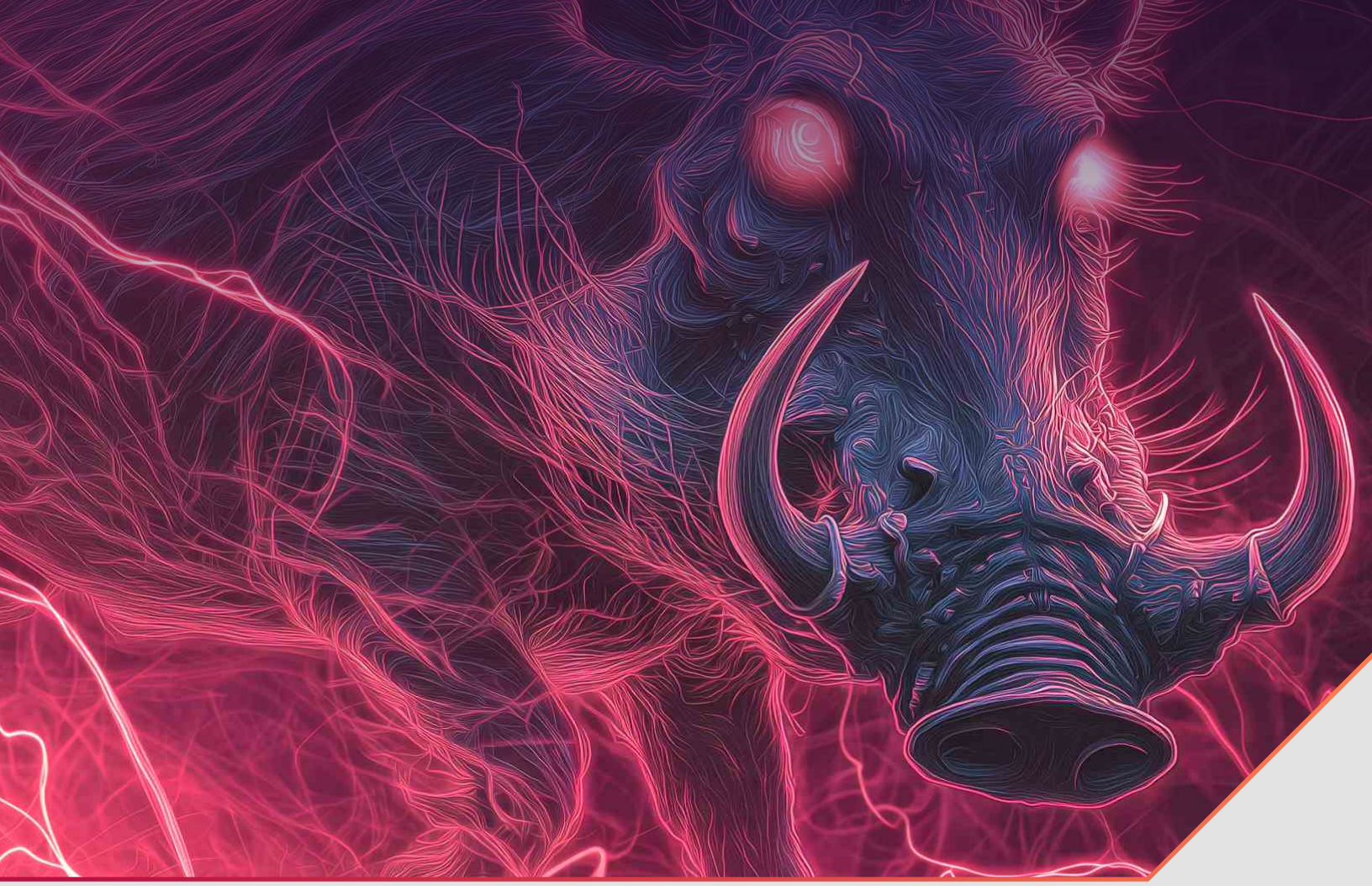
STRIKE
By SecurityScorecard

Thousands of ASUS Routers Hijacked in Global Operation “WrtHug” in a Suspected China-Backed Campaign



SecurityScorecard

Synopsis

SecurityScorecard research, in consultation with ASUS, details Operation “WrtHug,” a widespread compromise of ASUS routers. It leverages the proprietary AiCloud service with Nth day vulnerabilities in order to gain high privileges on End-Of-Life ASUS WRT routers. A shared, self-signed TLS certificate with an unusually long 100-year expiration identifies compromised devices.

This campaign currently affects an estimated thousands of unique devices worldwide, predominantly in Taiwan, U.S., Russia and to a lesser extent, some Southeast Asian and European countries.

This research identified hackers leveraging six distinct vulnerabilities to propagate this campaign: CVE-2023-41345, CVE-2023-41346, CVE-2023-41347, CVE-2023-41348, CVE-2024-12912, and CVE-2025-2492. STRIKE’s intelligence assessment finds the targeted devices, methods, and timing mirror previous intrusion campaigns linked to China Nexus actors. They are not unlike the LapDogs ORB, which the STRIKE threat intelligence team recently uncovered.

Even more notably, vulnerabilities CVE-2023-41345, CVE-2023-41346, and CVE-2023-41347 are directly associated with the command injection vulnerability CVE-2023-39780, which is tied to another ongoing suspected China-linked ORB operation known as “AyySSHush,” which GreyNoise reported was targeting ASUS devices since earlier this year.

This research highlights the growing trend of malicious threat actors targeting routers and other network devices in mass infection operations. These are commonly (but not exclusively) linked to China Nexus actors, who execute their campaigns in a careful and calculated manner to expand and deepen their global reach.

Executive Summary

As state-sponsored global Operational Relay Box (ORB) intrusion campaigns seem to accelerate and become more prevalent across multiple actors and nations, Operation WrtHug offers further insights into their proliferation. The operation aligns with China Nexus threat actors' tactics, techniques, and procedures (TTPs) as well as geopolitical interests and adversaries, with nearly half of all nodes within the network located in Taiwan.

The operation comprises:

- Thousands of compromised devices worldwide.
- The hackers appear to exclusively target ASUS WRT routers.
- Most devices appear to be End-Of-Life (EoL) devices, compromised via Nth day vulnerabilities leveraging the AiCloud service and OS injection vulnerabilities.
- Compromised devices present a self-signed TLS certificate with an unusually long expiration period.
- 30-50% of targeting is centralized in Taiwan, with other clusters of targets in South Korea, Japan, Hong Kong, Russia, central Europe, and the United States.
- Attack pattern and vulnerability severity indicate potential Command Injection capabilities if not Root-level privileges.

Table of Contents

Operation “WrtHug”

SecurityScorecard's STRIKE team uncovered a sweeping compromise operation targeting exclusively ASUS routers around the globe in recent months. The STRIKE team first identified this global infrastructure campaign while researching a suspicious self-signed Transport Layer Security (TLS) certificate proliferating across thousands of devices with clusters of geographic targets.

The campaign is not explicitly an ORB, but STRIKE assesses that it bears striking resemblance to other Chinese ORB and botnet operations.

The campaign exploits a web-app based feature designed to offer users convenient remote access to their home networks and connected storage, which unfortunately also represents an often-exposed attack surface. The attackers seemingly leveraged the ASUS AiCloud service in this case to deploy a targeted global intrusion set.

AiCloud-based vulnerabilities represent only a piece of a larger set of vulnerabilities and attack vectors. The main indicator of compromise (IOC) in this campaign (the unique and self-signed TLS certificate) overwhelmingly appears on AiCloud services with few exceptions. These exceptions show it on the management panel in addition to the AiCloud service.

Between 30-50% of the infected devices are tied to an IP address located in Taiwan (based on IP geolocations), and we don’t think that’s a coincidence. Operation WrtHug also targets southeast Asian countries, Russia, central Europe, and the United States, and is infecting thousands of devices around the globe at the moment.

The current estimation of infected devices varies between different scanning tools available. Over the past six months, our proprietary scanners and those from Driftnet (see query here) indicate roughly 50,000 unique IPs held by compromised devices presenting the WrtHug campaign around the globe.

The operation, which we examine further below, is not an isolated incident: It is just one part of an intensifying interest from China-backed hacking teams in identifying and refining new methods to establish, adapt, and relocate espionage infrastructure with global reach and tailored precision. We recently revealed research on a China-Nexus ORB that highlights the evolving threat.

The Suspected Certificate

We first found the suspicious shared TLS certificate (Sha1 1894a6800dff523894eba7f31cea8d05d51032b4) earlier this year, which helped us unearth this operation. As is the case with many ORBs targeting Small Office/Home Office (SOHO) devices, this certificate is self-signed.

Using self-signed certificates is not an uncommon occurrence for internet of things (IoT) devices and routers, since many local web applications and services requiring remote access generate their own TLS certificates locally. For that reason, two devices running the same service with a self-signed certificate will not typically share the same encryption key. The certificate thumbprint, expiration start and end dates, and some metadata typically vary between devices.

SSL Certificate

```
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            de:1c:4a:f4:53:c9:7d:b0
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=aa, ST=a, L=a, O=a, OU=a, CN=a
        Validity
            Not Before: Apr 25 17:15:51 2022 GMT
            Not After : Apr  1 17:15:51 2122 GMT
        Subject: C=aa, ST=a, L=a, O=a, OU=a, CN=a
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:bf:ac:63:d6:04:c1:46:92:9e:4f:1d:46:63:ad:
                    b9:12:2f:14:2a:b0:14:91:d1:f5:05:23:2f:2b:7a:
                    7a:e1:e5:3f:b0:66:19:ca:8d:5d:57:74:64:2c:e7:
                    58:f3:7f:35:83:52:12:54:bf:41:87:6c:2c:b9:6f:
                    ea:3b:5a:bf:c2:1a:c6:16:78:44:fc:a9:03:f3:5a:
                    df:f7:49:eb:46:ec:86:68:7b:6c:2f:24:32:6c:ab:
                    16:66:81:98:a4:c4:a1:a7:8f:ca:94:d8:38:49:70:
                    b5:9c:69:de:60:39:cd:b7:42:da:7b:7e:20:ff:b7:
                    82:5c:9e:fc:8a:a9:94:b4:61
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha256WithRSAEncryption
```

Compromised devices in the WrtHug operation all share the exact same self-signed certificate, which is our first indication that something is out of the ordinary. In a highly unusual turn of events, the certificate boasts an expiration date set for 100 years from April 2022. This is an extremely high and uncommon shelf life for a single TLS certificate.

(In contrast, a benign TLS certificate that ASUS generates locally for said services has the following as subject and issuer data: (CN=router.asus[.]com,C=US) and should have a shelf life of approximately 10 years.)

99% of the services presenting this certificate are ASUS AiCloud, a proprietary service designed to enable access to local storage via the internet. Both in appearance and in the DOM, the AiCloud page appears to remain intact. A smaller portion of the infected devices present this certificate on the Apache based web server for the management panel.

We assess that these two different services are yet another indication of a deeper compromise of the devices itself.

End-Of-Life Achilles' Heel and the AyySSHush Connection

After consulting with the ASUS security team on product-specific vulnerability details, a few vulnerabilities emerged as potential targets in Operation WrtHug:

- **CVE-2023-41345, CVE-2023-41346, CVE-2023-41347, and CVE-2023-41348:** These nearly two-year-old vulnerabilities enable authenticated attackers to perform direct OS command injection on ASUS WRT devices using insufficient filtering related to token modules. These three vulnerabilities are associated with the command injection vulnerability CVE-2023-39780. CISA's known exploited vulnerabilities catalog incorporated this vulnerability in 2025, although it has been reported for nearly two years.
- **CVE-2024-12912:** Arbitrary command execution vulnerability, with a CVSS score of 7.2.
- **CVE-2025-2492:** Improper authentication control vulnerability that may lead to unauthorized function execution via a crafted request, with a CVSS score of 9.2.

GreyNoise reported in May that CVE-2023-39780 was the initial access vector for the AyySSHush ORB. Their research found a widespread campaign targeting ASUS devices with the vulnerability. It established a foothold by enabling SSH access on port 53282, using an actor-held public SSH key for remote access.

Another significant note, is that despite targeting the same vulnerability on the same set of EoL devices, and despite no sign of post-infection vulnerability patching by the threat actor, we observed only seven IPs that present signs of compromise in both campaigns (see results via this Censys search query).

This leads us to speculate that WrtHug and AyySSHush may be a single, evolving campaign or two separate campaigns from the same actor. It could also be two campaigns from coordinated actors.

For the time being, we lack substantial evidence beyond the shared vulnerability to support these speculations. We will continue to track Operation WrtHug as a separate campaign until such evidence arises.

It is important to emphasize that all of the observed vulnerabilities used in Operation WrtHug are known and have officially been patched, and thus mainly target EoL or outdated devices.

SecurityScorecard consulted with the ASUS security team on the specific vulnerabilities that we suspected in this campaign and they were able to assess that most targeted devices were EoL models. There were two exceptions that were merely outdated and lacking the latest firmware.

AiCloud services that present the WrtHug TLS certificate seem to have not been changed or altered on a superficial level. Both compromised and non-compromised devices run AiCloud on a local lighttpd webserver, using versions 1.4.29 or 1.4.39.

We have also been able to observe a small number of compromised devices presenting the WrtHug certificate on the management panel web server running on Apache httpd version 2.0.

As for these web application versions for ASUS routers, ASUS security pointed out applied mitigations and security backports to address security concerns regarding the older webserver versions.

The following is a list of detected models of ASUS routers targeted in Operation WrtHug:

- ASUS Wireless Router 4G-AC55U
- ASUS Wireless Router 4G-AC860U
- ASUS Wireless Router DSL-AC68U
- ASUS Wireless Router GT-AC5300
- ASUS Wireless Router GT-AX11000
- ASUS Wireless Router RT-AC1200HP
- ASUS Wireless Router RT-AC1300GPLUS
- ASUS Wireless Router RT-AC1300UHP

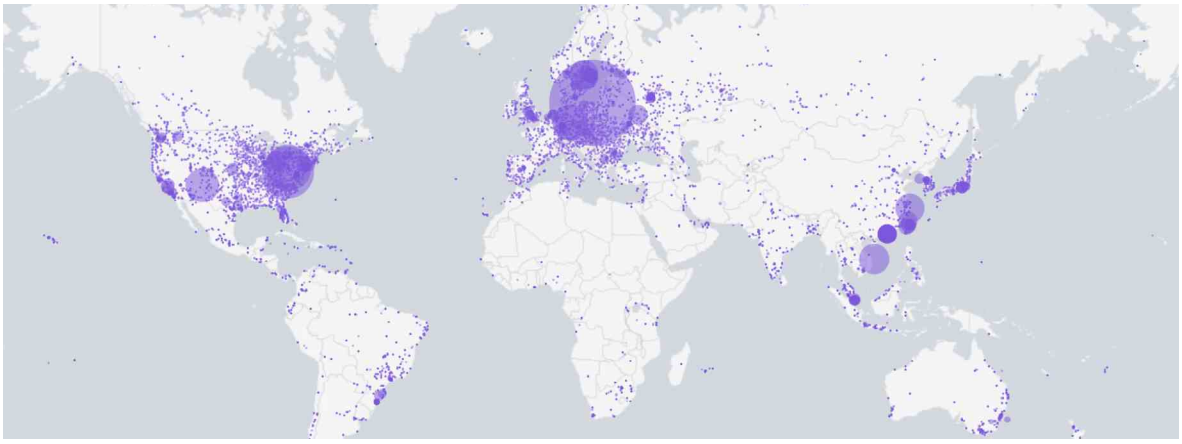
Global Telemetry

As we have seen with other botnets and ORB Networks, the threat actors are not compromising devices at random. They may use a self-spreading mechanism or share a common component. This in turn may provide clues about the long-term intentions of the operating actor.

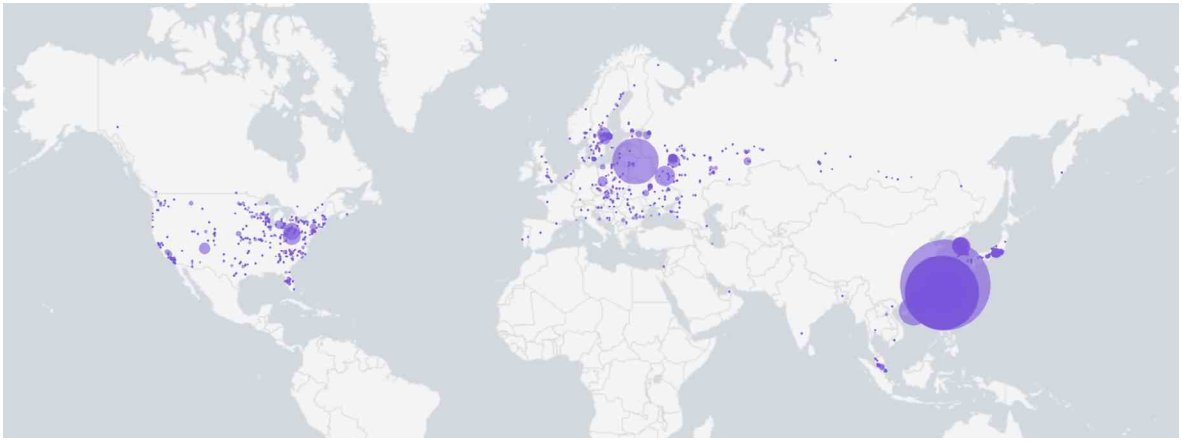
In the case of WrtHug, our proprietary scanners observed highly concentrated targeting in Taiwan, as well as clusters in other southeast Asian countries, Russia, central Europe, and the United States. You can view the targeting in our maps.

We also observe this localized targeting trend by examining the certificate with Open-Source attack surface platforms such as Driftnet. You can explore the Driftnet query here.

We compared our internal data on visible ASUS devices to observed infected devices to assess whether this may have been the result of a visibility bias. Our collected data shows certain clustering of total ASUS devices in central Europe, North America. There is a slightly smaller yet significant cluster in southeast Asia, including South Korea, Japan, Taiwan, and Hong Kong.



Now, compare it to the heat map results of WrtHug:



(Note: Cluster sizes presented on the heat map are proportionate to the relevant sample size).
A fully interactive heat map of infected devices is presented below.

When examining the geographical spread of WrtHug in comparison to the AyySSHush campaign, we observe some significant overlaps in targeted countries and regions. AyySSHush appears to be heavily concentrated in the United States and Sweden in more significant numbers. Taiwan follows these countries as third on the list. We assess that this disparity in targeting neither weakens nor strengthens our hypothesis of a potential underlying coordination between the two campaigns.

Heat Map

Attribution

We observe three main geographic clusters of compromised ASUS routers on the infected heat map. The threat actors paid significant attention to infecting devices in Southeast Asia and Taiwan, both of which are significantly overrepresented compared to the rest of the world. There appear to be no infected ASUS devices on mainland China, outside of Hong Kong.

Earlier this year, GreyNoise reported on "AyySSHush" as a suspected China Nexus ORB operation that has specifically targeted ASUS devices. Both AyySSHush and WrtHug leveraged the OS command injection vulnerability CVE-2023-39780, to spread across EoL routers.

This campaign does not occur in a vacuum either, as reports on expansive ORB operations originating from Chinese-affiliated actors seem to have escalated over the past year.

Due to this noticeable alignment with previous TTPs in ORB campaigns from Chinese advanced persistent threat (APT) actors, as well the geographical focus of the campaign, we assess with low-to-moderate confidence that Operation WrtHug is an ORB facilitation campaign from an unknown China-affiliated actor.

While unconfirmed, we also speculate (albeit with no confidence level for now) that there is some behind-the-scenes coordination between the WrtHug and AyySSHush campaigns. Dual-compromised nodes are very low despite the somewhat narrow pool of potential victims.

We also speculate about collaboration because both target ASUS devices vulnerable to OS command injection vulnerabilities associated with CVE-2023-39780. Neither actor shows signs of post-exploitation patching, essentially leaving the “door” open for the other.

SecurityScorecard’s STRIKE threat intelligence team will continue to monitor and assess Operation WrtHug and related activities as they continue to unfold.

Mitigation

All vulnerabilities in Operation WrtHug are known and ASUS has officially addressed and patched them. This aligns with our observation of the threat actor targeting outdated and EoL devices.

To further explore previous security advisories on the vulnerabilities leveraged in WrtHug, please view the ASUS product security advisory here or check how to make your devices more secure with the ASUS Support resource FAQ.

Shields Up on Routers in 2025

The past few years mark a dramatic increase in widespread and sophisticated intrusion campaigns targeting networking devices and IoTs. SOHO routers have been on the receiving end of many of these campaigns.

In our previous research on the China-Nexus “LapDogs” ORB, we unveiled attackers relying on custom malware to infect devices. We demonstrated how they might target firmware from specific vendors, while still maintaining some capability to target a variety of other vendors.

In the case of LapDogs, the threat actors zeroed in on compromising Ruckus Wireless devices. But this year also marked a trend of targeting ASUS routers via a combination of vendor-specific and non vendor-specific vulnerabilities.

This is best exemplified by the emergence of high-profile botnets such as the aforementioned "AyySSHush" campaign, as well as SEKOIA’s report on the broader "ViciousTrap" intrusion set.

These campaigns have demonstrated a clear evolution in attacker methodology. Persistent, resourced hackers are moving beyond simple brute-force attacks to multi-stage infections that exploit a variety of vulnerabilities.

By chaining command injections and authentication bypasses, threat actors have managed to deploy persistent backdoors via SSH, often abusing legitimate router features to ensure their presence survives reboots or firmware updates.

Evolving Red Flags

SecurityScorecard’s STRIKE threat intelligence team leverages a variety of proprietary scanning tools to uncover widespread infections, such as botnets, ORB Networks and other intrusion campaigns. This research enables us to unearth threat actors’ hacking operations that target large swaths of internet facing systems, such as the WrtHug or LapDogs operations.

One of the recurring early signs of an infection we look for is alterations in the public encryption key presented on a given device. We also look for copy-pasted metadata on the TLS certificate (especially with self-signed ones) and sharing among multiple, seemingly unrelated, endpoints. These clues can mark the early signs or the end result of a successful compromise.

Conclusion

Operation WrtHug marks another escalation in the threat landscape for SOHO devices. This coordinated campaign, likely from China-backed actors, leveraged Nth day vulnerabilities on ASUS WRT routers to establish a persistent presence. The unique, long-expiration TLS certificate serves as a key indicator of compromise.

This incident underscores the critical need for regular updates, vigilance against outdated services, and proactive monitoring to counter sophisticated, state-sponsored intrusion campaigns that continually evolve their tactics to achieve global espionage reach.

IOCs

Indicator	Type	Details
1894a6800dff523894eba7f-31cea8d05d51032b4	SHA-1	The specific WrtHug certificate
46.132.187[.]85	IPv4	Device likely compromised by both WrtHug and AyySSHush.
46.132.187[.]24	IPv4	Device likely compromised by both WrtHug and AyySSHush.
221.43.126[.]86	IPv4	Device likely compromised by both WrtHug and AyySSHush.
122.100.210[.]209	IPv4	Device likely compromised by both WrtHug and AyySSHush.
59.26.66[.]44	IPv4	Device likely compromised by both WrtHug and AyySSHush.
83.188.236[.]86	IPv4	Device likely compromised by both WrtHug and AyySSHush.
195.234.71[.]218	IPv4	Device likely compromised by both WrtHug and AyySSHush.
Subject: CN=a,OU=a,O=a,L=a,ST=a,C=aa	Subject leaf data	
Issuer: CN=a,OU=a,O=a,L=a,ST=a,C=aa	Subject leaf data	

Final Thoughts

This research was made possible thanks to our colleagues at ASUS, who were willing to consult with SecurityScorecard on this research project and improve the online safety of ASUS device owners and others alike.

At STRIKE, we put collaboration and information sharing at the forefront, choosing a more thorough investigation and better mitigation. If you are a colleague in the cybersecurity or broader IT industry, we encourage you to choose similarly over all other competing motivations, despite the obvious allure. We also invite you to reach out with any suggestions or offers to share information or collaborate on research and mitigation efforts to make the internet safer for everyone.

Contact STRIKE for Incident Response

SecurityScorecard's STRIKE Team has access to one of the world's largest databases of cybersecurity signals, dedicated to identifying threats that evade conventional defenses. With proactive risk management and a rapid response approach, SecurityScorecard offers companies protection against third-party risks and the ability to counter active threats like WrtHug.

Discover how SecurityScorecard and its STRIKE Team can strengthen your enterprise's security.

For STRIKE media inquiries, contact us here.

STRIKE By SecurityScorecard

SecurityScorecard.com
info@securityscorecard.com