Hive Pro

Threat Level

Red

HiveForce Labs

# THREAT ADVISORY

## ATTACK REPORT

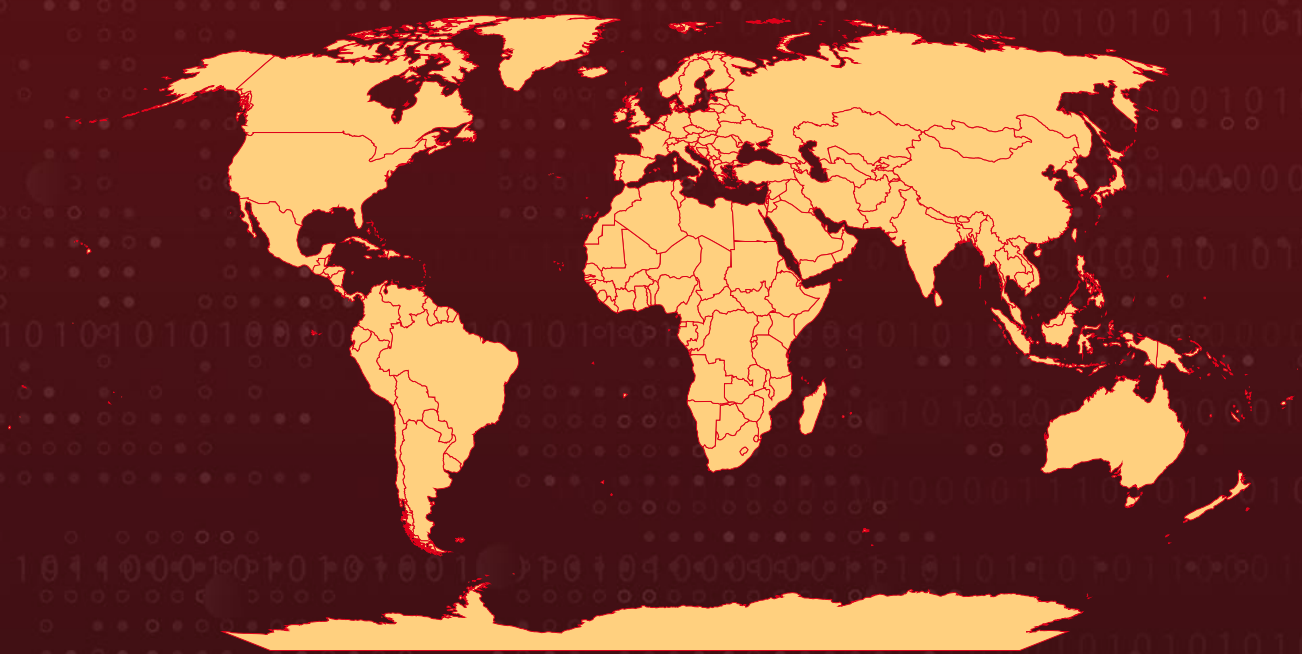
# Aquabotv3: The Next Evolution of Mirai in DDoS Attacks

| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| January 31, 2025 | A1 | TA2025027 |

# Summary

**Attack Discovered:** January 2025
**Targeted Countries:** Worldwide
**Malware:** Aquabotv3
**Attack:** A new Mirai botnet variant, Aquabotv3, is spreading this time offering DDoS-as-a-service by exploiting vulnerabilities in Mitel SIP phones. What sets this strain apart is its ability to establish direct communication with attacker-controlled command-and-control (C2) servers. Researchers have identified it as an evolution of Aquabot, that actively exploits CVE-2024-41710, a command injection flaw in Mitel SIP devices. This development highlights the growing sophistication of botnet operations and the increasing risks to unpatched enterprise communication systems.

## Attack Regions



## CVEs

| CVE | NAME | AFFECTED PRODUCT | ZERO-DAY | CISA KEV | PATCH |
|---|---|---|---|---|---|
| CVE-2024-41710 | Mitel SIP Phones Command Injection Vulnerability | Mitel SIP Phones | ✗ | ✗ | ✓ |
| CVE-2018-17532 | Teltonika RUT9XX OS Command Injection Vulnerability | Teltonika RUT9XX | ✗ | ✗ | ✓ |
| CVE-2023-26801 | lb-link bl-lte300_firmware Command Injection Vulnerability | lb-link bl-lte300_firmware | ✗ | ✗ | ✗ |
| CVE-2022-31137 | Roxy Wi Remote Code Execution Vulnerability | Roxy Wi | ✗ | ✗ | ✓ |
| CVE-2018-10562 | Dasan GPON Routers Command Injection Vulnerability | Dasan GPON home routers | ✗ | ✓ | ✗ |
| CVE-2018-10561 | Dasan GPON Routers Command Injection Vulnerability | Dasan GPON home routers | ✗ | ✓ | ✗ |

# Attack Details

**#1**

Aquabot, a botnet based on the infamous Mirai malware, has undergone significant upgrades over time. The first version closely followed Mirai's original design, while the second introduced techniques to hide itself and stay active on infected systems for longer. Now, the third version, Aquabotv3, brings a major innovation direct communication with its C2 server in response to specific system signals. This makes the botnet more adaptable, harder to detect, and more difficult to shut down.

**#2**

In early January 2025, researchers discovered active exploit attempts targeting CVE-2024-41710 a known vulnerability in Mitel SIP phones. The attack payload was almost identical to a publicly available proof-of-concept (PoC), designed to download and execute a script which then installed Mirai malware on compromised systems. Further analysis confirmed that this attack was linked to Aquabot's latest version, which shares features with its predecessor but also introduces several new capabilities.

**#3** Aquabotv3 retains Mirai's traditional DDoS attack methods but adds a new function called "defend_binary()." This feature allows the malware to listen for specific system signals and respond accordingly. When the malware detects such a signal, it marks itself as "defended" and immediately sends a message to its C2 server over a TCP connection, informing the operators that a system event has been intercepted. Additionally, Aquabotv3 can terminate specific processes, such as locally running command-line shells, to prevent users from manually stopping it, ensuring it remains active on the system.

**#4** To avoid detection, Aquabotv3 uses obfuscation techniques. It renames itself as "httpd.x86" and maintains communication with its C2 server while staying hidden from security tools. In addition to targeting Hadoop YARN, Aquabotv3 exploits several known security vulnerabilities, including CVE-2018-10561, CVE-2018-10562, CVE-2018-17532, CVE-2022-31137, CVE-2023-26801, and a remote code execution flaw affecting Linksys E-series devices.

**#5** Aquabot have been actively advertising it as a "DDoS-as-a-service" on Telegram. Many of these sellers falsely claim that their service is meant for security testing or educational purposes. However, they are running and managing large-scale botnets. One notable example includes a website they promoted as a tool for testing DDoS mitigation, which was later found to be distributing Mirai malware, proving that Aquabot is actively used for cyberattacks rather than legitimate research.

# Recommendations

**Apply Patch:** To protect against known exploits like CVE-2024-41710 and other vulnerabilities, it's crucial to apply the latest security updates to IoT devices, routers, and servers. Keeping your systems up-to-date helps prevent attackers from taking advantage of these flaws, ensuring better security and reducing the risk of a successful exploit.

**Monitor Anomalies:** Stay vigilant by continuously monitoring network traffic for any unusual activity, such as unexpected outbound connections to known command-and-control (C2) servers. Detecting these anomalies early can help identify potential threats before they cause significant damage.

**Restrict Network Exposure:** Segment VoIP systems from the internet and internal corporate networks. Implement firewall rules to block unauthorized traffic to and from SIP devices. Disable unused SIP features to minimize the attack surface.

**Strengthen Endpoint Defense:** Implement advanced Endpoint Detection and Response (EDR) solutions to effectively detect, analyze, and mitigate in-memory malware activity, ensuring comprehensive protection against sophisticated threats.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| **TA0042** Resource Development | **TA0002** Execution | **TA0003** Persistence | **TA0005** Defense Evasion |
| **TA0007** Discovery | **TA0011** Command and Control | **TA0040** Impact | **T1588** Obtain Capabilities |
| **T1588.006** Vulnerabilities | **T1588.005** Exploits | **T1059** Command and Scripting Interpreter | **T1498** Network Denial of Service |
| **T1071** Application Layer Protocol | **T1057** Process Discovery | **T1036** Masquerading | **T1001** Data Obfuscation |
| **T1583** Acquire Infrastructure | **T1583.005** Botnet | **T1203** Exploitation for Client Execution | |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| IPv4 | 89[.]190[.]156[.]145, 91[.]92[.]243[.]233, 213[.]130[.]144[.]69, 154[.]216[.]16[.]109, 193[.]200[.]78[.]33, 173[.]239[.]233[.]47, 141[.]98[.]11[.]67, 141[.]98[.]11[.]175, 173[.]239[.]233[.]48, 173[.]239[.]233[.]46 |

| TYPE | VALUE |
| --- | --- |
| Domains | dogmuncher[.]xyz, cardiacpure[.]ru, fuerer-net[.]ru, eye-network[.]ru, intenseapi[.]com, cloudboats[.]vip, theeyefirewall[.]su, awaken-network[.]net |
| SHA256 | 597b84ba23e16b24ec17288981bbf65c84b6ba3bb07df6620378a1907692fb86, 6a070dc9614dbb9a76092258fdc8bd758f69126c73787dc7d2af9aebd436e7ec, b41e29e745b69f3e8c11d105e7e050fd9e08ff1e22efd97fd4c239a9095d708b, b5d1cf8b222162567f46281e792145774689c205701a02f3723cf6fb13a429de, 1e74bcd24e30947bd14cef6731ca63f69df060ba3dcac88b2321171335a6e8ef, e06c3f5c32aaa422e66056290eb566065afe2ce611fe019f3ba804af939ac1a3 |

## Patch Link

CVE-2024-41710:
https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-24-0019

CVE-2018-17532:
https://wiki.teltonika-networks.com/view/RUT900_Firmware_Downloads_(legacy_WebUI)

CVE-2022-31137:
https://github.com/roxy-wi/roxy-wi/releases/tag/v8.1.4

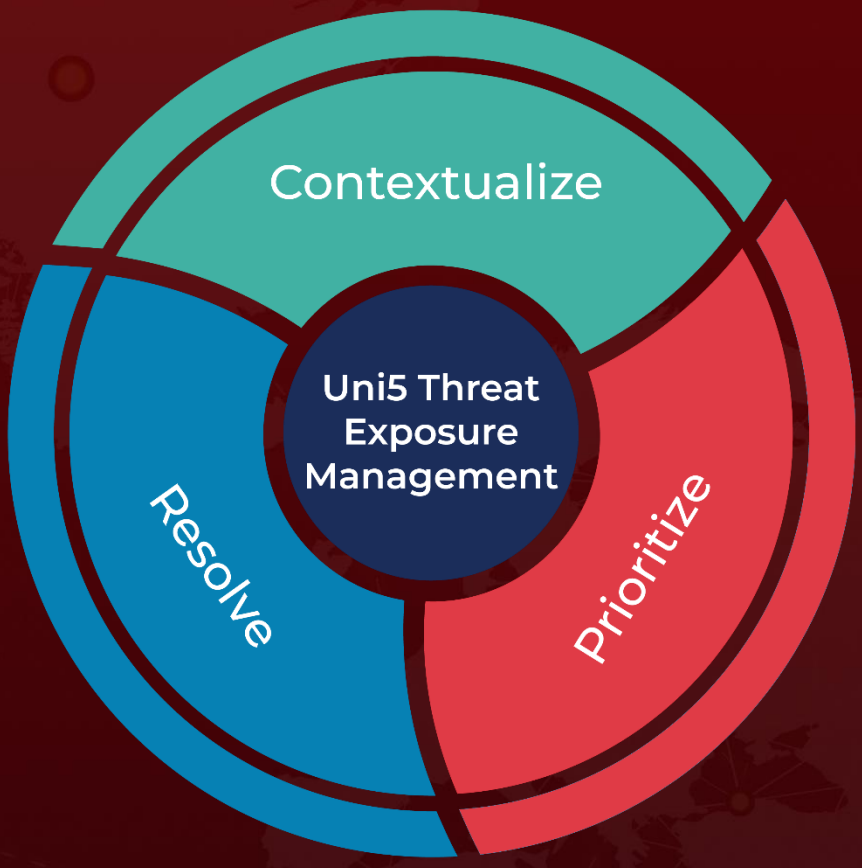
## References

https://www.akamai.com/blog/security-research/2025-january-new-aquabot-mirai-variant-exploiting-mitel-phones

# What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.




REPORT GENERATED ON

**January 31, 2025 • 7:10 AM**



More at www.hivepro.com