Understanding the Mirai Botnet: Architecture, Attack Mechanism and Defense Strategies

Dr R Anurekha
Assistant Professor
Department of Information Technology
Institute of Road and Transport Technology
Erode – 638316, Tamil Nadu, India

Abstract: The Mirai botnet is one of the most well-known and impactful malware strains targeting Internet of Things (IoT) devices. Since its emergence in 2016, Mirai has been responsible for launching large-scale Distributed Denial-of-Service (DDoS) attacks by exploiting weak credentials in IoT devices. This paper explores the working mechanism of Mirai, including its infection vector, command-and-control structure, attack strategies and impact on cybersecurity. Additionally, we analyze its legal implications, including cybercrime laws and government responses and discuss modern countermeasures, such as machine learning-based detection, network segmentation and firmware security enhancements. Understanding Mirai's operation is crucial in developing resilient IoT security frameworks to mitigate botnet-driven cyber threats.

Keywords: **Mirai botnet, IoT security, DDoS attacks, botnet architecture, malware analysis, cybercrime laws**

I. INTRODUCTION

Botnets have emerged as a significant threat to cybersecurity, enabling cybercriminals to launch Distributed Denial-of-Service (DDoS) attacks, data breaches and spam campaigns. Among these, the Mirai botnet, which surfaced in 2016, has been particularly notorious due to its ability to exploit vulnerable IoT devices and conduct large-scale DDoS attacks.

Mirai operates by scanning the internet for IoT devices with default or weak credentials and infecting them with malware, allowing attackers to launch high-volume, coordinated attacks. The impact of Mirai was widely felt when it targeted Dyn DNS, disrupting major websites like Twitter, Netflix and Reddit.

The rapid proliferation of IoT devices, coupled with inadequate security measures, has made botnet attacks like Mirai a growing concern. Many IoT manufacturers prioritize ease–of–use over security, shipping devices with hardcoded passwords and outdated firmware, making them easy targets for malware infections. Once a device is compromised, it becomes part of a botnet, contributing to malicious activities such as DDoS attacks, spam distribution and cryptojacking.

Furthermore, Mirai's source code was publicly released in 2016, leading to the emergence of multiple variants and adaptations. These evolved botnets incorporate advanced exploitation techniques, such as zero-day vulnerabilities and artificial intelligence-driven evasion tactics, making detection and mitigation increasingly challenging.

The consequences of Mirai–like attacks extend beyond service disruptions. Organizations face financial losses, reputational damage and potential regulatory penalties when their systems are compromised. Additionally, attacks on critical infrastructure, such as healthcare systems, financial services and government networks, highlight the need for stringent security policies and proactive defense mechanisms.

Understanding Mirai is essential for developing robust IoT security measures, as its architecture and methodologies have inspired numerous botnet variants. This paper examines Mirai's attack mechanisms, legal implications and defense strategies, aiming to provide a comprehensive insight into one of the most damaging cyber threats to date.

II. MIRAI BOTNET ARCHITECTURE AND INFECTION PROCESS

The architecture of the Mirai botnet consists of multiple key components working together to identify, infect and control vulnerable IoT devices.

2.1. Scanning Module (Bot Scanner)

Mirai operates by systematically scanning the internet for IoT devices that are still configured with factory-default usernames and passwords. The scanner checks for open Telnet (port 23/2323) and SSH (port 22) services, which often have weak or default credentials. These devices, including routers, IP cameras and DVRs, often lack strong security protections, making them prime targets for infection. Once a vulnerable device is found, Mirai attempts to log in using a hardcoded list of commonly used

username-password pairs. If successful, the malware installs itself and prepares the device to receive remote commands from the botnet operators.

2.2. Infection Module (Loader)

After gaining access, Mirai executes a lightweight downloader script to retrieve the main malware payload from a remote server. The payload is usually disguised to evade signature-based antivirus detection. Once installed, Mirai runs in the device's volatile memory (RAM) rather than writing to disk, ensuring that rebooting the device removes the malware (though reinfection can occur quickly).

2.3. Command-and-Control (C2) Server

Compromised IoT devices report back to a central C2 server, which is responsible for receiving and storing a list of infected bots, Sending attack commands to bots when needed and coordinating DDoS attacks by directing bots to target IPs and execute specific attack types.

The C2 infrastructure allows the attackers to issue commands to the infected devices, coordinating large-scale cyberattacks. The C2 server enables

- **Launching DDoS attacks**: Attackers can direct thousands of infected devices to flood a target with traffic, overwhelming its network.
- **Self-propagation**: The malware continuously scans for additional vulnerable IoT devices to infect, expanding the botnet.
- **Eliminating competing malware**: The C2 server also closes the unused ports to prevent other botnets from taking over the infected device. Mirai actively removes other malware strains from infected devices to maintain control over its botnet network.

2.4. Botnet Management (Admin Interface)

The botnet operators (attackers) interact with the botnet through an admin panel, typically accessible via a secured interface. From here, they can initiate DDoS attacks, view active bots and infection statistics and update malware payloads to bypass security patches.

2.5. Attack Execution Module

Once commanded by the C2 server, infected devices launch DDoS attacks against a target. Different attack methods include flooding attacks, protocol attacks and application layer attacks.

2.6. Persistence and Propagation

Mirai is designed to be memory-resident – it does not make permanent changes to the infected device's storage. Instead, it operates in volatile memory, which allows it to evade traditional forensic detection methods. However, this also means that a simple reboot of the infected device can remove Mirai. Despite this limitation, the botnet remains highly effective because of its continuous scanning and reinfection mechanisms. Once a device is rebooted, it often gets reinfected almost immediately if its security vulnerabilities remain unpatched.

To further expand its reach, Mirai propagates itself by instructing infected devices to scan random IP addresses, searching for other vulnerable IoT devices. This automated process ensures that the botnet can grow rapidly, allowing attackers to maintain a vast network of compromised devices ready to execute cyberattacks.

III. DDoS ATTACKS USING MIRAI

The Mirai botnet is particularly effective due to its ability to generate high-volume, complex DDoS attacks using a variety of attack vectors. These attacks aim to exhaust a target's network bandwidth, system resources, or application-layer capacity, rendering services inaccessible. The most common DDoS strategies used by Mirai include:

3.1. Volume-Based Attacks

These attacks focus on flooding the target's network bandwidth with massive amounts of traffic, preventing legitimate requests from being processed. They include:

- **UDP Floods**: The infected IoT devices send a high volume of User Datagram Protocol (UDP) packets to random ports on the target system, consuming bandwidth and overwhelming the victim's resources.
- **ICMP Floods (Ping Floods)**: Mirai-infected devices send an overwhelming number of Internet Control Message Protocol (ICMP) echo requests (pings) to the target, exhausting bandwidth and processing power.
- **SYN Floods**: A TCP SYN flood attack exploits the three-way handshake mechanism in TCP connections. Mirai bots send numerous SYN requests to a server but never complete the handshake, causing the victim's system to hold excessive half-open connections and consume resources.

3.2. Protocol Attacks

These attacks exploit weaknesses in network protocols, often targeting stateful network devices such as firewalls and load balancers. Common protocol-based attacks used by Mirai include:

- **TCP State Exhaustion Attacks**: Overloads TCP-based servers, firewalls and intrusion prevention systems (IPS) by exhausting their ability to track open connections.

- **Fragmented Packet Attacks:** Mirai bots send intentionally fragmented network packets that force the victim's system to reassemble them, consuming CPU and memory resources.

3.3. Application Layer Attacks

These attacks target specific services running on a web server, aiming to exhaust computing resources rather than just bandwidth. They often require fewer packets but can be just as disruptive. Mirai utilizes:

- **HTTP Floods**: The botnet continuously sends HTTP GET or POST requests to a website, overloading the web server with fake traffic.
- **Slowloris Attacks**: Mirai bots initiate partial HTTP requests and keep connections open indefinitely, consuming server resources without triggering traditional traffic-based defenses.

Each of these attack types can be combined into multi-vector DDoS attacks, making Mirai highly adaptable against different defense mechanisms.

IV. THE Dyn DNS ATTACK (2016)

Dyn was one of the largest Domain Name System (DNS) providers globally, offering services that helped translate domain names (e.g., twitter.com) into IP addresses. Major corporations such as Twitter, Netflix, Reddit, Spotify and Amazon relied on Dyn's infrastructure for web accessibility. A successful attack against Dyn meant that users across the internet could not reach these websites, even though the servers were operational.

On October 21, 2016, Mirai launched a massive DDoS attack against Dyn in three distinct waves, disrupting internet services across North America and Europe.

- **First Wave (Morning Attack)** – The attack began in the early morning (around 7 AM Eastern Time), with a massive flood of DDoS traffic targeting Dyn's DNS servers. The Mirai botnet utilized hundreds of thousands of IoT devices, including routers, security cameras and digital video recorders (DVRs), to send enormous amounts of junk traffic to Dyn's network. Dyn's servers struggled to handle the load, causing intermittent outages across major platforms.
- **Second Wave (Midday Surge)** – After a brief recovery period, Dyn was hit again around noon, with even greater intensity. This second wave completely crippled Dyn's infrastructure, making many websites unreachable to users. Websites such as PayPal, PlayStation Network and Airbnb were severely impacted.
- **Third Wave (Final Attempt & Mitigation Efforts)** – A third, weaker wave followed in the afternoon, but by then, Dyn's security teams and ISPs had started implementing countermeasures to mitigate the attack. Traffic filtering techniques and network rerouting helped reduce the impact and by evening, services were mostly restored.

4.1. Impact of the Attack

The attack on Dyn was unprecedented in terms of scale and impact, setting records as one of the largest DDoS attacks in history, peaking at over 1.2 Tbps. The consequences included:

- **Massive Internet Downtime**: Many of the world's most popular websites were completely inaccessible for several hours, affecting millions of users. The disruption spread beyond the United States, impacting users in Europe and parts of Asia.
- **Increased Awareness of IoT Vulnerabilities**: The attack demonstrated how insecure IoT devices could be weaponized, prompting industry-wide concerns over default credentials and lack of firmware updates. Following the attack, major IoT manufacturers were urged to improve security standards.
- **Regulatory and Industry Response:** Cybersecurity firms, governments and ISPs started developing stricter security guidelines for IoT devices. The U.S. Department of Homeland Security (DHS) and the Federal Trade Commission (FTC) launched investigations into IoT security. Companies like Google, Microsoft and Amazon invested in DDoS protection services and DNS redundancy strategies to mitigate future attacks.

The Dyn DNS attack underscored the urgent need for stronger IoT security, requiring manufacturers to eliminate default passwords, enforce firmware updates, and comply with regulatory security standards. To enhance resilience, organizations must implement DNS infrastructure redundancy by using multiple DNS providers and leveraging DDoS mitigation services to absorb attack traffic. Additionally, advanced DDoS protection is essential, as traditional firewalls and intrusion detection systems (IDS) proved ineffective against such large-scale attacks.

V. LEGAL IMPLICATIONS OF MIRAI ATTACKS

The Mirai botnet's massive DDoS attacks highlighted the legal and regulatory gaps in cybersecurity, particularly in IoT device security. As a result, law enforcement agencies and governments worldwide have taken steps to prevent similar attacks by strengthening cybercrime laws, prosecuting the perpetrators and implementing stricter security standards for IoT manufacturers.

5.1 Cybercrime Laws

Several international cybercrime laws govern botnet attacks like Mirai, enuring that perpetrators can be prosecuted under strict legal frameworks. The most relevant laws include:

Computer Fraud and Abuse Act (CFAA) – United States

Enacted in 1986, the CFAA criminalizes unauthorized access to computer systems, making it applicable to DDoS attacks, botnet operations and malware distribution. Individuals found guilty of launching DDoS attacks can face up to 10 years in prison, with additional fines.

General Data Protection Regulation (GDPR) – Europe

The GDPR introduced strict cybersecurity regulations, making companies liable for failing to secure user data. It mandates IoT manufacturers to implement strong security measures to prevent botnet infections like Mirai. Organizations failing to secure IoT devices from Mirai-like threats can face fines of up to €20 million or 4% of annual global revenue.

Information Technology (IT) Act – India

The IT Act, 2000 criminalizes unauthorized access, hacking and DDoS attacks in India. Section 66 of the act penalizes cybercrimes, including botnet-related offenses, with imprisonment of up to 3 years and heavy fines.

5.2 Government and Industry Responses

The Mirai botnet attacks triggered global regulatory action, leading to new government policies, industry standards and cybersecurity collaborations. Some significant Government Initiatives to Strengthen IoT Security include

U.S. IoT Cybersecurity Improvement Act

This federal law mandates stricter IoT security requirements, ensuring that government agencies only purchase secure IoT devices. It requires elimination of default credentials and regular software updates to prevent botnet infections.

European Union Cybersecurity Act

Established a certification framework for IoT devices, ensuring that manufacturers design secure hardware and software. Encourages companies to conduct regular penetration testing to identify and patch vulnerabilities.

Asia-Pacific and Other Global Efforts

Japan passed legislation allowing ethical hacking of IoT devices to identify vulnerable products before cybercriminals exploit them. China introduced new IoT security regulations to hold manufacturers responsible for unprotected devices.

Industry Actions to Combat Botnets

Elimination of Default Credentials

Major IoT manufacturers (e.g., Cisco, Huawei, Netgear) have removed default usernames and passwords, reducing the risk of Mirai-style infections. Devices now require strong password creation upon initial setup.

Cloud-Based DDoS Mitigation Services

Companies like Cloudflare, Akamai and AWS Shield offer automated DDoS protection that detects Mirai-style botnet traffic and blocks attacks in real time.

Collaboration Between Law Enforcement and Cybersecurity Firms

The FBI, Interpol and cybersecurity researchers actively track Mirai variants and work to shut down botnet-controlled infrastructure. A global law enforcement effort took down hundreds of Mirai-controlled servers and arrested multiple botnet operators.

The legal consequences of Mirai attacks have led to tougher cybersecurity regulations, criminal prosecutions and enhanced IoT security standards. Governments, law enforcement and the private sector continue to adapt to emerging threats by strengthening cybercrime laws and enforcing strict security guidelines for IoT manufacturers. By understanding the legal landscape and regulatory responses, organizations can take proactive steps to secure IoT ecosystems and prevent botnet-driven cyberattacks in the future.

VI. CONCLUSION

The Mirai botnet marked a turning point in cybersecurity by exposing the vulnerabilities of Internet of Things (IoT) devices and demonstrating the devastating impact of large-scale Distributed Denial-of-Service (DDoS) attacks. Despite legal actions and improved security measures, botnets like Mirai continue to evolve, exploiting poorly secured IoT ecosystems and posing persistent threats to global networks. Addressing this challenge requires a multi-layered security approach integrating network defenses, machine learning-based detection and robust IoT security enhancements.

Network-based defense mechanisms such as Intrusion Detection and Prevention Systems (IDS/IPS) help monitor traffic anomalies, while rate limiting and filtering mitigate excessive connection attempts, reducing the risk of DDoS amplification. However, traditional defense methods are often reactive, requiring advanced threat detection techniques to combat the dynamic nature of botnets.

To improve real-time detection, machine learning-based approaches leverage supervised learning models and deep learning techniques to identify botnet traffic patterns before they escalate into full-scale attacks. These AI-driven methods significantly enhance threat intelligence and proactive mitigation strategies.

At the core of long-term security is IoT security enhancement, which includes eliminating default credentials, enforcing regular firmware updates and adopting zero-trust security models to prevent

unauthorized access. Manufacturers and regulatory bodies play a critical role in enforcing security standards, ensuring that IoT devices are designed with built-in cybersecurity measures rather than being left vulnerable to exploitation.

Looking ahead, future challenges in cybersecurity will be shaped by AI-driven botnets, which can autonomously adapt to defense mechanisms and quantum computing advancements, which may render current encryption methods obsolete. Additionally, the lack of global regulatory enforcement for IoT security highlights the need for international cybersecurity frameworks to address emerging cyber threats in a unified manner.

In conclusion, while significant progress has been made in mitigating Mirai-style attacks, the evolving nature of cyber threats necessitates continuous innovation in security technologies and global cooperation. Strengthening IoT defenses, enhancing AI-driven threat detection and establishing universal cybersecurity regulations will be essential to protecting critical infrastructure from next-generation botnet attacks.

REFERENCES

[1]. C. Kolias, G. Kambourakis, A. Stavrou and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," in Computer, vol. 50, no. 7, pp. 80-84, 2017, doi: 10.1109/MC.2017.201.

[2]. N. Hoque, D. K. Bhattacharyya and J. K. Kalita, "Botnet in DDoS Attacks: Trends and Challenges," in IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2242-2270, 2015.

[3]. S. T. Zargar, J. Joshi and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," in IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2046-2069, 2013, doi: 10.1109/SURV.2013.031413.00127.

[4]. S. Khattak, N. R. Ramay, K. R. Khan, A. A. Syed and S. A. Khayam, "A Taxonomy of Botnet Behavior, Detection, and Defense," in IEEE Communications Surveys & Tutorials, vol. 16, no. 2, pp. 898-924, 2014, doi: 10.1109/SURV.2013.091213.00134.

[5]. J. Mirkovic and P. Reiher, A taxonomy of DDoS attack and DDoS defense mechanisms ACM SIGCOMM Computer Communications Review, vol. 34, no. 2, pp. 39-53, April 2014.

[6]. S. Ranjan, R. Swaminathan, M. Uysal and E. Knightly, DDoS-Resilient Scheduling to Counter Application Layer Attacks under Imperfect Detection IEEE INFOCOM06, 2015.

[7]. R. K. C. Chang, Defending against flooding-based distributed denial of service attacks: A tutorial Computer J. IEEE Commun. Magazine, vol. 40, no. 10, pp. 42-51, 2012.

[8]. J. Liu, Y. Xiao, K. Ghaboosi, H. Deng and J. Zhang, Botnet: Classification Attacks Detection Tracing and Preventive Measures EURASIP J. Wireless Communications and Networking, 2009.

[9]. Priyanka and M. Dave, "A review of recent Peer-to-Peer botnet detection techniques," 2015 2nd International Conference on Electronics and Communication Systems (ICECS), Coimbatore, India, 2015, pp. 1312-1317, doi: 10.1109/ECS.2015.7124797.

[10]. W. Ding, W. Ren, Z. Xia and L. Wang, "Botnet tracing based on distributed denial of service activity analysis," 2015 8th International Conference on Biomedical Engineering and Informatics (BMEI), Shenyang, China, 2015, pp. 685-689, doi: 10.1109/BMEI.2015.7401590.