Pacific Rim: Inside the Counter-Offensive—The TTPs Used to Neutralize China-Based Threats

10/31/2024

Executive Summary

For more than five years, Sophos has been investigating multiple China-based groups targeting Sophos firewalls, with botnets, novel exploits, and bespoke malware.

With assistance from other cybersecurity vendors, governments, and law enforcement agencies we have been able to, with varying levels of confidence, attribute specific clusters of observed activity to Volt Typhoon, APT31 and APT41/Winnti.

Sophos X-Ops has identified, with high confidence, exploit research and development activity being conducted in the Sichuan region. Consistent with China's vulnerability disclosure legislation, X-Ops assesses with high confidence that the developed exploits were then shared with multiple distinct state-sponsored frontline groups with differing objectives, capabilities, and post-exploitation tooling.

Over the tracked period Sophos has identified three key evolving attacker behaviors:

- A shift in focus from indiscriminate noisy widespread attacks (which X-Ops has concluded were failed attempts to build operational relay boxes [ORBs] to aid future targeted attacks) to stealthier operations against specific high-value and critical infrastructure targets primarily located in the Indo-Pacific region. Victim organizations include nuclear energy suppliers and regulators, military, telecoms, state security agencies, and central government.
- Evolution in stealth and persistence capability. Notable recent TTPs include increased use of living-off-the-land, insertion of backdoored Java classes, memory-only Trojans, a large and previously undisclosed rootkit (with design choices and artifacts indicative of cross-platform multi-vendor capability), and an early experimental version of a UEFI bootkit. X-Ops believe this is the first observed instance of bootkit use specifically on a firewall.
- Threat actor OPSEC improvements including sabotaging firewall telemetry collection, impacting detection and response capability, and hampering OSINT research via a reduced digital footprint.

In response to calls from NCSC-UK (as expounded upon by NCSC-UK Chief Technology Officer Ollie Whitehouse) and from CISA (in the agency's Secure-By-Design best practices article), our goal is to transparently highlight the scale and widespread exploitation of edge network devices by state-sponsored adversaries.

In the interests of our collective resilience, we encourage other vendors to follow our lead.

Table of Contents

- Key takeaways for defenders
- Conclusions
- Timeline and technical appendices

Key takeaways for defenders

Edge network devices are high-value targets that well-resourced adversaries use for both initial access and persistence.

Defender's detection and response strategies need to take this into account. To aid defenders, Sophos has:

- Provided TTPs and IOCs in the appendix of the detailed timeline to help defenders identify detection opportunities
- Outlined the steps it takes to detect and respond to attacks against its customers' firewalls

State-sponsored attackers use both zero-day and known vulnerabilities to attack edge devices.

This targeting is not unique to Sophos firewalls; as evidenced by published CVEs, all edge devices are a target.

- Closely follow your vendors device hardening guide (Sophos' is here) to reduce attack surface and limit exploitability of zero-day vulnerabilities, paying particular attention to administrative interfaces
- Enable hotfixes, if supported, and implement processes to monitor your vendors' vulnerability disclosure communications — and quickly respond accordingly
- Ensure you are running supported hardware and software for which your vendor is committed to releasing security updates

State-sponsored targeting is not limited to high-value espionage targets.

-
    - Threat actors use edge devices as operational relay boxes (ORBs) to attack onward targets and obfuscate the true origin of attacks
    - In a tightly connected digital ecosystem, many organizations form part of a critical infrastructure supply chain and may be targeted by actors seeking to disrupt critical services

Summary timeline

A full timeline of the activity described in this overview report can be found in the technical addendum to this article. Links to relevant parts of the timeline are provided for each of the sections below to provide detailed context.

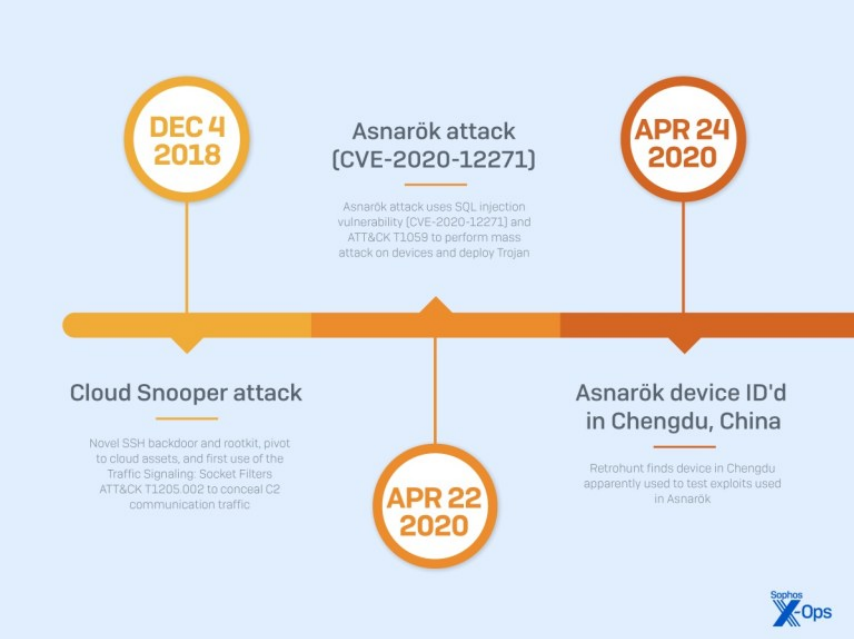

Figure 1: An abridged timeline of Pacific Rim activity, December 2018 to April 2020

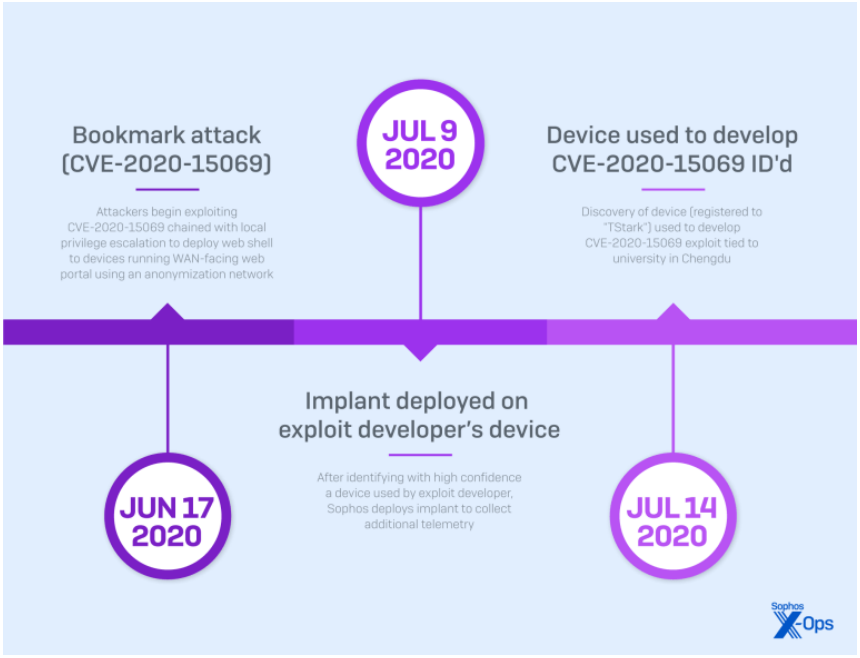

Figure 2:June to July 2020

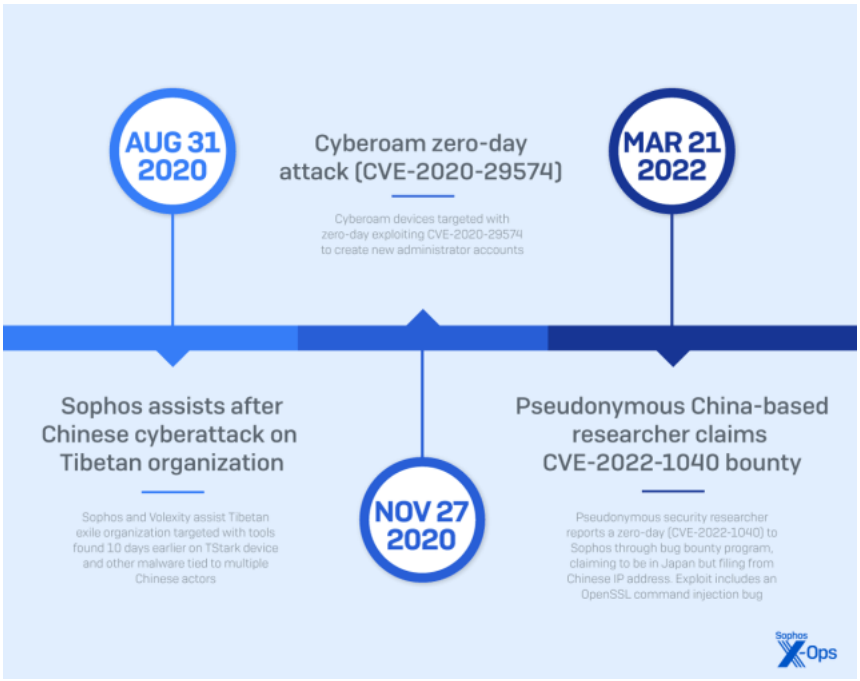

Figure 3: August 2020 to March 2022

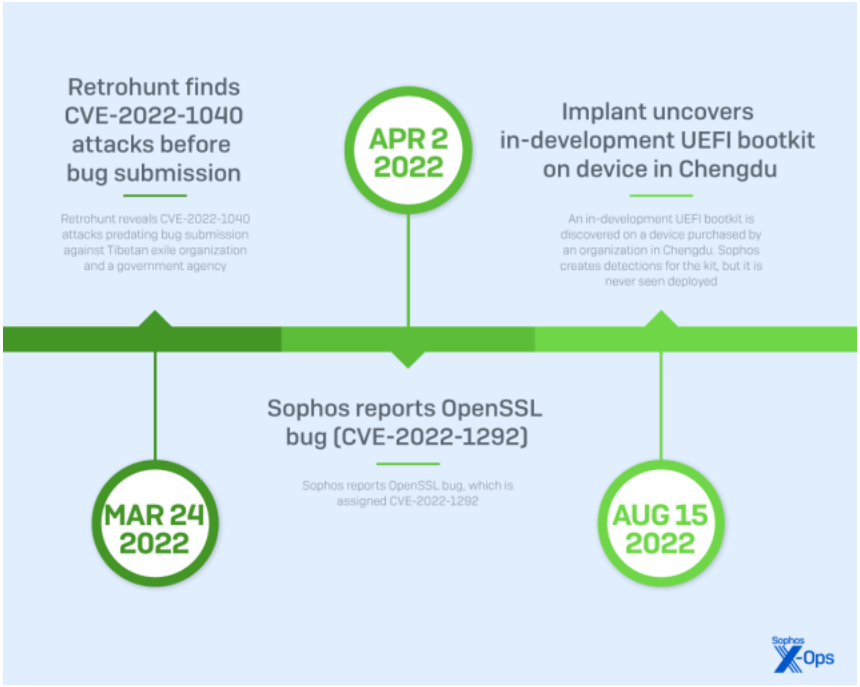

Figure 4: March 2022 to August 2022

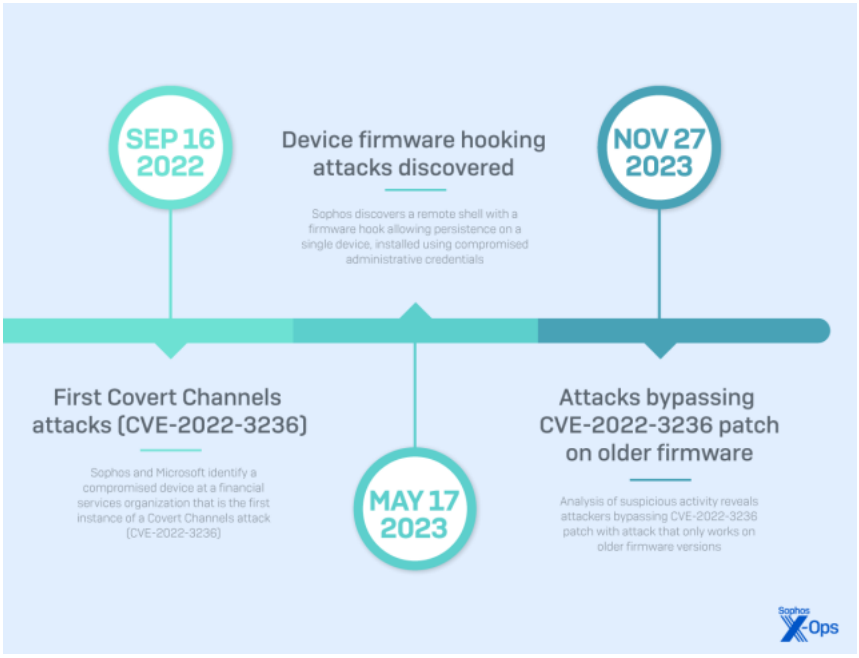

Figure 5: September 2022 to November 2023.

Initial intrusion and reconnaissance

The first attack was not against a network device, but the only documented attack against a Sophos facility: the headquarters of Cyberoam, an India-based Sophos subsidiary. On December 4, 2018, analysts on the Sophos SecOps team detected that device performing network scans. A remote access trojan (RAT) was identified on a low-privilege computer used to drive a wall-mounted video display in the Cyberoam offices.

While an initial investigation found malware that suggested a relatively unsophisticated actor, further details changed that assessment. The intrusion included a previously unseen, large, and complex rootkit we dubbed Cloud Snooper, as well as a novel technique to pivot into cloud infrastructure by leveraging a misconfigured Amazon Web Services Systems Manager Agent (SSM Agent).

While we published an analysis of the intrusion with some details in 2020, we did not at the time attribute the attack.

We now assess with high confidence that this was an initial Chinese effort to collect intelligence that would aid in the development of malware targeting network devices.

Mass attacks

- Asnarök (CVE-2020-12271), April 2020

- Bookmark feature buffer overflow (CVE-2020-15069), June 2020
- Cyberoam account creation attack (CVE-2020-29574), November 2020

Beginning in early 2020 and continuing through much of 2022, the adversaries spent considerable effort and resources to engage in multiple campaigns to discover and then target publicly reachable network appliances. In a rapid cadence of attacks, the adversary exploited a series of previously unknown vulnerabilities they had discovered, and then operationalized, targeting WAN-facing services. These exploits led to the adversary being able to retrieve information stored on the device, as well as giving them the ability to deliver payloads inside the device firmware and, in some cases, to devices on the LAN (internal to the organization's network) side of the device.

Sophos became aware of these noisy types of attacks soon after they began. When they were discovered, Sophos chose to make as broad and as public a disclosure as possible, as reflected by the series of X-Ops blog posts, conference presentations, and seminars based on our analysis and work to counter each of the threats. For example, the report on the first wave in April 2020 (which we dubbed Asnarök) published within a week of the commencement of widespread attacks and was updated as the actor behind them shifted attack flow.

Sophos also conducted outreach to organizations that no longer subscribed to updates but still maintained operational (and vulnerable) devices in their networks, to warn them of the risks of potential automatic botnet attacks on their public-facing devices.

In two of the attacks (Asnarök and a later attack dubbed "Personal Panda"), X-Ops uncovered links between bug bounty researchers responsibly disclosing vulnerabilities and the adversary groups tracked in this report. X-Ops has assessed, with medium confidence, the existence of a research community centered around educational establishments in Chengdu. This community is believed to be collaborating on vulnerability research and sharing their findings with both vendors and entities associated with the Chinese government, including contractors conducting offensive operations on behalf of the state. However, the full scope and nature of these activities has not been conclusively verified.

A timeline of the mass attacks on devices can be found in the detailed timeline.

Shifting to stealth

- Personal Panda (CVE-2022-1040), March 2022
- Covert Channels (CVE-2022-3236), September 2022
- Under-the-radar attacks (unpatched devices), July 2022 – Present

In mid-2022 the attacker changed tactics to highly targeted, narrowly focused attacks against specific entities: government agencies; critical infrastructure management groups; research and development organizations; healthcare providers; retail, finance, and military-adjacent businesses; and public-sector organizations. These attacks, utilizing diverse TTPs, were driven less by automation and more by an "active adversary" style, in which the actors manually executed commands and ran malware on the compromised devices.

A variety of stealthy persistence techniques were developed and utilized throughout these attacks, most notably:

- A custom, fully featured userland rootkit
- Use of the TERMITE in-memory dropper
- Re-packing legitimate Java archives with Trojanized class files
- An experimental UEFI bootkit (observed only on an attacker-controlled test device)
- Valid VPN credentials obtained both from on-device malware and via an Active Directory DCSYNC
- Hooking firmware-upgrade processes to survive firmware updates

While exploitation of known CVEs (those listed above) was the most common initial access vector used to deploy the above, X-Ops also observed cases of initial access using valid administrative credentials from the LAN side of the device, suggesting the use of perimeter devices for persistence and remote access after obtaining initial network access via other means.

Improvements in OPSEC

Throughout the campaigns, the actors became increasingly adept at hiding their activities from immediate discovery by blocking telemetry from being sent from the device to Sophos.

As early as April 2020, the attackers made efforts to sabotage the hotfix mechanism of devices they compromised. Later, they added targeting of the telemetry system of devices to prevent Sophos from getting early warning of their activity.

The actors also discovered and blocked telemetry-gathering on their own test devices after Sophos X-Ops utilized that capability to collect data on exploits while they were being developed.

Additionally, the operational security practices of the exploit developers improved over time. X-Ops saw the trail of data we could follow with open-source intelligence practices shrink considerably from earlier attacks.

Conclusions

Threat actors have carried out these persistent attacks for more than five years. This peek behind the curtain at our past and ongoing investigations into these attacks is the arc of a story we intend to continue telling over time, so long as it doesn't interfere with or compromise law enforcement investigations in progress.

The adversaries appear to be well-resourced, patient, creative, and unusually knowledgeable about the internal architecture of the device firmware. The attacks highlighted in this research demonstrate a level of commitment to malicious activity we have rarely seen in the nearly 40 years of Sophos' existence as a company.

Sophos X-Ops is happy to collaborate with others and share additional detailed IOCs on a case-by-case basis. Contact us via pacific_rim[@]sophos.com.

For the full story, please see our landing page: Sophos Pacific Rim: Sophos defensive and counter-offensive operation with nation-state adversaries in China.

Acknowledgments

Sophos would like to acknowledge the contributions of ANSSI, Bugcrowd, CERT-In, CISA, Cisco Talos, Digital Shadows (now part of Reliaquest), FBI, Fortinet, JCDC, Mandiant, Microsoft, NCA, NHCTU, NCSC-NL, NCSC-UK, NSA, Palo Alto Networks, Recorded Future, Secureworks and Volexity to this report, or to investigations covered in this report.