



Security Holdings

Why Panda Loves USB?

Observing Targeted Attacks by Chinese APTs



Yuta Sawabe / Kazuya Nomura

Yuta Sawabe

- SOC analyst at NTT Security Holdings
- Primarily involved in log analysis and malware analysis.
- Spoken at CODE BLUE, JSAC and Botconf in the past.

Kazuya Nomura

- SOC analyst at NTT Security Holdings
- Responding to IDS/IPS/EDR log detection
- Interested in malware analysis and data visualization.
- Spoken at CODE BLUE, JSAC in the past.

Introduction

APT groups each have sophisticated attack flows

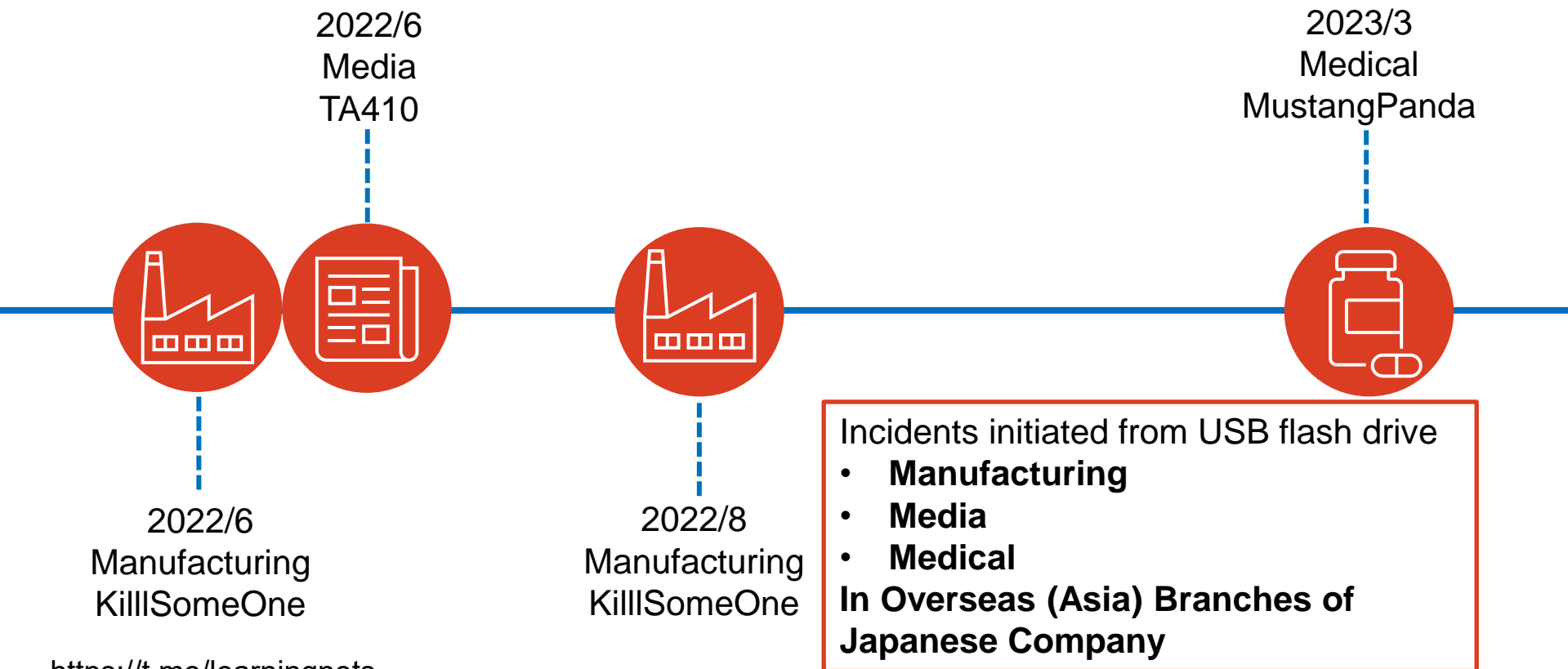
Otherwise, **traditional methods** are still effective for initial access

- Fake Software Installer
- Malicious Decoy Document Files
- **Compromised USB Flash Drive**

Traditional Japanese SOC(?)



Introduction



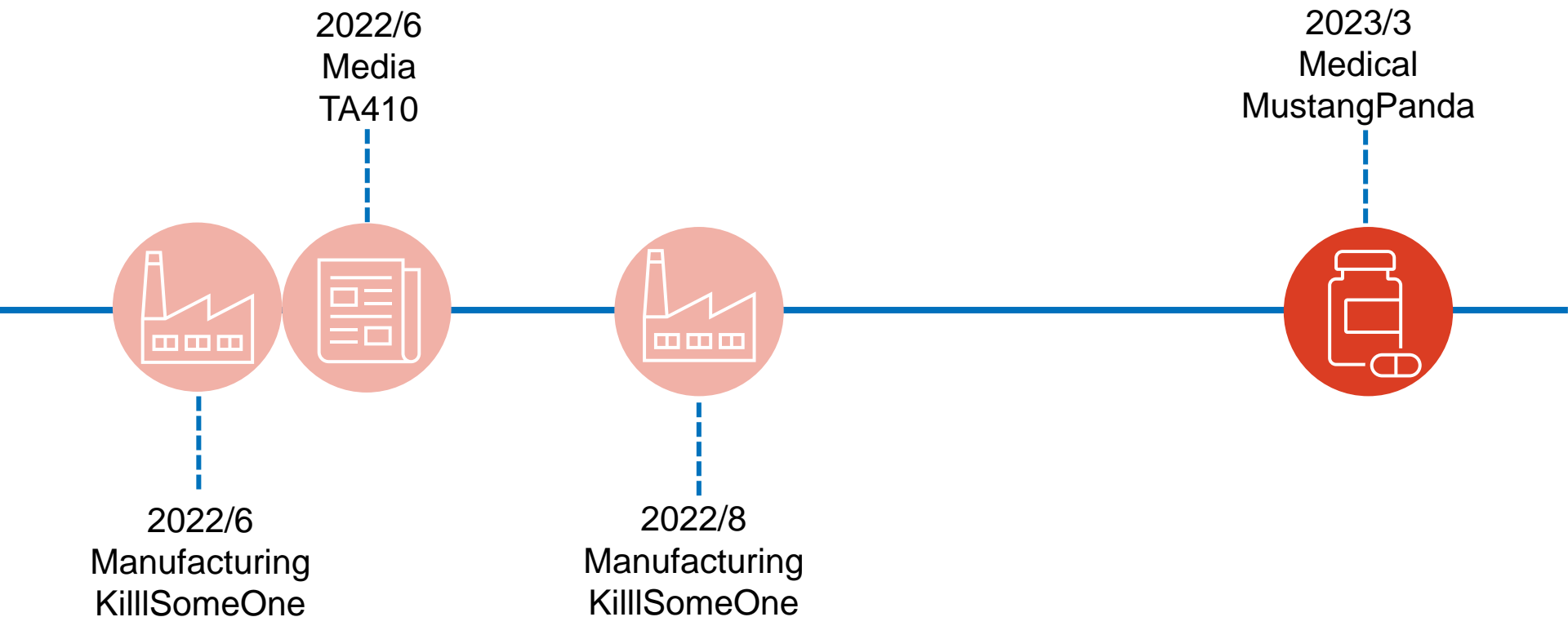
The APT groups&Campaigns covered in this presentation.

- Mustang Panda
- TA410
- KillSomeOne

Why are USB flash drives favored for attacks even in advanced targeted attacks?

Mustang Panda

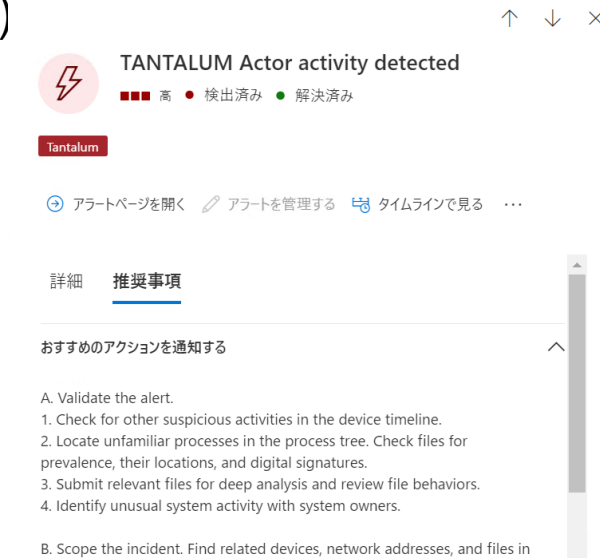
Mustang Panda



- Targeting **non-governmental organizations from various countries.**
- “WispRider” (≡ PlugX) malware was deployed via USB flash drive
- Situations we observed
 - Initiated from USB flash drives at overseas branches.
 - Malware was found on multiple hosts and USB flash drives
 - C2 infrastructure was already inactive

More Details of Detected Incident

- Detected by MDE (Microsoft Defender for Endpoint)
- Alerted “TANTALUM Actor Activity Detected”
 - Signature by Microsoft
 - TANTALUM = Mustang Panda
- May be triggered by suspicious USB Drive Activity
 - In our SOC, We observed only 2 case of “TANTALUM Actor Activity Detected”
 - In both case, malicious .exe was executed from USB drive



The screenshot shows a security alert notification. At the top right are navigation icons (up, down, close). The alert title is "TANTALUM Actor activity detected" with a lightning bolt icon. Below the title is a status bar with three colored dots: red (高), orange (検出済み), and green (解決済み). A red pill-shaped label contains the word "Tantalum". Below this are three action links: "アラートページを開く", "アラートを管理する", and "タイムラインで見る". A tabbed interface shows "推奨事項" (Recommendations) selected. Under this tab, there is a section "おすすめのアクションを通知する" (Recommended actions to notify) with a list of instructions: A. Validate the alert. 1. Check for other suspicious activities in the device timeline. 2. Locate unfamiliar processes in the process tree. Check files for prevalence, their locations, and digital signatures. 3. Submit relevant files for deep analysis and review file behaviors. 4. Identify unusual system activity with system owners. B. Scope the incident. Find related devices, network addresses, and files in

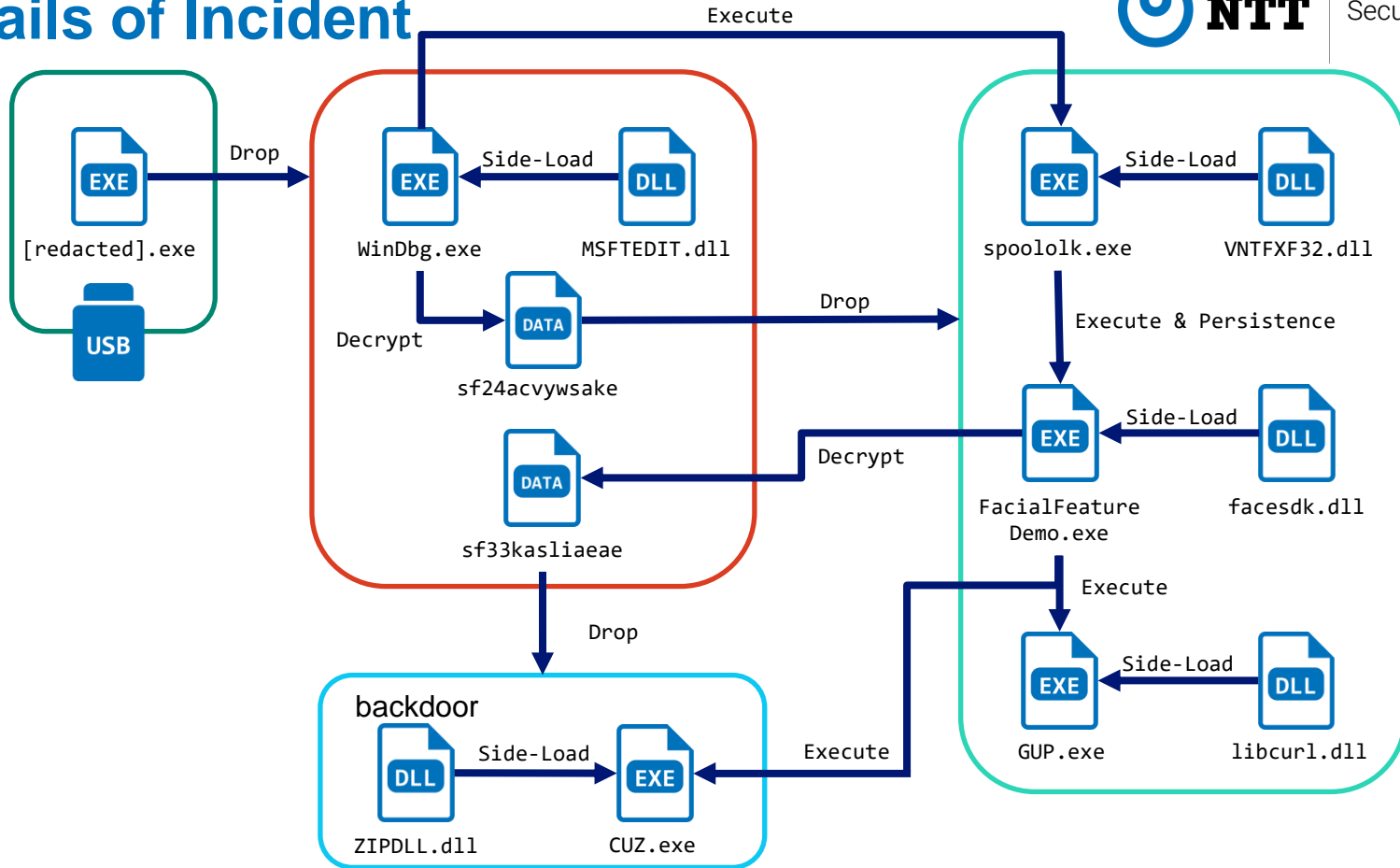
More Details of Detected Incident



- Multiple file creation activity on multiple USB drive in MDE TimeLine
 - Aims lateral movement

Event Time	Action Type	File Name	Folder Path
2023-03-05T07:25:07.146	FileCreated	[Drive Name] .exe	E:
2023-03-05T07:17:31.166	FileCreated	[Redacted] .exe	E:
2023-03-05T07:17:30.779	FileCreated	MSFTEDIT.dll	E:
2023-03-05T06:33:25.549	FileCreated	.exe	E:
2023-03-05T06:33:25.362	FileCreated	MSFTEDIT.dll	E:
2023-03-05T05:10:27.065	FileCreated	.exe	E:
2023-03-05T05:10:26.831	FileCreated	MSFTEDIT.dll	E:
2023-03-05T04:36:36.074	FileCreated	.exe	E:
2023-03-05T04:36:35.900	FileCreated	MSFTEDIT.dll	E:

Details of Incident



- WispRider
 - Used by multiple APT groups, such as UNC4698[1]
- Check Point reported some interesting facts about Mustang Panda (Camaro Dragon)[2]
 - In March 2023.
 - One of victim participated medical conference, sharing presentations via USB flash drive
 - As a result, malware was spread in his home hospital
 - Collateral damage...?

[1]Mandiant, "The Spies Who Loved You: Infected USB Drives to Steal Secrets",
<https://www.mandiant.com/resources/blog/infected-usb-steal-secrets>

[2]Check Point, "BEYOND THE HORIZON: TRAVELING THE WORLD ON CAMARO DRAGON'S USB FLASH DRIVES",
<https://research.checkpoint.com/2023/beyond-the-horizon-traveling-the-world-on-camaro-dragons-usb-flash-drives>

In December 2022, The sample "SE" mentioned in the report published by Avast [3] matches the characteristics of our case precisely.

SE

Now we are finally getting to a more complex setup. These archives include several versions with very similar structures and sometimes with varying payloads. Functional changes are presented below; note that these do not include changes in side-loading which will be discussed later on. All versions feature a few evasion tricks that use registry tricks to hide files and file extensions.

Version	Version changes
SE1	Uses volume name for USB installer executable
SE3/SE4/SSE	Uses Delphi launcher (the one attributed to Mustang Panda), persistence integrated into <i>LPVDPOCX.OCX</i> (equivalent of <i>facesdk.dll</i> from SE1)
SE5	Uses volume name for USB installer executable, rollbacks to old USB installer
SE6	No significant functional changes
SE7	No significant functional changes

[3] Avast, "Hitching a ride with Mustang Panda", <https://decoded.avast.io/threatintel/apt-treasure-trove-avast-suspects-chinese-apt-group-mustang-panda-is-collecting-data-from-burmese-government-agencies-and-opposition-groups/>

Mustang Panda



Security Holdings

- C2
 - 91[.]245.253.72
 - 193[.]42.36.214
 - Appear to have ceased operation around December 2022.

A file(*) exhibiting behavior that perfectly matches the attack flow was uploaded on VirusTotal (VT).

- Posted on: November 23, 2022
- Posted by: JP (Community)
- The file is an SFX Archive, and its behavior after execution matches the current attack flow.
- The mmCERT from Myanmar has given a bad rating to the file in the Community tab of VT.
 - › Myanmar is a prominent target country for the Mustang Panda group.
 - › Avast's report also mentions attacks targeting Myanmar.

Nearly all of the victims have close ties to Myanmar and it seems that both the Burmese government and opposition groups are being targeted. We have seen data originating from various departments of several Burmese ministries. Even

(*)sha256 : 63a16fdbed2949651ec2a2b5436cd02ded9a0e8c6465d72b0a6b648051838c3d

Mustang Panda



Security Holdings

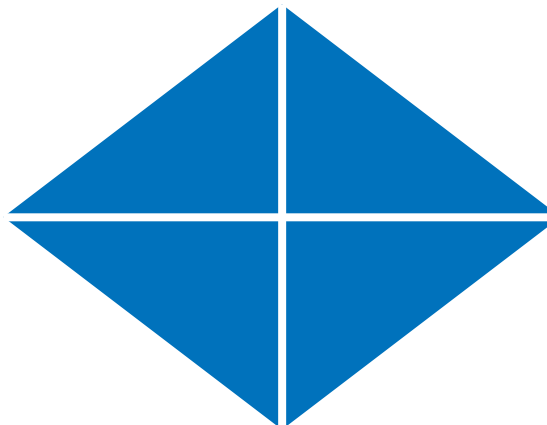
Adversary

Group

- Mustang Panda

Infrastructures

- Hosting
 - HZ Hosting
 - M247 Europe



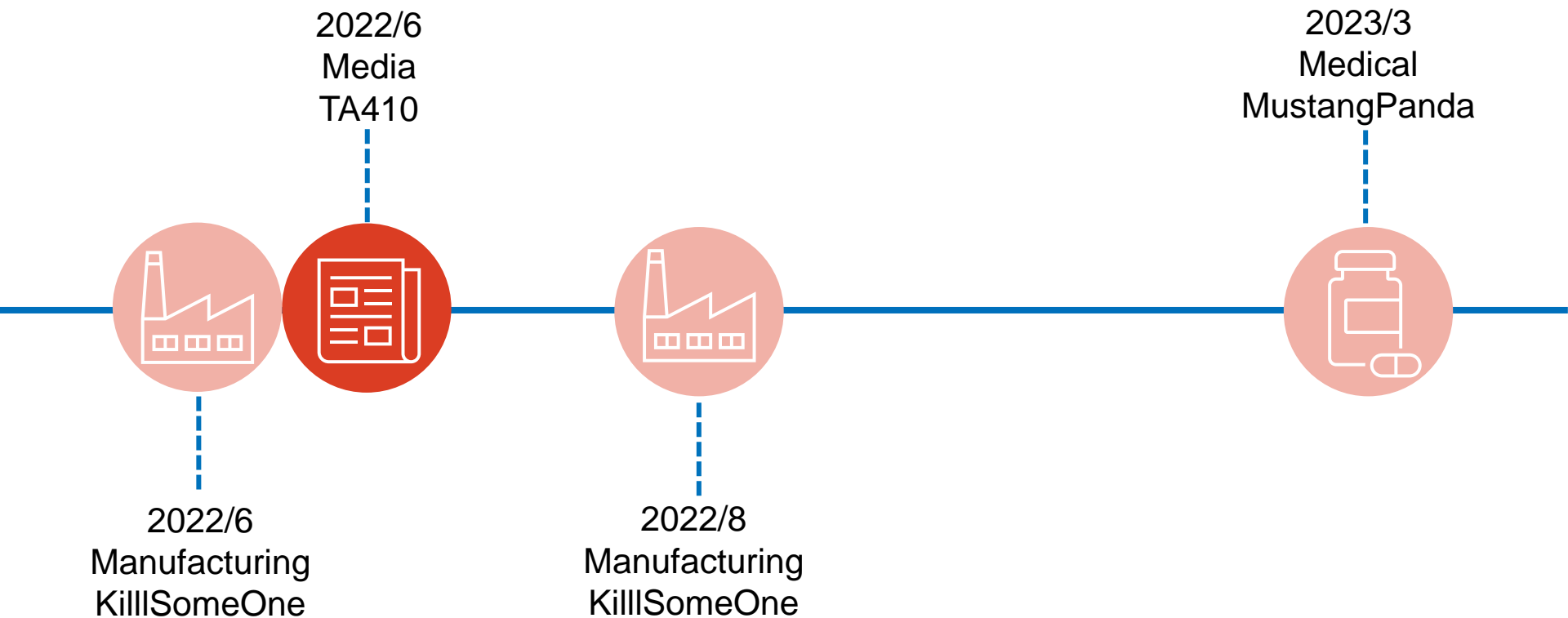
Capabilities

- USB Device
- DLL Side-Loading
 - MSFTEDIT.dll
 - VNTFXF32.dll
 - facesdk.dll
 - libcurl.dll
 - ZIPDLL.dll
- WispRider

Victims

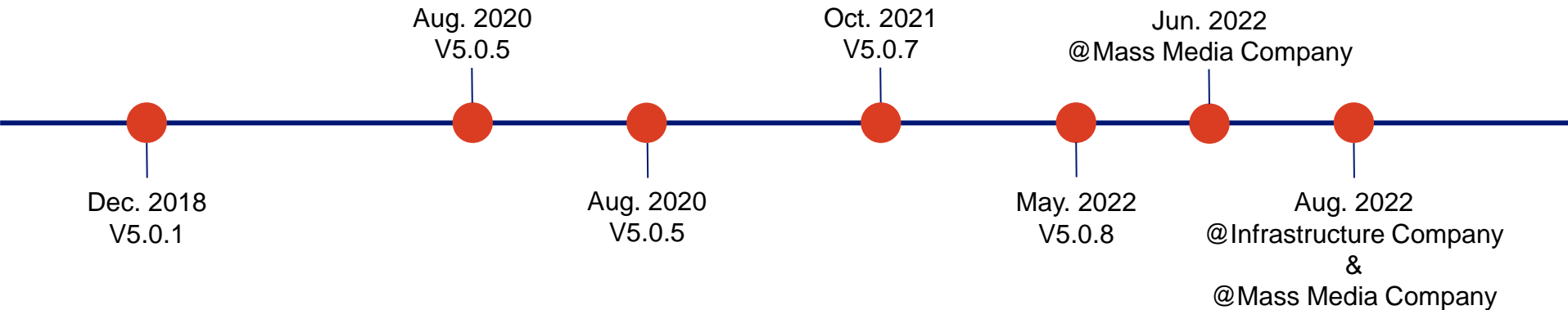
- Country: Japanese Company
- Sector: Medical Device Maker

TA410



- Targeted Attack Group utilizing the malware FlowCloud
- Since 2022, observed attacks targeting Japanese companies in SOC
 - Possibly targeting Japanese companies explicitly
- Summary
 - Execution of malicious files from USB flash drives at overseas locations
 - Establishment of communication with Command and Control (C2) and confirmation of data transmission.

- Observation history of FlowCloud in our SOC



- We observed attacks in Mass Media & Infrastructure companies in 2022

More Details of Detected Incident



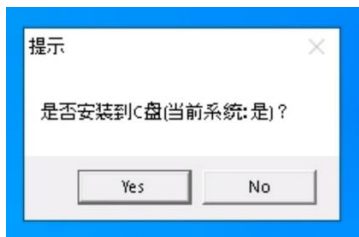
Security Holdings

- Observed by CrowdStrike Falcon
 - “Execution Command and Scripting Interpreter Follow Through”
 - Execution of legitimate setlang.exe
 - Now, Location of setlang.exe
“C:\Program Files(x86)\MSBuild\Microsoft\ExpressionBlend\msole”
has been reported by other vendors. [4]

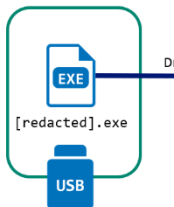
[4]ESET, “A lookback under the TA410 umbrella: Its cyberespionage TTPs and activity”,
<https://www.eset.com/jp/blog/welivesecurity/lookback-ta410-umbrella-cyberespionage-ttps-activity/>

<https://t.me/learningnets>

- Attack Flow of FlowCloud:

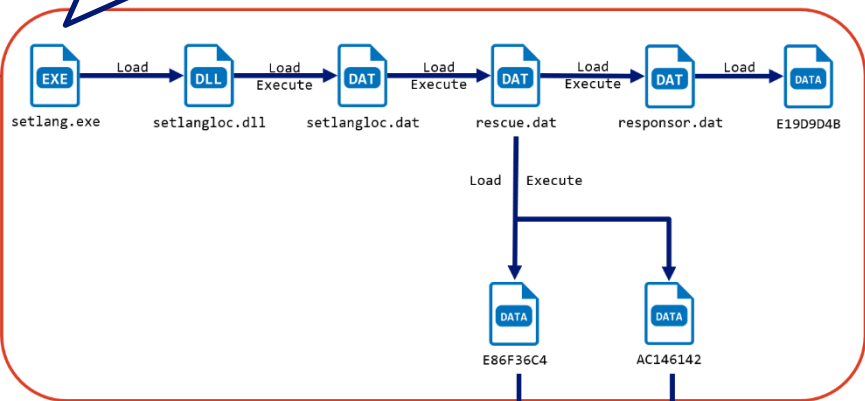


Display of a decoy dialog



Execution from USB flash drives

Sideloaded of legitimate setlang.exe



Drop & Execute

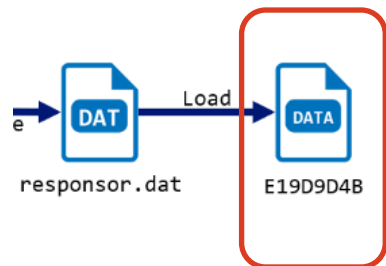


- Data deployed in memory during installation

```
1 #产品名称, 这些会在配置生成程序中使用并应用到前端
2 [product]
3 product_chs_name=火箭
4 product_name=PCArrowI
5 product_version=v5.0.8
6
7 [general]
8 created_folder=:\Program Files\MSBuild\Microsoft\Expression\Blend\msole
9 install_folder=:\Program Files\MSBuild\Microsoft\Expression\Blend\msole
```

Chinese
Comment

- Configuration deployed in memory



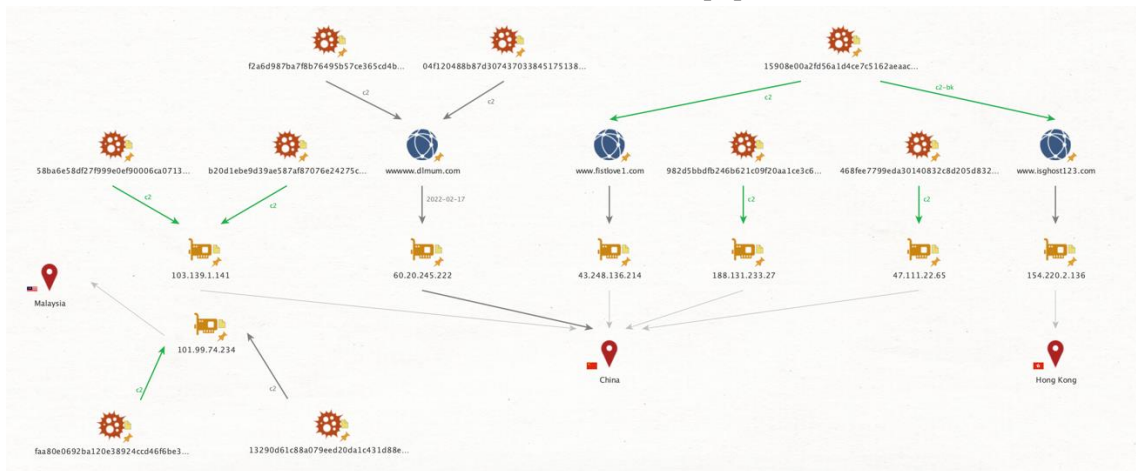
```
1 server_config {
2   product_name: "PCArrowI"
3   product_version: "v5.0.8"
4   id: "0608_20221026194010_*****"
5   root: ""
6   file_server: "103.139.1.141"
7   file_server_port: "562"
8   file_server_bak: ""
9   file_server_bak_port: ""
10  exchange_server: "103.139.1.141"
11  exchange_server_port: "563"
12  exchange_server_bak: ""
13  exchange_server_bak_port: ""
14  file_server_key: "***"
15  xchg_server_key: "***"
16  file_key: "***"
17  is_audio_only: false
18  id_prefix: "0608"
19 }
20
21 polycys {
22   keyboard_policy {
23     state: true
```

Usage of non-standard
port numbers for
communication
destination

- Rootkit
- Utilizes EPROCESS structure
 - Each Windows version has different offset variables.
 - Supports Windows 11 Version 21H2.

```
155     }
156     else if ( (dwBuildNumber == 19041 || dwBuildNumber == 19042 || dwBuildNumber == 19043 || dwBuildNumber == 22000)
157             && dwMajorVersion == 10
158             && !dwMinorVersion )
159     {
160         *offsets = 0x440;           // UniqueProcessId
161         offsets[1] = 0x448;       // ActiveProcessLinks
162         offsets[2] = 0x5A8;       // ImageFileName
163         offsets[3] = 0x5C0;       // SeAuditProcessCreationInfo
164         offsets[4] = 0x518;       // SectionObject
165         return ret;
166     }
167     return 0xC0000001;
168 }
```

- Correlation diagram of infrastructure and samples
- Main communication destinations point to China → Targeting within China?
 - Droppers communicating with the same C2 (www.dlmum[.]com)
 - Past associations with TA428 have been identified [5]



[5] nao_sec, "Royal Road! Re:Dive", <https://nao-sec.org/2021/01/royal-road-redive.html>

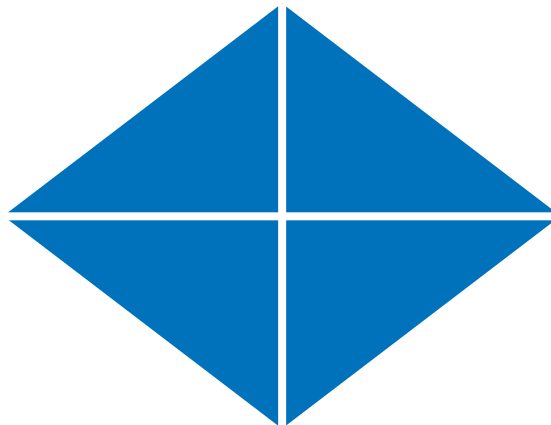
Adversary

Group

- TA410

Infrastructures

- Sharing C2 w/TA428



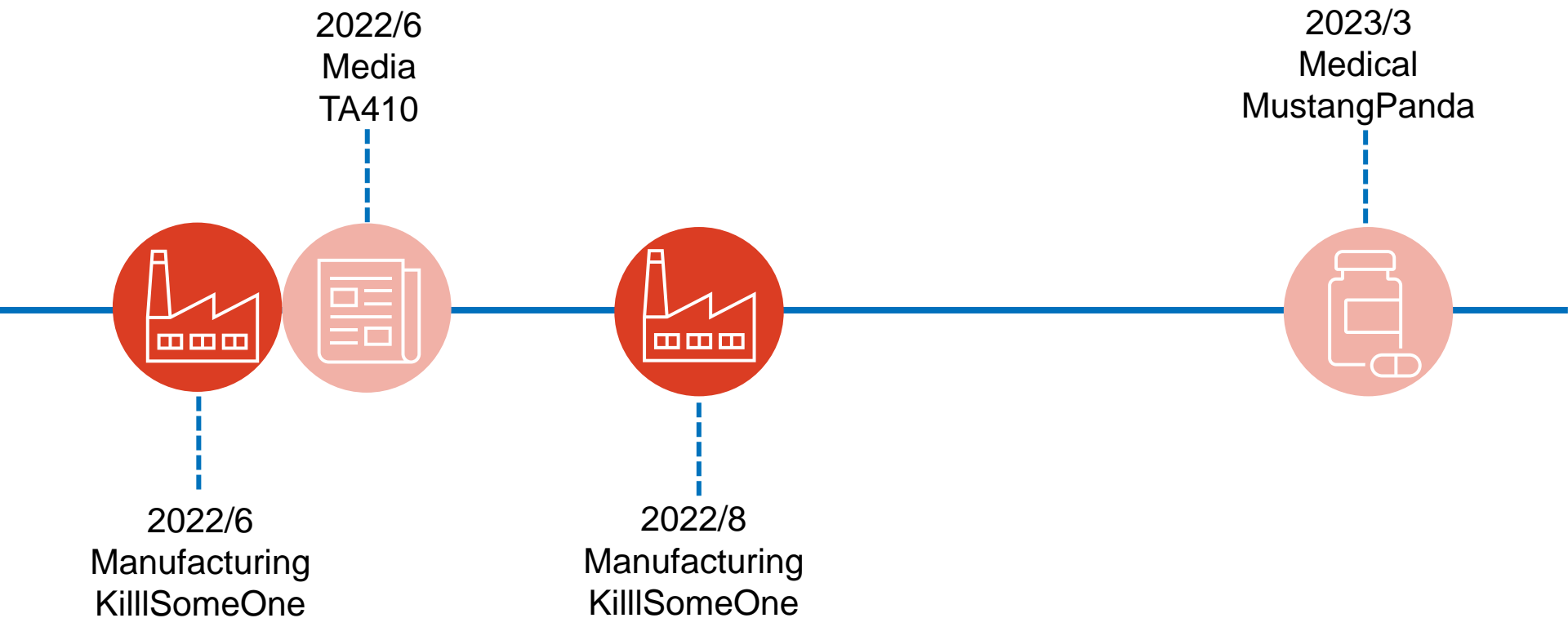
Capabilities

- USB Device
- DLL Sideload
 - setlang.exe
 - setlang.dll
- Use FlowCloud

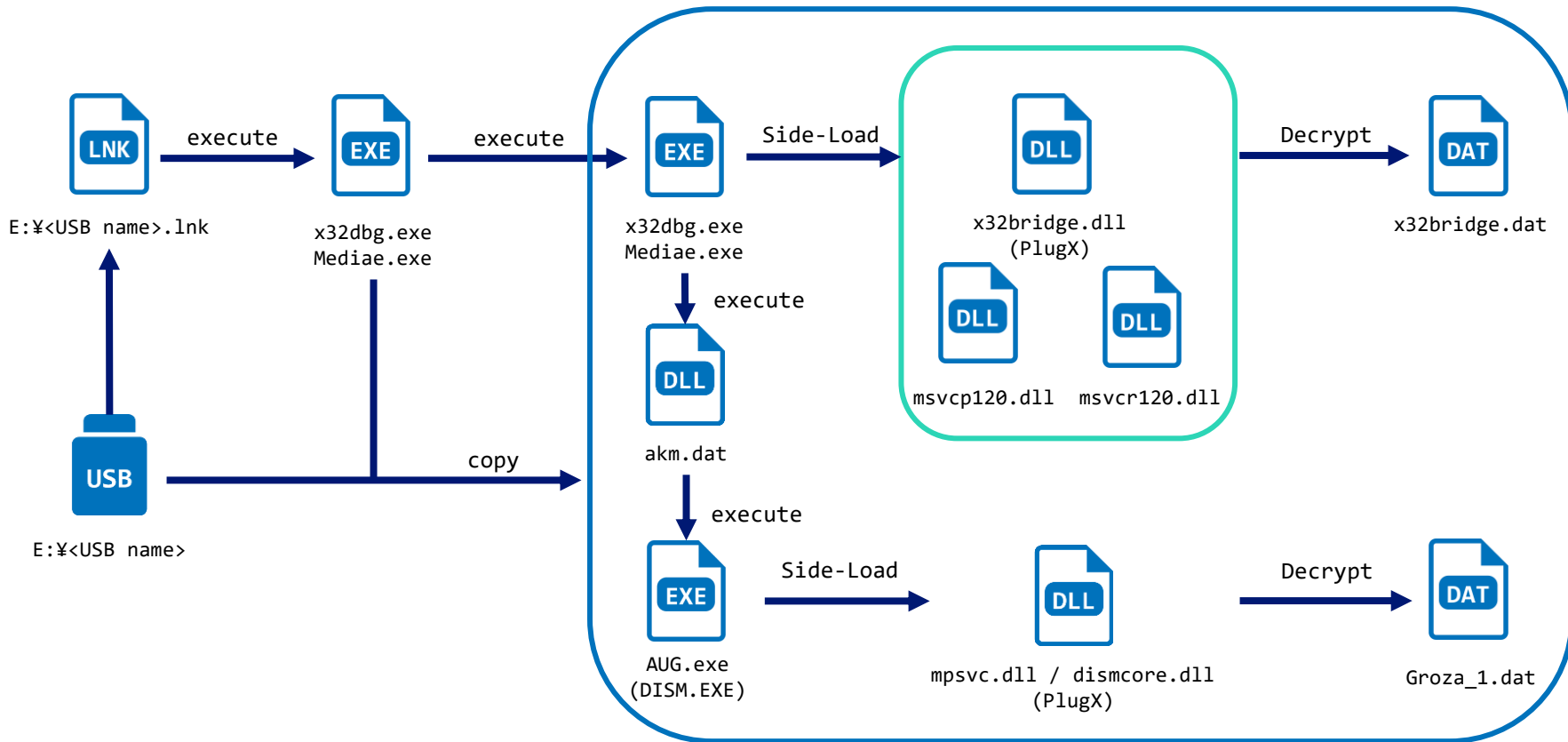
Victims

- Country: Japanese Company
- Sector: Mass Media & Infrastructure

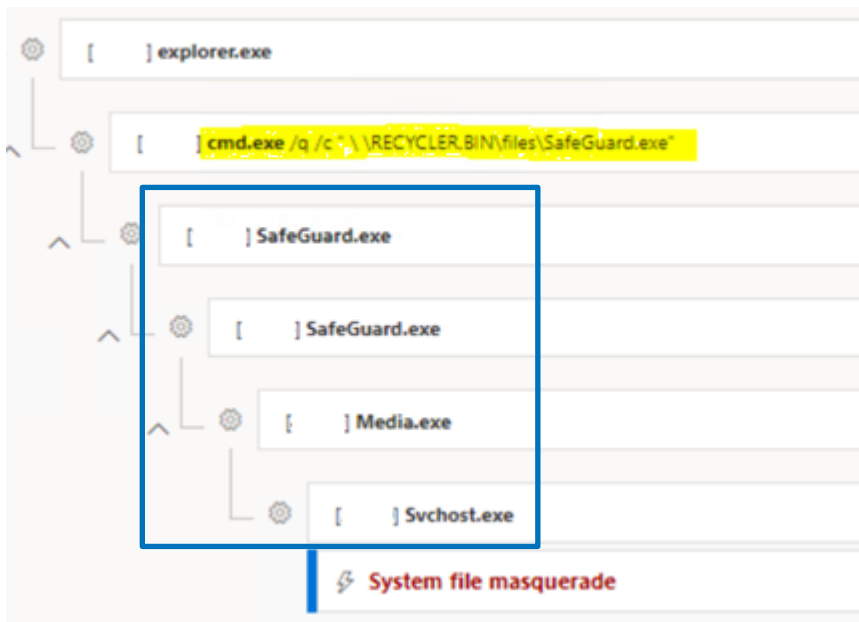
KillSomeOne



- Attack campaigns observed since 2020
- China-nexus APT Group
- LNK files and EXE files on USB flash drive
- DLL Side-Loading
- Finally infected with PlugX
- Targeting Japanese manufacturing and heavy industry overseas locations (South-East Asia)



System file masquerade



System file masquerade

■ ■ ■ 低 ● 検出済み ● 新規

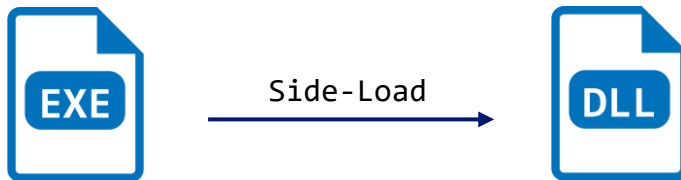
A file that masquerades as a Windows system file by using the same file name has launched. Attackers often name malware components using the names of legitimate system files to evade detection.

SafeGuard.exe / Media.exe / Svchost.exe

- Adobe legitimate files (Adobe CEF Helper.exe)
- Vulnerable to dll side-loading

EDR Detections

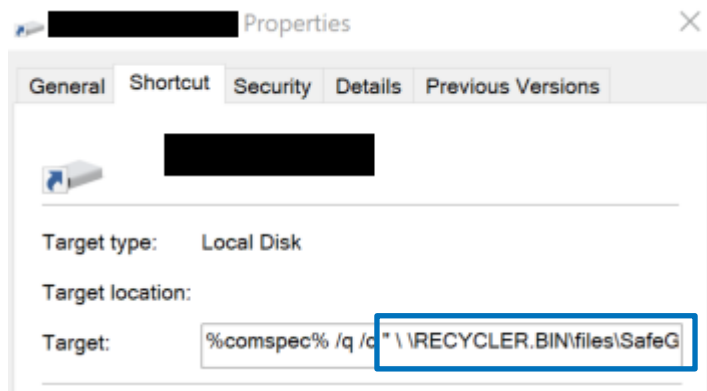
- Side-load dll files placed outside the canonical path
- Abused dlls have not changed over time



Loader exe	Original File	Loaded dll
Aug.exe	MsMpEng.exe	mpsvc.dll
AUG.exe	DISM.exe	dismcore.dll
SafeGuard.exe	Adobe CEF Helper.exe	hex.dll
Mediae.exe	x32dbg.exe	x32bride.dll

Hiding Malicious Files on USB flash drives

- Use whitespace (U+00A0) in folder paths
- Cannot see the file by referencing the path specified in the LNK file
- Information leakage with hidden folders in PlugX variants [6]



Adversary

Group

- China-nexus APT

Capabilities

- USB Device
- DLL Side-Loading
 - mpsvc.dll
 - dismcore.dll
 - hex.dll
 - x32bride.dll
- Use PlugX
- Use whitespace (U+00A0) in folder paths

Infrastructures

- ?

Victims

- Country: Japanese Company
- Sector: Manufacturing / Heavy Industry

Why USB ?

- China-nexus APT
- Incidents at overseas branches of Japanese companies
- Attacks originating from USB flash drives



Q. What are the differences between areas prone to USB incidents and those that are not?

Starting Points for USB-based Attacks



Security Holdings

- **Malicious Insider**
 - Used in information leaks and sophisticated attacks
 - High hurdles to penetration within the target organization
- **Social Engineering**
 - Send malicious USB flash drives to target users
 - TA410
- **Lateral Movement from Infected Hosts**
 - Malware is copied to a USB device connected to the infected host
 - Spread throughout the organization via USB devices
 - Mustang Panda / KillISomeOne

Differences in Attacks by Region



Security Holdings

	Asia	Europe / U.S.
Cybercrime	○	?
APT	◎	?

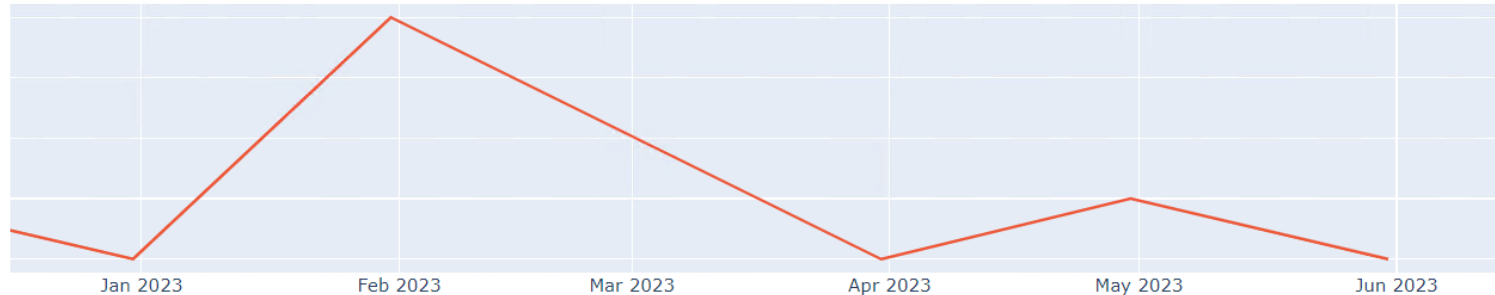
Are users in Asia infected because of high USB usage and low security awareness?

Spray-and-Pray Attacks using USB Devices



Security Holdings

- Raspberry Robin
 - Worm that downloads malicious dll files from compromised QNAP NAS
 - Spread via USB and shared folders
- Regularly observe Raspberry Robin related incidents
 - Also observe at Japanese media outlets in Japan



Number of successful attack incidents observed by the SOC related to "Raspberry Robin"

APT Attacks using USB Devices



Security Holdings

- Russian APT uses USB malware to attack Ukraine [7]
 - Reuse old malware (ANDROMEDA) and its C2 infrastructure
 - USB flash drive is still in effect as initial access
- China-nexus APT Group are expanding its target area
 - Mustang Panda attacks European Government agencies with HTML Smuggling [8]
 - TA410 campaigns target US utilities company [9]

[7] <https://www.mandiant.com/resources/blog/turla-galaxy-opportunity>

[8] <https://research.checkpoint.com/2023/chinese-threat-actors-targeting-europe-in-smugx-campaign/>

[9] <https://www.proofpoint.com/us/blog/threat-insight/ta410-group-behind-lookback-attacks-against-us-utilities-sector-returns-new>

Differences in Attacks by Region



	Asia	Europe / U.S.
Cybercrime	○	○
APT	◎	△

China-nexus APT prefers to use USB not for geographical reasons

- Isolated environment from the Internet
 - Can reach environments inaccessible to other attacks
 - Sensitive information is handled in an environment isolated from external networks
- Environments where USB is used routinely
 - where policies are not strictly enforced
 - where file sharing services are not available on closed networks

Q. Could the target environment be a factor?

USB Device Usage by Industry



Security Holdings

Presentation Only

- USB flash drive is still in effect as initial access
 - China nexus APTs prefer utilizing USB drives
 - Incidents originating from USB flash drives are occurring even in large companies
 - even in domestic companies with thorough management

- USB-based attacks can be effective in environments that are isolated from outside networks or where USB is used routinely
- China-nexus APTs are likely to have increased the number of USB-based attacks because of the prevalence of this type of environment in the types of industries targeted by them

What Should We Do



Security Holdings

- USB Port Restrictions
- In-house training to raise security awareness
- Reinforcement of security policy
- Introduction of EDR products / Creation of custom signature
- Detection starting from data leakage

- Targeted attacks originating from USB flash drive
 - Mustang Panda / TA410 / KillISomeOne
 - Observed these attacks at overseas branches of Japanese companies.
- China-nexus APTs favor USB flash drives for their operations
 - Target regions are not being compromised because of lax security policies.
 - They have refined attack methods by adapting to environments where USB devices are used

Thank you!

**For questions / comments:
ntts.nsj-so-info@global.ntt**