VULNERABILITIES

GreyNoise Discovers Stealthy Backdoor Campaign Affecting Thousands of ASUS Routers

GreyNoise Research May 28, 2025

This activity was first discovered by GreyNoise on March 18, 2025. Public disclosure was deferred as we coordinated the findings with government and industry partners.

GreyNoise has identified an ongoing exploitation campaign in which attackers have gained unauthorized, persistent access to thousands of ASUS routers exposed to the

internet. This appears to be part of a stealth operation to assemble a distributed network of backdoor devices — potentially laying the groundwork for a future botnet.

The tactics used in this campaign — stealthy initial access, use of built-in system features for persistence, and careful avoidance of detection — are **consistent with those seen in advanced, long-term operations, including activity associated with advanced persistent threat (APT) actors and operational relay box (ORB) networks.** While GreyNoise has made no attribution, the level of tradecraft suggests a well-resourced and highly capable adversary.

The attacker's access survives both reboots and firmware updates, giving them durable control over affected devices. The attacker maintains long-term access without dropping malware or leaving obvious traces by chaining authentication bypasses, exploiting a known vulnerability, and abusing legitimate configuration features.

The activity was uncovered by Sift — GreyNoise's proprietary AI-powered network payload analysis tool — in combination with fully emulated ASUS router profiles running in the GreyNoise Global Observation Grid. These tools enabled us to detect subtle exploitation attempts buried in global traffic and reconstruct the full attack sequence.

Read the full technical analysis.

Timeline of Events

March 17, 2025: GreyNoise's proprietary AI technology, Sift, observes anomalous traffic.

March 18, 2025: GreyNoise researchers become aware of Sift report and begin investigating.

March 23, 2025: Disclosure deferred as we coordinated the findings with government and industry partners.

May 22, 2025: Sekoia announces compromise of ASUS routers as part of ‘ViciousTrap.’

May 28, 2025: GreyNoise publishes this blog.

Summary of Findings

- **Thousands of ASUS routers are confirmed compromised**, with the number steadily increasing.
- Attackers gain access using brute-force login attempts and authentication bypasses, including techniques not assigned CVEs.
- Attackers exploit CVE-2023-39780, a command injection flaw, to execute system commands.
- They use legitimate ASUS features to:
  - Enable SSH access on a custom port (TCP/53282).
  - Insert attacker-controlled public key for remote access.
- **The backdoor is stored in non-volatile memory (NVRAM) and is therefore not removed during firmware upgrades or reboots.**
- No malware is installed, and **router logging is disabled to evade detection.**
- The techniques used reflect long-term access planning and a high level of system knowledge.

How GreyNoise Found It

The campaign was surfaced by Sift, GreyNoise’s AI-powered analysis tool for detecting novel and anomalous network activity. Sift flagged just three HTTP POST requests — targeting ASUS router endpoints — for deeper inspection.

These payloads were only observed on our fully emulated ASUS profiles running factory firmware. This infrastructure allowed GreyNoise to:

- Capture full PCAP of the requests and router behavior.
- Reproduce the attack in a controlled environment.
- Confirm how the backdoor is installed and how it persists.

Without emulated profiles and deep inspection, this attack would likely have remained invisible. The attacker disables logging and uses official router features, leaving few traces.

Confirmed Exploitation Chain

1. Initial Access

- Brute-force login attempts.
- Two authentication bypass techniques (no CVEs assigned).

2. Command Execution

- Exploitation of CVE-2023-39780 to run arbitrary commands.

3. Persistence

- SSH access is enabled via official ASUS settings.
- Attacker inserts a custom public SSH key.
- Configuration is stored in NVRAM, not on disk.

4. Stealth

- Logging is disabled before persistence is established.
- No malware is left behind.

Scope and Visibility

- **As of May 27, nearly 9,000 ASUS routers are confirmed compromised**, based on scans from Censys — a platform that continuously maps and monitors internet-facing assets across the global internet. Censys reveals what's exposed; GreyNoise shows which of those assets are being actively targeted.
- The number of affected hosts is growing.
- **GreyNoise sensors saw just 30 related requests across three months**, demonstrating how quietly this campaign is operating.

Indicators of Compromise

IP addresses involved in this activity:

```
101.99.91.151
101.99.94.173
79.141.163.179
111.90.146.237
```

COPY

BLOCK MALICIOUS IPS

Backdoor port:

```
TCP/53282
```

COPY

Attacker SSH public key (truncated):

```
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAo41nBoVFfj4HlVMGV+YPsxMDrMlbdDZ...
```

COPY

Has ASUS Released a Patch?

- ASUS patched CVE-2023-39780 in a recent firmware update.
- The initial login bypass techniques are patched but do not have assigned CVEs.
- The attacker's SSH configuration changes are **not removed by firmware upgrades.**

If a router was compromised before updating, the backdoor will still be present unless SSH access is explicitly reviewed and removed.

Recommendations

- Check ASUS routers for SSH access on TCP/53282.
- Review the *authorized_keys* file for unauthorized entries.
- Block the four IPs listed above.
- If compromise is suspected, perform a full factory reset and reconfigure manually.

Block IPs & Read the Full Analysis

For payload details, firmware analysis, and attack reconstruction:

Read the full technical analysis.

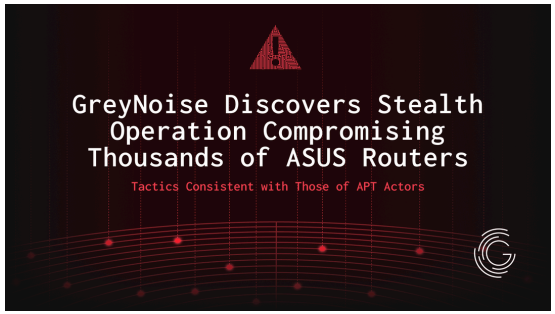
BLOCK MALICIOUS IPS

GreyNoise is developing an enhanced dynamic IP blocklist to help defenders take faster action on emerging threats. Click here to learn more or get on the waitlist.

Like or share:

Related content

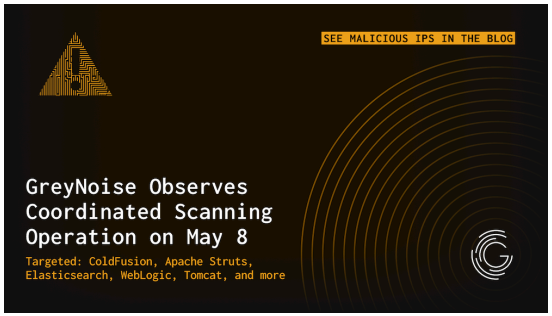
View all related articles →



VULNERABILITIES

GreyNoise Discovers Stealthy Backdoor Campaign Affecting Thousands of ASUS Routers

GreyNoise Research May 28, 2025



VULNERABILITIES

Coordinated Cloud-Based Scanning Operation Targets 75 Known Exposure Points in One Day

Noah Stone May 27, 2025

VULNERABILITIES

Ivanti EPMM Zero-Days: Reconnaissance to Exploitation

boB Rudis May 16, 2025

GreyNoise Love