Tracking AyySSHush: a Newly Discovered ASUS Router Botnet Campaign

censys.com/blog/tracking-ayysshush-a-newly-discovered-asus-router-botnet-campaign

Author

Himaja Motheram
Security Researcher | Co-Host, Storm ⚡Watch Podcast

Himaja Motheram is a Security Researcher who is passionate about continuous learning and tackling complex challenges in vulnerability measurement. As a co-host of the Storm ⚡Watch podcast, she discusses emerging threats, industry trends, and new research. As a proud University of Michigan graduate, she values sharing knowledge and tools to help the security community.

Executive Summary:

- A **new, stealthy ASUS router botnet**, dubbed **AyySSHush**, abuses **trusted firmware features** through a multi-stage attack sequence to backdoor routers and **persist across firmware updates**, evading traditional detection methods.
- GreyNoise observed the campaign in **March 2025**; Censys scan data reveals its **global footprint** and how it's evolved over the past five months
- **4,504 ASUS devices** show indicators of compromise as of **May 28, 2025**, identified by having SSH running on **port TCP/53282** — a relatively strong indicator of AyySSHush compromise since this **high, nonstandard port** is specifically used by the botnet
- The compromises are **globally spread** with an **APAC concentration**: the top affected countries include the **U.S., Sweden, Taiwan, Singapore, and Hong Kong**.
- **Residential ISPs** across Asia, Europe, and the U.S. appear to be the main targeted networks, aligning with the typically observed **residential proxy botnet strategy** that mimics legitimate users to evade detection.

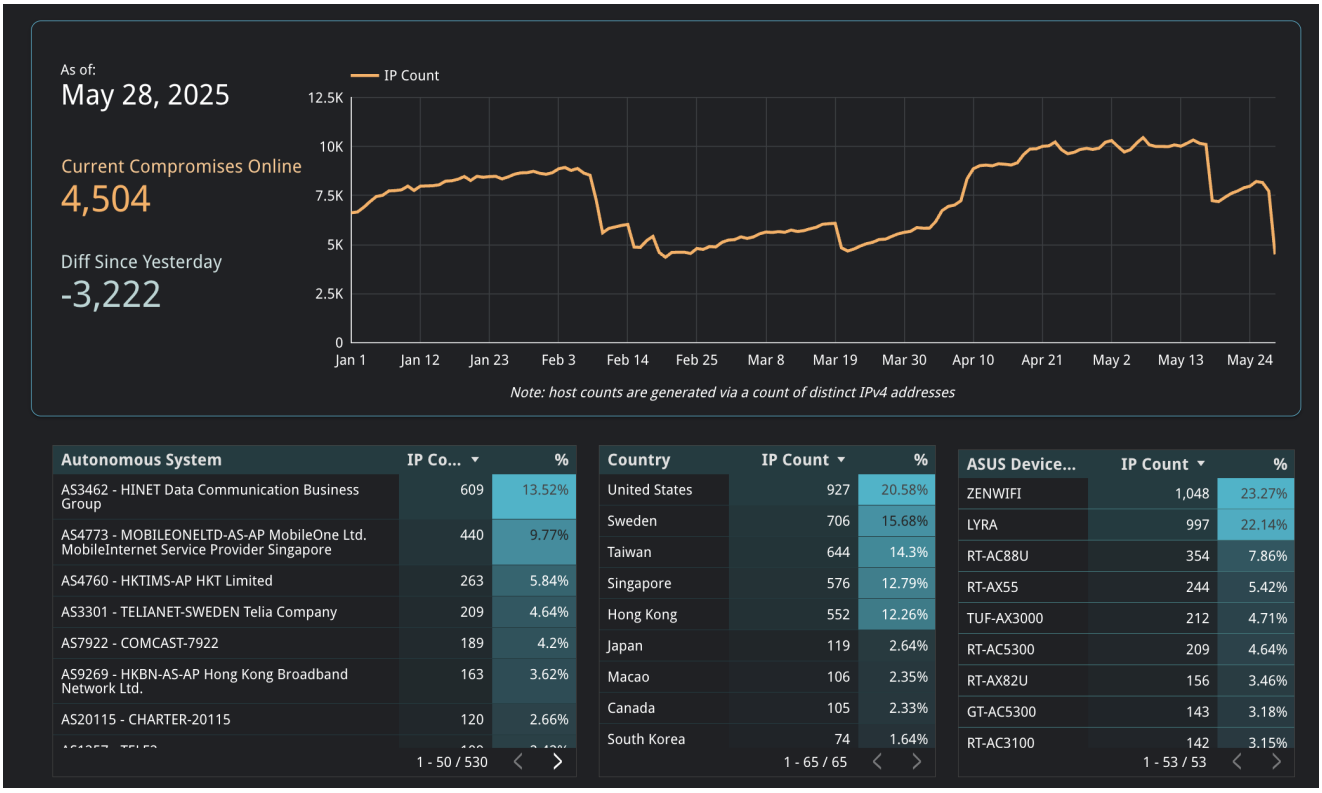
- Historical trends in compromises observed online reveal a **highly dynamic** scale of botnet operations that rapidly scaled **up and down by 50%** in a matter of weeks
- Attackers leverage **ASUS's own built-in configuration tools** to inject SSH keys that **survive firmware resets** -- **patching alone isn't enough**.
- Check out our**live dashboard**tracking exposed ASUS devices with indicators of compromise

Introduction

On March 18 2025, researchers at GreyNoise uncovered a sophisticated botnet campaign targeting ASUS routers. Dubbed **AyySSHush**, the operation exploits legitimate features of ASUS's AiProtection system to implant persistent SSH backdoors that survive firmware resets. This is an alarming example of threat actors exploiting vendor-sanctioned capabilities to establish a persistent, hard-to-detect presence in consumer-grade hardware.

Censys has been tracking this botnet's global footprint in partnership with findings from both **GreyNoise** and **Sekoia** researchers.

To aid in ongoing tracking and research, we've launched a **live dashboard that tracks exposed ASUS routers showing indicators of AyySSHush compromise**. The data updates daily and provides real-time insight into global trends.



What's Unique About This Botnet?

According to GreyNoise's research, the attackers exploit a combination of old and new vulnerabilities to compromise and gain persistence on these routers in a multi-stage attack sequence:

- **Initial access**:
  Launch brute-force attacks targeting login.cgi to compromise devices with weak credentials **OR** exploit older authentication bypass vulnerabilities to gain admin access
- **Command Injection**:
  - Send malicious POST requests to /start_apply.htm targeting the AiProtection_HomeProtection.asp page (an AI router security feature offered by ASUS)
  - Exploit **CVE-2023-39780**, an authenticated command injection vulnerability (originally discovered by security researcher leeya_bug) through a malicious OAuth Google refresh token parameter
  - Run the command touch /tmp/BWSQL_LOG to create an empty file that enables BandWidth SQLite LOGging (BWDPI), a legitimate TrendMicro feature embedded in ASUS routers
  - Abuse this for persistent logging capabilities
- **SSH Backdoor Installation**
  - Enable SSH access across both LAN and WAN interfaces
  - Bind SSH to an unusual, high-numbered port: **TCP/53282**
  - Inject their SSH public key into /etc/ssh/authorized_keys via legitimate router settings
  - Establish exclusive SSH access that bypasses normal authentication mechanisms

The real kicker is that in this last step, the attacker leverages ASUS's own built-in configuration management system to ensure persistence – a very clever abuse of normally trusted features. Since the SSH key is added via the router's official config interface, it is **retained across firmware updates**, meaning they can maintain access even after CVE-2023-39780 is patched. This means that **even users who proactively upgrade their router firmware to patch vulnerabilities may remain unknowingly compromised**. Factory resets may not always clear the backdoor either, depending on the router's specific configuration and features.

This makes AyySSHush a **particularly stealthy and resilient campaign** and part of a broader shift in threat actor TTPs toward “living off the firmware.” It’s also hard to ignore the irony of a botnet successfully compromising routers by exploiting the very security features designed to protect against such attacks.

The AyySSHush botnet has not been formally attributed to any specific group or nation. However, researchers at Sekoia identified a shared command-and-control IP address between AyySSHush and an edge device exploitation campaign carried out by a threat actor dubbed ViciousTrap. It still remains unclear who the operators of AyySSHush are.

Censys' Perspective

To get a picture of the potential scale and spread of AyySSHush, we queried Censys internet scan data for ASUS routers with **TCP/53282** open. Our goal was to quantify the current state of global exposure and map trends in ASUS models, networks, and regions most affected by compromises.

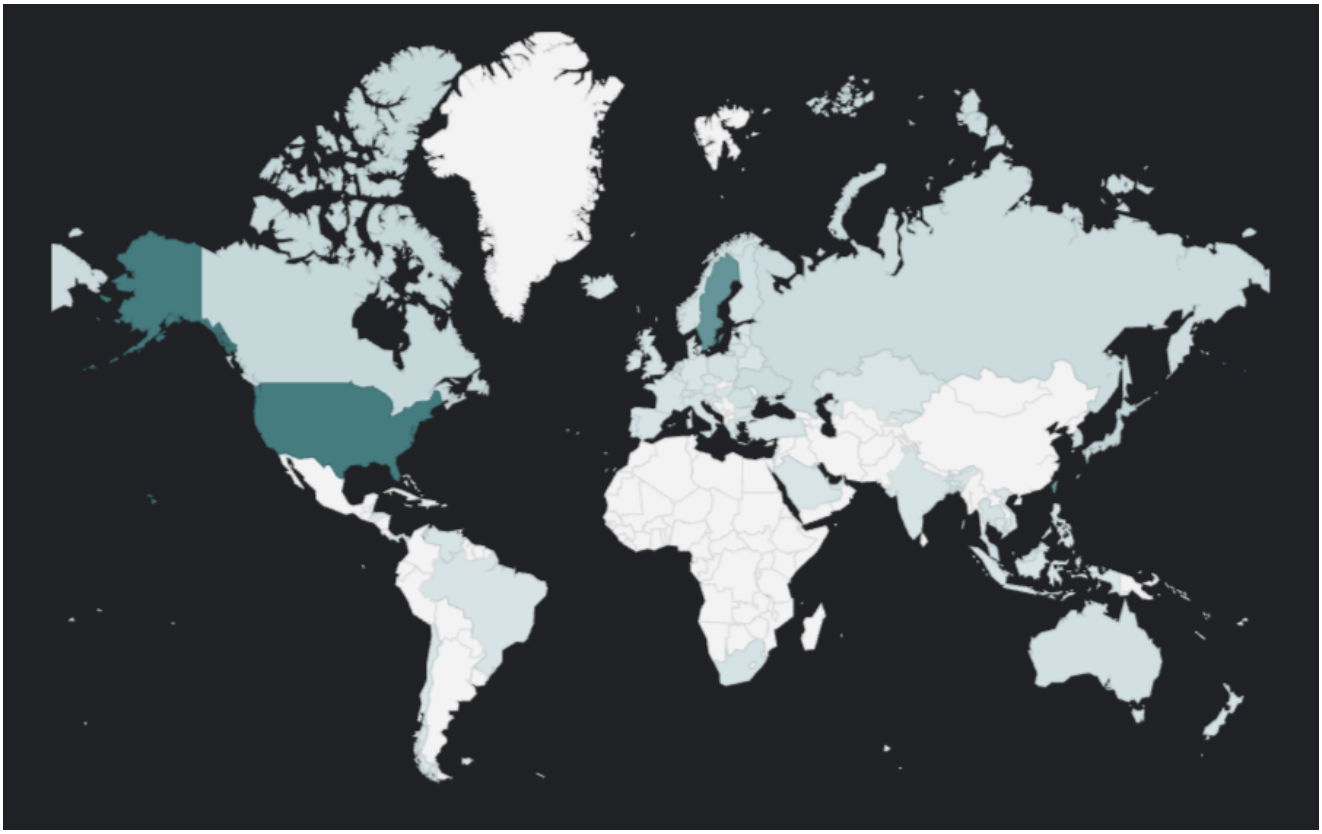
As of May 28, 2025, there are **4,504 potentially compromised ASUS routers** with TCP port 53282 exposed - corroborating findings from other sources that there are thousands of vulnerable devices that could be part of a botnet infrastructure. Note that this number **differs from other publicly reported numbers** because we've chosen to filter out known honeypot and tarpit configurations.

It appears that ASUS **mesh networking systems** are disproportionately targeted, with **ZenWiFi and Lyra models** accounting for nearly half (45.4%) of all compromised devices at 1,048 and 997 infections respectively. Traditional router models like the **RT-AC88U, RT-AX55, and TUF-AX3000** make up the next tier of compromised devices, which includes both consumer and gaming-focused product lines.

ASUS Device Model	Count ▾	%
ZENWIFI	1,048	23.27%
LYRA	997	22.14%
RT-AC88U	354	7.86%
RT-AX55	244	5.42%
TUF-AX3000	212	4.71%
RT-AC5300	209	4.64%
RT-AX82U	156	3.46%
GT-AC5300	143	3.18%
RT-AC3100	142	3.15%
BLUE CAVE	140	3.11%

Top 10 ASUS Devices Showing Signs of AyySSHush Compromise:

The geographic distribution shows that compromises are mostly geolocated in the **U.S., Sweden, Taiwan, Singapore, and Hong Kong**, in that order. The **United States leads globally** with over 900 compromised devices (20.58%), though the overall pattern indicates this botnet has achieved significant international reach. It's interesting that many of these are in **Asia-Pacific regions**, with Taiwan, Singapore, and Hong Kong accounting for nearly 40% of all compromised devices. There's overlap here with the top 5 countries we observe running ASUS devices overall: the U.S., Hong Kong, Taiwan, Sweden, and China. **Note: The presence of compromised routers in a particular country does not indicate the attacker's location. Compromised devices could be operated by anyone, anywhere.**



Map of Currently Exposed ASUS Devices Showing Signs of AyySSHush Compromise:

Country	Count ▼	%
United States	927	20.58%
Sweden	706	15.68%
Taiwan	644	14.3%
Singapore	576	12.79%
Hong Kong	552	12.26%
Japan	119	2.64%
Macao	106	2.35%
Canada	105	2.33%
South Korea	74	1.64%
Ukraine	72	1.6%

Top 10 Countries Hosting Potentially Compromised ASUS Devices:

Our scans reveal a **heavy concentration of compromised devices within major telecommunications providers**, with Asian and European telecoms like HINET (Taiwan), MobileOne (Singapore), HKT Limited (Hong Kong), and Telia (Sweden) accounting for over a third of all infections, as well as a presence of **major US providers** like **Comcast and Charter**.

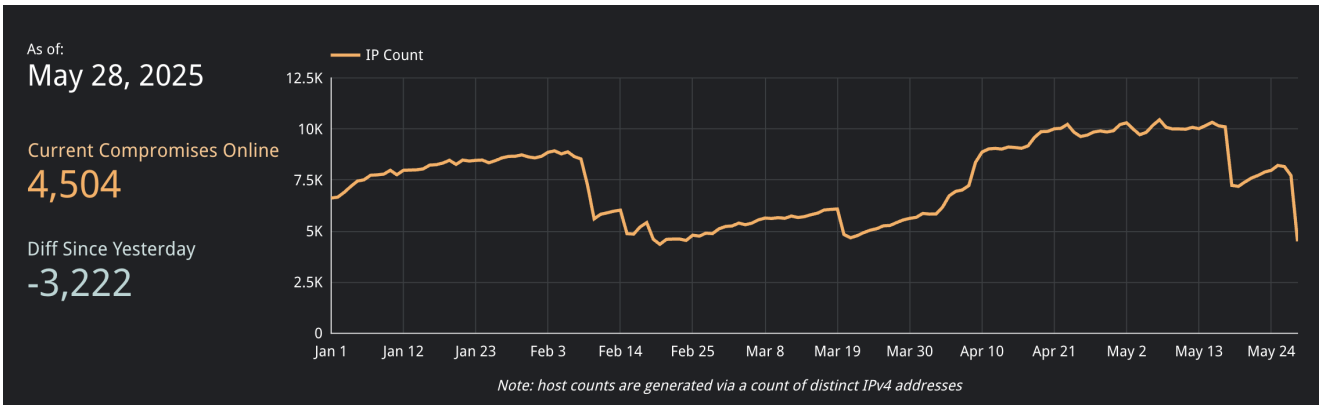
Attackers are known to specifically target residential broadband networks like these because it makes detection more difficult. **Telecom infrastructure provides ideal cover** for malicious proxy networks and ORB (open residential botnet) operations because residential IP addresses appear more legitimate to security systems, bypass many IP-based blocking mechanisms, and can blend in with normal consumer traffic patterns that ISPs expect to see.

This botnet has clearly achieved global reach across residential networks, likely with the aim of creating a distributed proxy infrastructure that can be leveraged for malicious activities while avoiding detection.

Autonomous System	Count ▼	%
AS3462 - HINET Data Communication Business Group	609	13.52%
AS4773 - MOBILEONELTD-AS-AP MobileOne Ltd. MobileInternet Service Provider Singapore	440	9.77%
AS4760 - HKTIMS-AP HKT Limited	263	5.84%
AS3301 - TELIANET-SWEDEN Telia Company	209	4.64%
AS7922 - COMCAST-7922	189	4.2%
AS9269 - HKBN-AS-AP Hong Kong Broadband Network Ltd.	163	3.62%
AS20115 - CHARTER-20115	120	2.66%
AS1257 - TELE2	109	2.42%
AS2119 - TELENOR-NEXTEL Telenor Norge AS	105	2.33%
AS4609 - CTM-MO Companhia de Telecomunicacoes de Macau SARL	103	2.29%

Top 10 Networks Hosting Potentially Compromised ASUS Devices:

Historical Trends: A Volatile Botnet



Five Month Trendline of Exposed Potentially Compromised ASUS Devices (Jan-May 2025)

We used Censys' historical data to track evolution of the potential botnet infrastructure over the past five months. The data reveals a relatively **volatile operation** – doubling from ~5,800 to over 10,000 devices in one month, then **dramatically shrinking by half within a single week**.

Five-Month Evolution (January - May 2025):

- **January - Early February: Steady Growth**
  - The number of potential infections was at 6,622 at the beginning of the year, then steadily climbed by nearly 2,000 over the course of a month (Jan 1 - Feb 8)
  - Gradual increase suggests the actor was systematically scanning for targets while trying to avoid detection
- **Early February: Major Disruption**
  - Sharp 50% decline from ~8,500 to ~4,300 devices over two weeks (Feb 8-20)
  - Could have been triggered by anything, but possibly by security researcher disclosure.
- **February - March: Stable Period**
  - Botnet maintained relatively stable device count between 5,000-6,000 through end of March, very slowly increasing, with a few drops
  - Unclear what operations were during this time, but suggests they were relying on established persistent infrastructure
- **April - Early May: Major Expansion**
  - Nearly doubled in size from ~5,800 to over 10,000 compromised devices over a few weeks (April 3-21)
  - Peak of 10,454 devices on May 7 represents the botnet's largest observed footprint
  - Could be an indication of new exploitation campaigns
- **Late May: Current Decline**
  - Steep drop over the past week back down to 4,504 devices, with the data showing a drop in over 3,200 compromised hosts exposed online since yesterday
  - Recent media attention and security community focus may be driving this change
  - Could also indicate botnet operators shifting tactics or infrastructure

Regardless of this recent major drop, the continued presence of thousands of potentially infected hosts online indicates that this is well-established, resilient botnet infrastructure. This is unsurprising given how difficult IoT botnets are to eliminate once established, especially when they exploit trusted features to maintain access – oftentimes, a user would not be able to detect anything amiss unless they knew exactly what to look for and where. The scale of this suggests it’s not the work of casual threat actors but rather a **well-resourced, coordinated operation with long-term goals**. What those exact goals are remains to be understood.

Detection and Mitigation

Identifying ASUS Routers Exposing TCP/53282 On Your Network

Censys uses passive internet scanning across all 65,535 ports to identify potentially compromised devices, but cannot directly access local filesystem artifacts. Organizations should use the provided query to identify hosts of concern within their networks, then directly examine those ASUS devices for the specific filesystem artifacts and SSH key added during compromise.

The following Censys Platform query can be used to identify potentially compromised ASUS devices:

```
host.services:(port="53282" and protocol="SSH") and
(host.services.software.vendor:"Asus" or host.services.hardware.vendor:"Asus"
or host.services.operating_systems.vendor:"Asus" or host.services.software.vendor:"AS
US"
or host.services.hardware.vendor:"ASUS" or host.services.operating_systems.vendor:"AS
US"
or host.services.endpoints.http.html_title:"ASUS Wireless Router")
```

GreyNoise has shared a few IoCs, including:

Malicious SSH Public Key

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAo41nBoVFfj4HlVMGV+YPsxMDrMlbdDZJ8L5mzhhaxfGzpHR8Geay/xDlV
DS
J8MJwA4RJ7o21KVfRXqFblQH4L6fWIYd1ClQbZ6Kk1uA1r7qx1qEQ2PqdVMhnNdHACvCVz/MPHTVebtkKhEl9
8MZiMOvUNP
tAC9ppzOSi7xz3cSV0n1pG/dj+37pzuZUpm4oGJ3XQR2tUPz5MddupjJq9/gmKH6SJjTrHKSECe5yEDs6c3v6
uN4dnFNYA5
MPZ52FGbkhzQ5fy4dPNf0peszR28XGkZk9ctORNCGXZZ4bEkGHYut5uvwVK1KZOYJRmmj63drEgdIioFv/x6I
cCcKgi2w==
```

Filesystem Artifacts

- /tmp/BWSQL-LOG
  A log file created by the malware during the infection process
- /tmp/home/root/.ssh/authorized_keys
  core persistence mechanism of AyySSHush, where the attacker will inject their SSH key during compromise

Known Malicious AyySSHush C2s observed by GreyNoise

- 101[.]99[.]91[.]151
- 101[.]99[.]94[.]173
- 79[.]141[.]163[.]179
- 111[.]90[.]146[.]237

References:

- https://www.labs.greynoise.io/grimoire/2025-03-28-ayysshush/
- https://leeyabug.top/ASUS-SQLI
- https://blog.sekoia.io/vicioustrap-infiltrate-control-lure-turning-edge-devices-into-honeypots-en-masse/
- https://blog.sekoia.io/polaredge-unveiling-an-uncovered-iot-botnet/