National Telecommunication Institute

MIRAI BOTNET

RESEARCH

Prepared by: Ahmed Moataz Abdelmonem Elrefaey

National Telecommunication Institute

Abstract

The Mirai botnet remains a prominent and persistent threat within the Internet of Things (IoT) ecosystem. First observed in 2016, Mirai transformed poorly secured IoT devices into a large-scale distributed platform capable of launching volumetric DDoS attacks and other malicious activities. Although its original source code was publicly released years ago, Mirai continues to evolve through multiple variants that leverage weak authentication, exposed management interfaces, and newly disclosed vulnerabilities. This paper examines Mirai's architecture, infection vectors, historical impact, indicators of compromise, and practical mitigation strategies, and offers an analytical perspective on systemic causes that sustain Mirai-like campaigns.

1. Introduction

The proliferation of networked devices—cameras, routers, digital video recorders, and other embedded systems—has created a vast attack surface for adversaries. Many of these device's ship with minimal security controls and receive infrequent firmware updates. Mirai exploited these conditions to enroll large populations of devices into botnets that deliver coordinated attacks at internet scale. Beyond the malware itself, Mirai is instructive as an example of how design decisions, vendor practices, and operational policies collectively produce persistent risk.

2. Background and Evolution

Mirai emerged publicly in 2016 and quickly became notorious after several high-profile DDoS incidents. The leak of Mirai's source code enabled a proliferation of forks and derivatives, each adapting to new targets, CPU architectures, and exploitation techniques. Over subsequent years, actors produced variants that expanded support to additional device architectures, added new propagation modules, and, in some cases, integrated alternate payloads such as proxying or resource mining. The result is an active ecosystem rather than a single, static malware strain.

3. Architecture and Core Components

A Mirai-style botnet typically comprises three functional layers:

- **Infected Devices (Bots):** Lightweight malware binaries that execute on compromised IoT devices, often loaded into memory to avoid persistent storage and to evade simplistic

firmware checks. Bots await commands and can execute attacks, scan for new targets, and fetch payload updates.

- **Command-and-Control (C2):** Centralized or partially distributed servers orchestrate the botnet, issuing attack commands, coordinating downloads, and managing operator control channels.
- **Propagation/Loader Infrastructure:** Scanners discover new vulnerable hosts across the IPv4 space; loader infrastructure delivers architecture-appropriate binaries or exploits to complete compromise.

This modular architecture enables rapid adaptation: new scanning patterns, credential dictionaries, or exploit modules can be integrated without rewriting the core attack logic.

4. Infection Vectors

Mirai and its derivatives primarily propagate via two mechanisms:

- **Credential-based compromise:** Many IoT devices retain factory-default credentials or otherwise weak authentication. Mirai's original approach used a dictionary of common username/password pairs to brute-force Telnet/SSH services and gain shell access.
- **Exploit-driven compromise:** Newer variants incorporate publicly disclosed vulnerabilities (command injection, unauthenticated RCEs, logic flaws in management interfaces) to achieve remote code execution without credential guessing. This shift toward CVE exploitation increases infection speed and expands the set of viable targets.

5. Operational Impact and Notable Incidents

Mirai-powered attacks demonstrated that large pools of low-capability devices can generate enormous aggregate bandwidth and packet rates, enabling volumetric and protocol-layer DDoS that disrupt critical infrastructure and consumer services. Notable operational impacts include takedowns and severe degradations of major online services during past incidents, and ongoing use of Mirai-style networks for denial-of-service, proxying, and other criminal activities. The continued discovery of Mirai variants years after its initial exposure underscores the persistent operational relevance of the threat.

National Telecommunication Institute

6. Indicators of Compromise (IoCs) and Detection Signals

Typical indicators of Mirai infection include:

- Unexplained increases in outbound traffic originating from IoT hosts.
- Repeated login attempts or scanning behavior observed in logs for management interfaces.
- Presence of unfamiliar processes or binaries in device memory (on devices that allow inspection).
- Sudden network performance degradation or anomalous contact patterns to uncommon endpoints.

Detection strategies focus on network-level telemetry, anomaly detection for device behavior baselines, and timely ingestion of threat intelligence that highlights emergent C2 artifacts and scanning signatures.

7. Mitigation and Defensive Measures

Mitigation requires both device-level hygiene and network-level controls:

- **Credential hygiene:** Enforce immediate replacement of factory-default credentials and require unique, strong passwords on all devices.
- **Disable unnecessary remote management:** Turn off or tightly restrict remote administration interfaces (e.g., UPnP, Telnet, unneeded web management) that expose devices to the public Internet.
- **Network segmentation:** Place IoT devices on isolated network segments or VLANs with strictly limited cross-segment privileges, reducing lateral movement risk.
- **Egress filtering and rate limiting:** At network gateways, implement egress controls and rate limits to prevent a single compromised device from generating large-scale outbound attack traffic.
- **Patch and update management:** Maintain a prioritized program for firmware updates and vulnerability remediation for network edge devices and management servers.
- **Monitoring and response:** Deploy IDS/IPS and anomaly detection tuned for IoT behavioral baselines; integrate automated alerting and containment workflows.

These measures, when combined, materially reduce both the probability of compromise and the potential impact of an infection.

8. Analytical Perspective: Why Mirai Persists

Mirai's longevity is less of a function of coding sophistication and more a consequence of systemic weaknesses across the IoT ecosystem. Three structural issues drive persistence:

1. **Vendor practices:** Devices are frequently shipped with weak defaults, lacking mandatory first-use credential changes or robust automatic update mechanisms.
2. **Operational constraints:** ISPs and enterprises often prioritize connectivity and ease-of-use over segmentation and strict egress controls, leaving devices exposed.
3. **User behavior and economics:** Consumers and small organizations rarely prioritize firmware maintenance or invest in network segmentation for low-cost devices.

Addressing Mirai therefore requires coordinated changes across product design, service provider policy, and user education—technical fixes alone are necessary but not sufficient.

9. Conclusion

The Mirai botnet exemplifies how distributed, low-capability devices can be aggregated into powerful attack platforms when security practices and system design choices are neglected. Effective defense demands a systemic approach that spans secure device defaults, enforceable update mechanisms, network architecture that contains infected hosts, and continuous monitoring. Only by addressing the sociotechnical roots of IoT insecurity can Mirai-like threats be meaningfully reduced.