Mirai Malware and Its Impact on IoT Security: Security Threats and Defense Mechanisms

Eustacy Jhade V. Eugenio
School of Information Technology, Mapúa University, ejveugenio@mymail.mapua.edu.ph

Micko Lucas
School of Information Technology, Mapúa University, mplucas@mymail.mapua.edu.ph

Christian Paglinawan
School of Information Technology, Mapúa University, cpaglinawan@mymail.mapua.edu.ph

Abstract

Mirai virus is known since 2016 and now has become a critical source of insecurity for the internet of things. This botnet takes over the devices infected by it to orchestrate massive Distributed Denial of Service attacks. This essay will describe the construction of Mirai, how it works, and how it has grown with time, with special attention to how it acquires its botnet using default login credentials in most IoT devices. Now that the source code of Mirai has been published, new variants of this virus have emerged and it has seen a tremendous growth in global DDoS attacks. The paper shall discuss how Mirai works, its impact on the security of IoT, and how the possible attacks can be mitigated. The increasing integration of IoT devices in our lives and modern infrastructures call for discussing threats like Mirai and other viruses. We will now see how Mirai works and discuss greater implications in the context of IoT security. It would be quite crucial for organizations to know how Mirai and its variations work and which vulnerabilities it attacks so they can better prepare against this kind of threat. Because of the ease and efficiency that IoT devices provide, it is imperative to fill up holes exposed by Mirai and similar infections to keep the digital environment safe.

CCS CONCEPTS

Additional Keywords and Phrases: Mirai malware, IoT security, DDoS attacks, cybersecurity, network defense, botnet, default credentials, security vulnerabilities.

ACM Reference Format:

Eustacy Jhade V. Eugenio, Micko Lucas, Christian Paglinawan. 2024. Mirai Malware and Its Impact on IoT Security: Security Threats and Defense Mechanisms. In Woodstock '18: ACM Symposium on Neural Gaze Detection, June 03–05, 2018, Woodstock, NY. ACM, New York, NY, USA, 10 pages. NOTE: This block will be automatically generated when manuscripts are processed after acceptance.

1. INTRODUCTION

1.1 Emergence of Mirai Malware in Iot devices

Internet of Things (IoT) devices have brought a huge impact on people's lives in many ways, such as medical treatment, smart homes, and military research, namely, the smart city [2]. These evolving systems enhance the urban living by improving the essential needs of one city,As cities increase their convenience, and a better quality of life.The IoT devices can be accessed from anywhere, from home, office and vehicles to make everyday tasks simpler[4].The convenience of these technology make the residents life more efficient,Allowing the user to manage everything through their devices with just a few taps the sense of easy to access leads how the Iot continue to advance.

When Mirai botnet emerged in 2016 it changed the whole internet threat landscape when initially it released a volume of 600 Gbps of distributed-denial-of-service (DDos) attacks, overtime the volume of botnets doubled until it reached 1 Tbps DDos attacks in major internet infrastructure and service providers. The Mirai source code was made public that led to different variants such as JOSHO or MASUTA that uses the same framework and process for scanning, infection and communications but has user-specific adjustments in passwords, in identifying itself and where the bots report to. This spurred multiple variants of Mirai bots in having more control of Iot devices worldwide [1].

The emergence of Mirai malware underscored the critical security vulnerabilities in IoT devices. By utilizing default credentials, Mirai can rapidly infect devices, creating a vast botnet that is capable of launching large-scale DDoS attacks. As more IoT devices are integrated into home and business environments, their accessibility to unauthorized users becomes a severe risk. Devices such as security cameras, routers, and smart appliances are often connected with little attention to securing their access points. Mirai's rapid propagation demonstrated how easily a small vulnerability can be exploited at scale, with attackers using simple dictionary attacks to compromise millions of devices [10].

1.1.1 Mirai Malware Architecture

Before discussing the defense mechanisms for Mirai malware, its architecture displayed in figure 1 must be understood. There are three main components in its architecture which are the bot, loader, and Command and Control. There are three types of bots that can be encountered [8].

Type of Mirai Bot	**Function**
Scanner Module	It creates random IP addresses to match the vulnerable IP address of Iot devices where it will connect to the device with a TCP handshake.
Attacker Module	It is responsible for executing the commands from a Command and Control server to distribute an DDoS attack
Killer Module	It terminates the Mirai-like software in the Iot device for the bot to implement its own Mirai software.

Table 1 Type of Mirai Bots [8]

When the bots infected the device it will use multiple combinations to attempt to find the correct username and password of the Iot devices. When the bots get the username and password of the device the loader will now report it to the C&C server to break into the device to install the malware [8].

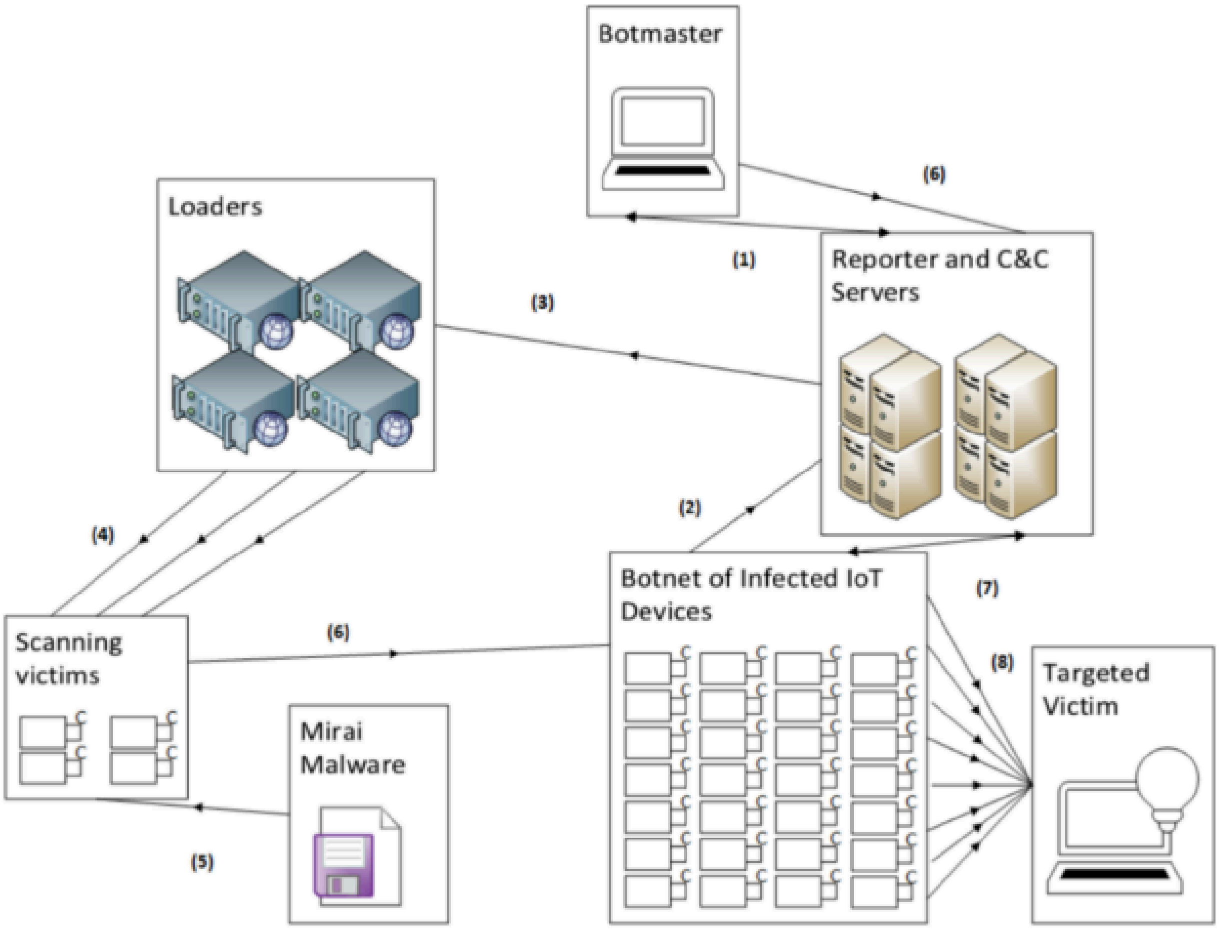


Figure 1 Architecture of Mirai Malware [8]

1.2 Relevance of understanding Mirai Malware of its threats and building defense mechanisms.

Mirai malware is dangerous to Iot devices because of the volumes of DDos attacks that it can send to devices such as servers, telecoms, websites, routers, and networks. Mirai Malware attacks commits crime in damaging devices and stealing information from Iot devices such as security footage and mining bitcoins from networks. Mirai malware can cost expensive damages to company and user properties because device’s information is being stolen or being tampered by DDos attacks that can become a DDos botnet itself. Mirai Malware scanning makes it dangerous to identify IPv4 addresses that leads to DDos attacks [3].

Mirai malware's importance in today's digital ecosystem stems from the expanding number of internet-connected IoT devices. IoT devices are frequently left with default settings, making them a prime target for malware like Mirai, which exploits lax security procedures. Mirai's assaults caused widespread disruptions, financial losses, and raised attention of IoT vulnerabilities. As IoT use grows, knowing how malware like Mirai functions is critical for enhancing defenses and preserving the security of global digital networks. [11].

1.3 Objective of the Study

The objectives of this study are to describe the effects of Mirai virus on Internet of Things devices, comprehend how enterprises responded to the attack to lessen its risks, and learn how the malware operates. The following are the goals of this study:

- Investigate the mechanisms by which Mirai malware exploits vulnerabilities in IoT systems, such as weak default credentials and network configurations.
- Analyze preventive measurements implemented by security experts to reduce Mirai's spread and its impact on IoT infrastructure.
- Examine the structure and functionality of Mirai, its mechanisms, propagation, attack coordination, and adaptation to evolving IoT environments.

This project intends to contribute to the current body of knowledge on IoT security by examining these objectives. It will inform businesses, developers, and policymakers on the security measures needed to safeguard IoT infrastructures from future malware threats. [3, 12].

1.4 Scope and Delimitation

This paper focuses on the analysis of Mirai malware's impact on IoT security and examines both its architecture and its specific impact on IoT device vulnerabilities, such as unsecured communication protocols. This research does not delve into economic implications of large-scale attacks, although it does acknowledge the potential for significant financial impact on affected sectors. The study is limited to IoT devices commonly targeted by Mirai, such as security cameras, routers, and other consumer-level appliances. Additionally, it addresses the limitations of current defensive mechanisms but does not cover all possible solutions in-depth. Future research may expand upon this study by evaluating other malware families that exploit IoT vulnerabilities, assessing economic impacts, or exploring emerging countermeasures beyond the scope of this research [6]. While this research highlights general mitigation techniques, it does not provide a comprehensive evaluation of all possible countermeasures; rather, it aims to set a foundation for further studies on IoT security. Additionally, the study's findings are primarily applicable to consumer-level IoT devices, as it does not address enterprise-grade IoT security measures extensively.

1.5 Significance of the study

This research tries to better understand how Mirai exploits IoT vulnerabilities, with a focus on the malware's technical design, attack techniques, and security implications. This article will provide insights into enhancing security practices for IoT devices by looking at real-world examples and evaluating Mirai's evolution after its source code was publicly released. It will also go over countermeasures, such as tighter password protocols, regular upgrades, and improved network security, to reduce the risks posed by similar future attacks. This paper will help to a better understanding of Mirai's impact, assisting industries, security experts, and researchers in establishing stronger defenses and awareness measures. By breaking down Mirai's methods and emphasizing practical prevention measures this study will enhance IoT security standards and strenghten networks against comparable cyberattacks in the future. Many users more often use a default password and sometimes forget crucial updates of the device that can lead to vulnerability to threats of viruses. With this research we encouraged the user to be security conscious that minimizes the threat and can help to reduce the attacks of their Iot devices.

2. DISCUSSION

2.1 Mechanisms of Mirai Malware Exploiting IoT Vulnerabilities

The Mirai malware preys on the basic security configurations weakness most IoTs possess. Taking advantage of devices retaining their default passwords or weak ones, the malware successfully exploits the susceptibility of the devices to create the large botnet. It initiates an attack sequence where Mirai scans the internet for devices which remain unguarded, most of them having factory-set credentials, like "admin" or "password." Users do not normally change the default settings from these default settings, thereby giving Mirai the window to execute brute-force login attempts on IoT devices ranging from security cameras, routers, to even smart home appliances. Mirai installs malware and then connects to its central Command-and-Control C&C server, which it would allow the attackers for synchronizing large coordinated attacks of Distributed Denial-of-Service DDoS [15].

Mirai has a three-tiered architecture consisting of scanner, attacker, and killer modules. It contains the scanner module continuously searching for other vulnerable devices; it is added quickly to the botnet. Once a gadget gets compromised, the command or the attacking module goes forward and carries out a DDOS against targeted users' services so that to throttle down their bandwidth through that attack. Simultaneously, the killer module does its duty as some counter-attacking unit whereby it will identify various process malware which is developed with other devices and that ensures that the Mirai group has total control on any infected botnet [8]. This makes Mirai not only diversified but very efficient as well since it recruits thousands of IoT devices within hours. Through such streamlined processes, the attacker may exploit even the smallest vulnerability of an IoT device in extremely devastating ways, which requires minimal efforts from attackers themselves as how significantly its operation of the malware is highly automated.

2.1.1 Case analysis of the Mirai Malware attack in 2016

Malicious malware called Mirai builds an IoT device botnet. In September 2016, a DDoS assault against the Kerbs On Security website that reached 620 Gbps brought it to the attention of the public. Following that, it was employed in an assault that peaked at 1 Tbps against the French hosting business OVH.[4].These kinds of incidents increased the concerns of the security of connected technology. It calls attention to the exposure of the Internet of things(Iot) calling for better security protocols and higher security practices. That led to awareness of both consumers/users and manufacturers.But the most well-known Mirai DDoS assault targeted DNS provider Dyn, rendering a number of well-known websites inaccessible, including GitHub, Twitter, Reddit, Netflix, and many more. [4].

Although there had been reports of Mirai since August 31, 2016, it wasn't until mid-September that the major DDoS assaults on Krebs on Security and OVH [74] made news (Figure 1). Later, DNS provider Dyn and Liberian telecom company Lonestar Cell were the targets of several more well-publicized hacks. When the Mirai author was discovered in early 2017, the players involved in the project came to light. [3].Little attention was paid to Mirai's initial public report in late August 2016, and the spacecraft largely stayed hidden until mid-September. It gained notoriety at the time when it was used to launch enormous DDoS assaults on OVH, one of the biggest web hosting companies in the world, and Krebs on Security, the blog of a well-known security writer [7].These attacks contribute to the eagerness on the impulse and strategy of the attackers but on the other hand where it censored the need to strengthen cybersecurity protocols and measures to fortify it against serious threats.

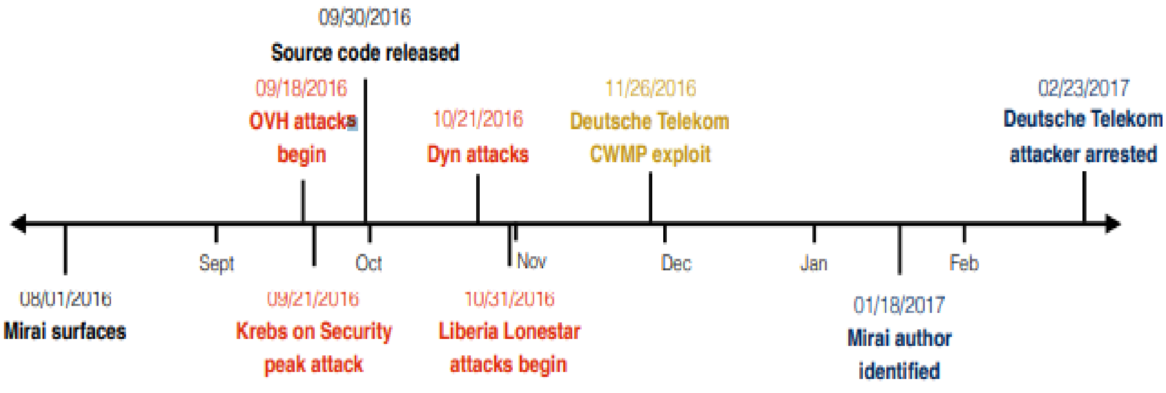


Figure 2: Mirai TImeline —- Major attacks(red),exploits(yellow),and events(black) related to the Mirai botnet [3]

Our telemetry shows that Mirai became live on August 1st, when the infection began from a single bulletproof hosting IP, even if the world didn't discover about it until the end of August. Although the world did not discover Mirai until the end of August, our telemetry shows that it became active on August 1st, when the infection began from a single bulletproof hosting IP. From that point on, Mirai expanded rapidly, doubling in size every 76 minutes during those early hours[7].As more devices get attacked by the malware the Continuation of widespread strikes became more obvious and the potential of increasing in apparent large scale of threat is more prominent this would eventually capture the global attention .

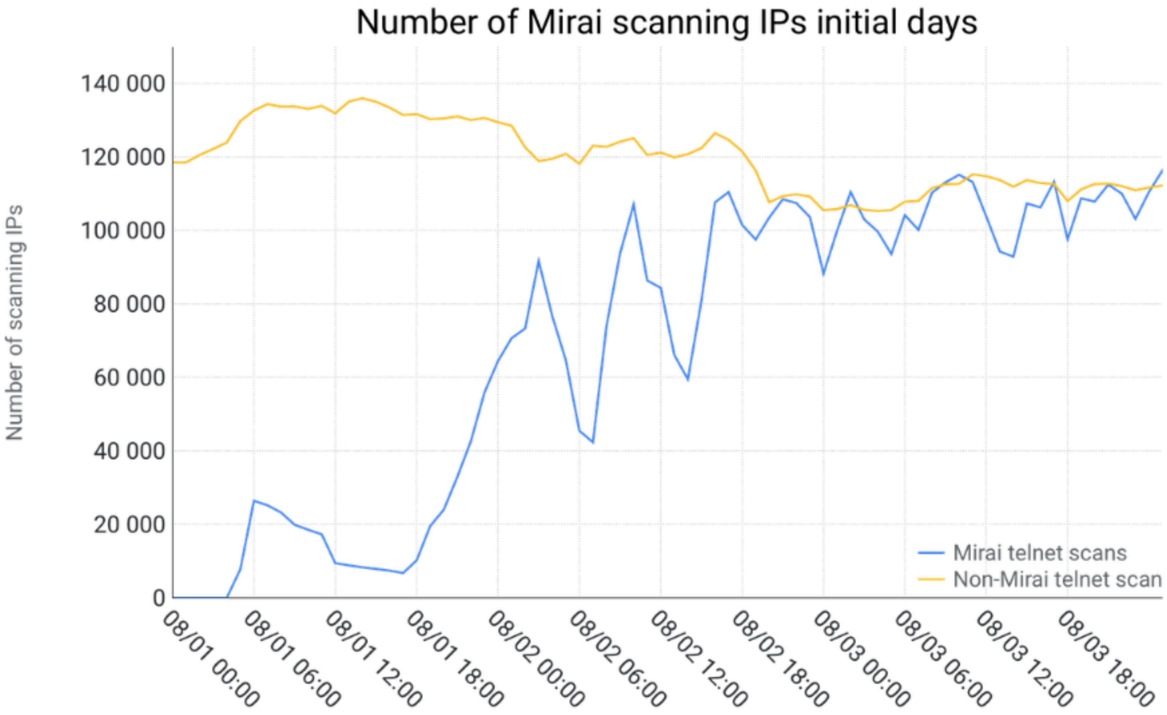


Figure 3: Number of Mirai scanning IPs initial days [7]

2.2 Defence Mechanisms for Mirai Malware

Mirai will continue to pose a threat until the vulnerable devices are secured, yet the people who are attacked by Mirai have little control over how these devices are secured.There are several ways to defend Corero SmartWall ONE from Mirai-style assaults. For clients who aren't currently using the SecureWatch® Managed Service offering, our Security Operations Team (SOC) may activate additional mitigating tools in addition to their comprehensive knowledge of Mirai assaults[10].

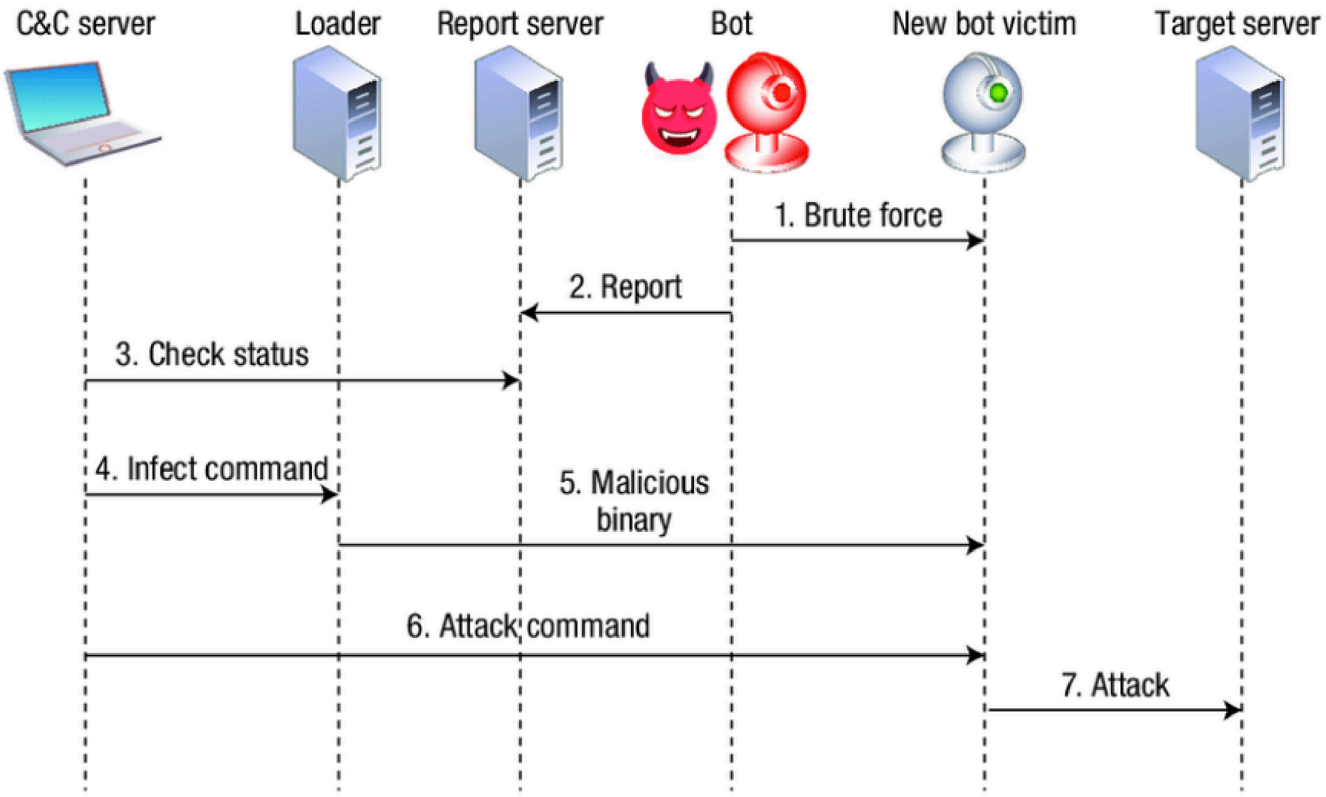


Figure 4 Mirai Botnet Operation and communication[18]

Best practices that can apply to improve the defence mechanism for the Mirai malware such asRegular firmware upgrades are essential to the security of IoT devices because they address security vulnerabilities that viruses like Mirai may exploit. These updates not only address known security flaws but also enhance device performance. To ensure compliance, organizations should use automated update systems that notify users of available updates and emphasize their importance. User education is essential since many users neglect to apply updates, leaving their devices vulnerable. and the other best practices for defense mechanisms is intrusion detection systems (IDS) that may provide real-time alerts that allow for a prompt reaction to any attacks, they are essential for keeping an eye on network traffic for questionable activity. Businesses may obtain a complete view of their security environment by utilizing both host-based and network-based intrusion detection systems. This capability is further enhanced by integration with Security Information and Event Management (SIEM) systems, which aggregate logs and alerts to provide a comprehensive picture of security occurrences. However, to keep these systems working issues like resource demands and false positives must be resolved.

2.2.1 Countermeasures against Mirai Malware

The fact that Mirai malware is persistent and evolving is challenging to cybersecurity research; thus, broad mechanisms have been designed to enhance the reduction of dangers offered by botnet attacks. Major defenses are IDS. They scan the network for strange patterns of traffic due to an IoT attack. There are two main kinds of detection for IDS. Signature-based detection identifies threats by finding a match of network traffic with known attack signatures, while anomaly-based detection monitors to identify deviations from normal behaviors as potential threats. Although each has its advantage - signature-based detection will quickly identify a known threat; however, anomaly-based detection can potentially offer an adaptive defense mechanism against new, unidentified patterns of attacks [8].Intrusion detection systems are used in monitoring the router's traffic when it determines an unusual traffic pattern to identify if there are potential threats in infecting the Iot devices with malware. There are two methods in implementing IDS [8].

IDS detection Method	**Definition**
Signature-Based Detection	It determines an attack by comparing a known threat's traffic pattern.
Anomaly-Based Detection	It analyzes all of the traffic by monitoring the general traffic if it deviates to an abnormal traffic pattern.

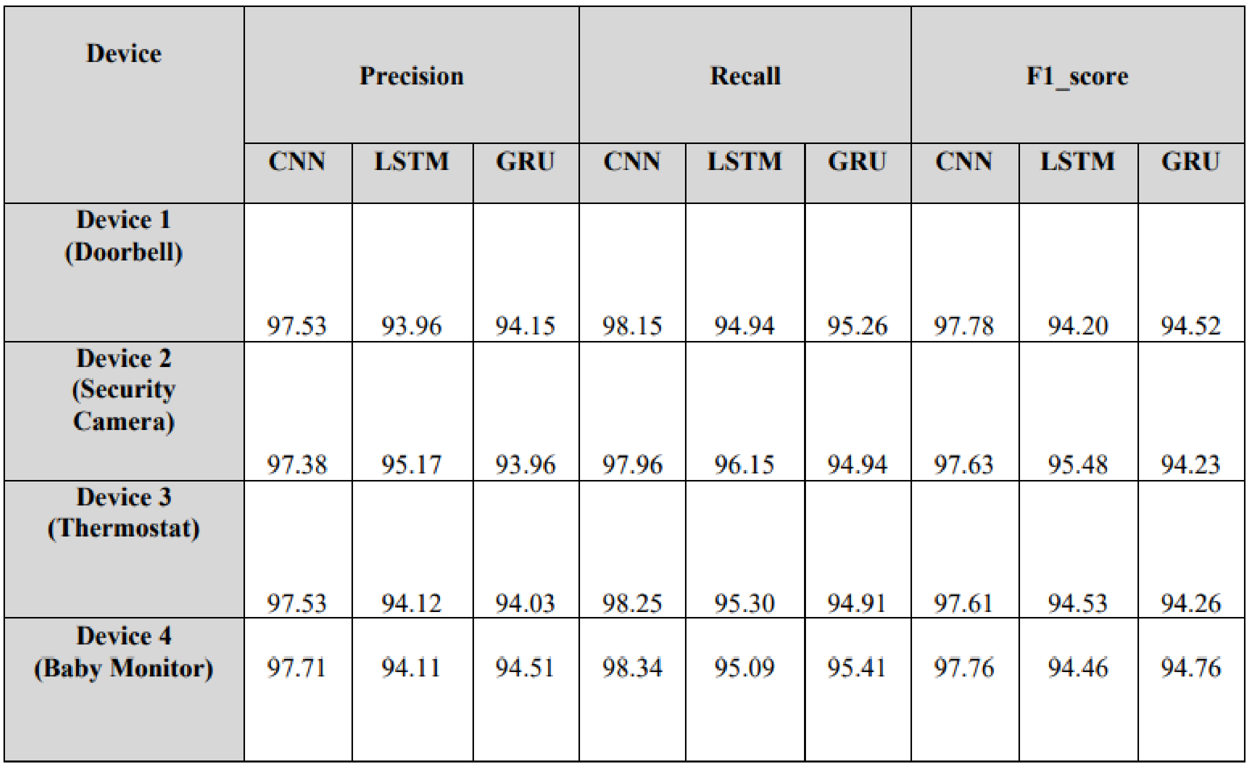
Table 2 IDS detection Methods [8]

This defense mechanism is used to protect an Iot device from unauthorized access, malicious activities and policy violations by monitoring its network traffic. When the IDS recognizes an unusual traffic pattern it can alert the administration to prevent the Iot device being vulnerable to DDos attacks, data breaches, and botnets. Different companies and organizations are finding ways to efficiently implement an IDS in their systems to protect their Iot devices [8]. IDS can improve its performance because it can handle more large-scale data to detect botnet attacks in Iot devices..Three deep-learning models are found to be effective in monitoring traffic networks [9]. Other deep learning models that include **Convolutional Neural Networks** and **Long Short-Term Memory** networks have enriched IDS capabilities further. Large training of these models with the datasets of normal as well as attack network traffics will make CNN find very accurate patterns in DDoS attacks. However, LSTMs look for dependencies in time-sequenced data to look for long-term patterns which can expose persistent botnet activities. For example, CNN-based IDS systems have achieved above 99% accuracy in detecting botnet activity in IoT environments, increasing their use for real-time threat mitigation [9].

Deep-Learning Models	Definition
Convolutional Neural Network (CNN)	This is used to detect different variations of network traffic of botnet attacks by recognizing the patterns of the data.
Long Short-Term Memory (LSTM)	This is used to detect time-related dependencies by learning the patterns of unusual traffic data overtime
Gated Recurrent Unit (GRU)	It is the same as LSTM but uses lesser parameters that focus on dependencies that are sequential in network traffic for more efficiency.

Table 3 Deep-Learning Models [9]

It is to be found that CNN is the best model to use in implementing deep-learning models in an IDS because of its ability to efficiently recognize the threat's pattern of DDos attacks. It is shown in Figure 3 the results of the experiment when implementing the deep-learning models in the IDS. CNN scored the highest precision, recall and F1 score to determine the model that can identify efficiently the botnet attacks of the Mirai Malware [9].



Device	Precision			Recall			F1_score		
	CNN	LSTM	GRU	CNN	LSTM	GRU	CNN	LSTM	GRU
Device 1 (Doorbell)	97.53	93.96	94.15	98.15	94.94	95.26	97.78	94.20	94.52
Device 2 (Security Camera)	97.38	95.17	93.96	97.96	96.15	94.94	97.63	95.48	94.23
Device 3 (Thermostat)	97.53	94.12	94.03	98.25	95.30	94.91	97.61	94.53	94.26
Device 4 (Baby Monitor)	97.71	94.11	94.51	98.34	95.09	95.41	97.76	94.46	94.76

Figure 5 Evaluation Matrix of the four devices using the three deep-learning models to identify threat and attacks

Mirai Malware uses network scanning by sending sys scans to find devices that have their ports open to execute a brute-force attack on the device. When executing a brute-force attack on a device it usually uses usernames and passwords listed by the C&C server to find the correct credentials in order to put a Mirai Malware in the device [8]. The execution of the brute-force attack can be guessing the username and passwords by dictionary attacks by using common credentials to access and infect the device that can be vulnerable with DDos attacks [10].

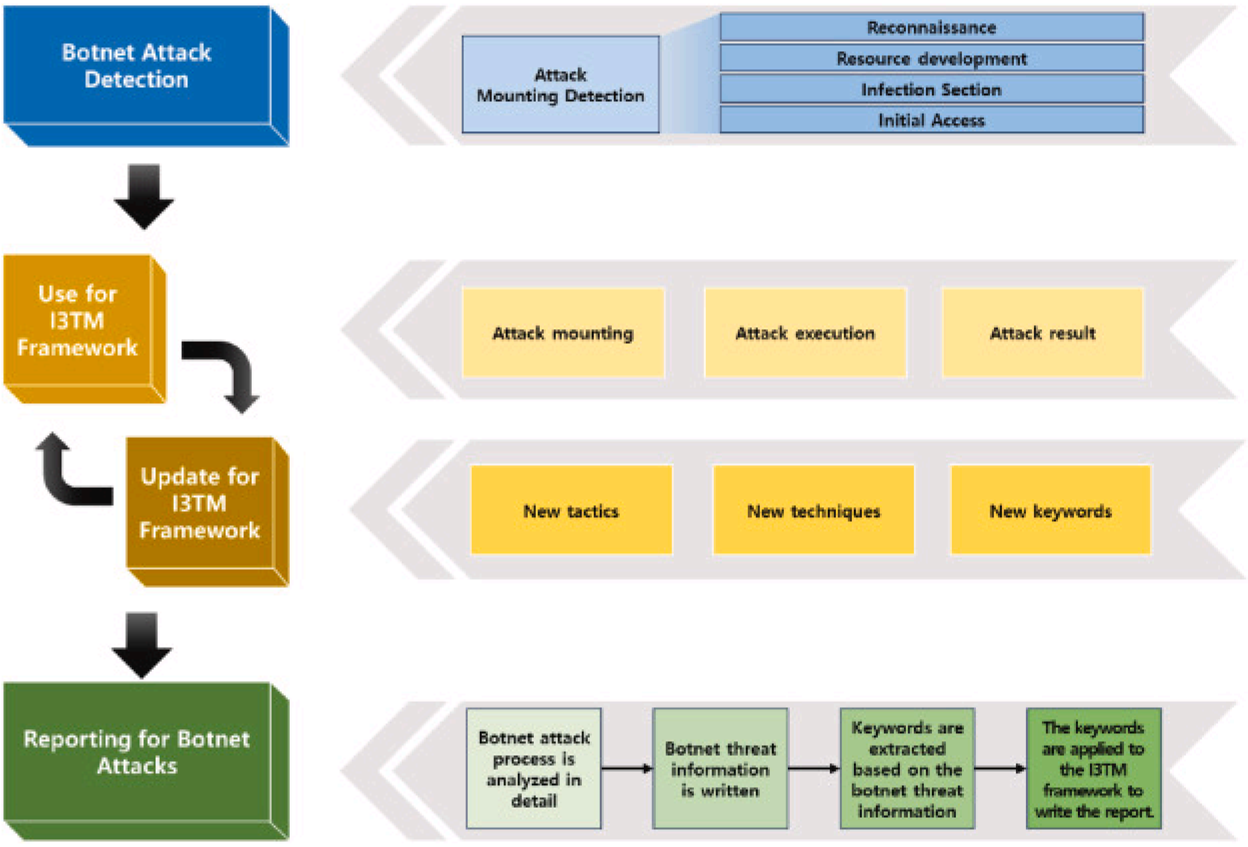
2.2.2 Adaptive IoT Network Security Through Network Segmentation and Honeypots

Besides the above IDS and deep learning methods, adaptive network approaches provide additional protection against botnet threats, such as network segmentation and IoT honeypots. Network segmentation means breaking up the network into several, isolated segments so that Mirai's spread is restricted when it reaches connected IoTs. This would not only confine the infected devices but also mitigate the damage done by any attack on crucial infrastructure. For example, if the IoTs were segmented from corporate or operation systems, then Mirai infection was restricted, and otherwise it could have made the required services halt.

IoT honeypots are a proactive defense and attract malware like Mirai to controlled environments where the security teams can observe how it works and gather some valuable data on its tactics, techniques, and procedures. This allows cybersecurity researchers the ability to study the evolutionary changes in malware and provide targeted countermeasures which can evolve with new versions of Mirai. For example, IoT honeypots have been used for monitoring the emerging Mirai variants and found insights of the new evasion strategies deployed by the malware, like circumventing traditional IDS and firewall rules[20].

2.3 Impact of Mirai Malware on the Evolution of Malware

Mirai was first introduced in 2016, and it could be said that that marked the turning point of the world of cybersecurity, especially about how malware attacks IoT devices. The source code of the malware became public and hackers have been working on it, leading to different strains with similar characteristics. This open-source release resulted in an increase of IoT-targeting malware variants, with attackers changing Mirai's structure to exploit more vulnerabilities and adapt to various IoT setups [13]. As a result, malware versions such as Bashlite and Okiru emerged, leveraging Mirai's modular structure to develop improved evasion strategies, attack coordination, and more advanced infection mechanisms [14].



Botnet Attack Detection
Attack Mounting Detection
Reconnaissance
Resource development
Infection Section
Initial Access
Use for I3TM Framework
Attack mounting
Attack execution
Attack result
Update for I3TM Framework
New tactics
New techniques
New keywords
Reporting for Botnet Attacks
Botnet attack process is analyzed in detail
Botnet threat information is written
Keywords are extracted based on the botnet threat information
The keywords are applied to the I3TM framework to write the report

Figure 6 I3TM framework [15]

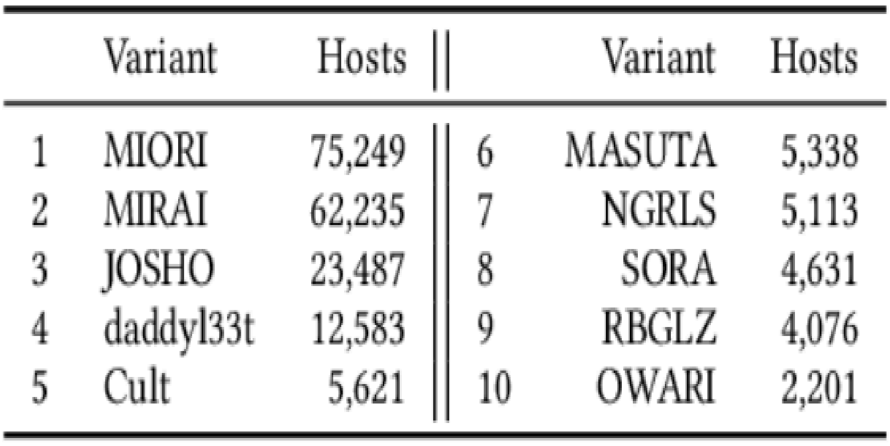
The I3TM framework, which uses certain strategies and approaches designed for IoT security, is one of the things that the Mirai malware offered. It allows for quick detection and reaction to botnet assaults on IoT devices in 5G environments. It improves the overall resilience of IoT networks against changing botnet tactics by regularly updating its analysis and reporting procedures to accommodate new threats [15].

Mirai has not only sparked a surge of similar botnet-based malware, but it has also put pressure on network administrators and IoT device makers to improve security protocols. Despite these initiatives, it has proven challenging to stay ahead of the constantly changing malware threats due to the increasing variety of IoT devices. Targeting devices ranging from routers to networked cameras and even medical IoT devices, attackers have developed malware that is more resilient as they continue to learn from Mirai's propagation strategies and botnet design [15]. Given that new variants like Mozi and Hajime show how Mirai's legacy continues to influence malware design and deployment worldwide, this changing threat landscape emphasizes the necessity of continuous research and proactive security measures [14].

2.3.1 Detailed Analysis of Variants

Mirai malware has developed into a variety of variations throughout time, each with unique traits and abilities that increase its potency as a cybersecurity threat. JOSHO and MASUTA, two of the most well-known of these variations, are built on the original Mirai foundation but have particular changes that allow them to adapt to different scenarios and target new vulnerabilities.

The JOSHO version of Mirai retains the core components of the original botnet while improving its scanning and infection capabilities. This variation offers a more advanced credential guessing mechanism that makes use of bespoke dictionaries tailored to certain device types. By utilizing this strategy, JOSHO may defeat security features that would otherwise prevent generic password assaults.Another popular variant, MASUTA, broadens Mirai's capabilities while employing novel evasion tactics to avoid detection by existing security measures. It features a more scattered command structure, making it more difficult for security teams to stop the botnet by focusing on a single command and control server.[17]



	Variant	Hosts		Variant	Hosts
1	MIORI	75,249	6	MASUTA	5,338
2	MIRAI	62,235	7	NGRLS	5,113
3	JOSHO	23,487	8	SORA	4,631
4	daddyl33t	12,583	9	RBGLZ	4,076
5	Cult	5,621	10	OWARI	2,201

Figure 2: Unique hosts for the top 10 advertised botnets.[1]

2.3.2 Advances in Deep Learning Approach Mirai malware

The evolution of Mirai malware has pushed the state-of-the-art in deep learning-based IoT security strategies. The notoriety of the malware has brought about a need for enhanced models that would predict and identify malware patterns before they can spread across the network. Recent studies have shown that deep learning models, particularly CNNs and RNNs, are highly effective in identifying and classifying IoT malware. 1D-CNN has been demonstrated to have high classification accuracy between benign and malicious network traffic, making it appropriate for real-time detection of IoT attacks, including Mirai variants. Such, 1D-CNN models are optimized for reducing their computational load; thus the efficiency of such models also ensures even when used under very resource-limited IoT scenarios to reach above 99% accuracy in common datasets used for IoT, as on CIC IoT 2023 and CIC-MalMem-2022[19].

Mirai spread through brute-force dictionary attacks suggests a need for more refined detection systems that identify patterns within the vast amounts of IoT traffic data. It involves deep learning models, self-attention mechanism-based models, that can isolate key features and emphasize data points that could indicate suspicious behavior; hence the accuracy is increased. In a model where self-attention layers have been included and Z-normalization is applied to the features of the dataset to standardize, researchers have developed state-of-the-art detection systems that can adapt in real-time to emerging threats with decreased false positives and increased detection rate across the spectrum of different types of attacks [19].

This will promise real-time application as the use of IoT devices is rapidly increasing worldwide. The future research direction emphasizes extending the datasets such as CIC IoT 2023 by incorporating more real-world scenarios that would ultimately support the detection of evolving Mirai-inspired attacks. Adaptive learning models will ultimately focus on improving the resiliency of IoT networks, however. Deep learning consequently becomes an especially crucial component in constant battles against complicated malware threats.

3. CONCLUSION

3.1 Findings and Implications for IoT Security

It shows the way Mirai malware influence on IoT security goes beyond the DDoS attacks that characterized its usage for the first time. By abusing weak authentication, Mirai spread across IoT devices rapidly and forced the world to focus on inherent vulnerabilities characterizing the IoT ecosystem.

This is basically how the Mirai malware works, from an architecture point of view but in the concrete modular way to attack, how the minimalist security settings of the IoT devices are utilized to create large botnets which have the possibility to freeze the important infrastructure and services. Increasing diversity and spreading of IoT devices further aggravates the threat with so many lacking standards due to their costs and convenience to the users [10, 11]. The open-source release of Mirai's code has further complicated the threat landscape, enabling the creation of numerous variants that continue to exploit the weaknesses of IoT devices. As Mirai-inspired malware evolves, the importance of enhanced security measures becomes ever more critical.

This work emphasizes that for fully secured IoT networks, manufacturer- and user-side enforcement must be carried out in such a manner that there must be stringent security measures applied at the manufacturing and installation phases, such as insisting on strong, unique passwords for access and ensuring updated firmware. These are first layers of defense that may prevent unauthorized access and their usage [13].

3.2 Future Directions for Research and Defense:

The future research should develop adaptive AI-driven security models that detect and neutralize threats in real-time to counter the ever-changing threat posed by Mirai and similar malware. Notably, the study points out the potential of deep learning models like CNNs and RNNs in improving Intrusion Detection Systems (IDS). These models are particularly useful in the IoT context, where they can autonomously analyze vast amounts of network data to detect anomalies associated with botnet activities. Expanding research in machine learning, particularly within anomaly detection and behavior-based analytics, is essential to ensure that detection systems remain effective against new, sophisticated malware variants [8].

Another set of suggestions made by the paper focuses on secure-by-design device manufacturers for IoT with architectures of zero-trust structure and network segmentation, a structure that avoids all potential malicious access, along with the containment of malware on one isolated network segment which cuts the scope of such threats. Future studies could emphasize better ways of doing these zero-trust protocols across IoT devices with constraints that can be in relation to resources. In addition, international regulations will enforce the standard framework for IoT security, ensuring that devices that will be introduced in the market must meet minimum security requirements. This will limit the malware exploitation threats within the IoT environment [14]. In conclusion, even though the heritage of Mirai is now dominating the environment of IoT security, the danger that the malware directed towards the IoT will present can be combated if better security measures are infused, legislation created, and modern technological developments taken into account. Therefore, developing new defense mechanisms for this new threat means ensuring IoT devices will be sources of strength rather than weaknesses in the world of connections.

REFERENCES:

[1] Christian Doerr and Harm Griffioen. 2020. Examining Mirai's Battle over the Internet of Things. Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, 743-756. https://dl.acm.org/doi/pdf/10.1145/3372297.3417277

[2] Huanran Wang et al. 2021. An evolutionary study of IOT malware. *IEEE Internet of Things Journal* 8, 20 (October 2021), 15422–15440. DOI:http://dx.doi.org/10.1109/jiot.2021.3063840

[3]Antonakakis, M., et al. (2017). Understanding the Mirai Botnet. In USENIX Security Symposium (pp. 1093–1110). https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf

[4]Hamdija Sinanovic and Sasa Mrdovic. 2017a. Analysis of mirai malicious software. *2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)* (September 2017), 1–5. DOI:http://dx.doi.org/10.23919/softcom.2017.8115504

[5]De Donno, M. *et al.* (2018) 'DDoS-capable IOT malwares: Comparative Analysis and Mirai Investigation', *Security and Communication Networks*, 2018, pp. 1–30. doi:10.1155/2018/7178164.

[6]Cloudflare. (2017). Inside Mirai: The Infamous IoT Botnet – A Retrospective Analysis. *Cloudflare Blog*. Retrieved from https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/

[7]Aishwarya Sawant Bhosle . 2021. Defense Against Mirai. California State University, Chico. Retrieved from https://scholarworks.calstate.edu/downloads/6108vj80x

[8]Vibhakar Mansotra, Antariksh Sharma, and Kuljeet Singh 2023. Detection of Mirai Botnet Attacks on IoT Devices Using Deep Learning. Journal of Scientific Research and Technology (JSRT), 1(6), 174-187. https://doi.org/10.5281/zenodo.8330561

[9]Huy Nguyen. 2024. Understanding the Mirai botnet attack type. (September 2024). Retrieved October 29, 2024 from https://www.corero.com/mirai-botnet-ddos-attack-type/

[10]Kolias, Constantinos & Kambourakis, Georgios & Stavrou, Angelos & Voas, Jeffrey. (2017). DDoS in the IoT: Mirai and other botnets. Computer. 50. 80-84. 10.1109/MC.2017.201.

[11]Bertino, Elisa & Islam, Nayeem. (2017). Botnets and Internet of Things Security. Computer. 50. 76-79. 10.1109/MC.2017.62.

[12]Doerr, C., & Griffioen, H. (2020). Examining Mirai's Battle over the Internet of Things. Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, 743-756. https://doi.org/10.1145/3372297.3417277

[13]Avira Protection Labs. 2023. How are Mirai variants infecting the IOT landscape? (February 2023). Retrieved October 29, 2024 from https://www.avira.com/en/blog/how-is-the-mirai-variant-infecting-the-iot-landscape

[14]Chunduri, Hrushikesh & Kumar, T. & Putrevu, Venkata Sai Charan. (2021). A Multi Class Classification for Detection of IoT Botnet Malware. 10.1007/978-3-030-76776-1_2.

[15]Jin, H. *et al.* (2024) 'A threat modeling framework for IOT-based botnet attacks', *Heliyon*, 10(20). doi:10.1016/j.heliyon.2024.e39192.

[17]Griffioen, H. and Doerr, C. (2020) 'Examining Mirai's battle over the internet of things', *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security* [Preprint]. doi:10.1145/3372297.3417277.

[18]Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. 2017. DDoS in the IOT: Mirai and other botnets. *Computer* 50, 7 (2017), 80–84. DOI:http://dx.doi.org/10.1109/mc.2017.201

[19]Taşcı, B. (2024). Deep-learning-based approach for IOT attack and malware detection. *Applied Sciences*, *14*(18), 8505. https://doi.org/10.3390/app14188505

[20]M. F. Razali, M. N. Razali, F. Z. Mansor, G. Muruti and N. Jamil, "IoT Honeypot: A Review from Researcher's Perspective," 2018 IEEE Conference on Application, Information and Network Security (AINS), Langkawi, Malaysia, 2018, pp. 93-98, doi: 10.1109/AINS.2018.8631494.