to discover and manage the local IoT devices using a malicious website where the IoT devices present behind NATs can also be found. This model identifies the local IoT devices when a victim visits the malicious web page. The infected devices can be controlled to identify information such as software version, SSID, model number, Owner name, status, and a unique ID. Moreover, the work proposes various countermeasures to prevent this attack and compares model performance in different operating systems, devices, and web browsers.

12. *Click Fraud (A12)*: Click fraud is the attack in which the marketing of companies is fraudulently manipulated by clicking pay-per-click advertisements in an unauthorized manner [70]. In the case of IoT, a bot acts as a legitimate visitor and tricks the platform. For example, the creators of Mirai Worm were convicted for leasing it for DDoS and click fraud attacks [80]. TheMoon, ZHTrap belongs to the same worm category and focuses on click fraud as their attack in IoT devices.

13. *Other attacks*: Some other attacks are not expected as the attacks mentioned above. It includes the White Hat attack, which notifies the vulnerabilities(A13) in the device to the user so that the user can take the necessary steps to prevent further attacks [26], downloading or removing other malware like Backdoor (A14), infecting other IoT devices(A15), downloading anime videos(A16).

5.4 Attack surfaces

An attack surface is the vulnerable parts, or the exploitable vulnerabilities in the system [165] that cause risks to the devices. The traditional attack surface classification can be classified into network attack surface, human attack surface, and software attack surface. Unlike other malware, attacks by IoT malware are not limited to any one part of the device. Therefore, unlike the general classification, attack surfaces are classified into network and network device-level, service-level, firmware-level, and device-level attack surfaces. Table 5 illustrates the mapping of various IoT malware to its attack type and surfaces.

1. *Network and network devices*: IoT itself is known as a network of interconnected devices. Sometimes, this network and network devices can be an attack surface due to the vulnerabilities in the system.

    - *Network (S1)*: Each IoT malware behaves differently in the network attack surface. For example, When IoT malware like Silex of the Virus category removes the network configuration while infecting the device [96], another IoT malware, Blueborne of the Trojan category, sniffs the traffic by penetrating the 'air gapped' network.

      In DoS attacks, the network is the attack surface, and there exist works like [49] for its detection. This work converts network traffic data into an image and performs detection. However, in most works, the attack types are more focused than the attack surface.
    - *Firewall (S2)*: Firewall, a network-level attack surface, is a security system that controls the incoming as well as outgoing traffic passing through the system using a set of predefined rules [93]. Usually, firewalls will be there between these devices and the internet. However, when malware infects the IoT device, it drops firewall rules and makes changes to the network configuration changes. This opens the IoT devices to attacks like DDoS UDP flooding, DDoS TCP-SYN flooding, phishing etc. One example is Silex Virus [90, 96].

      However, most companies and homes use traditional firewalls that cannot detect data packets and their content due to the absence of features like anti-spam and anti-virus. Hence thorough examination of the data packets was required. As a solution for this problem, Unified Threat Management came into existence with these features. But, due to repeated inspections that cause increased latency and pro-

Table 5 Attack surfaces and attack types of IoT malware

Category	Malware	Attack Surface										Attack Type															
		S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16
Worm	Mirai	X				X						X											X		X		
	Hajime	X				X																		X			
	Aidra					X						X													X		
	Darlloz/Zollard		X			X							X														
	Satori	X			X	X						X	X				X										
	Sefa					X							X												X		
	Okane					X						X															
	Okiru					X						X															
	ZHtrap					X						X							X				X		X	X	
	Persirai	X			X				X			X						X							X	X	
	Gitpaste-12		X		X			X		X		X	X					X							X		
	Moose	X	X	X		X						X		X			X										
	Shishiga		X									X															
	Mozi	X		X		X						X		X	X			X	X							X	
	Carna			X		X																		X	X		
	Echobot	X	X							X		X						X	X		X						
	Wicked					X						X						X	X								
	Masuta	X				X						X						X	X								
	Tori	X		X		X									X			X	X								
	Bushido					X						X															
	JenX					X				X		X						X	X								
	Miori	X				X						X						X	X								
	Sora	X			X	X						X														X	
	Omni					X						X										X					
	Fritzfrog								X	X								X	X								
	TheMoon	X				X						X										X	X				
	Yowai					X						X													X		
	OMG	X	X									X															
	Owari					X						X															
	Ouija					X						X			X											X	
Spyware	VPNFilter	X	X	X	X	X	X		X						X	X		X	X		X				X	X	
	Psybot	X				X						X							X								
	Gamut				X	X				X				X													
	Hide and Seek			X											X		X										

Table 5 (continued)

Category	Malware	Attack Surface										Attack Type															
		S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16
	Xarcen/XORDDoS	X				X			X			X			X			X	X								
	Spybot	X		X								X			X												
	Skeeyah			X		X	X		X						X	X					X	X					
Ransomware	Necurs	X			X							X	X							X							
	Cr1ptT0r			X		X														X					X		
	Hades	X		X		X									X					X							
	Razor			X		X									X					X							
	Lulz			X	X									X	X					X					X		
	Muhstik				X	X	X			X		X	X							X					X	X	
Backdoor	Bashlite					X						X	X					X							X		
	Kaiji					X						X															
	Tsunami	X				X						X					X										
	IRCflu					X				X									X						X		
	Brickerbot	X		X		X	X		X		X				X	X		X	X								
	IoTReaper/IoTroop	X										X			X				X		X				X		
	Elknot/BillGates/Mayday					X						X															
	Gr1n				X	X				X				X													
	Setag	X				X								X						X							
	Karu					X		X				X			X												
	InterPlanetaryStorm					X				X		X	X														
Trojan	Blueborne	X		X				X	X						X					X							
	ProxyM	X	X																			X					
	Luabot	X	X									X						X	X								
	Emotet	X			X	X									X												
	AirDropBot/Cloudbot					X						X															
	Leet					X						X															
	Pnscan	X				X																			X		
	dark_nexus	X				X						X															
	Hydra	X										X															
	Demonbot	X				X				X		X						X									
	APEP					X						X															
	Ares					X						X			X												
	Kluh					X						X															
	Qbot	X	X		X							X			X										X		

Table 5 (continued)

Category	Malware	Attack Surface										Attack Type															
		S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16
Virus	Silex				X				X							X											
	Amnesia	X		X					X			X	X		X												
	Wifatch					X						X												X			
	Joker			X	X													X									
	Cereal	X																									X
	HEH			X		X				X			X		X			X									

cessing, a firewall known as the Next-Generation Firewall was proposed. In [90], different attacks like DDoS UDP flooding, DDoS TCP-SYN flooding, phishing, and SQL Injection were carried out in the IBM ISS Proventia firewall and Next-Generation Firewall. Based on the results, the authors concluded that the IBM ISS firewall blocked only DDoS UDP flooding, and NGF prevented all the attacks.

- *Communication channels (S7)*: The channels that connect several IoT devices are another attack surface. This includes the protocols that have security vulnerabilities [166]. One such wireless protocol is Bluetooth which acts as a communication protocol in IoT devices. However, it has been proved that Bluetooth can also work as an attack vector and vulnerability due to the emergence of the new IoT malware called Blueborne Trojan [98]. The impact of dangers caused by IoT malware can be understood when we know that Blueborne doesn't even need Bluetooth to be paired between devices. Due to this reason, this IoT malware is also known as Airborne malware.

  In works like [86], the experimental study for security is conducted on Bluetooth devices. In this work, the Bluetooth dynamic analysis tested essential parameters in Security Management Protocols (SMP) for key cracking and fake device formation. Similarly, [92] presented a penetration testing tool for IoT devices that communicate via Bluetooth, WiFi, and ZigBee.

2. *Services*: Services are another attack surface in IoT devices, divided into two sub-levels, as shown below.

- *Software as a service (S4)*: IoT Software is a group of programs or data that helps the IoT device work and execute specific tasks. Unfortunately, vulnerabilities in software are increasing in a peak manner, and it is understandable from IoT malware Satori from the worm category as they target the software vulnerabilities in the routers [95].

  Satori is discussed in [87] where an IoT malware network activity detection model, EDIMA, is proposed, which extracts the features from the incoming traffic samples. Once the features were extracted, various ML algorithms, including DT, SVM, and NB, were used to classify IoT malware.
- *Server as a service (S9)*: Server, a software-level attack surface, is a computer program or device that offers a service to another computer program and its user, also known as the client. Servers like SSH and Github are often exploited by IoT malware like Gitpaste of the worm category, which affects the service provided by those servers [25].

Several authentication methods were proposed using the Chain of Trust and Threat models to secure these servers. Works like [85] were also proposed, where security keys supporting authentication and registration are used to secure IoT servers and devices using encryption. The proposed model was developed with the goals of easiness, security, and privacy.

3. *Firmware (S6)*: IoT Firmware, often called the heart of IoT devices, offers adequate communication commands with other devices. The most common attack on the firmware is the PDoS attack, where the firmware is sabotaged due to IoT malware such as Silex Virus, Brickerbot Trojan, and so on [96].

   Even though there exist several analysis solutions for firmware vulnerabilities, most focus on the analysis improvement rather than integrating them for a model that audits the firmware, network services, and web interfaces. Despite this, in [86], the problem is solved by proposing a modular, extendable, and configurable model with a web interface for the Quality Assurance team and users. Unlike existing works, static and dynamic analyses were performed on the kernel, bootloader, file systems, and unpacked firmware images. The outcome of the work revealed that most firmware contained hard-coded addresses, username-password combinations, certificates, etc.
4. *Devices*: In addition to the above attack surfaces, specific components of the devices also act as the attack surfaces.

   - *Ports (S5)*: Ports are the communication endpoints where the network connection starts and ends. Ports are mainly affected by IoT malware which belongs to the worm category. Most existing IoT malware finds vulnerabilities in the port for the first step of infection of the device. One example is the Mirai worm, which identifies open TELNET TCP ports and infects the machine. Once it infects the device, the malware moves to the second phase of the attack [97].

     A work [91] used IoTPoT as the source of IoT malware samples where the limited IP addresses mainly connect with Telnet-specific requests. IoT malware characterization is performed in this work by identifying the correlations in adversarial IPs and strings. Based on the finding, the authors determined that some malware samples contained the keywords "Corona" and "Covid", demonstrating that covid related IoT malware attacks were also present in the code-reusing situations. Moreover, results proved that the proposed method helps identify the correlated IoT malware.
   - *Storage(S3)*: In IoT, data capturing and computation capabilities are provided by edge storage, making the system deliver the insights after analyzing it. Still, IoT malware also finds ways to attack the storage in IoT devices. Brickerbot from Backdoor is the best example, as it corrupts the Multi-Media Card and Memory Technology Device storage. In addition, Silex Virus, the malware mentioned in the network and firewall attack surface, also affects the storage [96] proves that IoT malware is not limited to any one attack surface.

     Brickerbot is also mentioned in [88] by explaining its attack types and the prevention mechanisms, such as periodic device updates, firewall setup, and authentication techniques. The authors also explain how AI is used to attack devices which is not widely discussed in the existing papers.
   - *Memory (S8)*: Even though a device's memory is confused with storage, the main difference between memory and storage is that memory is a component that offers short-term access. Meanwhile, storage is a component that provides long-term access. In IoT, memory is also an attack surface that gets corrupted due to malware activities. IoT malware Amnesia, which belongs to the Virus category, is one example of memory corruption in addition to attacks like DDoS and data exfiltration [94].

     MAD-IoT, proposed in [89], detects the anomalies in IoT device memory content by placing a memory agent in an isolated environment. In addition, due to the heterogeneity of devices, different measurement agents are created using a portable technique called IMAGE: Integrity Measurement Agent GEneration. The memory contents thus gathered are fed into ML algorithms for identifying normal device operations.
   - *Hardware (S10)*: Hardware is a term used to collectively mention a device's physical parts like motherboard, monitor, CPU, etc. IoT malware like Brickerbot Backdoor affects the devices' hardware, permanently making them unusable devices [76].

     Usually, the hardware is affected by permanent DoS attacks on the devices. A brief explanation of PDoS due to the multiple join requests from LoRaWAN protocol is discussed in [50].

5.5 Target devices

In the Internet of Things, the 'things' refer to any devices, actuators, sensors, or monitors interacting with the environment for data collection and several other purposes [167]. Even though the device can be user-friendly, the problem with the IoT device is that security is not given importance compared to customer satisfaction. Due to these reasons, the number of attacks on IoT devices increases daily. This attribute indicates the different IoT devices that are attacked by IoT malware.

Routers (TD3) [48] are the most exploited device among various IoT devices by different IoT malware, including Masuta, Mirai [113], Darlloz, WiFatch, Hajime, Ttint [117] Remaiten, etc. Mirai also attacks devices including printers (TD1) [114], CCTVs (TD5) [115], Smart TVs (TD4) [118], Smart Toys (TD14) [116], Video camera (TD2), gaming consoles (TD16), Thermostats (TD18), etc. The open ports in IP cameras (TD8) are likewise exploitable and thus considered the second most prominent victim in IoT devices. On the other hand, IoT malware Hajime often affects webcams (TD7) and DVR (TD6)s, whereas the IoT malware Darlloz exploits the PHP vulnerabilities of set-top boxes(TD9). Other devices such as Modems (TD10), SmartPhone (TD11), Video players (TD12), storage devices (TD13), Smart Bulb (TD15), and NVR (TD17) are also the victims of IoT malware. Overall, it can be said that IoT malware is not limited to any particular device, and malware can be from any category, such as Worm, Trojan, Backdoor, Virus, etc.

In [37], Raspberry Pi devices were attacked with backdoor scripts, whereas in [92], Raspberry Pi is considered as an IoT device for analyzing their proposed penetration testing tool. Similarly, [46] experimented with a smart light bulb for data exfiltration attack. [113] discussed on Mirai and Bashlite that targets the Routers with vulnerable points. Furthermore, [34] discussed various Ransomware attacks on Thermostats, Smart TVs, and Smart bulbs, along with their processes and preventive solutions.

Table 6 depicts the IoT malware and devices they often target.

5.6 Target device architecture

Different device architectures exist for IoT devices, with specific objectives like performance. This section discusses the different target architectures of devices attacked by IoT malware.

1. *MIPS (TDA1)*: MIPS (Microprocessor without Interlocked Pipelined Stages) is a RISC ISA (Reduced Instruction Set Computer Instruction Set) [106] present in numerous devices such as cameras, routers, transmitters, etc. As devices like routers and cameras can be part of the IoT system, MIPS architecture can be considered a target architecture. WiFatch from the Virus category, Hydra from the Trojan category, and Tsunami from the Backdoor category are the few IoT malware that affects MIPS architecture devices.

   In [1], different IoT malware strewed across different IoT architectures, including MIPS, was considered the input for IoT malware detection. Unlike other existing works, the model could also focus on various obfuscation attacks.
2. *MIPSEL (TDA2)*: MIPSEL is similar to MIPS except that MIPS has a big-endian architecture, whereas MIPSEL is a little-endian architecture. Spybot, Skeeyah from the Spyware category, and Echobot, Wicked from the Worm category often attack devices of MIPSEL architecture.

   [168] considers MIPSEL samples along with MIPS and ARM samples for similarity-based malware classification. The work uses the Jaccard index and t-SNE to identify the similarities and outcomes, revealing that the proposed model performs well in malware classification.
3. *ARM (TDA3)*: ARM (Advanced RISC Machines) is an advanced RISC for device processors used for different environments [104]. These architectures often contain chips and modules linked to memory, interfaces, etc. WiFatch belongs to the Virus category, and Luabot, which belongs to the Trojan category, are some of the IoT malware that impacts devices of the ARM architecture.

   Owing to the growth of architecture-specific IoT malware attacks, in [99], a deep learning approach was used for malware detection based on ARM architecture samples. As this was related to ARM, the authors suggested considering the model in different architectures in future work.
4. *X86/64 (TDA4)*: x86/x64 is an architecture that allows 16-bit and 32-bit applications to run with the applications of 64-bit due to the compatibility mode [112]. As a result, these architectures are now widely used in IoT devices, and the devices with this architecture are usually called CISC processors. Satori, Sefa, Okane, and Okiru in the Worm category are widely known for attacking x86/64 architecture devices.

   As IoT malware source codes can be cross-compiled and attacked in different devices, the researchers started focusing on architecture-specific and malware-specific samples for their works. An IoT malware classification model [100] that used Haralick texture features and ML methods has considered a dataset with Mirai and Bashlite samples which spans their attacks on various architectures like MIPS, X86, SUPERH, etc.
5. *Intel 80386 (TDA5)*: The Intel 80386 is a 32-bit microprocessor that speeds from 12Mhz to 40Mhz with a paging translation unit and supports advanced virtual memory [105]. While the IoT Malware Mirai in the worm category, Bashlite in the Backdoor category, etc., attacks devices of Intel 80386 architecture, some malware source codes are cross-compiled by the attackers to attack this architecture.

Table 6 IoT Malware and Target Devices

Category	Malware	Targe Devices																	
		TD1	TD2	TD3	TD4	TD5	TD6	TD7	TD8	TD9	TD10	TD11	TD12	TD13	TD14	TD15	TD16	TD17	TD18
Worm	Mirai	X	X	X	X	X									X				X
	Hajime					X	X	X	X										
	Aidra			X															
	Darlloz/Zollard			X		X				X									
	Satori		X	X		X		X											
	Sefa								X										
	Okane			X		X	X												
	Okiru		X		X									X					
	ZHtrap			X		X	X												
	Persirai			X					X										
	Gitpaste-12		X	X					X										
	Moose			X							X								
	Shishiga			X							X								
	Mozi			X			X	X						X					
	Carna			X						X									
	Echobot			X					X										
	Wicked			X		X	X												
	Masuta			X															
	Tori			X		X			X										
	Bushido			X															
	JenX			X													X		
	Miori			X															
	Sora			X															
	Omni			X	X	X													
	Fritzfrog			X															
	TheMoon			X							X								
	Yowai			X		X	X												
	OMG			X			X		X										
	Owari			X		X	X		X					X					
	Ouija			X	X											X			
Spyware	VPNFilter			X	X														
	Psybot			X							X								
	Gamut			X															
	Hide and Seek			X	X		X		X										

Table 6 (continued)

Category	Malware	Targe Devices																	
		TD1	TD2	TD3	TD4	TD5	TD6	TD7	TD8	TD9	TD10	TD11	TD12	TD13	TD14	TD15	TD16	TD17	TD18
	Xarcen/XORDDoS				X														
	Spybot			X															
	Skeeyah				X				X			X							
Ransomware	Necurs			X					X										
	Cr1ptT0r			X										X					
	Hades			X	X				X			X							
	Razor				X						X	X	X						
	Lulz			X															
	Muhstik			X															
Backdoor	Bashlite		X	X			X												X
	Kaiji			X															
	Tsunami			X			X		X						X				
	IRCflu						X					X							
	Brickerbot			X											X	X			
	IoTReaper/IoTroop			X			X		X					X				X	
	Elknot/BillGates/Mayday	X		X															
	Gr1n					X			X		X								
	Setag	X		X					X			X							
	Karu			X			X		X										
	InterPlanetaryStorm						X					X							
Trojan	Blueborne				X														
	ProxyM			X	X		X				X	X							
	Luabot					X													
	Emotet			X			X												
	AirDropBot/Cloudbot			X															
	Leet			X		X		X	X										
	Pnscan			X															
	dark_nexus			X		X	X												
	Hydra			X							X								
	Demonbot						X												
	APEP	X		X															
	Ares			X	X				X	X									
	Kluh			X															
	Qbot			X															

Table 6 (continued)

Category	Malware	Targe Devices																	
		TD1	TD2	TD3	TD4	TD5	TD6	TD7	TD8	TD9	TD10	TD11	TD12	TD13	TD14	TD15	TD16	TD17	TD18
Virus	Silex			X															
	Amnesia					X	X												
	Wifatch			X															
	Joker			X								X							
	Cereal																		
	HEH			X															

Along with MIPS, Intel 80386 was another architecture considered the input samples in the IoT malware detection model, MTHAEL [1]. The work could focus on different feature selection algorithms followed by an Ensemble learning model.

6. *ARC (TDA6)*: ARC (Argonaut RISC Core) is a 32-bit CPU family used in different SoC (system-on-chip) devices such as mobiles, IoT applications, digital homes, etc. [103]. Furthermore, it is known for its good performance and code density for host SoC applications. Therefore, most IoT devices use ARC processors, and IoT malware Okiru from the Worm category is the first malware that targets ARC devices.

   Okiru discussed in [107] was discovered to have different kinds of router attack exploit code hardcoded, which is not found in IoT malware like Satori. Furthermore, 114 credentials are used for telnet attacks, unlike other malware that uses short databases.

7. *PowerPC (TDA7)*: PowerPC, also termed PPC, is a RISC ISA used initially for PCs and now used in IoT devices like Routers [109]. It is widely used in Apple products such as PowerBook, iBook, and iMac. Due to its wide usage, the attacks like Mirai and Bashlite from worm and backdoor categories target devices of PowerPC architectures.

   In [1], PowerPC IoT malware samples are used in the IoT malware detection model in addition to MIPS architecture. However, unlike other existing works, the work focused on feature selection algorithms, ML methods, and obfuscation attacks with these cross-architecture malware samples.

8. *SuperH (TDA8)*: SuperH, also called SH, is a 32-bit RISC ISA implemented by microprocessors and microcontrollers embedded systems [111]. WiFatch, the IoT malware from the Virus category, targets devices of SuperH architectures and the MIPS and ARM architectures.

   [100] has presented an IoT malware classification model that evaluated using a dataset with IoT malware, including Mirai and Bashlite samples of SuperH architecture and the MIPS, X86, architectures. This model created a grayscale image from these samples, then used for feature extraction, followed by IoT malware classification.

9. *SPARC (TDA9)*: SPARC (Scalable Processor Architecture) is a RISC ISA in which the "Scalable" keyword indicates its ability to scale the embedded processors to large server processors with the same core instruction set [110]. However, according to the reports, SPARC architectures are affected by the IoT malware Mirai and Bashlite from worm and backdoor categories similar to PowerPC architecture.

   As the IoT malware behaviour in each architecture differs, the researchers elucidate their proposed models using malware samples from different architectures. One such work is presented in [102], where byte sequences are collected from 111K benign and 111K malware of SPARC and several other architectures for IoT malware detection.

10. *Motorola m68k (TDA10)*: This is a 16-bit or 32-bit CISC (Complex Instruction Set Computer) microprocessor that implements a 32-bit instruction set, with a 24-bit address bus, 32-bit registers, 16-bit internal data bus [108]. As it does not use memory segmentation, it is more effortless to program and widely used in PCs with GUI, including Macintosh, Amiga, etc.

    [101] articulated a model with malware samples from different architectures, including Motorola m68k architecture for the malware classification in IoT devices.
11. *Renesas (TDA11)*: Renesas architecture devices are fast, cheap, reliable, and eco-friendly compared to other architectures. However, the IoT malware attacks from Razor, and Lulz from the Ransomware category can also occur in this architecture.

    [31] identified various toolchains used for IoT malware using samples from different architectures, including Renesas. The authors determined that 13 building tools present on the web were used for malware creation.

IoT Malware Mapping to Target device architectures is portrayed in Table 7.

5.7 Device access mechanisms

As IoT devices can be accessed from Intranet and Internet, the IoT malware access the devices through some basic access mechanisms. This attribute discusses the various access mechanisms in which the IoT Malware accesses the target IoT devices.

1. *Brute force Attack (AM1)*: In a brute force attack, an attacker gains access to a secured system by continually entering credentials automatically or manually [122]. As most IoT devices either use default credentials or don’t use credentials, Telnet and SSH brute force attacks cause numerous IoT attacks [123]. Interestingly, most IoT malware, including Okane, Okiru, ZHtrap, Persirai, Gitpaste-12 from the worm category, VPNFilter, and Psybot from Spyware, access the device through Brute-force attacks.

   [120] applied an automatic brute-force attack to SMS authentication code to evade existing protections and crack IoT device user accounts. However, in this work, the smartphone number of the user is assumed to be previously known to the attacker. In addition, this study helped discover six account-login vulnerabilities in the smart lock, smartwatch, smart router, and the sharing car.
2. *CVE Exploit (AM2)*: Common Vulnerabilities and Exposures, also known as CVE, lists publicly revealed computer security vulnerabilities along with CVE IDs to help the user to recognize unique vulnerabilities and coordinate the creation of security tools and solutions [125]. Sometimes, these CVEs are exploited by IoT malware which affects numerous IoT devices and enables attackers to control devices [124]. For example, Lulz and Muhstik from the Ransomware category and Bashlite from the Backdoor category use different CVEs for accessing the devices.

   In [92], a penetration testing tool, PENTOS, is presented for IoT devices that communicate via Bluetooth, WiFi, and ZigBee. In this work, the information gathered in their initial step is analyzed using the publicly available CVEs in addition to Nmap and fping.
3. *Target-specific Access Mechanism (AM3)*: Sometimes, IoT malware is created for specific targets with access mechanisms specifically for that target. For example, it might be the devices in a country [59], industry [14] and so on. At times, VPNFilter is spyware that targets Ukrainian hosts and slows down the industry activities using a C&C server that is specific for this specific country [59].

   [45] discussed a machine learning detection model for detecting different IoT malware attacks, including Spying which is the most common target-specific attack.

Mapping of IoT Malware to Access mechanisms is illustrated in the Table 7.

5.8 IoT malware characteristics

This attribute discusses the various characteristics shown by IoT malware and the usual attack behaviour.

1. *Detection of Virtual Environment (C1)*: To evade detection and analysis by security personnel, certain IoT Malware determines whether they are running in a virtual environment such as VMWare or VirtualBox. Once checked, the malware wipes all its evidence using certain commands [132]. Gamut, VPNFilter from Spyware, and Necurs from Ransomware are the few IoT Malware that detects Virtual Environment’s presence.

   Virtual machine detection by Amnesia is explored in [169], where the malware wipes essential folders from the file system with the Linux “rm -rf” shell command to kill any evidence they might have gathered.

Table 7 Mapping of IoT Malware to Target device architectures and Access mechanisms

Category	Malware	Target Device Architectures											Access Mechanism		
		TDA1	TDA2	TDA3	TDA4	TDA5	TDA6	TDA7	TDA8	TDA9	TDA10	TDA11	AM1	AM2	AM3
Worm	Mirai	X	X	X	X	X		X	X	X			X		
	Hajime	X	X	X									X		
	Aidra	X	X	X	X			X	X				X		
	Darlloz/Zollard	X	X	X		X		X						X	
	Satori	X	X	X	X	X	X	X	X	X			X	X	
	Sefa	X	X	X	X			X					X	X	
	Okane	X	X	X	X	X	X	X	X	X			X	X	
	Okiru			X	X		X	X					X	X	
	ZHtrap	X		X	X								X	X	
	Persirai	X	X	X									X	X	
	Gitpaste-12	X		X	X								X	X	
	Moose	X		X									X		
	Shishiga	X	X	X	X	X		X	X	X			X		
	Mozi	X		X									X	X	
	Carna	X		X	X								X	X	
	Echobot	X	X	X	X	X	X	X	X	X				X	X
	Wicked	X	X	X	X	X		X	X	X			X	X	
	Masuta	X		X	X									X	
	Tori	X	X	X	X	X	X	X	X	X			X		
	Bushido	X		X	X	X		X	X	X			X	X	
	JenX	X		X	X									X	
	Miori	X	X	X	X	X	X	X	X	X			X	X	
	Sora	X	X	X									X	X	
	Omni	X		X	X	X		X					X		
	Fritzfrog				X	X							X		
	TheMoon	X				X							X		
	Yowai	X	X	X	X	X		X	X				X	X	
	OMG	X	X	X	X	X		X	X	X			X	X	
	Owari	X	X	X	X	X	X	X	X	X			X	X	
	Ouija	X	X	X	X	X	X	X	X	X			X		
Spyware	VPNFilter	X		X		X							X	X	
	Psybot	X	X	X	X	X		X	X	X			X		
	Gamut	X	X			X								X	
	Hide and Seek	X			X	X			X	X			X	X	

Table 7 (continued)

Category	Malware	Target Device Architectures											Access Mechanism		
		TDA1	TDA2	TDA3	TDA4	TDA5	TDA6	TDA7	TDA8	TDA9	TDA10	TDA11	AM1	AM2	AM3
	Xarcen/XORDDoS			X		X		X		X			X		
	Spybot	X	X	X		X							X	X	
	Skeeyah	X	X	X		X							X	X	
Ransomware	Necurs	X		X		X								X	
	Cr1ptT0r	X		X	X								X		
	Hades	X		X		X							X		
	Razor	X		X	X	X		X		X		X		X	
	Lulz				X	X						X		X	
	Muhstik	X		X										X	
Backdoor	Bashlite					X		X		X		X	X	X	X
	Kaiji	X		X									X		
	Tsunami	X	X	X	X	X		X	X				X		
	IRCflu	X	X	X	X	X		X			X		X		
	Brickerbot	X		X					X				X	X	
	IoTReaper/IoTroop	X	X	X		X				X		X		X	
	Elknot/BillGates/Mayday			X										X	
	Gr1n	X	X	X	X	X	X	X	X	X	X	X	X		
	Setag	X	X	X	X									X	
	Karu	X	X	X	X	X	X	X	X	X	X	X	X	X	
	InterPlanetaryStorm	X	X	X	X	X		X					X		
Trojan	Blueborne	X		X		X		X		X				X	
	ProxyM	X	X	X	X	X	X			X					
	Luabot			X		X							X		
	Emotet	X		X										X	
	AirDropBot/Cloudbot	X	X	X										X	
	Leet	X	X	X	X	X		X	X	X			X		
	Pnscan	X		X	X			X					X		
	dark_nexus	X		X	X	X		X		X	X	X	X		
	Hydra	X											X	X	
	Demonbot				X									X	
	APEP	X	X	X	X	X	X	X	X	X			X	X	
	Ares	X	X	X									X		
	Kluh	X		X										X	
	Qbot	X		X	X	X							X		

Table 7 (continued)

Category	Malware	Target Device Architectures											Access Mechanism		
		TDA1	TDA2	TDA3	TDA4	TDA5	TDA6	TDA7	TDA8	TDA9	TDA10	TDA11	AM1	AM2	AM3
Virus	Silex	X											X		
	Amnesia	X		X										X	
	Wifatch			X	X				X				X		
	Joker	X		X	X	X	X							X	
	Cereal														
	HEH	X	X	X	X	X		X					X		

2. *Survive the reboot (C2)*: Several IoT Malware copies themselves to the directory /etc/init.d/ in the device's embedded GNU/Linux system, where startup programs are stored. This is done to make sure that the malware survives the reboot and freshly infects the device again [137]. Brickerbot in the Backdoor category, VPNFilter, and HNS from the Spyware category do this survival in IoT devices.

   Mirai, an IoT malware discussed in several works including [26, 27, 31, 128] also survive a reboot and freshly infects the devices.

3. *Stealth (C3)*: Stealth is a characteristic of IoT malware that tries to hide its presence to avoid detection mechanisms. Usually, the malware hides in files, boot sectors, and partitions and deliberately avoids detection. Satori, Gitpaste-12, and Moose from the Worm category are well-known for their stealthy behaviour.

   Since the Mirai source code was released in 2016, countless customized versions have been made with different characteristics. One such latest advancement in Mirai makes it stealthy and hidden from the detection mechanisms [134].

4. *Turns the device into a proxy server, network, or honeypots (C4)*: Some IoT malware turns the devices into the network, honeypot, and proxy servers once they infect the device. This characteristic is mainly exhibited by ZHTrap, Moose, TheMoon, and OMG from the worm category.

   OMG, the Mirai variant uses an open-source software known as 3proxy for serving as a proxy server once it infects the device. The setup starts by generating two random ports - one for the socks_proxy_port and the other for the http_proxy_port. Once the ports are created, they are notified to the CnC [139].

5. *Reboot prevention (C5)*: Another important characteristic of IoT malware is the prevention of reboot to discourage wiping out of the malware from the device. As a reboot can solve most IoT malware infections, malware authors have updated this mechanism in their recent works. Similar to reboot survival, the IoT malware from worm categories, including Mirai and Hajime, is also widely shown.

   The anti-reboot features in Mirai kill the watchdog process to bypass an auto-reboot of infected device [14]. Interestingly, it is also noted that Mirai is the top IoT malware that mainly exhibits all these advancements.

6. *Port closing (C6)*: Usually, unused ports are closed to reduce security issues, thereby reducing the attacks. However, a few IoT malware consider the port closing to ensure that no other malware is trying to access the port for the attack. For example, Persirai and Carna belong to the worm category and exhibit port closing.

[138] discuss Darlloz malware which scans for samples of Aidra malware in IoT devices. If any related files are identified, it is deleted and tried to close the communications port used by it.

7. *Creation of new variants (C7)*: Developing a new malware is time-consuming and takes effort. Nevertheless, as a solution to this problem, malware authors release their source codes to the public so that other attackers can make new variants with additional features. The best example is the release of the worm Mirai's source code, from which several other malware was created.

   [135] elucidated on Mirai malware which has created several variants that target different CPU architectures. It also discusses the emergence of Okiru, the variant of Mirai, and how it targets the second most prevalent type of architecture - ARC processors.

8. *Provide services like DDoS-for-hire, Ransomware (C8)*: As mentioned in the above sections, IoT malware is widely used for attacks, including DDoS attacks. Nevertheless, some IoT malware provides DDoS and Ransomware as a service rather than performing the attack. Muhstik, the Ransomware, and Bashlite, the Backdoor, are the IoT malware that offers these services.

   JenX botnet discussed in [133] offers a DDoS service with an assured 290-300Gbps bandwidth. Yet, security officials can take down this malware as it uses a centralized architecture.

9. *Huge Packet Size (C9)*: During the malware attack in IoT devices, the network traffic will have malicious characteristics. One such behaviour is the huge packet size of the traffic. All IoT malware does not show this unusual size, which is why it is considered a specific characteristic by Leet, the Trojan malware.

   The attack caused by Leet is presented in [129], which explains the 650 Gbps DDoS flood with packets greater than 150 million per second (Mpps). The attack bursts initiated from spoofed IPs made tracing the botnet's location impossible.

10. *Use only one exploit (C10)*: Exploits take advantage of the security flaws or vulnerabilities in the devices. As most IoT malware considers various exploits while attacking the devices, some use only one exploit.

    [170] discusses the BotenaGo IoT malware that targets devices with more than 30 Exploits. Once the vulnerability is successfully exploited, the malware will execute remote shell commands.

11. *Victim device architecture detection (C11)*: Victim device architecture detection is another characteristic where the malware sends the payload corresponding to the device's architecture. This is exhibited mainly by the IoT malware, which belongs to the worm category, including Mirai and Echobot.

    [15] explains this characteristic in their work, along with examples of IoT malware.

12. *Periodic Command Execution (C12)*: Periodic command execution is like a CRON job that performs specific command executions during a certain interval. Elknot Backdoor, amnesia virus and Gitpaste-12 worm are the few IoT malware trigger periodic command execution.

    [131] explains how Gitpaste-12 negotiates and brute forces the systems before setting up a CRON job that it downloads from Pastebin. Once this is done, the same script will be called again every minute.

13. *Binary Removal (C13)*: Binary removal is another behaviour IoT malware shows once the execution starts. This is done so that malware needs to reside in the device's Random Access Memory, and it prevents the detection mechanisms. Persirai, Hajime from the Worm category, and Psybot from spyware do this behaviour once they start the execution.

    Binary removal is mentioned in [15] along with victim device architecture detection as a characteristic. This is considered a critical behaviour as it affects the detection mechanisms.

14. *Name stealing (C14)*: Similar to stealth and binary removal characteristics, name stealing is also a feature where the malware steals a process's name, thereby preventing it from anti-malware techniques. However, it is a rare characteristic used by a few malware, including Echobot, a worm categorized as IoT malware.

    Echobot is a well-known Mirai variant that targets corporates and enterprise management systems. Based on the studies, the researchers found that Echobot remains a threat and will not slow down quickly [130].

15. *Name assignment (C15)*: Name assignment is similar to name stealing except that instead of stealing the name, a random name is given to the process for the malware. Mirai and JenX, the IoT malware that belongs to the worm category, perform name assignments for their processes.

    Mirai's various characteristics are explained in works including [31, 128]. Several studies found that Mirai is one of the malware that exhibits a wide range of characteristics added to the attacks.

16. *UPX header insertion (C16)*: Malformed UPX (Ultimate Packer for Executables) headers are inserted by IoT malware authors to make the analysis complex, thereby preventing the security analysts from discovering it. Hajime and Elknot from the worm and backdoor category are the two malware that primarily displays this characteristic.

    In [127], the researchers realized that the Hajime malware binary was compressed with an altered version where the UPX header is changed from its default value. The authors also identified that this was done to restrict the reverse-engineering techniques.

17. *DGA algorithm (C17)*: Domain generation algorithms are shown by various IoT Malware for generating many domain names as rendezvous points with their C&C servers. Among IoT Malware, Mirai in worm and VPNFilter in Spyware categories are the ones that exhibit DGAs.

    In [136], security researchers alert that recent variants of the Mirai have domain generation algorithm (DGA) features not shown in previous Mirai samples. Moreover, they have also mentioned that Mirai shows certain other behaviour in addition to this.

IoT malware that exhibits these characteristics is illustrated in Table 8.

5.9 Programming languages

IoT security researchers articulate that malware developers increasingly diverge to unique or unfamiliar programming languages to impede reverse engineering and analysis efforts. Moreover, it is identified that each of these languages is relatively new, supporting cross-platforms and avoiding traditional signature-based detection tools. Top malware programming languages used in IoT malware are selected based on the information gathered from various sources, including [158, 160, 161].

Mirai, one of the most widely known IoT malware, uses two programming languages, including C (L1) [161] and Go (L2) [161] where the former is used for the agent, and the latter is used for the controller. Hajime [159], Sefa, and Okane are other malware that uses C as their programming language. As mentioned in [11], Luabot, an IoT malware, uses Lua (L5) programming language. In contrast, a list of commonly used IoT malware programming including [13], PHP (L3) [157], Perl (L4) [164], VisualBasic (L6) [163], C++ (L7) [162], Delphi (L8) [13], and Shell commands (L9) [13] are also used by different IoT Malware.

More details on the programming language used by IoT malware are discussed in Table 8.

5.10 Protocols

This attribute discusses the different protocols used by IoT malware to infect the devices. Protocols are a set of rules followed for communication between two entities. As each IoT malware behaves differently, the protocols they target also differ.

1. *Telnet (P1)*: Telnet is an application protocol for offering a bidirectional interactive text-oriented communication with the help of a virtual terminal connection [152]. Telnet is considered the most insecure communication protocol among various protocols as most IoT malware targets this, including malware from Worm, Trojan, and Backdoor categories.

   A P2P IoT malware HEH is introduced in [155], which targets various IoT devices with exposed telnet services. Moreover, the researchers also discovered that the attack is irrespective of the MIPS, x86, PPC ARM, or any other architecture.

2. *TCP (P2)*: Transmission Control Protocol is a transport protocol used on top of Internet Protocol to provide reliable packet transmission [171]. In IoT, Cybersecurity researchers disclosed various flaws in embedded TCP/IP stacks affecting millions of IoT devices [140]. Some IoT malware includes Persirai and Satori from the worm category.

   [151] discusses how researchers detected IP cameras vulnerable to Persirai malware. Unfortunately, as many users are unaware of the vulnerabilities, it is easier for attackers to access the IP Camera interface through TCP Port 81.

3. *FTP (P3)*: File transfer protocol (FTP) is a communication protocol that helps file transfer between devices over a network [141]. However, IoT malware like Mirai targets this protocol for attacking the devices.

   According to researchers, 14.6% of all routers had either FTP or Telnet services open, which are also vulnerable to Bruteforce attacks [142]. One such example is the TP-Link routers, with 9.3% of them having an FTP service open to the internet, with 55% operating with a weak password.

4. *SSH (P4)*: Secure Shell Protocol is a cryptographic network protocol to operate network services securely in an unsecured network with applications including remote login and command-line execution [156]. Like other protocols, SSH is also used for attacking devices by IoT Malware, including IRCflu, Brickerbot, IoTReaper, and Elknot from the worm category.

   Kaiji, one of the IoT Malware, performs brute-force attacks against IoT devices with open SSH ports. Once infected, the C&C servers go offline, exposing the infected devices to other attackers [149].

5. *HTTP (P5)*: Hypertext Transfer Protocol is an application-layer protocol mainly designed to communicate between web servers and browsers [144]. Shishiga and OMG from the worm category are the two IoT malware that targets HTTP protocol.

   Shishiga malware targets IoT devices using four protocols: SSH, Telnet, HTTP, and BitTorrent. Like other IoT malware, the infection vector of Shishiga is prevalent: brute-forcing weak credentials [147].

6. *BitTorrent (P6)*: BitTorrent is a communication protocol for P2P file sharing, which allows users to transfer data

Table 8 IoT Malware-Characteristics, Protocols and Programming Languages

Category	Malware	Characteristics																	Protocols								Programming Language								
		C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15	C16	C17	P1	P2	P3	P4	P5	P6	P7	P8	L1	L2	L3	L4	L5	L6	L7	L8	L9
Worm	Mirai			X		X		X				X				X		X	X		X						X	X							
	Hajime			X		X								X			X		X					X			X								
	Aidra						X												X								X								
	Darlloz/Zollard						X												X										X						
	Satori			X				X					X							X						X		X							
	Sefa							X											X								X								
	Okane							X											X								X								
	Okiru							X											X								X								
	ZHtrap				X														X								X								
	Persirai						X							X						X					X	X	X								
	Gitpaste-12			X									X						X									X							
	Moose			X	X														X									X							
	Shishiga							X											X			X	X	X							X				
	Mozi							X											X					X			X								
	Carna						X												X								X								
	Echobot							X				X			X				X			X				X	X								
	Wicked							X											X								X								
	Masuta							X											X								X								
	Tori			X															X									X							
	Bushido								X										X								X								
	JenX								X							X				X						X		X							
	Miori								X										X								X	X							
	Sora							X												X							X								
	Omni							X											X								X	X							
	Fritzfrog			X																X		X						X							
	TheMoon				X															X						X	X								
	Yowai																		X								X								
	OMG				X																		X				X								
	Owari							X											X								X								
	Ouija							X											X								X								
Spyware	VPNFilter	X	X			X							X					X		X		X				X				X					
	Psybot							X						X					X	X		X					X					X			
	Gamut	X																	X													X			
	Hide and Seek		X									X							X	X						X	X								
	Xarcen/XORDDoS							X				X	X													X	X								
	Spybot						X							X					X								X								
	Skeeyah			X																X							X								

Table 8 (continued)

Category	Malware	Characteristics																	Protocols								Programming Language								
		C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15	C16	C17	P1	P2	P3	P4	P5	P6	P7	P8	L1	L2	L3	L4	L5	L6	L7	L8	L9
Ransomware	Necurs	X						X												X												X			
	Cr1ptT0r			X																	X								X						
	Hades							X											X								X								
	Razor			X																X							X								
	Lulz								X										X										X						
	Muhstik								X											X									X						
Backdoor	Bashlite						X												X	X							X								
	Kaiji							X											X			X						X							
	Tsunami	X					X																				X								
	IRCflu							X														X						X							
	Brickerbot		X																X			X													X
	IoTReaper/IoTroop			X		X	X												X			X							X		X				
	Elknot/BillGates/ Mayday							X					X				X					X				X							X		
	Gr1n							X											X								X						X		
	Setag													X						X													X		
	Karu							X												X									X						
	InterPlanetaryStorm							X														X						X							
Trojan	Blueborne								X																	X			X						
	ProxyM				X																		X						X						
	Luabot				X														X												X				
	Emotet	X																					X				X								
	AirDropBot/ Cloudbot							X											X								X								
	Leet									X										X							X								
	Pnscan							X												X		X					X								
	dark_nexus								X										X								X								
	Hydra							X											X			X					X								
	Demonbot							X												X							X								
	APEP							X											X								X								
	Ares							X											X														X		
	Kluh							X														X						X							
	Qbot	X						X												X							X								
Virus	Silex		X																X			X													X
	Amnesia	X					X						X							X														X	
	Wifatch						X												X							X				X					
	Joker							X												X							X								
	HEH							X											X			X						X							

or files in a decentralized manner [146]. Nevertheless, this is also affected by IoT Malware like Shishiga.

Shishiga [147] uses four protocols, including BitTorrent, for infecting the devices. In this malware, the infection vector is the prevalent brute-forcing attack [147].

7. *UPnP (P7)*: Universal Plug and Play (UPnP) is a protocol that permits the devices available on the network to open as well as close ports automatically to connect to each other [154]. Even though UPnP is not widely attacked by IoT malware, Persirai, one worm malware, uses this protocol to affect IoT devices.

   Persirai malware targets IP cameras with open Universal Plug and Play (UPnP) ports, and once it is infected, it connects them to a command and control server [150]. To avoid these attacks, researchers usually suggest disabling UPnP services.
8. *Customized protocols (P8)*: Sometimes, the IoT malware creates a communication protocol with the help of binary commands. These customized protocols are mainly created by IoT malware belonging to the worm category, including Persirai, TheMoon, etc.

   In [15], customized protocols and other communication protocols used by IoT malware are discussed. Moreover, the authors have mapped the IoT malware that uses these protocols.

IoT malware and its mapping to protocols are illustrated in Table 8.

6 IoT malware

1. *Mirai*: Mirai is a self-propagating worm which infects vulnerable IoT devices by exploiting CVE-2020-10173, CVE-2020-5902, CVE-2020-7115, CVE-2020-7209 [172] etc. Once infected, the malware controls the devices using command and control (C&C) servers and claims the device as its own by removing the existing malware from it [173]. Mirai has a replication module and an attack module, where the replication module focuses on spreading the malware. The attack module executes various attacks like DDoS attacks, click fraud [174] etc. Interestingly, the malware uses a few Russian strings in its samples.
2. *Hajime*: Hajime is a Mirai variant which scans TCP port 8291 and leverages vulnerabilities like CVE-2018-14847 and CVE-2018-7445 for attackers to read and write arbitrary files. Furthermore, it can also perform brute-force attacks [175, 176]. According to researchers and industrialists, the malware uses a two-part system where the first part is a file transfer that copies a more considerable download program. The second part downloads, contact the P2P network and initiates a mass vulnerability scan [177].
3. *Aidra*: Aidra, an IoT malware, is known as an “IRC-based mass router scanner exploit” with an open-source code [178]. It is responsible for new malware like IRCTelnet as it lifts portions of source code from Aidra [179]. Researchers name it Aidra, and the malware author calls it LightAidra. Aidra is known for executing DDoS attacks and coin mining. The malware requires two servers, one for binary hosting and the other to issue commands to the botnet. As persistence is not supported, a device reboot can remove the malware [180].
4. *Darlloz/Zollard*: Darlloz infects the IoT devices by exploiting a PHP vulnerability, CVE-2012-1823 [181–183] and scans the device to check the presence of another IoT malware, Aidra. If any related files are discovered, the malware deletes them and blocks the ports used by Aidra [138]. Another version of Darlloz, “cpuminer,” mines coins like Mincoins or Dogecoins from the device [184].
5. *Satori*: Satori is a Mirai variant that exploits vulnerabilities like CVE-2014-8361), Remote Code Execution vulnerability [185] in IoT devices like routers. Since this malware is a Mirai variant, some attack libraries from Mirai are taken for performing UDP Flood, SYN Flood, TCP ACK Flood, and GRE Flood attacks [186]. Moreover, Satori malware is responsible for mining Ethereum [95].
6. *Sefa*: ThinkPHP is a Chinese open-source PHP framework, and the remote code execution vulnerability within this framework results in various malware attacks on IoT devices [187]. Among the IoT malware that exploits ThinkPHP vulnerability, BlueHero and Sefa are the widely known [188]. WORD, a member of the KS hacking group, has previously worked with WICKED malware, later focused on the SEFA botnet for a comprehensive attack [189].
7. *Okane*: Okane is an IoT malware propagating similar to Mirai where weak credentials are brute-forced, or 0-day exploits are used on vulnerable IoT devices [190]. In addition to the existing DDoS attacks, two new DDoS methods, including attack_method_tcpxmas and attack_method_std, are also considered in this malware. Moreover, some unusual entries root/t0talc0ntr0l4!, admin/adc123 and mg3500/merlin were uncovered on the brute force lists of the malware [191].
8. *Okiru*: Okiru, a Mirai variant, is considered the first malware to target IoT devices with Argonaut RISC Core (ARC) processors. This malware adds a more extensive set of credentials and an encrypted brute force module in addition to the existing functionalities of Mirai malware. Moreover, it has similarities to another Mirai

variant known as Satori. It has been floating around since 2018, and similar to Mirai, it is mainly for DDoS attacks [192]. Since the malware is built upon the existing Mirai malware, researchers believe it can be further modified to create a new variant.

9. *ZHtrap*: ZHtrap is an IoT malware that implements a honeypot mechanism for capturing attacks from other botnets and using the gathered data to hijack their infrastructures. Vulnerabilities exploited by this malware includes CVE-2020-25506, CVE-2021-27561, CVE-2021-27562, CVE-2021-22502, CVE-2019-19356, and CVE-2020-26919 [193, 194]. Moreover, ZHtrap uses a Tor C&C server to communicate with other botnet nodes and hide malicious traffic. The malware is known for performing DDoS attacks and executing additional malicious payloads [195].
10. *Persirai*: Persirai is an IoT malware that mainly targets vulnerable IP Cameras based on Original Equipment Manufacturer (OEM) products [196]. This malware uses various vulnerabilities, including CVE-2017-8221, CVE-2017-8224, CVE-2017-8222, CVE-2017-8223, and CVE-2017-8225, for exploiting the Universal Plug and Play (UPnP) enabled devices with open TCP port 81 [197]. Once infected, the device communicates with the C&C server to download software for being a part of the botnet that executes UDP-based DDoS attacks. Moreover, this malware can also deploy the command injections and infect other IP Cameras [198]. To avoid detection, the malware deletes itself once executed and runs only in the memory. Interestingly, to prevent other hackers from accessing the device, the perspire author blocks the exploit they used and keeps the infected device to themselves [199].
11. *Gitpaste-12*: Gitpaste-12 is an IoT malware that targets GitHub and Pastebin and is named after 12 known vulnerability exploits CVE-2017-14135, CVE-2020-24217, CVE-2017-5638, CVE-2020-10987, CVE-2014-8361, CVE-2020-15893, CVE-2013-5948, EDB-ID: 48225, EDB-ID: 40500, CVE-2019-10758, CVE-2017-17215 [200] within the worm. The malware performs different activities, including removing defence mechanisms like SELinux, firewalls, attack prevention, monitoring software, etc. Furthermore, it is used for cryptocurrency mining and other attacks, mainly targeting a /8 CIDR range of IP addresses [201].
12. *Moose*: Moose is an IoT malware that primarily targets MIPS and ARM-based IoT devices and creates a botnet to steal unencrypted network traffic and provide proxy services to the operator [202]. According to the researchers, Moose spreads itself using the name “elan2” [203]. Researchers also discovered that the botnet could create fake social media accounts and uses random numbers or letters as user names [204]. The malware then uses these capabilities to perform illegitimate view counts, likes and followers in various social media accounts. Moreover, DNS hijacking and Man-in-the-Middle (MitM) attacks are also executed by this malware citeNJCCICTh15:online. However, unlike most IoT malware, Moose has no persistence on the target device [203].
13. *Shishiga*: Shishiga is an IoT malware targeting IoT devices and exploiting Telnet and SSH ports using a brute-force attack. Once the device is infected, the malware sets an HTTP server and uses a BitTorrent protocol to search for new versions of Shishiga files to get updated with the latest version [205]. Shishiga uses the Lua programming language, which offers a more flexible design [206]. Over a short period, researchers witnessed minor changes in the malware with the rewritten module, which indicates that the malware is still creating new variants [207].
14. *Mozi*: Mozi is a P2P botnet that utilizes a BitTorrent-like network and targets IoT devices like DVRs and networking equipment using various unpatched vulnerabilities and weak Telnet credentials [208]. The primary aim of Mozi is to launch DDoS attacks in addition to the other attacks, including spamming, data exfiltration, cryptocurrency mining, DNS spoofing, HTTP session hijacking and payload execution [209, 210]. Researchers identified that the DHT configuration modules in this malware could help develop the codes for new functional nodes [211].
15. *Carna*: Carna is an IoT malware developed for measuring the Internet extent by naming it “Internet Census of 2012”. Carna is named after the Roman deity to protect inner organs and health. Like most IoT malware, devices with default passwords or no passwords are exploited by this malware. The data collected, including the IPV4 addresses after the attack, was compiled into a gif depicting the internet usage for 24 h [212, 213].
16. *Echobot*: Echobot is another variant of Mirai that uses 70 different exploits for its infection vectors [15, 214] and also is entirely modular, i.e. new exploits are added and removed by its author quite frequently. Echobot uses exploits available in cameras, DVRs, routers, video conferencing equipment, etc. and was built for all CPU architectures. To infect the most devices possible, this botnet employs both dictionary assaults and exploits. Latest updates to Echobot malware include network device exploits that are more than 10+ yrs old to target these old systems which remained in service and whose vulnerabilities were never patched.
17. *Wicked*: Unlike most IoT malware, Wicked uses known exploits like CVE-2016-6277 and CVE-2018-10561 instead of brute-forcing the vulnerable target devices. The malware exploits the device based on

ports 8080, 80, 8443, and 81 and uploads a payload [215]. Since the malware's code includes a string called "SoraLOADER," researchers consider it a spreader for the IoT malware, Sora, a Mirai variant. Moreover, it is also identified that the malicious website with the malware code contains the keyword "Owari," and the payload delivered is the Omni bot. Accordingly, it would appear that Omni, Owari, and Sora are all related to the Wicked bot [216]. Wicked also exhibits persistence, making the devices persist the malware [217].

18. *Masuta*: Masuta is a variant of Mirai that uses a modified version of the Mirai botnet whose cipher is altered, which is used to initiate the attacks. Utilizing a built-in list of common passwords and default credentials, it employs strategies similar to Mirai to circumvent the security of the targeted IoT devices [218].
19. *Tori*: Torii botnet is named after the Japanese word "gate" as it uses Tor and a network of devices to obscure network traffic [219]. After VPNFilter and HNS(Hide and Seek), this is the third IoT botnet that exhibits persistence. Its removal is possible only by resetting the device to its default configuration [220]. The malware binaries are downloaded via HTTP or FTP protocols, and for maintaining persistence, it uses at least six techniques simultaneously, including automatic execution through injected code into bashrc, "@reboot" clause in crontab, System Daemon, modification of the SELinux Policy Management, /etc/inittab [221]. Once this is done, the second-stage payload is executed and connected to the C&C server and performs different attacks like exfiltrating data, encrypting communication, and utilizing anti-debugging techniques [222].
20. *Bushido*: Bushido botnet is a variant of Mirai that offer a DDoS-for-hire service. It uses different combinations of usernames and passwords from Mirai, allowing it to target other vulnerable devices that Mirai cannot affect. Also, it has 13 attack options, whereas Mirai has only 10 [223].
21. *JenX*: JenX is a DDoS botnet that uses hosted servers to identify and infect new devices leveraging these three known vulnerabilities (CVE-2017-17215, CVE-2015-2051 and CVE-2014-8361), which have gained popularity in IoT botnet world [133, 224].
22. *Miori*: Miori malware propagates in two methods: via a vulnerability known as Remote code execution present in the ThinkPHP framework(CVE-2018-20062) or brute-forcing the open Telnet ports. Once the device is infected, rather than the binary-based version for communicating to the C&C server, the malware uses a text-based protocol for encryption [225]. Moreover, a console will be created to initiate the Telnet for performing brute-force on other IP addresses and perform distributed denial of service attacks [226].
23. *Priority*: There are no online resources for this malware that we can discover.
24. *Sora*: Sora is a variant of Mirai designed to exploit two vulnerabilities (CVE-2017-17215 and CVE-2018-10561), allowing it to execute remote code execution and manage the infected devices. Once the device gets infected, In the first stage, a downloader is dropped from the C&C server for delivering and executing the payload, and in the second stage, the attack chain is initiated [227].
25. *Omni*: Omni, an updated version of the IoTReaper, has the same network architecture format and is widely infected in the Polycom HDX devices for audio and video conferencing [228]. Since the open-source packages, including wget and busy box, are available in the devices' embedded firmware, attackers find it easy to download binaries. The infected devices are then used to launch brute-force and DDoS attacks and as proxy devices for routing malicious communications [229].
26. *Fritzfrog*: FritzFrog is a P2P botnet decentralized in nature with more than 20 variants detected in the wild [230]. The malware brute-forces the SSH server of vulnerable devices and executes in memory to evade detection mechanisms. Moreover, the malware is capable of propagating over the SSH protocol. Since the primary goal of FritzFrog is to mine cryptocurrency, a monero miner, XMRig, is deployed and linked to the public pool web.xmrpool.eu through the port 5555 [231].
27. *TheMoon*: TheMoon is an IoT P2P worm that uses a command execution vulnerability to exploit its victims; it explicitly targets Linksys and Asus routers and uses a backdooring mechanism to ensure that other IoT botnet will not infect the same device [15, 232]. The command execution vulnerability allows TheMoon to send malicious UDP packages to vulnerable routers, bypassing authentication processes and executing code on the device, taking it over from the device owner, and it will add new firewall rules to make sure the adversary can access the device remotely as well.
28. *Yowai*: Yowai is an IoT worm and botnet based on Mirai exploit websites built using the ThinkPHP open-source framework to compromise web servers using dictionary attacks on default credentials and take control of these routers for distributed denial of service attack [233].
29. *OMG*: OMG is a variant of IoT malware Mirai and keeps its various capabilities, including usage of brute force for logging in open Telnet, SSH and HTTP ports, DoS attack, etc. However, OMG turns the devices into proxy servers commonly used for performing malicious operations [234]. Once initialized, it connects to the C&C port 50023 and sends a message (0x00000000) to recognize itself as a new bot in the

botnet. Then, the server sends a string that mentions the command on how the device can be used as a proxy server [235]. Interestingly, OMG is the foremost Mirai variant that comprises DDoS functionality and the capability to set up proxy servers [236].

30. *Owari*: Owari is a variant of Mirai that leveraged CVE-2017-17215 to exploit more than 18,000 infected devices to perform a DDoS attack. It uses a MySQL server for C&C, allowing attackers to keep interacting with infected systems [237, 238].
31. *Ouija*: Ouija is a botnet that uses stager script, which is, in most cases, bash downloader scripts to download malicious payloads and execute them for infection. After payload execution finishes, it deletes the initial payload from disk using rm -rf command [239].
32. *VPNFilter*: The VPNFilter malware is a multi-stage, modular worm with various features to support operations for intelligence gathering and destructive cyberattacks. It was primarily used for corporate espionage and not to create large-scale DDoS attacks. It can monitor the SCADA system, map all a company's local networks, and create a reverse VPN that allows botmasters to connect remotely and target a company's internal network. It can also initiate a MITM attack by redirecting HTTPS traffic to HTTP for eavesdropping on the communication. It is a complex botnet categorized as an Advanced Persistent Threat (APT). It uses HTTPS and TOR to communicate with its botmasters. It can add virus on the fly to Windows exe file in clear traffic, encrypt data, and exfiltrate it [15, 240].
33. *Psybot*: Psybot is a centralized IRC botnet that operates by brute-forcing SSH and telnet credentials using a dictionary with roughly 6000 users and 13,000 passwords. It targets MIPS architecture and also uses the D-link bypass exploit as well. It can execute DDoS attacks using UDP, ICMP and Syn flood features as well [11, 15].
34. *Gamut*: Gamut Botnet is a decentralized network of Trojans specializing in sending spam emails that attempt to build rapport with the recipients. The Gamut Botnet malware payloads are downloaded when the targeted users open the spam email. That will further compromise the computer network. Currently, Necurs and Gamut are responsible for 60, and 37 percent of spam email traffic generated globally [75, 241–243].
35. *Hide and Seek*: Hide and Seek is P2P botnet that establishes communication between peers via a customized P2P protocol [15]. Hide and Seek botnet is not designed for DDoS attacks; however, espionage behaviour is observed in it. When it was first discovered and analyzed, Hide'n Seek could not persist after a reboot of its victim. However, three significant features were added in October 2018: first, Hide and Seek gained persistence through the botnet's daemonization. Second, the malware acquired the capability to infect Android devices through the ABD protocol. Additionally, it gained the capacity to set up Coin-Miner software and command its botnet to mine the cryptocurrency Monero. This protocol uses techniques to restrict researchers' ability to analyze the network. Each peer has a maximum number of constantly updated peers in its list, typically 512 (customized to the peer's available memory). A full update of the list takes about 18 h. A dedicated crawler has to be created by researchers to speed up the scan of the network. However, its size cannot be estimated with any certainty due to the quickly evolving nature of the network. Also, to prevent poisoning attacks, every communication and update are signed with ECDSA. Code from both Mirai and Reaper is reused in Hide and Seek, including the scanner from Mirai and certain exploits from Reaper.
36. *Xarcen/XORDDoS*: XOR DDoS is a small Chinese botnet targeting Linux systems (IoT and servers). It attacks the network by producing large amounts of data, such as nonsensical strings in the SYN and DNS [15]. It uses XOR-based encryption for its communications. XORDDoS is known for employing Secure Shell (SSH) brute force attacks to take remote control of target devices [244]. XORDDoS uses evasion and persistence mechanisms that make its operations robust and stealthy. It incorporated various evasion tactics, including hiding the malware's activities, anti-forensic techniques to break process tree-based analysis, etc. In recent campaigns, XORDDoS conceals malicious activity by overwriting sensitive files with a null byte. It is also able to support various Linux Distributions through multiple persistence mechanisms.
37. *Spybot*: Spybot is a worm that typically infects computers via peer-to-peer (P2P) file sharing, more specifically via the Kazaa file-sharing network [245]. It can infect computers with weak administrative credentials and spread via various standard backdoor Trojan horses. Hackers occasionally use the worm to create simple-access programmes for IRC and FTP channels.
38. *Skeeyah*: Skeeyah is a trojan-style malware that infiltrates computers covertly and gives cybercriminals control over compromised systems. It usually facilitates the infiltration of other malware on the infected system by opening backdoors to the victims' devices. This infection may result in several issues, such as privacy concerns and subsequent computer infections [246].
39. *Necurs*: Necurs is modular botnet malware capable of various threats such as spam distribution, information theft, ransomware and disabling security services and elements [75]. Necurs is primarily a botnet-for-hire that

can spread any malware a client desires. This includes the well-known GameOver Zeus trojan, which over a decade ago, infected the internet, as well as the Dridex malware used by Evil Corp and others. It gives its zombie computers much freedom by using a domain generation algorithm, or DGA, to generate 2,048 potential domains every four days. Necurs can prevent antivirus updates on older computers, which can have many unintended consequences [247].

40. *Cr1ptT0r*: Cr1ptT0r is Ransomware built for embedded systems targets network attached storage (NAS) equipment exposed to the internet to encrypt data available on it [248]. The DNS-320 router created by D-link has been used to spread the Cr1ptT0r Ransomware. Despite still being used by many computer users, this router has been decommissioned due to the numerous vulnerabilities it was linked to. In 2018, a hard-coded backdoor into this router was discovered, giving hackers access to the victim's network without authorization.
41. *Hades*: Hades ransomware is a human-operated ransomware tool used in targeted attacks on large organizations. It is an extension of the WastedLocker ransomware, created to get around the US government's sanctions. It was later rebranded as Phoenix Locker. Hades and WastedLocker share a lot of code, although Hades has some minor feature additions and code obfuscation [249].
42. *Razor*: Razor is Ransomware that encrypts files with the ".razor" extension to prevent access to data (files, photos, and videos). Then, it attempts to extort money from victims by demanding a "ransom" in the cryptocurrency Bitcoin in exchange for access to their files [250]. To encrypt files, it looks for those with specific file extensions. Important productivity documents, pictures, videos, and files like .doc, .docx, .xls, and .pdf are among the files it encrypts. The infection will alter the extension of these files to Razor when discovered, rendering you unable to access them. Each encrypted file's name is changed by this Ransomware to the following format: name.id-ID.razor
43. *Yagi*: There are no online resources for this malware that we can discover.
44. *Lulz*: Lulz is a ransomware that encrypts the victim's data with the AES-256 encryption algorithm, changes their wallpapers, renames the encrypted file names and demands a payment [251]. The authors of Lulz advertise it as RaaS (Ransomware-as-a-Service). Once within the victim device, It encrypts 195 file types on the local and connected devices. The Ransomware is written in Golang, allowing the payload to evade machine learning and signature-based antivirus engine detection mechanisms. It is also designed to leave the computer once it recognizes it is running in a sandbox or virtual environment
45. *Muhstik*: Muhstik is another variant of Mirai that has existed since at least 2018 and is reported to infect IoT devices using web application vulnerabilities. Cryptomining and DDoS attack services are used to monetize the botnet. Since its creation, Muhstik has constantly used the same infrastructure and relies on IRC for command and control. Although home routers are the primary means of IoT device proliferation, there have been several attempts to propagate exploits for Linux servers as well [252]. DD-WRT, the Tomato router, and the GPON home router are among the routers that are targeted. Some of the vulnerabilities exploited by Muhstik include Oracle WebLogic Server bugs (CVE-2019-2725 and CVE-2017-10271), Drupal RCE flaw (CVE-2018-7600) and Lua sandbox escape flaw (CVE-2022-0543).
46. *Bashlite*: Bashlite is also known as BASHLITE, Gafgyt, Lizkebab, Torlus, LizardStresser, Qbot, Bash0day and Bashdoor was developed as an IRC backdoor that searches IP address ranges for vulnerable devices that run the BusyBox shell intending to infect them. It can perform various DDoS attacks like Syn and UDP Flooding [15]. The Gafgyt variants were able to exploit multiple device vulnerabilities like CVE-2017-18368, CVE-2017-17215, CVE-2014-8361 etc. It spreads by brute-forcing passwords and usernames from a built-in dictionary. The malware connects to random IP addresses and makes login attempts, reporting any successful ones to the command and control server. Since it was written in C, it can target different computer architectures; binaries of the Bashlite family have been discovered in all IoT CPU architectures like ARM, MIPS, SuperSH etc.
47. *Kaiji*: Kaiji is a malware that was created expressly to infect Linux-based servers and smart Internet of Things (IoT) devices before abusing these systems to execute DDoS attacks [149]. The botnet is not currently able to infect unpatched devices via exploits. Instead, IoT devices and Linux servers that have left their SSH port open to the internet are targeted by the Kaiji botnet's brute-force attacks. The "root" account is only targeted because the botnet needs root access to infected devices to alter raw network packets for DDoS attacks and other operations.
48. *Tsunami*: Tsunami is an IRC centralized botnet. According to Researchers, It is an evolution of Chuck Norris malware because their binaries include a lot of common strings. Additionally, some of their C2s' IP addresses are the same for both pieces of malware. It uses the Tsunami/Kaiten open-source DDoS protocol to provide DDoS services [15].
49. *IRCflu*: IRCflu is an open-source IRC bot which has a flexible message & command handler. It is currently

used as a backdoor to a compromised SSH server. The IRCflu bot can, among other things, carry out shell commands that are sent to it in an IRC private message. Attackers probably intended to use this IRCflu to gain access to infected machines and maybe download further malware, like cryptocurrency miners, or to provide remote access to the botnet for sale to the highest bidder. IRCflu has never been utilized in this manner, indicating that hackers vary their attack strategies by using legitimate technologies to elude detection by security solutions [253].

50. *Brickerbot*: BrickerBot is an IoT malware that mainly focuses on altering the device's firmware rather than concentrating on DDoS attacks like most IoT malware. This is done by performing dictionary attacks and running various malicious Linux commands, including altering the device's storage and kernel parameters, restricting internet connection, tampering with its performance, and removing all files on the device that cause permanent damage to the device. BrickerBot has two versions, one which targets IoT devices running BusyBox with vulnerable Telnet or Secure Shell (SSH), and the other that targets Linux-based devices which has TOR exit nodes to evade its activities [254, 255]. Since it affects the firmware, the device must be replaced or reinstalled with hardware [256].
51. *IoTReaper/IoTroop*: IoTReaper is a botnet that incorporates some code from the well-known Mirai botnet but does not crack any passwords [257]. Instead, it is solely concerned with exploiting vulnerabilities in IoT devices. At the moment, IoT Reaper focuses on nine unique firmware flaws impacting cameras, video recorders, and home routers made by companies including Linksys, D-Link, Vacron, Nuuo, Netgear, AvTech, Maginon, and Avacom, among others. New vulnerabilities could be added anytime as the malware is still being tweaked and upgraded. The goal of the botnet and its impact were unknown at the time this paper was being authored. However, the following cyberattacks are possible, including large-scale DDoS and the facilitation of other malware that targets, disrupts, or disables the systems it is running on.
52. *Elknot/BillGates/Mayday*: Elknot is also known as the BillGates Trojan, which has been used to launch DDoS attacks on devices with insufficient security. Both Linux and Windows platforms are susceptible. Elknot allows its controllers to carry out any attacks they desire once it completely controls an infected computer's functionality. It can perform several attacks, including HTTP Flood (Layer7), DNS reflection floods, TCP Flood, ICMP Flood, and UDP Flood. Criminals can rent Elknot to create their versions of the threat, disrupt machines, and carry out destructive actions anywhere they choose [258].
53. *Gr1n*: Gr1n is a botnet that uses default user and password combinations to attack IoT devices through Telnet. Researchers claim it is built in C and appears to deploy itself first as a downloader (through bins.sh or getbins.sh) before downloading several executables for various CPU architectures [259].
54. *Setag*: Setag is a backdoor that can initiate DDoS attacks while stealing system data. It has also been observed utilizing an exploit for the Apache Struts 2 remote code execution vulnerability CVE-2017-5638. This malware checks for tampering and can prevent debugging. Additionally, this malware copies itself and changes the systems tools on the afflicted system, moving them to the /usr/bin/dpkgd directory. It drops a script into the /etc directory to make a copy of itself for persistence [260].
55. *Karu*: Karu is TDSS TDL4 backdoor malware that alters the Master Boot Record and tracks the user's online behaviour. It might also download additional malicious files, weakening the compromised system. This backdoor includes mutexes to ensure that only one copy is active. For it to load before the operating system starts up, it alters the Master Boot Record (MBR) of the afflicted system. When certain strings are identified in the Web address, it tracks the user's browsing patterns and sends the data to particular URLs. Additionally, it alters the search engine's returning results to deceive visitors into clicking dangerous links or seeing adverts [261].
56. *InterPlanetary Storm*: InterPlanetary Storm cross-platform P2P botnet infects Mac, Android devices, Windows, Linux machines and IoT devices. Threat actors had used it to infiltrate targets through dictionary attacks on SSH servers and execute PowerShell code on compromised targets. It is based on the InterPlanetary File System (IPFS), a distributed file system protocol for storing and exchanging data. Once compromised, the systems are set up to function as socks5 proxies. As a result, the infected devices join a peer-to-peer network and communicate directly, strengthening the botnet's resistance to takedown attempts [262, 263]. This raises the likelihood that the botnet's developers may charge other cybercriminals to use them as proxy servers for their traffic.
57. *Blueborne*: BlueBorne, an IoT malware, can sniff or redirect the traffic through "air-gapped" networks between Bluetooth-enabled devices for accessing data and spreading malware laterally to adjacent devices [98]. The malware first locates the Bluetooth devices and identifies the device's MAC address, Operating System and adjusts its attack accordingly [264]. It can

initiate a man-in-the-middle attack [265] and exploits the devices by using 8 vulnerabilities, including CVE-2017-1000251, CVE-2017-1000250, CVE-2017-0785, CVE-2017-0781, CVE-2017-0782, CVE-2017-0783, CVE-2017-8628, CVE-2017-14315 [264].

58. *ProxyM*: ProxyM is a malware that mainly targets Linux devices and launches a SOCKS proxy server on an infected device for anonymously performing malicious activities [74]. Moreover, this malware was used for relaying web traffic and hacking websites using XSS (Cross-Site Scripting), SQL injections, and Local File Inclusion (LFI) [74]. Different variants of Proxym are arising, and the malware targets various architectures, including MIPS, ARM, PowerPC etc. [266], which infects routers, set-top boxes, and other similar equipment.
59. *Luabot*: LuaBot is the first trojan entirely coded in Lua language targeting Linux platforms to recruit them in DDoS botnet. It is capable of performing Layer 7 DDoS attacks. It is a malware that targets Linux systems, loT devices, and web servers and is similar to Mirai in that it makes infected systems into bots that are part of a larger botnet under the attacker's control. On the target, the basic malware sets up a SOCKS proxy. The SOCKS proxies used by this botnet's author and operator appear to be available for purchase by other malware operations so they can conceal the source of their attacks [267, 268]. Luabot has the appearance of an ELF binary.
60. *Emotet*: Emotet is a Trojan propagated through spam emails. Malicious scripts, document files with built-in macros, or malicious links can deliver the infection. The authors of Emotet have exploited the malware to build a botnet of compromised machines to which they sell access using an infrastructure-as-a-service (IaaS) model, also known as MaaS (Malware-as-a-Service), Cybercrime-as-a-Service (CaaS), or Crimeware in the cybersecurity world [269]. Emotet is also renowned for providing ransomware operations with access to compromised systems. To avoid being discovered and analyzed, Emotet employs several techniques. Notably, Emotet can determine whether it's operating inside a virtual machine (VM) and will become inactive if it finds a sandbox environment [270].
61. *AirDropBot/Cloudbot*: AirDropBot malware targets infecting as many IoT devices as possible and behaves similarly to Mirai and Gafgyt malware. Due to this reason, researchers first ignored its presence. However, the malware behaves in two ways where one targets small devices by acting as bots, and the latter acts as a vulnerability scanner for larger systems. Even though it is still not in the last development stage, the main objective is to infect devices and eliminate its competitors [271].
62. *Leet*: Leet is the first IoT malware that rivals the Mirai, and it is named after a character string in the payload. Unlike Mirai, which uses hardcoded SYS file sizes, this malware traffic was developed by regular SYN payloads and large SYN packets of around 799 to 936 bytes [272]. Moreover, this malware takes data from actual system files and sends it to the target by embedding it in the TCP packets used for DDoS attack [273].
63. *Pnscan*: PNScan is an IoT Malware mainly targeting ARM, MIPS, or PowerPC architectures routers in the IP Address Block 183.83.0.0/16 by brute-forcing using three sets of credentials. Once the device is infected, it forks several times and creates various files within the device. Furthermore, the threat listens to the TCP ports targeting the IP range and sends HTTP/1.1 requests through SSL to twitter.com on port 443 to conceal its malicious network traffic [274]. Interestingly, the malware was upgraded, and the new version pnscan2 performs the brute-force attack using a special dictionary [275].
64. *Dark Nexus*: Dark Nexus is a botnet that infiltrates various devices, including routers (from Dasan Zhone, D-Link, and Asus), video recorders, and thermal cameras, by using credential stuffing attacks [276]. It employs a DDoS technique that masks traffic as harmless browser-generated traffic and utilizes synchronous and asynchronous Telnet scanners for infection and victim reporting. It uses socks5 proxies, possibly renting access to the botnet. The device's reliability and proper operation are maintained using a debugging module available in the botnet [277].
65. *Hydra*: Hydra was router malware that functioned automatically as an open-source tool. IRC handled it, and its primary function was to use brute force to get access to routers to launch DDoS attacks. A built-in list of default passwords and a D-Link authentication bypass exploit might be used to gain access to the router. Before compiling the code, the malicious user had to alter one of the source files to add the URL for the C&C IRC server and the link to download the malicious malware [278].
66. *Demonbot*: Similar to Mirai, DemonBot is a distributed denial-of-service (DDoS) botnet. It does not behave like a worm, in contrast to Mirai, and spreads via centralized servers. It can respond to commands to launch UDP (randomized) or TCP-based DDoS attacks and an STD (UDP fixed payload) attack. Additionally, it supports the STOMP command, which initiates an assault in sequence, starting with STD and moving through UDP and TCP. It specifically targets unprotected Apache Hadoop systems through a bug in Hadoop's YARN ("Yet Another Resource Negotiator") component.

67. *APEP*: APEP is a variant of Mirai which spread by dictionary attacks via Telnet. Other than that, APEP can also propagate by exploiting the vulnerability CVE-2017-17215, which involves another RCE vulnerability and affects Huawei HG532 router devices, for its attacks [279].
68. *Ares*: The Ares Botnet spreads its malicious code by searching the internet for vulnerable STBs (Set-Top Boxes) that use a stripped-down Android OS version. The “Android Debug Bridge” must also be enabled on the IoT device for the Ares Botnet malware to penetrate successfully. If the Ares Botnet successfully connects a device to its network, it can take control of it and use it to look for other vulnerable STBs and spread the threat to them. It appears that the attackers are mostly mining cryptocurrency using the seized equipment. But such a sizable botnet may also launch extremely effective DDoS (Distributed-Denial-of-Service) assaults [280].
69. *Kluh*: Kluh is a malware that may infect Linux operating systems, and it was developed by the Chinese hacker collective known as ChinaZ. Infecting Linux-powered routers is its primary objective. It can launch DDoS attacks such as HTTP Flood, Spoofed SYN Flood, SYN Flood, and other DDoS attacks by sending mass requests to DNS servers [281].
70. *Qbot*: QBot is a banking Trojan used to steal banking information (banking passwords, information about online banking sessions, victims’ personal information, etc.). It is also called Qakbot, QBot, QuackBot, and PinkslipBot [282]. Qbot infects targets through a variety of attack vectors. Phishing emails with malicious files, attachments, or password-protected folders with the files attached are used to spread QBot. However, its creators have also created features that let QBot spread itself, avoid detection and debugging, and put other malware on infected computers. A dropper like Emotet has been seen to spread some malware variants. Most Qbot variants are VM-aware, and some feature polymorphic skills [283]. One of Qbot’s more recent tactics is that after infecting a computer, it activates a unique “email collector module” that harvests all email threads from the victim’s Outlook client and uploads them to a predefined remote server. Since the spam email pretends to continue an ongoing genuine email conversation, it is easier to fool consumers into clicking on infected files. Then these stolen emails are used for subsequent malspam operations [284].
71. *Silex*: Silex is a destructive malware that spreads and wipes devices’ firmware, requiring a whole firmware reinstallation to restore the device. The malware targets devices with ARM architecture and UNIX-like OS that uses default credentials [285]. The infection also drops the firewall rules, removes network configurations, flushes the IP tables, and halts the devices [96].
72. *Amnesia*: Amnesia is a centralized IRC botnet that can launch various DDoS attacks, including UDP and HTTP floods. It is very similar to Mirai and has the same ability to identify virtualized environments and delete itself from the machine when VM is detected using a command like “rm -rf”. This functionality is frequently found in Windows and Android malwares designed to hinder malware analysis. By taking advantage of a vulnerability in this company’s devices, it primarily targets TVT Digital DVR [15].
73. *Wifatch*: Wifatch was a P2P botnet exploiting weak credentials on telnet and SSH protocols [15]. It was also compiled for multiple architectures. The worm could look for and remove all previous infections and add a message to the logs warning the device owner and requesting that they change the IoT’s password. It is written in the Perl programming language. Wifatch botnet is a whitehat botnet and is not aimed at launching DDoS attacks but instead to safeguard the IoT devices from other botnets, as per the explanations from the malware authors.
74. *Joker*: Joker is a malware bundled with several unsuspecting apps distributed via the Google Play Store and other platforms. The malware secretly engages with ad networks to click on banner ads and sign up for premium subscription services. Joker can read the victim system’s SMS messages, contact lists, and device data. It gathers information from compromised networks, listens to private conversations, and sends it to a remote attacker [286] because it has a small code footprint and is, therefore, difficult to detect.
75. *Exo*: Exo, sometimes known as Exobot, is an Android trojan that can steal SMS messages, lock devices with a password (behaving like ransomware), and more. Exo is compatible with Android 4, 5, and 6. Moreover, malware buyers advertise that Exo can operate without root access and that consumers cannot remove it directly, necessitating a full phone reflash to remove it [287].
76. *Cereals*: Cereals is an IoT malware known for its peculiar characteristic of exploiting one vulnerability that resides in the message notification feature of the D-Link firmware of NAS and NVR devices. Using this vulnerability, attackers send malformed HTTP requests to the in-built server of the device and execute commands with root privileges. Moreover, the malware tries to patch the devices to prevent them from further hijacking [288].
77. *HEH*: Unlike most IoT malware, HEH does not exhibit attacks like DDoS or coin mining; instead runs shell commands for wiping all the device partitions. This

malware exploits the devices with open Telnet ports 23, 2323, and SSH ports by brute-forcing the credentials [289]. This is done to spread the malware and attain its activation mechanism [290].

7 IoT malware detection methods

Nowadays, IoT device security is ensured by using malware detection mechanisms and prevention methods. In this, we focus on two types of detection methods, including traditional detection methods and Learning-based detection methods. The best way to classify traditional IoT malware detection approaches is by considering two analysis techniques: dynamic and static. Even though these analysis mechanisms are also used in learning systems, we focus on the subtypes of machine and deep learning-based learning systems.

7.1 Traditional detection models

1. *Static analysis-based detection methods*: The static approach is conducted by examining the input samples without executing them so that the structure and different characteristics of the malware can be identified.

   Static-based disassembly analysis is developed by [168] for calculating similarities in the malware for classification. Disassembly won't work well if the samples are packed, so they were checked first to determine whether they are packed. The similarity is calculated for non-packed samples using the Jaccard index by extracting the samples' opcodes based on the opcode's N-grams. Once identified, a similarity matrix is created and based on it, and samples are visualized in a 2-D plane with t-SNE. Results proved that disassembly worked well as similar samples are mapped closely, and distinct samples are mapped far.

   A modular framework is introduced by [291] for automatic analysis and clustering of malware samples using various components, including eOrchestrator, Static analysis, deployment module, connection, dynamic analysis, clustering samples, and visualization. eOrchestrator is the main module that makes a pipeline that connects the rest of the modules. Once the sample is received, a static analysis module gets the information. The deployment module checks the analyzed file architecture, and the virtual machine activates if the architecture is supported. Then the dynamic analysis is done by executing the file for a certain amount of time, and the execution traces obtained are parsed. The similarity is identified with other obtained samples based on a threshold value and added to a similar cluster. In case the threshold is not reached, a new cluster is created.

   [292] developed a web traffic detection system-Owl-Eye that uses HMM (Hidden Markov Model) methods to calculate the web request's malicious score. The input web request was preprocessed, and the key-value pair was generated using a key handler and value handler. The extracted feature vectors are fed into four trained HMM modules: normality detection, abnormality detection, WAF (Web Application Firewall), and customized specific APIs detection modules. If a web request is found, the difference between an abnormal score and a normal score is calculated, and if it is greater than the threshold, it is considered an attack.
2. *Dynamic analysis-based detection methods*: Non-graph-based methods mainly deal with opcodes images as features and consider algorithms other than AI-based techniques.

   [293] introduced a dynamic analysis-based malware detection tool for a router called C500-toolkit, which emulates and analyzes both the web interface and OS of the firmware image of the router. This tool had three components: C500-Extractor, which extracts the firmware image extractor component, C500-Standardization, which standardizes the firmware image; and C500-Detector, which detects the malware in router firmware.

   [294] presented an automatic IoT runtime platform where users upload suspicious ELF files and dynamically analyze for malicious behaviour identification. This work emulates various architectures with QEMU (Quick EMUlator)), and the malicious files are identified. Moreover, the uploaded file's traffic logs and system calls are also generated.

7.2 Learning-based detection models

As mentioned above, malware detection mechanisms are not limited to traditional methods. Due to the promising advancement, researchers and industrialists have become more interested in IoT malware detection using deep learning and machine learning.

1. *Machine Learning-based methods*: Machine learning involves complex algorithms automatically learning and refining patterns from vast data. As it can enhance performance and develop 'intelligence' over time, it is widely used in most detection algorithms.

   In Machine learning methods, feature extraction is considered one of the most important steps as it determines the model's performance. Therefore, in this section, we classify different ML detection methods based on the type of features. It includes:

   - *Images*: As images possess thousands of pixel values, their relationship and correlation can help detect IoT malware.

An IoT malware classification using Haralick texture features and machine learning methods such as KNN (K-nearest neighbour), NB (Naive Bayes), and RF (Random Forest) is proposed in [100] where the dataset is converted into a grey-scale image followed by the creation of a GLCM (Gray Level Co-occurrence Matrix). Then, the textual features from the image were extracted using the five Haralick features, and ML methods were applied to them. Results proved that RF is the best classification method, which can be applied in all platforms and environments as images are used for detection.

- *Opcodes*: Opcodes, also known as instruction codes, are a part of machine language instruction that tells the processor the job to be done.

  Opcodes are used as features in [295] where a classification method known as a Fuzzy pattern tree is applied to detect malware using four datasets: IoT, Vx-Heaven, Kaggle, and Ransomware. The opcode sequence from the data set identified the beneficial features using the Class-wise information gain approach and control flow graph and applied with the Fuzzy pattern tree and Fast fuzzy pattern tree. To assess the model's competency, the authors compared it with state-of-the-art ML methods. Another work [101] also considers opcodes as their features from the malicious and benign samples, and the features extracted from the benign samples were saved in the detection dataset directly. In contrast, the features of labelled malicious samples were preserved in both the detection and classification dataset. Once the preprocessing is done, the detection model identifies whether the new unknown samples entering the system are malicious. If malicious, it will be stored in the classification model to find the malware family, and the result will show the malware family. The model was compared with the existing works and proved that the performance is better than the current models.
- *ELF*: Executable and Link Format is a file format for executables, DLLs, and shared objects in a Linux-based system that stores machine-independent and machine-dependent features.

  ELFs are considered features in [101] along with opcode features. This work finds characteristics from both types of features to make the model robust and get an accurate result.
- *Network Traffic*: Traffic moving across a network captured during dynamic analysis is the most prominent feature in IoT malware detection.

  EDIMA, proposed in [87] extracts the features from the incoming network traffic samples and classifies them using the ML Model Constructor, which is trained using the different ML algorithms with feature vectors and labels collected from the Packet Traffic Feature Database. When the number of devices is higher, the sub-sampling module is used where only a fraction of incoming traffic is considered. If some malicious activity is detected, based on the policies in the Policy Module, the network administrator determines the following actions to be taken, like blocking traffic, etc.
- *Hybrid features*: As static and dynamic features can help detect malware, a hybrid of these features is used for better effectiveness and performance.

  In [296], static features like permissions, API calls, etc., were extracted using the Androguard tool. Dynamic features like system calls were extracted by running the application in the Genymotion emulator. In this work, two novel techniques based on the distance from the malware cluster centre (Euclidean distance and l1-norm are used) and based on probability measures derived from kernel-based learning (KBL) are considered for the selection of adversarial samples. Three ML algorithms, such as SVM, RF, and Bayesian, were also used to identify the approach's effectiveness, proving that the KBL technique is better in all these algorithms.

2. *Deep Learning-based IoT Malware detection methods*: As machine learning algorithms need a separate feature extraction process, deep learning algorithms extract the features automatically. Therefore, this section discusses the top deep-learning algorithms used for IoT malware detection.

- *CNN*: Convolutional Neural Network, also known as Convnets, consists of numerous layers that process and extract features. The main advantage of this algorithm is its less computation than a regular neural network without losing the essence of the data.

  A hybrid intelligent architecture using Autoencoder and CNN is analyzed in [297] with the initial and training phases. Features of ransomware-related malware collected from different IoT devices are extracted using the Autoencoder to identify the essential features that contribute to malware detection. Then, hidden layer results were exfoliated in the Autoencoder environment, and random rules were used to make it available to CNN, which trains the data for malware classification. CNN is also used in the IoT malware detection-based model MTHAEL [1]. The opcodes from ELF files were disassembled using the object dump tool, and the opcode sequences thus obtained were applied with feature extraction models and fed into the Ensemble learner with CNN and RNN models. [298] presents a dynamic analysis for IoT malware detection, DAIMD, which uses the CNN algorithm for analyzing the images created from the behavioural data obtained from dynamic execution. Unlike most existing works, memory, system call, network, process, and virtual file system behaviours were analyzed in this work. The behaviours thus identified were compressed during feature preprocessing and converted into an image type. The outcome of the experiments indicated that the DAIMD model could accurately detect variant malware that risks IoT devices.

- *RNN*: Recurrent Neural Network handles sequential data and considers current and previously received input. The previous input is remembered in RNN due to its internal memory.

  [299] used an RNN-based deep learning approach for IoT malware detection on ARM-based malware files and benign files collected from the VirusTotal threat intelligence platform. However, a linguistics process was used in this work to convert every sample into a numerical sequence. Moreover, rather than the standard RNN model, Bidirectional Neural Networks were also evaluated. RNN is also applied in MTHAEL [1] as a base learner in the Ensemble model. [300] investigated the malicious network connections using an RNN-LSTM method which supports the firewall in the system. The malicious data is updated in the database for retraining the RNN using the NAdam Training Algorithm. Moreover, the firewall is also updated, and the connection is blacklisted. On the other hand, if the connection is benign, it is added to the whitelist connections neurons are applied to do it.
- *LSTM*: Long Short-Term Memory network is similar to RNN except that the operations within LSTM cells allow the LSTM to keep or forget information. Moreover, it tackled the problem of long-term dependencies of RNNs.

  [99] used an LSTM-based deep learning approach for malware detection where 32-bit ARM-based malware files and benign files of ELF format were fed into the object dump tool for decompiling, and the decompiled code was then pruned to extract the opcode sequence in each sample. Text mining based on TF-IDF was used to create feature vectors and fed into the LSTM model for classification. Another work [301] used a fastText model with two phases, such as (i) the learning phase, where a fastText model and Bi-LSTM perform learning on the dataset and (ii) the execution phase, where malware is classified based on the learning. Here, the opcodes and API function names were embedded using the fastText model, and labels were embedded with one-hot encoding. This multidimensional vector created in the preprocessing stage was passed to the input layer of Bi-LSTM and based on the learning process, the testing was done. LSTM is used along with RNN in [300] for the malicious network connection. Bi-LSTM deep learning model is presented in [118] for server-side malicious traffic monitoring. The packets captured are parsed by the network analyzer, extracting packet-level features, basic statistical features, and NetFlow-level features often observed for malware and benign programs. Once the extracted feature vectors are saved, they are used as inputs to train the Bi-LSTM deep learning model for malware detection. A hybrid obfuscated IoT malware detection method, HyMalD is proposed in [302], which uses a bidirectional long short-term memory (Bi-LSTM) and spatial pyramid pooling network (SPP-Net) for static and dynamic analysis. In this work, the Shannon entropy is first calculated as it is an indicator of obfuscated IoT malware. If it is less than the threshold, static analysis is performed by considering three steps: feature extraction, vector creation, and classification. However, suppose the Shannon value is less than the threshold. In that case, dynamic analysis is performed where similar stages are followed like static analysis, except in the second stage, where an image is created instead of a vector. This is done by executing the obfuscated malware files in a virtual environment.
- *Autoencoder*: Autoencoder is trained to learn efficient representations of the input data by reducing the size of inputs into a smaller representation. Unlike PCA, this algorithm is more efficient and learns underlying patterns.

  Autoencoder is used along with CNN in [297] where the results of the hidden layer were exfoliated using Autoencoder and applied with random rules for making it available to CNN for malware classification.
- *DBN*: Deep Belief Network uses probabilities and unsupervised learning to produce outputs containing undirected and directed layers.

  [9] that uses two different deep learning approaches based on Deep Belief Network, such as CDT-DBN and DDT-DBN, also has a separate feature extraction process. Components of the model include malware triggering, behavioural log collection, preprocessing, feature extraction, DBN training, and malware detection. The models were analyzed based on the number of hidden units and epochs. Results found that DDT-DBN performs better in a higher number of epochs with fewer hidden units, and CDT-DBN performs better when a lower number of epochs and lower hidden units.

3. *Hybrid detection methods*: In the hybrid detection method, two or more algorithms are combined for IoT

malware detection to rectify the drawbacks of one algorithm by uniting it with another algorithm. Even though some works don't yield good results when combined, researchers still use them to try new models.

In [128], a local IoT detection system is implemented in IoT clients using CNN, and a remote cloud classification system is assumed to be implemented with some ML algorithms in a cloud server. The malware binary is translated as a sequence of 8 bits and converted to a grey-scale image, then re-scaled into 64x64 for feeding to the input layer. The model's performance is then compared using two-class and three-class classifications, which shows that the two-class classification showed an accuracy of 94.0%, better than the three-class classification. The classification result is then delivered to the remote Cloud server for deeper analysis, which updates and distributes newly trained detectors to the IoT clients in a periodic manner.

A work by [303] has two stages: training and Inference phases. In the training phase, the latent representation, a compressed form of the input data, is constructed, which helps in the binary classification methods such as SVM (Support Vector Machines), KNN, DT, etc. Test data is fed into the encoder in the inference phase, and the output is passed to the classifier. As Autoencoder works similarly to PCA and t-SNE, those two methods are compared to identify whether the proposed model performs better. Moreover, the authors have combined three types of malware categories from different IoT devices to determine any difference in malware behaviour in other devices.

8 Challenges and research opportunities

Security in IoT has been a matter of concern, and most of the issues are identified as the lack of security standards and hardware issues. However, this section focuses on the challenges and future research directions in IoT Malware.

Instead of minor data theft, the primary objective of infecting IoT devices with malware is often to prepare for a big attack in the future. In contrast to Personal Computer (PC) malware samples, which typically target a single-machine type, IoT malware samples usually support a variety of CPU architectures. Even though malware detection for Windows has been extensively investigated, it presents several difficulties for the IoT industry. Although, the differences between PC and IoT malware in behavioural manners depend on the specific type of malware individually. There exist differences in the source code and architecture and in the operations as well, such as Mirai, a popular malware that compromises IoT devices. The infection phase that creates Mirai botnets in a traditional infection phase is distinct from the phase that produces IoT Mirai zombies on IoT networks. In the infection phase of traditional Mirai malware, bots directly control the phase. Nevertheless, from an Internet of Things (IoT) perspective, the Mirai zombie task merely scans the network for insecure devices to notify the Command & Control (C&C) server. IoT Mirai zombies do, in fact, simply notify the C&C server of the prospective zombies, and infection happens through communication with the C&C server [304]. Table 9 summaries some of the difference between PC and IoT Malware.

A study on the existing IoT malware detection approaches proves that researchers and industrialists are focusing on various ways to fill the security gaps in IoT. However, there are still various challenges in IoT Malware detection techniques that can be considered when developing novel methods in the future.

- **Availability of dataset**: Dataset is the most critical and primary aspect of malware detection techniques. In machine learning and deep learning techniques, the larger the data provided, the quicker the model can learn and improve [113]. However, there exists a severe lack of valid datasets for IoT Malware. IoTPOT and IoT-23 are the current benchmark IoT datasets in most IoT malware works. However, as most of the work uses the same dataset, any defects present within the dataset could impact the whole model. Moreover, the focus of each dataset might be specific, which might not be helpful in the proposed model. For example, IoTPoT is deployed on a restricted number of IP addresses, specifically interacting with Telnet requests [91]. Therefore, the generation of a dataset that is more realistic for real-world attacks is much more crucial.

  Future Scope: Generate a dataset by executing IoT malware samples in a group of real IoT devices with different architectures and operating systems.
- **Presence of diverse malware**: One of the interesting facts is that there is no universal naming for IoT malware, and the alias for some malware might be confusing. Various researchers follow distinct naming conventions for the collected malware samples that cause assigning diverse names for the identical samples, which makes the detection model complicated [305].

  Future Scope: Once the malware samples are collected, consider hashing, a standard technique used to identify malware uniquely so that the malware samples are not repeated with different names. In addition, it should include malware from various categories, such as worms, viruses, rootkits, spyware, etc.
- **Lack of Real-world experiments**: In dynamic analysis methods, as some IoT malware easily recognizes their execution in a virtual machine, they may bypass malware detection systems [298]. Even though the analysis

in real devices is more challenging and complex, the best detection approach needs to evaluate in a real-world environment.

Future Scope: Consider real devices to better analyse and evaluate the proposed model's effectiveness. Moreover, anti-VM detection techniques should also be developed.

- **Scalability of detection methods**: As IoT involves a group of heterogeneous devices with various abilities and requirements, the detection mechanisms need not focus on a particular architecture or operating system. During an IoT malware attack, the devices can be bots irrespective of their architecture and operating system, making the attack more complex. Moreover, as the malware varieties are also increasing, IoT malware detection could be challenging if the mechanism considered is not scalable.

  Future Scope: Develop module-based detection approaches that can be extended later when new malware of different architectures or operating systems are evolved.
- **Experimental Environment**: Working on real devices is expensive and time-consuming as the hardware and software aspects must be studied before the implementation. In this situation, most detection mechanisms prefer working in simulation environments that are cost-effective and flexible. However, the robust malware detection methods in the simulation environment might not be ideal for real devices. Furthermore, its effectiveness in a virtual environment cannot confirm that the model is efficient.

  Future Scope: Cost-effective approaches, including testbed-as-a-service [306] and re-usage of old IoT devices, can be considered while working with real testbeds.
- **Lack of Honeypots**: Honeypot is a security means that makes a virtual trap to attract attackers to capture their behaviour patterns, attack vectors, and security issues [307]. However, there are fewer existing honeypots for capturing IoT malware behaviour. As a result, there is a lack of behavioural patterns or rules that can be used in detection tools or mechanisms.

  Future Scope: Implement Honeypots that handle massive data and support more protocols and increased IoT devices to capture the behaviour of IoT malware.

Table 9 PC Malware Vs IoT Malware

	PC Malware	IoT Malware
Platform heterogeneity	Low	High
Malware family plurality	High	Low
Detection on the system	Easy	Hard
In-vivo analysis	Easy	Very Hard
Sandbox execution	Easy	Hard
Removal	Medium	Hard to impossible
Vulnerability assessment	Medium	Very Hard

- **Emphasis of Adversarial Attacks**: Adversarial attacks which contaminate the data are a specific way to get an inaccurate result from the model [1]. Nevertheless, the detection mechanisms that consider adversarial attacks are very few.

  Future Scope: While implementing the detection model, experimenting with adversarial attacks can improve the detection model.
- **Absence of cross-platform detection methods**: In most of the existing works, ARM-based IoT malware samples are used even though there exist different IoT devices of Intel, ARC, SPARC, MIPS architectures [99]. Focusing on a particular type of architecture won't solve the security issues in a group of IoT devices.

  Future Scope: Develop IoT malware detection methods that consider cross-architecture malware samples rather than concentrating on one type.
- **Selection of features**: The detection approaches usually focus on static or dynamic analysis for the proposed mechanisms. Even though dynamic analysis is considered, most works focus on network traffic, which might not be relevant for IoT malware that focuses on attack types such as data exfiltration and Permanent DoS attacks.

  Future Scope: Consider memory-related features [298] and log files for malware detection in addition to the widely used network features and opcode sequences.
- **Determination of Evaluation metrics**: This study has identified that nearly all machine learning or deep learning algorithms have been used in state-of-the-art works. Furthermore, ensemble learning, like stacking, boosting, etc., has also been introduced, producing better accuracy results. However, the evaluation metrics are limited to accuracy, which might not efficiently reflect the performance.

  Future Scope: Introduce novel evaluation metrics and focus on multiple metrics rather than concentrating on one.
- **Absence of software tools**: Most detection methods are not software-based approaches that can be applied in real devices [87].

  Future Scope: Create a software-based implementation to be integrated into actual devices, reducing the security issues in IoT devices.
- **Presence of obfuscation**: Usually, malware authors prevent malware detection by performing various obfuscation methods, including packing, encryption, etc., and only a few works like [302] consider the obfuscated malware detection in IoT. As most detection methods consider features like opcodes, obfuscation in IoT malware is still challenging.

  Future Scope: Consider the measure of randomness techniques in the model so that code obfuscation and data compression can also be detected.
- **Selection of ML Algorithms**: Selecting appropriate algorithms is crucial since picking the wrong algorithm

would produce incorrect output and waste time, effort, and accuracy. Similarly, choosing a bad data set will yield incorrect input and erroneous outcomes. Thus, using the relevant data sets and techniques, which may be investigated using machine learning to secure IoT environments, is crucial [308].

Future Scope: Review the dataset, ML algorithm use cases and task details before choosing the most appropriate one.

- **Lack of Intrusion Detection System (IDS)**: An intrusion detection system is a hardware or software application that monitors and watches out for malicious behaviour or broken rules on a network or system.

  Future Scope: Create a Software based IDS that monitors the IoT device based on the behaviour of the device in real-time.
- **Data Collection Issues**: Data collection is one of the biggest challenges in the IoT environment. Data-related problems include policies governing the privacy and protection of user information, Data in various forms or with ambiguous values, missing values, outliers, and incorrect data [309].

  Future Scope: Create standards, policies and data formats for data collection, retention and storage to address the issues mentioned above.
- **Lack of Reliable and Detailed IoT Security Protocol Stack**: A reliable, detailed, well-tested, and interoperable IoT Security Protocol Stack is presently under research. Due to immaturity, these comprehensive security features for protocols and standards are considerably behind reality [308].

  Future Scope: Design and develop a reliable, scalable, maintainable and well-tested IoT Security protocol stack.
- **Lack of Authentication and Access Control mechanisms**: IoT devices may be secured against unwanted access with the help of access control mechanisms. The IoT ecosystem, however, calls for access control systems that are more context-sensitive and fine-grained. Studies demonstrate the potential for context awareness and granularity in attribute-based access control models. It is possibly better to map current systems to alternative access control models to understand the advantages and hazards of access control. This will help to create solutions that are more context-aware [310]. Such solutions are not, however, included in the existing IoT application protocols MQTT and CoAP.

  Future Scope: Design and develop reliable, scalable, maintainable and well-tested Authentication and Access Control schemes for IoT environments.

9 Conclusion and future work

IoT, the third industrial revolution, has benefited the economy through various digitalizing fields such as education, military, healthcare, tourism, etc. However, the surging number of IoT devices and lack of security mechanisms have resulted in different oblivious attacks, including hacking, spying, intrusion mechanisms, malware attacks, etc. Most attacks are due to weak credentials, a lack of security standards, and user security awareness.

Researchers and security personnel started focusing on different detection and prevention mechanisms to solve this. Nevertheless, the absence of information and the growth of IoT Malware obstructs the perfect solutions for security attacks in IoT devices.

9.1 Future scope of IOT malware analysis and detection strategies

- *Making Reverse Engineering methods difficult*: Authors of malwares repackage the software binaries after deconstructing them to incorporate harmful code. We could utilize the crypto techniques to render it more difficult to decipher any application’s code and employ encryption techniques to make its code unconditionally incomprehensible [311].
- *Holistic Hybrid Analysis Tool*: Utilizing a powerful and effective tool to evaluate IoT device data and alert users if it includes malicious code that triggers harmful behaviours is necessary [311].
- *Model to Identify Zero-day Attacks*: We need clever and lightweight ML or DL-based models to identify malicious behaviour in applications in real-time or runtime and prevent zero-day attacks. We need a strong research orientation in this area because creating these detecting models is not so straightforward [311].
- *Standardized and Updated Dataset*: To efficiently accomplish malware detection analyses, we require standardized and updated datasets, which should be frequently updated with the latest discovered malware samples [311].
- *Laws and Regulations*: Countries should enact laws enforced globally to address issues with information security and cybersecurity-related threats [311]. Federal Bureau Investigation (FBI) declared cybersecurity law for the internet of things (IoT) devices in which they state that “if you found any toy is being compromised security terms then you have to report it”. To guarantee a particular degree of security is maintained for all devices, whether open source or proprietary, national or international security standards for the devices might be introduced [312].
- *Lightweight and Robust Trust Management and Security System*: Further research must be done to develop and standardize a lightweight and robust trust management system; along with it, all layers of IoT devices should be ensured with IDS, physical security and risk management. It is necessary to have this standard can

be applied to a variety of applications, enterprises, and industries. However, it may not be possible due to many constraints on the IoT device. IoT devices with similar restrictions might be grouped, and distinct standard security features could be developed for each group [313].

- *Training on Real-world Datasets*: Training of ML and DL-based models should be done using real-world datasets, and also the selection of appropriate ML and DL is crucial based on the task and available data set. A priority-based learning algorithm may be created to catch new malware and consider the attacks' frequency and severity. Further study should be done to develop hybrid ways of analyzing and detecting malware [313].
- *Planning and Strategies for Deployments*: While deploying IoT applications on public platforms, proper plans and strategies are crucial for protecting against malware, such as data encryption, before storing or transferring to the IoT device [313].
- *Transfer Learning*: It is defined as the ability to use a pre-trained model for different yet similar work. Transfer learning can enhance the existing ML or DL models with better results and less time [314]. More research can be conducted to use transfer learning in Malware analysis and detection as there is none on it.
- *Incremental Learning*: The effectiveness and reliability of ML or DL models may also be improved through incremental learning. A model may be trained on a very different set from the actual validation set since the data in a real-world scenario is constantly changing. Better outcomes may be obtained by combining the advantages of incremental and deep learning. The model may be altered under newly added features, making incremental learning a viable option for real-time analysis. The significant older findings can be set aside to extract information for forthcoming similar data [314].
- *Explainable AI(XAI)*: Explainable artificial intelligence (XAI) is a set of processes and methods that allows human users to comprehend and trust the results and output created by machine learning algorithms [315]. It may be used to characterize the model's decision-making process. Malware analysts and ML developers might use these to adjust the hyperparameters, determine the scope of detection, and spot any possible overgeneralization or overfitting that might lead to false positives or negatives. For a malware analyst to comprehend the interpretation, the model explanation must be described in simple malware behaviours rather than machine learning characteristics [315].
- *Anti-Adversarial Malware Strategies*: These should be used to measure the effectiveness of the ML models. It has two settings. First is the black box, where malware authors have little to no understanding of the model's internal structure and algorithm. White-box is the second situation, where the malware authors know the model's internal structure and algorithm adequately. The effort needed to dodge a model can be increased by implementing training techniques and rules that consider this. Thus resulting in a better and more robust model [316].
- *Defining IoT Device Security Levels*: Identifying the most prevalent security risks to which IoT devices are exposed is crucial. To establish this device's security level, developers should write tests against these vulnerabilities and use the information they get in the process [312].

To help the researchers and industrialists focus on this direction., our work is presented, including four mani contributions. First, we have conducted a study on multiple aspects of IoT malware, including 6 IoT malware categories, 16 attack types, 10 attack surfaces, 2 malware distribution architectures, 18 victim devices, 11 victim device architectures, 17 characteristics, 3 access mechanisms, 9 programming languages, and 8 protocols.

Second, a detailed analysis was done on 77 IoT malware between 2008 and 2022 by mapping the categories as mentioned above. Interestingly, we identified that some malware targeting PCs and Android devices evolved into targeting IoT devices.

Third, we reviewed various IoT malware detection methods, including traditional and learning-based ones. On the one hand, the traditional techniques were classified based on the analysis type, including static and dynamic analysis. On the other hand, learning-based detection methods were classified into machine learning-based methods, deep learning-based methods, and hybrid methods. The reviewed works were also compared based on the features, algorithms, testbed, dataset, and limitations.

Fourth, we identified 11 challenges that remain unaddressed due to IoT malware's evolving nature and the future research scopes that can solve the same.

Even though we have collected more than 150 IoT malware families, only 77 could map to different attributes based on the information collected from various sources; websites, journal articles, news feeds, tweets by IoT malware analysts, etc. Furthermore, it was challenging to map the attribute as different sources mentioned different information. In that case, we have selected the appropriate one based on the explanations given in the sources. Another challenge was the inconsistency in naming the malware families, where two different sources considered the same malware family with two different names. We welcome any modifications and recommendations related to the data. In the future, we plan to address these challenges and also, develop a robust and generalized IoT malware detection model.

Author contribution Princy Victor and Arash Habibi Lashkari surveyed IoT malware with 100 attributes based on IoT malware categories, attack types, attack surfaces, malware distribution architecture, victim devices, victim device architecture, characteristics, access mechanisms, programming languages, and protocols. Rongxing Lu and Tinshu Sasi conducted a detailed analysis of 77 IoT malware between 2008 and 2022 based on the categories. Pulei Xiong and Shahrear Iqbal summarized the existing challenges and future research scopes in IoT malware. Princy Victor wrote the manuscript with support from Arash Habibi Lashkari, Rongxing Lu, Tinshu Sasi, Pulei Xiong, and Shahrear Iqbal. All authors discussed the results and contributed to the final manuscript.

Funding This project was partly supported by collaborative research funding from the National Research Council of Canada's Artificial Intelligence for Logistics Program.

Data availability Not applicable.

Declarations

Ethics approval Not applicable.

Consent to publish Not applicable.

Conflict of interest We declare that no known conflicts of interest are associated with this publication.

References

1. Vasan D, Alazab M, Venkatraman S, Akram J, Qin Z (2020) Mthael: Cross-architecture IoT malware detection based on neural network advanced ensemble learning. IEEE Transactions on Computers 69(11):1654–1667. https://doi.org/10.1109/TC.2020.3015584
2. State of IoT 2021: Number of connected IoT devices growing 9% to 12.3 B. https://IoT-analytics.com/number-connected-IoT-devices/. Accessed 9 Jan 2022
3. Security HN. IoT malware attacks rose 700% during the pandemic. https://www.helpnetsecurity.com/2021/07/20/IoT-malware-attacks-rose. Accessed 10 Dec 2021
4. Mary DRK, Ko E, Kim SG, Yum SH, Shin SY, Park SH (2021) A systematic review on recent trends, challenges, privacy and security issues of underwater internet of things. Sensors 21(24). https://doi.org/10.3390/s21248262, https://www.mdpi.com/1424-8220/21/24/8262
5. Costin A, Zaddach J (2018) IoT malware: Comprehensive survey, analysis framework and case studies. BlackHat USA
6. Smith C, Miessler D (2014) Internet of Things HP security research study. https://d-russia.ru/wp-content/uploads/2015/10/4AA5-4759ENW.pdf
7. Chaabouni N, Mosbah M, Zemmari A, Sauvignac C, Faruki P (2019) Network intrusion detection for IoT security based on learning techniques. IEEE Commun Surv Tutor 21(3):2671–2701
8. Kenny L (2017) IoT: The internet of trouble. https://securityintelligence.com/
9. Huda S, Miah S, Yearwood J, Alyahya S, Al-Dossari H, Doss R (2018) A malicious threat detection model for cloud assisted Internet of Things (COT) based industrial control system (ICS) networks using deep belief network. J Parallel Distrib Comput 120:23–31
10. Parra GDLT, Rad P, Choo KKR, Beebe N (2020) Detecting Internet of Things attacks using distributed deep learning. J Netw Comput Appl 163:102662
11. De Donno M, Dragoni N, Giaretta A, Spognardi A (2017) Analysis of DDoS-capable IoT malwares. In: 2017 Federated Conference on Computer Science and Information Systems (FedCSIS), IEEE, pp 807–816
12. Hallman R, Bryan J, Palavicini G, Divita J, Romero-Mariona J (2017) Ioddos - the internet of distributed denial of sevice attacks. In: 2nd International Conference on Internet of Things, Big Data and Security. SCITEPRESS, pp 47–58
13. Shobana M, Rathi S (2018) IoT malware: an analysis of IoT device hijacking. International Journal of Scientific Research in Computer Science, Engineering and Information Technology
14. Vignau B, Khoury R, Hallé S (2019) 10 years of IoT malware: a feature-based taxonomy. In: 2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C), pp 458–465. https://doi.org/10.1109/QRS-C.2019.00088
15. Vignau B, Khoury R, Hallé S, Hamou-Lhadj A (2021) The evolution of IoT malwares, from 2008 to 2019: Survey, taxonomy, process simulator and perspectives. J Syst Architect 102143
16. Emotet malware starts to use IoT devices as proxy - SOC prime. https://socprime.com/news/emotet-malware-starts-to-use-iot-devices-as-proxy/. Accessed 23 May 2022
17. IoT and ransomware: a recipe for disruption - Security News. https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/iot-and-ransomware-a-recipe-for-disruption#:~:text=IoT%20ransomware%20is%20a%20ransomware,that%20shifted%20to%20smart%20TVs. Accessed 23 May 2022
18. Bytes M. Malware. https://www.malwarebytes.com/malware. Accessed 10 Dec 2021
19. Kaspersky: 1980s | Kaspersky IT Encyclopedia. https://encyclopedia.kaspersky.com/knowledge/years-1980s/. Accessed 10 Dec 2021
20. India A. What is IoT? Defining the Internet of Things (IoT) | Aeris. https://info.aeris.com/infographic-what-is-iot. Accesed 12 May 2022
21. Wikipedia. Internet of Things - Wikipedia. https://en.wikipedia.org/wiki/Internet_of_things. Accessed 12 May 2021
22. Bertino E, Islam N (2017) Botnets and Internet of Things security. Computer 50(2):76–79
23. Malware is a growing threat to IoT devices- find out how to protect your device! https://www.einfochips.com/blog/malware-is-a-growing-threat-to-IoT-devices-find-out-how-to-protect-your-device/. Accessed 10 May 2022
24. Specht S, Lee R (2003) Taxonomies of distributed denial of service networks, attacks, tools and countermeasures. CEL2003-03, Princeton University, Princeton, NJ, USA
25. O'Donnell L. Gitpaste-12 worm targets linux servers, IoT devices | Threatpost. https://threatpost.com/gitpaste-12-worm-linux-servers-IoT-devices/161016/. Accessed 21 Dec 2021
26. Yamaguchi S, Leelaprute P (2019) Hajime worm with lifespan and its mitigation evaluation against Mirai malware based on agent-oriented petri net pn 2. In: 2019 IEEE International Conference on Consumer Electronics (ICCE), IEEE, pp 1–4
27. Zhang X, Upton O, Beebe NL, Choo KKR (2020) IoT botnet forensics: a comprehensive digital forensic case study on mirai botnet servers. Forensic Sci Int: Digit Invest 32:300926
28. Johansen AG. What is a Trojan? Is it a virus or is it malware? https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html. Accessed 10 Dec 2021
29. Babu PD, Pavani C, Naidu CE (2019) Cyber security with IoT. In: 2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), vol. 1, pp 109–113. https://doi.org/10.1109/ICONSTEM.2019.8918782
30. Grimes RA. 9 types of malware and how to recognize them. https://www.csoonline.com/article/2615925/security-your-quick-guide-to-malware-types.html. Accessed 10 Dec 2021
31. Akabane S, Okamoto T (2020) Identification of library functions statically linked to linux malware without symbols. Procedia Comput Sci 176:3436–3445. 10.1016/j.procs.2020.09.053.

Knowledge-Based and Intelligent Information & Engineering Systems: Proceedings of the 24th International Conference KES2020

32. Bocetta S. Spyware in the IoT - this year's biggest security threat. https://informationsecuritybuzz.com/articles/spyware-in-the-IoT-this-years-biggest-security-threat/. Accessed 27 Dec 2021
33. Elmalaki S, Ho BJ, Alzantot M, Shoukry Y, Srivastava M (2019) Spycon: Adaptation based spyware in human-in-the-loop IoT. In: 2019 IEEE Security and Privacy Workshops (SPW), IEEE, pp 163–168
34. Zahra SR, Chishti MA (2019) Ransomware and internet of things: a new security nightmare. In: 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), IEEE, pp 551–555
35. Alshammari TB, Alanazi AS (2021) Security threats against the Internet of Things at home. In: 2021 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), pp 1–5. https://doi.org/10.1109/ICECCE52056.2021.9514258
36. Perry JS. IoT malware - anatomy of an attack - IBM developer. https://developer.ibm.com/technologies/IoT/articles/IoT-anatomy-IoT-malware-attack/
37. Yoon J (2020) Deep-learning approach to attack handling of IoT devices using IoT-enabled network services. Internet Things 11:100241
38. Wurm J, Hoang K, Arias O, Sadeghi AR, Jin Y (2016) Security analysis on consumer and industrial IoT devices. In: 2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC), IEEE, pp 519–524
39. Li W, Jin J, Lee JH (2019) Analysis of botnet domain names for IoT cybersecurity. IEEE Access 7:94658–94665
40. Wainwright P, Kettani H (2019) An analysis of botnet models. In: Proceedings of the 2019 3rd International Conference on Compute and Data Analysis, pp 116–121
41. Yin L, Luo X, Zhu C, Wang L, Xu Z, Lu H (2019) Connspoiler: Disrupting C&C communication of IoT-based botnet through fast detection of anomalous domain queries. IEEE Trans Ind Inform 16(2):1373–1384
42. (1) New Messages! https://www.crowdstrike.com/cybersecurity-101/botnets/. Accessed 17 Nov 2021
43. Acar G, Huang DY, Li F, Narayanan A, Feamster N (2018) Web-based attacks to discover and control local IoT devices. In: Proceedings of the 2018 Workshop on IoT Security and Privacy, pp 29–35
44. Alzahrani H, Abulkhair M, Alkayal E (2020) A multi-class neural network model for rapid detection of IoT botnet attacks. IJACSA
45. Bedi P, Mewada S, Vatti RA, Singh C, Dhindsa KS, Ponnusamy M, Sikarwar R (2021) Detection of attacks in IoT sensors networks using machine learning algorithm. Microprocess Microsyst 82:103814
46. Carpentier E, Thomasset C, Briffaut J (2019) Bridging the gap: Data exfiltration in highly secured environments using bluetooth IoTs. In: 2019 IEEE 37th International Conference on Computer Design (ICCD), IEEE, pp 297–300
47. Chen YW, Sheu JP, Kuo YC, Van Cuong N (2020) Design and implementation of IoT DDoS attacks detection system based on machine learning. In: 2020 European Conference on Networks and Communications (EuCNC), IEEE, pp 122–127
48. Dua A, Tyagi V, Patel N, Mehtre B (2019) Iisr: A secure router for IoT networks. In: 2019 4th International Conference on Information Systems and Computer Networks (ISCON), IEEE, pp 636–643
49. Hussain F, Abbas SG, Husnain M, Fayyaz UU, Shahzad F, Shah GA (2020) IoT DoS and DDoS attack detection using resnet. In: 2020 IEEE 23rd International Multitopic Conference (INMIC), IEEE, pp 1–6
50. Krejčí R, Hujňák O, Švepeš M (2017) Security survey of the IoT wireless protocols. In: 2017 25th Telecommunication Forum (TELFOR), IEEE, pp 1–4
51. Munshi A, Alqarni NA, Almalki NA (2020) Ddos attack on IoT devices. In: 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS), IEEE, pp 1–5
52. Murphy M (2017) The Internet of Things and the threat it poses to dns. Netw Secur 2017(7):17–19
53. Razzak F (2012) Spamming the Internet of Things: a possibility and its probable solution. Procedia Comput Sci 10:658–665
54. Shiaeles S, Kolokotronis N, Bellini E (2019) IoT vulnerability data crawling and analysis. In: 2019 IEEE World Congress on Services (SERVICES), IEEE, vol. 2642, pp 78–83
55. Wang B, Dou Y, Sang Y, Zhang Y, Huang J (2020) IoTcmal: Towards a hybrid IoT honeypot for capturing and analyzing malware. In: ICC 2020-2020 IEEE International Conference on Communications (ICC), IEEE, pp 1–7
56. Zahra A, Shah MA (2017) IoT based ransomware growth rate evaluation and detection using command and control blacklisting. In: 2017 23rd International Conference on Automation and Computing (ICAC), IEEE, pp 1–6
57. Zolanvari M, Teixeira MA, Jain R (2018) Effect of imbalanced datasets on security of industrial IoT using machine learning. In: 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), IEEE, pp 112–117
58. Arsene L. Hold my beer Mirai - Spinoff named 'LiquorBot' incorporates cryptomining - Bitdefender Labs. https://labs.bitdefender.com/2020/01/hold-my-beer-mirai-spinoff-named-liquorbot-incorporates-cryptomining/. Accessed 27 Dec 2021
59. Barbaschow A. Talos finds new VPNFilter malware hitting 500k IoT devices, mostly in Ukraine | ZDNet. https://www.zdnet.com/article/talos-finds-new-vpnfilter-malware-hitting-500k-IoT-devices-mostly-in-ukraine/. Accessed 27 Dec 2021
60. Bisson D. New 'Kaiji' Linux malware targeting IoT devices. https://securityintelligence.com/news/new-kaiji-linux-malware-targeting-IoT-devices/. Accessed 21 Dec 2021
61. CenturyLink. New Mozi malware family found. https://www.prnewswire.com/news-releases/new-mozi-malware-family-found-301040703.html. Accessed 11 May 2021
62. Cimpanu C. IoT botnet retooled to send email spam. https://www.bleepingcomputer.com/news/security/IoT-botnet-retooled-to-send-email-spam/. Accessed 27 Dec 2021
63. Cimpanu C. New Imeij IoT malware targets AVTech equipment. https://www.bleepingcomputer.com/news/security/new-imeij-IoT-malware-targets-avtech-equipment/. Accessed 11 May 2021
64. Cimpanu C. Prowli malware operation infected over 40,000 servers, modems, and IoT devices. https://www.bleepingcomputer.com/news/security/prowli-malware-operation-infected-over-40-000-servers-modems-and-IoT-devices/. Accessed 21 Dec 2021
65. Cyware. FritzFrog P2P botnet already breached 500 SSH servers | Cyware Alerts - Hacker News. https://cyware.com/news/fritzfrog-p2p-botnet-already-breached-500-ssh-servers-05e7fe5e. Accessed 27 Dec 2021
66. Design ACW. What is website 'hacking'? And Am I at risk? https://www.anorakcat.co.uk/blog/what-is-website-hacking-and-am-i-at-risk/. Accessed 18 Oct 2021
67. Dickson B. The IoT ransomware threat is more serious than you think - IoT security foundation. https://www.IoTsecurityfoundation.org/the-IoT-ransomware-threat-is-more-serious-than-you-think/. Accessed 16 Jan 2022
68. Fruhlinger J. DDoS explained: How distributed denial of service attacks are evolving | CSO Online. https://www.csoonline.com/article/3222095/ddos-explained-how-denial-of-service-attacks-are-evolving.html. Accessed 22 Feb 2022
69. imperva: Command injection. https://www.imperva.com/learn/application-security/command-injection/. Accessed 18 Oct 2021
70. Kenton W. Click fraud. https://www.investopedia.com/terms/c/click-fraud.asp. Accessed 18 Oct 2021

71. Labs AP. Katana: a new variant of the Mirai botnet | Avira Blog. https://www.avira.com/en/blog/katana-a-new-variant-of-the-mirai-botnet. Accessed 18 Jan 2022
72. Lord N. What is data exfiltration? | Digital Guardian. https://digitalguardian.com/blog/what-data-exfiltration. Accessed 21 Dec 2021
73. Nadeau M. What is cryptojacking? How to prevent, detect, and recover from it | CSO Online. https://www.csoonline.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html. Accessed 5 Nov 2022
74. Paganini P. Linux.ProxyM IoT botnet now used to launch hacking attacks against websitessecurity affairs. https://securityaffairs.co/wordpress/66537/malware/linux-proxym-IoT-botnet.html. Accessed 18 Jan 2022
75. Porgram HC. Botnet threat to the healthcare industry. https://www.hhs.gov/sites/default/files/botnet-threat-to-healthcare-industry.pdf?language=en. Accessed 16 Jan 2022
76. Radware. BrickerBot results in permanent denial-of-service. https://www.radware.com/security/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/. Accessed 11 May 2022
77. Trendmicrocom. PyRoMineIoT targets, infects, and spreads to vulnerable IoT devices - Security News. https://www.trendmicro.com/vinfo/in/security/news/cyber-attacks/pyromineIoT-targets-infects-and-spreads-to-vulnerable-IoT-devices. Accessed 21 Dec 2021
78. Cloudflare Website. What is a malicious payload? | Cloudflare. https://www.cloudflare.com/learning/security/glossary/malicious-payload/. Accessed 16 Jan 2022
79. Cloudflare Website. What is DNS? | How DNS works | Cloudflare. https://www.cloudflare.com/learning/dns/what-is-dns/. Accessed 16 Jan 2022
80. Website C. What is the Mirai botnet? | Cloudflare. https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/. Accessed 10 Mar 2021
81. Website H. What is a spam attack? | Support | Hornet, the gay social network. https://hornet.com/contributors/support/article/spam-attack. Accessed 18 Jan 2022
82. Website I. What is DNS spoofing | Cache poisoning attack example | Imperva. https://www.imperva.com/learn/application-security/dns-spoofing/. Accessed 21 Dec 2021
83. Zhang L. CERT analysis on IoT botnet and DDoS attacks - DZone IoT. https://dzone.com/articles/cert-analysis-on-IoT-botnet-and-ddos-attacks. Accessed 11 May 2022
84. Zhong W. Command injection | OWASP. https://owasp.org/www-community/attacks/Command_Injection#:~:text=Command%20injection%20is%20an%20attack,.)%20to%20a%20system%20shell. Accessed 27 Dec 2021
85. Alnahari W, Quasim MT (2021) Authentication of IoT device and IoT server using security key. In: 2021 International Congress of Advanced Technology and Engineering (ICOTEN), pp 1–9. https://doi.org/10.1109/ICOTEN52080.2021.9493492
86. Kagita MK, Bojja GR, Kaosar M (2021) A framework for intelligent IoT firmware compliance testing. Internet Things Cyber Phys Syst 1:1–7
87. Kumar A, Lim TJ (2019) Edima: Early detection of IoT malware network activity using machine learning techniques. In: 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), IEEE, pp 289–294
88. Kuzlu M, Fair C, Guler O (2021) Role of artificial intelligence in the internet of things (IoT) cybersecurity. Discover Internet Things 1(1):1–14
89. Myers J, Babun L, Yao E, Helble S, Allen P (2019) Mad-IoT: Memory anomaly detection for the Internet of Things. In: 2019 IEEE Globecom Workshops (GC Wkshps), IEEE, pp 1–6
90. Soewito B, Andhika CE (2019) Next generation firewall for improving security in company and IoT network. In: 2019 International Seminar on Intelligent Technology and Its Applications (ISITIA), IEEE, pp 205–209
91. Torabi S, Dib M, Bou-Harb E, Assi C, Debbabi M (2021) A strings-based similarity analysis approach for characterizing IoT malware and inferring their underlying relationships. IEEE Netw Lett
92. Visoottiviseth V, Akarasiriwong P, Chaiyasart S, Chotivatunyu S (2017) Pentos: Penetration testing tool for Internet of Thing devices. In: TENCON 2017–2017. IEEE Region 10 Conference, IEEE, pp 2279–2284
93. Firewall (computing) - Wikipedia. https://en.wikipedia.org/wiki/Firewall_(computing). Accessed 20 Oct 2021
94. IoT amnesia botnet puts at risk hundreds of thousands of DVRs due to unpatched flawsecurity affairs. https://securityaffairs.co/wordpress/57803/malware/iot-amnesia-botnet.html. Accessed 8 Nov 2021
95. Satori: The new malware family that affects cryptocurrencies - Swascan. https://www.swascan.com/swascan-satori/. Accessed 8 Nov 2021
96. Cimpanu C. New Silex malware is bricking IoT devices, has scary plans | ZDNet. https://www.zdnet.com/article/new-silex-malware-is-bricking-IoT-devices-has-scary-plans/. Accessed 21 Dec 2021
97. hakdefnet.org. Mirai updates from partners - HakDefNet. https://hakdefnet.org/2019/01/01/mirai-updates-from-partners/. Accessed 11 May 2022
98. Millman R (2017) Security researchers warn of ‘airborne’ IoT malware. Blueborne. https://internetofbusiness.com/security-researchers-warn-over-blueborne-IoT-malware/. Accessed 11 May 2022
99. HaddadPajouh H, Dehghantanha A, Khayami R, Choo KKR (2018) A deep recurrent neural network based approach for internet of things malware threat hunting. Future Gener Comput Syst 85:88–96
100. Karanja EM, Masupe S, Jeffrey MG (2020) Analysis of internet of things malware using image texture features and machine learning techniques. Internet Things 9:100153
101. Tien CW, Chen SW, Ban T, Kuo SY (2020) Machine learning framework to analyze IoT malware using elf and opcode features. Digit Threats: Res Pract 1(1):1–19
102. Wan TL, Ban T, Cheng SM, Lee YT, Sun B, Isawa R, Takahashi T, Inoue D (2020) Efficient detection and classification of Internet-of-Things malware based on byte sequences from executable files. IEEE Open J Comput Soc 1:262–275
103. ARC (processor) - Wikipedia. https://en.wikipedia.org/wiki/ARC_(processor). Accessed 27 Dec 2021
104. Arm architecture - Wikipedia. https://en.wikipedia.org/wiki/ARM_architecture. Accessed 27 Dec 2021
105. Intel 80386 – Wikipédia. https://fr.wikipedia.org/wiki/Intel_80386. Accessed 27 Dec 2021
106. MIPS architecture - wikipedia. https://en.wikipedia.org/wiki/MIPS_architecture. Accessed on 27 Dec 2021
107. Mirai variant targets arc CPU-based devices | securityweek.com. https://www.securityweek.com/mirai-variant-targets-arc-cpu-based-devices. Accessed 13 Jan 2022
108. Motorola 68000 - Wikipedia. https://en.wikipedia.org/wiki/Motorola_68000. Accessed 27 Dec 2021
109. PowerPC - Wikipedia. https://en.wikipedia.org/wiki/PowerPC. Accessed 27 Dec 2021
110. SPARC - Wikipedia. https://en.wikipedia.org/wiki/SPARC. Accessed 27 Dec 2021
111. SuperH - Wikipedia. https://en.wikipedia.org/wiki/SuperH. Accessed 27 Dec 2021
112. x86 - Wikipedia. https://en.wikipedia.org/wiki/X86. Accessed 27 Dec 2021
113. Haiba S, Mazri T (2021) Build a malware detection software for IoT network using machine learning. In: Proceedings of the 4th International Conference on Networking, Information Systems & Security, pp 1–8

114. Heightened DDoS threat posed by Mirai and other botnets | Cisa. https://www.cisa.gov/uscert/ncas/alerts/TA16-288A. Accessed 27 Dec 2021
115. Mirai malware infects CCTV camera | Blog | Darktrace. https://www.darktrace.com/en/blog/mirai-malware-infects-cctv-camera/. Accessed 27 Dec 2021
116. Smart toy security vulnerabilities archives - FS Studio. https://fsstudio.com/tag/smart-toy-security-vulnerabilities/. Accessed 27 Dec 2021
117. Cimpanu C. New Ttint IoT botnet caught exploiting two zero-days in Tenda routers | ZDNet. https://www.zdnet.com/article/new-ttint-IoT-botnet-caught-exploiting-two-zero-days-in-tenda-routers/. Accessed 21 Dec 2021
118. Wangwang W, Yunchun Z, Chengjie L, Xuchenming S, Yuting Z, Xin Z (2021) Network traffic oriented malware detection in IoT (internet-of-things). In: 2021 International Conference on Networking and Network Applications (NaNA), IEEE, pp 301–307
119. Cayre R, Nicomette V, Auriol G, Alata E, Kaâniche M, Marconato G (2019) Mirage: Towards a metasploit-like framework for IoT. In: 2019 IEEE 30th International Symposium on Software Reliability Engineering (ISSRE), IEEE, pp 261–270
120. Wang D, Ming J, Chen T, Zhang X, Wang C (2018) Cracking IoT device user account via brute-force attack to sms authentication code. In: Proceedings of the First Workshop on Radical and Experiential Security, pp 57–60
121. Bashlite updated with mining and backdoor commands. https://www.trendmicro.com/en_ca/research/19/d/bashlite-iot-malware-updated-with-mining-and-backdoor-commands-targets-wemo-devices.html. Accessed 21 Dec 2021
122. Brute force attack: Definition, types, and prevention | varonis. https://www.varonis.com/blog/brute-force-attack/. Accessed 21 Dec 2021
123. Brute force attacks on IoT - here to stay? | Allot blog. https://www.allot.com/blog/brute-force-attacks-iot/. Accessed 21 Dec 2021
124. Bug in millions of flawed iot devices lets attackers eavesdrop | Threatpost. https://threatpost.com/bug-iot-millions-devices-attackers-eavesdrop/168729/. Accessed 21 Dec 2021
125. What is a CVE? https://www.redhat.com/en/topics/security/what-is-cve. Accessed on 21 Dec 2021
126. What is Metasploit? The beginner's guide. https://www.varonis.com/blog/what-is-metasploit/. Accessed on 21 Dec 2021
127. Edward S, Profetis I. Hajime: Analysis of a decentralized internet worm for IoT devices. http://security.rapiditynetworks.com/publications/2016-10-16/hajime.pdf. Accessed 16 Jan 2022
128. Su J, Vasconcellos DV, Prasad S, Sgandurra D, Feng Y, Sakurai K (2018) Lightweight classification of IoT malware based on image recognition. In: 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), IEEE, vol. 2, pp 664–669
129. (1) New Messages! https://www.imperva.com/blog/650gbps-ddos-attack-leet-botnet/. Accessed 16 Jan 2022
130. Echobot Malware Now up to 71 exploits, targeting scada. https://www.f5.com/labs/articles/threat-intelligence/echobot-malware-now-up-to-71-exploits--targeting-scada. Accessed 16 Jan 2022
131. Gitpaste-12 malware via Github and Pastebin attacks Linux servers. https://cybersecuritynews.com/gitpaste-12-malware/. Accessed 16 Jan 2022
132. IoT malware starts showing destructive behavior | CSO Online. https://www.csoonline.com/article/3188429/IoT-malware-starts-showing-destructive-behavior.html. Accessed 27 Dec 2021
133. JenX: a new botnet threatening all. https://www.radware.com/security/ddos-threats-attacks/threat-advisories-attack-reports/jenx/. Accessed 16 Jan 2022
134. Mirai goes stealth - TLS & IoT malware - Lacework. https://www.lacework.com/blog/mirai-goes-stealth-tls-IoT-malware/. Accessed 27 Dec 2021
135. Mirai Okiru: New ddos botnet targets arc-based IoT devices | CSO Online. https://www.csoonline.com/article/3247794/mirai-okiru-new-ddos-botnet-targets-arc-based-IoT-devices.html. Accessed 16 Jan 2022
136. New Mirai variants have built-in domain generation algorithm | securityweek.com. https://www.securityweek.com/new-mirai-variants-have-built-domain-generation-algorithm. Accessed 16 Jan 2022
137. A new strain of IoT malware can survive a reboot | Boing Boing. https://boingboing.net/2018/05/09/boot-persistence.html. Accessed 27 Dec 2021
138. Spime watch: Linux.Darlloz, the internet-of-things worm | Wired. https://www.wired.com/2014/01/spime-watch-linux-darlloz-internet-things-worm/. Accessed 16 Jan 2022
139. internetofbusiness: OMG! Mirai malware variant turns IoT devices into proxy servers | Internet of Business. https://internetofbusiness.com/omg-mirai-malware-variant-turns-IoT-device-proxy-servers/. Accessed 16 Jan 2022
140. Amnesia:33 – Critical TCP/IP flaws affect millions of iot devices. https://thehackernews.com/2020/12/amnesia33-critical-tcpip-flaws-affect.html. Accessed 17 Jan 2022
141. File Transfer Protocol (FTP) definition. https://www.investopedia.com/terms/f/ftp-file-transfer-protocol.asp. Accessed 17 Jan 2022
142. Freaking out about fiendish IoT exploits? Maybe disable telnet, FTP and change that default password first? The register. https://www.theregister.com/2019/06/18/iot_default_security/. Accessed 27 Dec 2021
143. How to proactively defend against Mozi IoT botnet - Microsoft Security Blog. https://www.microsoft.com/security/blog/2021/08/19/how-to-proactively-defend-against-mozi-iot-botnet/. Accessed 27 Dec 2021
144. HTTP | MDN. https://developer.mozilla.org/en-US/docs/Web/HTTP. Accessed on 18 Jan 2022
145. IoT vulnerability assessment of the Irish IP address space. https://www.f5.com/labs/articles/threat-intelligence/IoT-vulnerability-assessment-of-the-irish-ip-address-space. Accessed 27 Dec 2021
146. IoT worm "Hajime" uses bittorrent protocols for communications | securityweek.com. https://www.securityweek.com/IoT-worm-hajime-uses-bittorrent-protocols-communications. Accessed 27 Dec 2021
147. Linux Shishiga malware using LUA scripts | WeLiveSecurity. https://www.welivesecurity.com/2017/04/25/linux-shishiga-malware-using-lua-scripts/. Accessed 18 Jan 2022
148. Mozi, another botnet using DHT. https://blog.netlab.360.com/mozi-another-botnet-using-dht/. Accessed 18 Jan 2022
149. New Kaiji malware targets IoT devices via SSH brute-force attacks | ZDNet. https://www.zdnet.com/article/new-kaiji-malware-targets-IoT-devices-via-ssh-brute-force-attacks/. Accessed 18 Jan 2022
150. The Persirai botnet - UHWO Cyber Security. https://westoahu.hawaii.edu/cyber/regional/gce-us-news/the-persirai-botnet/. Accessed 18 Jan 2022
151. Persirai: New IoT botnet targets IP cameras. https://www.trendmicro.com/en_ca/research/17/e/persirai-new-internet-things-IoT-botnet-targets-ip-cameras.html. Accessed 27 Dec 2021
152. Telnet - Wikipedia. https://en.wikipedia.org/wiki/Telnet. Accessed 17 Jan 2022
153. The UPnP security exploit affecting millions of home devices. https://www.minim.com/blog/the-upnp-security-exploit-affecting-millions-of-home-devices. Accessed 27 Dec 2021
154. What is UPnP? | NordVPN. https://nordvpn.com/blog/what-is-upnp/. Accessed 18 Jan 2022
155. Vijayan J. New 'HEH' botnet targets exposed telnet services. https://www.darkreading.com/vulnerabilities-threats/new-heh-botnet-targets-exposed-telnet-services. Accessed 27 Dec 2021
156. Wikipedia Contributors (2022) Secure shell – Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Secure_Shell &oldid=1065392858. Online. Accessed 18 Jan 2022
157. Backdoor: Linux/IoTReaper threat description - Microsoft Security Intelligence. https://www.microsoft.com/en-us/wdsi/threats/malware-

encyclopedia-description?Name=Backdoor:Linux/IoTReaper. Accessed 19 Jan 2022

158. Check point discovers three zero-day vulnerabilities in web programming language PHP 7 - Check Point software. https://blog.checkpoint.com/2016/12/27/check-point-discovers-three-zero-day-vulnerabilities-web-programming-language-php-7/. Accessed 27 Dec 2021
159. Hajime (malware) explained. https://everything.explained.today/Hajime_(malware)/. Accessed on 27 Dec 2021
160. Is this IoT malware acting for the greater good? | TechRadar. https://www.techradar.com/news/software/security-software/is-this-IoT-malware-acting-for-the-greater-good-1305919. Accessed 27 Dec 2021
161. Mirai (malware) - Wikipedia. https://en.wikipedia.org/wiki/Mirai_(malware). Accessed 27 Dec 2021
162. Necurs - hybrid spam botnet | CERT Polska. https://cert.pl/en/posts/2016/09/necurs-hybrid-spam-botnet/. Accessed 19 Jan 2022
163. Necurs evades detection via internet shortcut file. https://www.trendmicro.com/en_ca/research/18/d/necurs-evolves-to-evade-spam-detection-via-internet-shortcut-file.html. Accessed 19 Jan 2022
164. Wikipedia Contributors (2021) Linux.Wifatch – Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Linux.Wifatch &oldid=1054563047. Online. Accessed 19 Jan 2022
165. Contributor T. What is an attack surface? - Definition from whatis.com. https://whatis.techtarget.com/definition/attack-surface. Accessed 11 May 2022
166. White paper-ruckus IoT security. https://www.commscope.com/globalassets/digizuite/857777-wp-ruckus-IoT-security.pdf. Accessed 19 Jan 2022
167. Stone R. IoT cellular gateway routers - Do you need one? | Mushroom networks. https://www.mushroomnetworks.com/blog/IoT-cellular-gateway-routers-what-are-they-and-do-you-need-one/. Accessed 21 Dec 2021
168. Isawa R, Ban T, Tie Y, Yoshioka K, Inoue D (2018) Evaluating disassembly-code based similarity between IoT malware samples. In: 2018 13th Asia Joint Conference on Information Security (AsiaJCIS), IEEE, pp 89–94
169. IoT malware starts showing destructive behavior | CSO Online. https://www.csoonline.com/article/3188429/IoT-malware-starts-showing-destructive-behavior.html. Accessed 14 Jan 2022
170. Arghire I. 'Botenago' malware targets routers, IoT devices with over 30 exploits. https://www.securityweek.com/botenago-malware-targets-routers-IoT-devices-over-30-exploits#:~:text='BotenaGo'/. Accessed 16 Jan 2022
171. Transmission Control Protocol (TCP) (article) | Khan Academy. https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:the-internet/xcae6f4a7ff015e7d:transporting-packets/a/transmission-control-protocol--tcp#:~:text=The%20Transmission%20Control%20Protocol%20(TCP,duplicate%20packets%2C%20and%20corrupted%20packets. Accessed 17 Jan 2022
172. Mirai botnet attack IoT devices via CVE-2020-5902. https://www.trendmicro.com/en_us/research/20/g/mirai-botnet-attack-IoT-devices-via-cve-2020-5902.html. Accessed 25 May 2022
173. The Mirai botnet explained: How IoT devices almost brought down the internet | CSO Online. https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html. Accessed 25 May 2022
174. Inside the infamous Mirai IoT botnet: a retrospective analysis. https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/. Accessed 25 May 2022
175. Hajime botnet variant. https://exchange.xforce.ibmcloud.com/collection/Hajime-Botnet-Variant-857fdecabbdbd6f8acc8bf957f8c704a. Accessed 25 May 2022
176. Herwig S, Harvey K, Hughey G, Roberts R, Levin D (2019) Measurement and analysis of Hajime, a peer-to-peer IoT botnet. In: Network and Distributed Systems Security (NDSS) Symposium
177. (1) New Messages! https://www.synopsys.com/blogs/software-security/hajime-mirai-iot-botnet-turf-war/. Accessed 25 May 2022
178. Into the battlefield: a security guide to IoT botnets - Security news. https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/into-the-battlefield-a-security-guide-to-iot-botnets. Accessed 26 May 2022
179. Sign in risk assessment - new, more-powerful IoT botnet infects 3,500 devices in 5 days - for all the latest on all it tech like erp, cloud, bot, ai, IoT,m2m, netsuite, salesforce. https://erpinnews.com/sign-risk-assessment-new-powerful-IoT-botnet-infects-3500-devices-5-days/. Accessed 26 May 2022
180. NJCCIC threat profile Aidra botnet. https://www.cyber.nj.gov/threat-center/threat-profiles/botnet-variants/aidra-botnet. Accessed 26 May 2022
181. Linux.Darlloz - Wikipedia. https://en.wikipedia.org/wiki/Linux.Darlloz. Accessed 25 May 2022
182. Linux.Darlloz worm-targets Internet of Things | Waredot. https://waredot.com/academy/linux.darlloz-worm-targets-internet-of-things. Accessed 25 May 2022
183. Worm: Linux/Darlloz. A threat description - Microsoft Security Intelligence. https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Worm:Linux/Darlloz.A. Accessed 25 May 2022
184. The Darlloz Linux Worm diversifies to mine cryptocurrencies | Computerworld. https://www.computerworld.com/article/2488828/the-darlloz-linux-worm-diversifies-to-mine-cryptocurrencies.html. Accessed 25 May 2022
185. Satori (malware family). https://malpedia.caad.fkie.fraunhofer.de/details/elf.satori. Accessed 26 May 2022
186. Satori IoT botnet variant. https://www.radware.com/security/ddos-threats-attacks/threat-advisories-attack-reports/satori-IoT-botnet/. Accessed 26 May 2022
187. ThinkPHP remote code execution vulnerability used to deploy variety of malware (CVE-2018-20062). https://www.tenable.com/blog/thinkphp-remote-code-execution-vulnerability-used-to-deploy-variety-of-malware-cve-2018-20062. Accessed 26 May 2022
188. Threat alert: Multiple cryptocurrency miner botnets start to exploit the new thinkPHP vulnerability - Alibaba Cloud Community. https://www.alibabacloud.com/blog/threat-alert-multiple-cryptocurrency-miner-botnets-start-to-exploit-the-new-thinkphp-vulnerability_594369. Accessed 26 May 2022
189. Tracking the people behind botnets: a list of top 20 IoT blackhat hackers | by Newsky Security | Newsky Security. https://blog.newskysecurity.com/tracking-the-people-behind-botnets-a-list-of-top-20-IoT-blackhat-hackers-3a67d7bd3be0. Accessed 26 May 2022
190. Okane botnet - NHS Digital. https://digital.nhs.uk/cyber-alerts/2018/cc-2555. Accessed 16 May 2022
191. Unit 42 finds new Mirai and Gafgyt IoT/Linux botnet campaigns. https://unit42.paloaltonetworks.com/unit42-finds-new-mirai-gafgyt-IoTlinux-botnet-campaigns/. Accessed 16 May 2022
192. New malware and Mirai botnet variants pose significant threats - Corero | Corero. https://www.corero.com/blog/new-malware-and-mirai-botnet-variants-pose-significant-threats/. Accessed 11 May 2022
193. ZHtrap botnet: How it works and how to prevent it - Infosec Resources. https://resources.infosecinstitute.com/topic/zhtrap-botnet-how-it-works-and-how-to-prevent-it/. Accessed 26 May 2022
194. ZHtrap botnet uses honeypot to harvest infected devices | APNIC Blog. https://blog.apnic.net/2021/05/04/zhtrap-botnet-uses-honeypot-to-harvest-infected-devices/. Accessed 26 May 2022
195. New ZHtrap botnet malware deploys honeypots to find more targets. https://www.bleepingcomputer.com/news/security/

new-zhtrap-botnet-malware-deploys-honeypots-to-find-more-targets/. Accessed 26 May 2022
196. Persirai: New IoT botnet targets IP cameras. https://www.trendmicro.com/en_ca/research/17/e/persirai-new-internet-things-IoT-botnet-targets-ip-cameras.html. Accessed 11 May 2022
197. Persirai Botnet - NHS Digital. https://digital.nhs.uk/cyber-alerts/2018/cc-2805. Accessed 11 May 2022
198. The Persirai botnet - UHWO Cyber Security. https://westoahu.hawaii.edu/cyber/regional/gce-us-news/the-persirai-botnet/. Accessed 11 May 2022
199. 120,000 IoT cameras vulnerable to new persirai botnet say researchers | ZDNet. https://www.zdnet.com/article/120000-iot-cameras-vulnerable-to-new-persirai-botnet-say-researchers/. Accessed 11 May 2022
200. Gitpaste-12: a new worming botnet with reverse shell capability spreading via Github and Pastebin | Official Juniper Networks Blogs. https://blogs.juniper.net/en-us/threat-research/gitpaste-12. Accessed 16 May 2022
201. Gitpaste-12: a dozen exploits that silently lived on Github, attacked Linux servers. https://blog.sonatype.com/gitpaste-12. Accessed 16 May 2022
202. NJCCIC threat profile Linux/Moose. https://www.cyber.nj.gov/threat-center/threat-profiles/botnet-variants/linux-moose. Accessed 25 May 2022
203. The moose is loose: Linux-based worm turns routers into social network bots | Ars Technica. https://arstechnica.com/information-technology/2015/05/the-moose-is-loose-linux-based-worm-turns-routers-into-social-network-bots/. Accessed 25 May 2022
204. Linux/Moose malware makes comeback with new IoT botnet behind fake instagram, twitter profiles. https://www.ibtimes.co.uk/new-IoT-botnet-behind-fake-instagram-twitter-youtube-profiles-1592761. Accessed 25 May 2022
205. Linux Shishiga malware targeting IoT - information security buzz. https://informationsecuritybuzz.com/expert-comments/linux-shishiga-malware-targeting-IoT/. Accessed 23 May 2022
206. New strain of Linux malware could get serious | TechNewsWorld. https://www.technewsworld.com/story/new-strain-of-linux-malware-could-get-serious-84481.html. Accessed 23 May 2022
207. Shishiga - Linux malware - NHS Digital. https://digital.nhs.uk/cyber-alerts/2017/cc-1384. Accessed 23 May 2022
208. Mozi malware modified to present a more potent threat to industrial control systems | The Daily Swig. https://portswigger.net/daily-swig/mozi-malware-modified-to-present-a-more-potent-threat-to-industrial-control-systems#:~:text=Mozi%20is%20a%20peer%2Dto,service%20attacks%20or%20send%20spam. Accessed 12 May 2022
209. How to proactively defend against Mozi IoT botnet - Microsoft Security Blog. https://www.microsoft.com/security/blog/2021/08/19/how-to-proactively-defend-against-mozi-iot-botnet/. Accessed 12 May 2022
210. Cimpanu C. Mozi botnet gains the ability to tamper with its victims' traffic. https://therecord.media/mozi-botnet-gains-the-ability-to-tamper-with-its-victims-traffic/. Accessed 12 May 2022
211. This is why the Mozi botnet will linger on | ZDNet. https://www.zdnet.com/article/this-is-why-the-mozi-botnet-will-linger-on/. Accessed 12 May 2022
212. Carna botnet - Wikipedia. https://en.wikipedia.org/wiki/Carna_botnet. Accessed on 26 May 2022
213. Carna Botnet - Wikiwand. https://www.wikiwand.com/en/Carna_botnet. Accessed 26/May 2022
214. Cashdollar L. Latest Echobot: 26 infection vectors. https://www.akamai.com/blog/security/latest-echobot-26-infection-vectors. Accessed 10 May 2022
215. Wicked variant of Mirai botnet emerges | securityweek.com. https://www.securityweek.com/wicked-variant-mirai-botnet-emerges#:~:text=Wicked%20contains%20the%20string%20SoraLOADER,bot%2C%20a%20different%20Mirai%20variant. Accessed 17 May 2022
216. Wicked botnet uses passel of exploits to target IoT | Threatpost. https://threatpost.com/wicked-botnet-uses-passel-of-exploits-to-target-IoT/132125/. Accessed 17 May 2022
217. Wicked Mirai brings new exploits to IoT botnets. https://www.darkreading.com/IoT/wicked-mirai-brings-new-exploits-to-IoT-botnets. Accessed 17 May 2022
218. Beltov M. Mirai-based Masuta IoT botnet spreads in a worldwide attack. https://sensorstechforum.com/mirai-based-masuta-IoT-botnet-worldwide-attack/. Accessed 17 Oct 2022
219. New botnet torii showcases next stage of IoT abuse, researchers say - The Parallax. https://www.the-parallax.com/new-botnet-torii-IoT-abuse/. Accessed 17 May 2022
220. New IoT botnet Torii uses six methods for persistence, has no clear purpose. https://www.bleepingcomputer.com/news/security/new-IoT-botnet-torii-uses-six-methods-for-persistence-has-no-clear-purpose/. Accessed 17 May 2022
221. Torii, the latest IoT botnet is worse than Mirai | HOBI International, Inc. https://hobi.com/torii-the-latest-IoT-botnet-to-watch-out-for/torii-the-latest-IoT-botnet-to-watch-out-for/. Accessed 17 May 2022
222. Meet Torii, a new IoT botnet far more sophisticated than mirai variants | ZDNet. https://www.zdnet.com/article/meet-torii-a-new-IoT-botnet-far-more-sophisticated-than-mirai/. Accessed 17 May 2022
223. Joven R, Ananin E. DDoS-for-hire service powered by bushido botnet. https://www.fortinet.com/blog/threat-research/ddos-for-hire-service-powered-by-bushido-botnet-. Accessed 17 Oct 2022
224. Smii M. JenX, new IoT botnet. https://medium.com/secjuice/jenx-new-IoT-botnet-c412d5a446ee. Accessed 17 Oct 2022
225. Miori IoT botnet - NHS Digital. https://digital.nhs.uk/cyber-alerts/2019/cc-3143. Accessed 16 May 2022
226. Mirai malware attack as Miori delivered via RCE exploit. https://gbhackers.com/mirai-malware-attack-miori/. Accessed on 16 May 2022
227. Sora botnet. https://www.enigmasoftware.com/sorabotnet-removal/. Accessed 17 Oct 2022
228. Analysis of Linux.Omni - Security art work. https://www.securityartwork.es/2018/11/08/analysis-of-linux-omni/. Accessed 17 May 2022
229. OMNI bot variant discovered in polycom devices - WootCloud hypercontext powered security. https://wootcloud.com/press/omni-bot-variant-discovered-in-polycom-devices/. Accessed 17 May 2022
230. FritzFrog botnet returns to attack healthcare, education, government sectors | ZDNet. https://www.zdnet.com/article/fritzfrog-botnet-strikes-healthcare-education-government-sectors/. Accessed 17 May 2022
231. New FritzFrog P2P botnet has breached at least 500 enterprise, government servers | ZDNet. https://www.zdnet.com/article/new-fritzfrog-p2p-botnet-has-breached-at-least-500-enterprise-government-servers/. Accessed 17 May 2022
232. Botticelli B. IoT honeypots: State of the art botnet. https://fr.slideshare.net/BiagioBotticelli/state-of-the-art-IoT-honeypots. Accessed 17 Oct 2022
233. Abel R. Hakai and Yowai botnets abuse thinkPHP vulnerabilities. https://www.scmagazine.com/news/application-security/cybercriminals-are-exploiting-vulnerabilities-in-the-thinkphp-open-source-framework-to-expand-the-hakai-and-yowai-botnets. Accessed 17 Oct 2022
234. OMG Mirai variant turns IoT devices into proxy servers - Security News. https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/omg-mirai-variant-IoT-devices-proxy-servers. Accessed 16 May 2022
235. OMG botnet, the first Mirai variant that sets up proxy serversSecurity affairs. https://securityaffairs.co/wordpress/69449/malware/omg-botnet.html. Accessed 16 May 2022
236. OMG: New Mirai variant converts IoT devices into proxy servers. https://www.darkreading.com/vulnerabilities-threats/-

omg-new-mirai-variant-converts-IoT-devices-into-proxy-servers. Accessed 16 May 2022

237. Owari. https://malpedia.caad.fkie.fraunhofer.de/details/elf.owari. Accessed 17 Oct 2022
238. S, G. Hackers used default/weakest credentials for IoT botnet command and control server. https://gbhackers.com/IoT-botnet-owari-weakest-credential/. Accessed on 17 Oct 2022
239. Genetics of a modern iot attack. https://cujo.com/genetics-of-a-modern-iot-attack/. Accessed 17 Oct 2022
240. New VPNFilter malware targets at least 500k networking devices worldwide. https://blog.talosintelligence.com/2018/05/VPNFilter.html. Accessed 17 Oct 2022
241. Apt15's new backdoors; Two botnets dominate global spam. https://thewatchtower.io/news/apt15s-backdoors-two-botnets-dominate-global-spam/. Accessed 17 Oct 2022
242. Gamut botnet. https://www.spywareremove.com/removegamutbotnet.html. Accessed 17 Oct 2022
243. How to remove Gamut Botnet Trojan from computer. https://unboxhow.com/cybersecurity/remove-gamut-botnet. Accessed on 17 Oct 2022
244. Team MDR. Rise in Xorddos: a deeper look at the stealthy ddos malware targeting linux devices. https://www.microsoft.com/security/blog/2022/05/19/rise-in-xorddos-a-deeper-look-at-the-stealthy-ddos-malware-targeting-linux-devices/. Accessed 17 Oct 2022
245. Spybot worm. https://en.wikipedia.org/wiki/Spybot_worm. Accessed 17 Oct 2022
246. Meskauskas T. How to remove Win32/Skeeyah malware. https://www.pcrisk.com/removal-guides/14739-win32-skeeyah-trojan. Accessed 17 Oct 2022
247. Barrett B. How microsoft dismantled the infamous necurs botnet. https://www.wired.com/story/microsoft-necurs-botnet-takedown/. Accessed 17 Oct 2022
248. Ilascu I. Cr1ptT0r ransomware infects D-link NAS devices, targets embedded systems. https://www.bleepingcomputer.com/news/security/cr1ptt0r-ransomware-infects-d-link-nas-devices-targets-embedded-systems/. Accessed 17 Oct 2022
249. Ilascu I. Hades ransomware. https://digital.nhs.uk/cyber-alerts/2021/cc-3810. Accessed 17 Oct 2022
250. Ilascu I. Hades ransomware. https://malwaretips.com/blogs/remove-razor-virus/. Accessed on 17 Oct 2022
251. Meskauskas T. How to avoid file encryption by Lulz ransomware. https://www.pcrisk.com/removal-guides/16194-lulz-ransomware. Accessed 17 Oct 2022
252. Paganini P. The Muhstik botnet has been observed targeting redis servers exploiting the recently disclosed CVE-2022-0543 vulnerability. https://securityaffairs.co/wordpress/129549/cyber-crime/muhstik-botnet-targeting-redis-servers-using-recently-disclosed-vulnerability.html. Accessed 17 Oct 2022
253. Arsene L. SSH-targeting Golang bots becoming the new norm. https://www.bitdefender.com/blog/labs/ssh-targeting-golang-bots-becoming-the-new-norm/. Accessed 17 Oct 2022
254. Brickerbot malware emerges, permanently bricks IoT devices - Security news. https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/brickerbot-malware-permanently-bricks-iot-devices. Accessed 17 May 2022
255. Brickerbot, Mirai and the IoT malware knife fight | Digital guardian. https://digitalguardian.com/blog/brickerbot-mirai-and-iot-malware-knife-fight. Accessed 17 May 2022
256. Brickerbot malware attacks iot devices with permanent denial-of-service. https://www.bitdefender.com/blog/hotforsecurity/brickerbot-malware-attacks-iot-devices-with-permanent-denial-of-service?adobe_mc=MCMID%3D15804029632425564761935462236849527380%7CMCORGID%3D0E920C0F53DA9E9B0A490D45%2540AdobeOrg%7CTS%3D1508716800. Accessed 17 May 2022
257. IoT reaper. https://rhebo.com/en/service/glossar/IoT-reaper-25113/. Accessed 17 Oct 2022
258. Elknot. https://www.enigmasoftware.com/elknot-removal/. Accessed 17 Oct 2022
259. Elknot. https://evosec.eu/gr1n-new-malware-also-targets-iot-devices/. Accessed 17 Oct 2022
260. Karasek J, Augusto Remillano II TB. Multistage attack delivers billgates/setag backdoor. https://www.trendmicro.com/en_us/research/19/g/multistage-attack-delivers-billgates-setag-backdoor-can-turn-elasticsearch-databases-into-ddos-botnet-zombies.html. Accessed 17 Oct 2022
261. Dominguez K. Karu backdoor. https://www.trendmicro.com/vinfo/ru/threat-encyclopedia/malware/BKDR_TDSS.KARU/. Accessed 17 Oct 2022
262. Constantin L. Interplanetary storm cross-platform P2P botnet infects computers and IoT devices. https://www.csoonline.com/article/3584528/interplanetary-storm-cross-platform-p2p-botnet-infects-computers-and-IoT-devices.html. Accessed 17 Oct 2022
263. Turjeman E. Threat spotlight: New interplanetary storm variant targeting IoT devices. https://blog.barracuda.com/2020/10/01/threat-spotlight-new-interplanetary-storm-variant-IoT/. Accessed 17 Oct 2022
264. BlueBorne: Bluetooth vulnerabilities expose billions of devices to hacking - Nouvelles de Sécurité - Trend Micro FR. https://www.trendmicro.com/vinfo/fr/security/news/internet-of-things/blueborne-bluetooth-vulnerabilities-expose-billions-of-devices-to-hacking. Accessed 12 May 2022
265. New bluetooth malware affects billions of devices, requires no pairing - ExtremeTech. https://www.extremetech.com/mobile/255752-new-blueborne-bluetooth-malware-affects-billions-devices-requires-no-pairing. Accessed 12 May 2022
266. IoT botnet retooled to send email spam. https://www.bleepingcomputer.com/news/security/iot-botnet-retooled-to-send-email-spam/. Accessed 18 May 2022
267. LuaBot Linux/IoT malware. https://exchange.xforce.ibmcloud.com/collection/2b04d3f76f6fbd4b6bc7e3644b6e90f9. Accessed 17 Oct 2022
268. Paganini P. Luabot is the first linux ddos botnet written in LUA language. https://securityaffairs.co/wordpress/51155/malware/linux-luabot.html. Accessed 17 Oct 2022
269. Wikipedia: Emotet. https://en.wikipedia.org/wiki/Emotet. Accessed 17 Oct 2022
270. Emotet. https://www.malwarebytes.com/emotet. Accessed 17 Oct 2022
271. Malwaremustdie analyzes a new IoT malware dubbed Linux/AirDropBotSecurity affairs. https://securityaffairs.co/wordpress/91905/malware/linux-airdropbot-malware.html. Accessed 12 May 2022
272. Leet IoT botnet bursts on the scene with massive ddos attack | Malwaretips Community. https://malwaretips.com/threads/leet-IoT-botnet-bursts-on-the-scene-with-massive-ddos-attack.67169/. Accessed 12 May 2022
273. 650Gbps DDoS attack from Leet Botnet rivals Mirai attacks. https://www.bleepingcomputer.com/news/security/650gbps-ddos-attack-from-leet-botnet-rivals-mirai-attacks/. Accessed 12 May 2022
274. Linux.PnScan - How to protect - PCQuest. https://www.pcquest.com/linux-pnscan-how-to-protect/. Accessed on 12 May 2022
275. Linux.PnScan trojan is back to compromise routers and install backdoorssecurity affairs. https://securityaffairs.co/wordpress/50607/malware/linux-pnscan-return.html. Accessed 12 May 2022
276. Lakshmanan R. Dark nexus: a new emerging IoT botnet malware spotted in the wild. https://thehackernews.com/2020/04/darknexus-IoT-ddos-botnet.html. Accessed 17 Oct 2022
277. Investigations B, Unit F. New dark Nexus IoT botnet puts others to shame. https://www.bitdefender.com/files/News/CaseStudies/study/319/Bitdefender-PR-Whitepaper-DarkNexus-creat4349-en-EN-

interactive.pdf?awc=15520_1586505336_a71fa4366aed60aa31d15670b427773c. Accessed 17 Oct 2022

278. Heads of the Hydra. Malware for network devices. https://securelist.com/heads-of-the-hydra-malware-for-network-devices/36396/. Accessed 17 Oct 2022

279. Augusto Remillano II MV. Miori IoT botnet delivered via thinkPH exploit. https://www.trendmicro.com/en_ca/research/18/l/with-mirai-comes-miori-IoT-botnet-delivered-via-thinkphp-remote-code-execution-exploit.html. Accessed 17 Oct 2022

280. Ares Botnet. https://www.enigmasoftware.com/aresbotnet-removal/. Accessed 17 Oct 2022

281. Threats to Linux. https://news.drweb.com/show/review/?lng=en &i=9461. Accessed 17 Oct 2022

282. Yaakobi O. QBot malware: What is it and how does it work. https://www.datto.com/blog/qbot-malware-what-is-it-and-how-does-it-work. Accessed 17 Oct 2022

283. Backdoor Qbot. https://www.malwarebytes.com/blog/detections/backdoor-qbot. Accessed 17 Oct 2022

284. Ilgayev A. An old bot's nasty new tricks: Exploring qbot's latest attack methods. https://research.checkpoint.com/2020/exploring-qbots-latest-attack-methods/. Accessed 17 Oct 2022

285. Silex malware bricks IoT devices with weak passwords - Nouvelles de Sécurité - Rrend Micro FR. https://www.trendmicro.com/vinfo/fr/security/news/cybercrime-and-digital-threats/-silex-malware-bricks-IoT-devices-with-weak-passwords. Accessed 12 May 2022

286. Joker. https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Steckbriefe-aktueller-Botnetze/Steckbriefe/Joker/Joker.html. Accessed 17 Oct 2022

287. Cimpanu C (2018) New Exo android Trojan sold on hacking forums, dark web. https://www.bleepingcomputer.com/news/security/new-exo-android-trojan-sold-on-hacking-forums-dark-web/. Accessed 11 May 2022

288. For 8 years, a hacker operated a massive IoT Botnet just to download anime videos | ZDNet. https://www.zdnet.com/article/for-8-years-a-hacker-operated-a-massive-iot-botnet-just-to-download-anime-videos/. Accessed 12 May 2022

289. New HEH botnet can wipe routers and IoT devices | ZDNet. https://www.zdnet.com/article/new-heh-botnet-can-wipe-routers-and-IoT-devices/. Accessed 12 May 2022

290. The HEH virus - Telsy. https://www.telsy.com/the-heh-virus/, Accessed 12 May 2022

291. Carrillo-Mondejar J, Castelo Gomez JM, Nunez-Gomez C, Roldan-Gomez J, Martinez JL (2020) Automatic analysis architecture of IoT malware samples. Secur Commun Netw 2020:8810708. https://doi.org/10.1155/2020/8810708

292. Yong B, Liu X, Yu Q, Huang L, Zhou Q (2019) Malicious web traffic detection for Internet of Things environments. Comput Electric Eng 77:260–272

293. Tran NP, Nguyen NB, Ngo QD, Le VH (2017) Towards malware detection in routers with c500-toolkit. In: 2017 5th International Conference on Information and Communication Technology (ICoIC7), IEEE, pp 1–5

294. Cheng SM, Ban T, Huang JW, Hong BK, Inoue D (2020) Elf analyzer demo: Online identification for IoT malwares with multiple hardware architectures. In: 2020 IEEE Security and Privacy Workshops (SPW), IEEE, pp 126–126

295. Dovom EM, Azmoodeh A, Dehghantanha A, Newton DE, Parizi RM, Karimipour H (2019) Fuzzy pattern tree for edge malware detection and categorization in IoT. J Syst Architect 97:1–7

296. Khoda ME, Imam T, Kamruzzaman J, Gondal I, Rahman A (2019) Robust malware defense in industrial IoT applications using machine learning with selective adversarial samples. IEEE Trans Ind Appl 56(4):4415–4424

297. Depuru SK, Madhavi K (2019) Autoencoder integrated deep neural network for effective analysis of malware in distributed internet of things (IoT) devices. Int J Analytic Experiment Modal Anal

298. Jeon J, Park JH, Jeong YS (2020) Dynamic analysis for IoT malware detection with convolution neural network model. IEEE Access 8:96899–96911

299. Radhakrishnan G, Srinivasan K, Maheswaran S, Mohanasundaram K, Palanikkumar D, Vidyarthi A (2021) A deep-rnn and meta-heuristic feature selection approach for IoT malware detection. Materials Today: Proceedings

300. Wozniak M, Silka J, Wieczorek M, Alrashoud M (2021) Recurrent neural network model for IoT and networking malware threat detection. IEEE Trans Ind Inform 17(8):5583–5594

301. Sung Y, Jang S, Jeong YS, Hyuk J et al (2020) Malware classification algorithm using advanced word2vec-based bi-lstm for ground control stations. Comput Commun 153:342–348

302. Jeon J, Jeong B, Baek S, Jeong YS (2021) Hybrid malware detection based on bi-lstm and spp-net for smart IoT. IEEE Trans Ind Inform

303. Van CN, Phan VA, Nguyen KDT et al (2020) IoT malware detection based on latent representation. In: 2020 12th International Conference on Knowledge and Systems Engineering (KSE), IEEE, pp 177–182

304. Mahmoudyar N, Ghorbani AA, Lashkari AH. Graph-based IoT malware family classification. https://unbscholar.lib.unb.ca/islandora/object/unbscholar%3A10568/datastream/PDF/view. Accessed 3 Feb 2023

305. Lee YT, Ban T, Wan TL, Cheng SM, Isawa R, Takahashi T, Inoue D (2020) Cross platform IoT-malware family classification based on printable strings. 2020 IEEE 19th International Conference on Trust. Security and Privacy in Computing and Communications TrustCom, IEEE, pp 775–784

306. Hossain MM, Al Noor S, Karim Y, Hasan R (2017) IoTbed: a generic architecture for testbed as a service for internet of things-based systems. In: ICIoT, pp 42–49

307. Hakim MA, Aksu H, Uluagac AS, Akkaya K (2018) U-pot: a honeypot framework for upnp-based IoT devices. In: 2018 IEEE 37th International Performance Computing and Communications Conference (IPCCC), pp 1–8. https://doi.org/10.1109/PCCC.2018.8711321

308. Krishna RR, Priyadarshini A, Jha AV, Appasani B, Srinivasulu A, Bizon N (2021) State-of-the-art review on IoT threats and attacks: Taxonomy, challenges and solutions. Sustainability 13(16). https://doi.org/10.3390/su13169463, https://www.mdpi.com/2071-1050/13/16/9463

309. Khraisat A, Alazab A (2021) A critical review of intrusion detection systems in the Internet of Things: Techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. Cybersecurity 4(1):18. https://doi.org/10.1186/s42400-021-00077-7

310. Nath R, Nath HV (2022) Critical analysis of the layered and systematic approaches for understanding IoT security threats and challenges. Comput Electric Eng 100:107997

311. Qamar A, Karim A, Chang V (2019) Mobile malware attacks: Review, taxonomy & future directions. Futur Gener Comput Syst 97:887–909

312. Williams P, Rojas P, Bayoumi M (2019) Security taxonomy in IoT - a survey. In: 2019 IEEE 62nd International Midwest Symposium on Circuits and Systems (MWSCAS), pp 560–565. https://doi.org/10.1109/MWSCAS.2019.8884913

313. Khanam S, Ahmedy IB, Idna Idris MY, Jaward MH, Sabri Bin Md AQ (2020) A survey of security challenges, attacks taxonomy and advanced countermeasures in the Internet of Things. IEEE Access 8:219709–219743. https://doi.org/10.1109/ACCESS.2020.3037359

314. Mishra N, Pandya S (2021) Internet of Things applications, security challenges, attacks, intrusion detection, and future visions: a systematic review. IEEE Access 9:59353–59377. https://doi.org/10.1109/ACCESS.2021.3073408
315. Explainable AI - XAI. https://www.ibm.com/watson/explainable-ai. Accessed 3 Jan 2023
316. Saad S, Briguglio W, Elmiligi H (2019) The curious case of machine learning in malware detection. Proceedings of the 5th International Conference on Information Systems Security and Privacy. https://doi.org/10.5220/0007470705280535

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.