Why Ransomware Attack Actors Should be Identified

Hayato Sasaki

Manager of the Early Warning Group, Director of Policy, and Threat Analyst

JPCERT Coordination Center

Various detail levels of public attribution

- There are various detail levels of public attribution
  - Soft attribution: classification of attack groups by security analysts
  - Hard attribution: identification of attackers and entities behind by government agencies, etc.

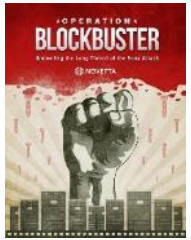
Organizations/governments behind are identified

Attackers are identified

Attack groups (and involved country/region) are identified

Sandworm

- Speculated/identified as Russian APT group
- Announced criminal prosecution of GRU personnel in Oct. 2020



Lazarus

- Speculated/identified as North Korean APT group
- Announced criminal prosecution of involved actors in Sep. 2018 and Feb. 2021

APT1

- Speculated/identified as Chinese APT group
- Mandiant identified the actor in Jan. 2013
- U.S. DOJ announced criminal prosecution in May. 2014

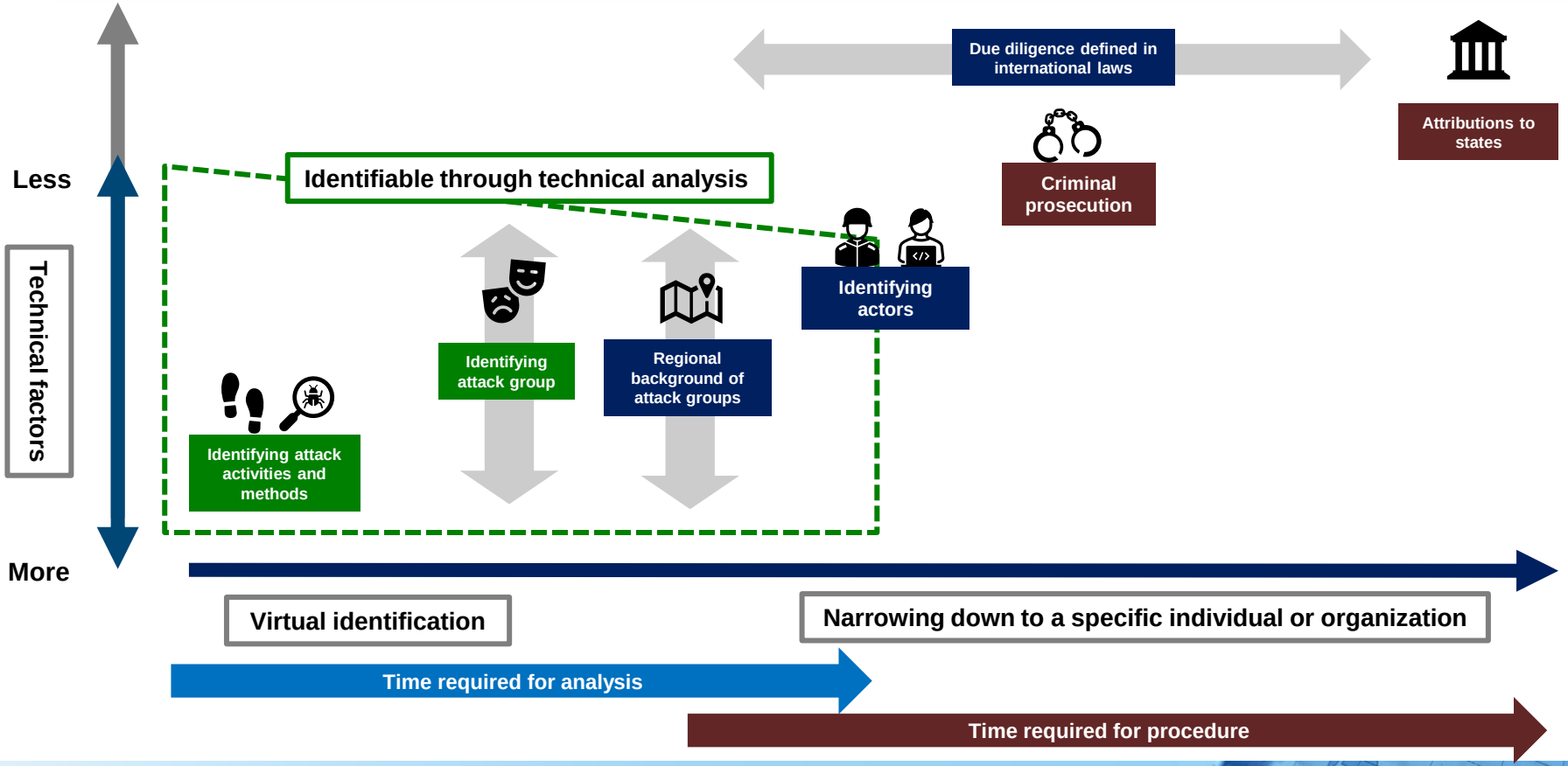
Kimsuky

- Speculated to be North Korean APT group
- Primary target is South Korea
- No actor or organization behind have been identified so far

SideCopy

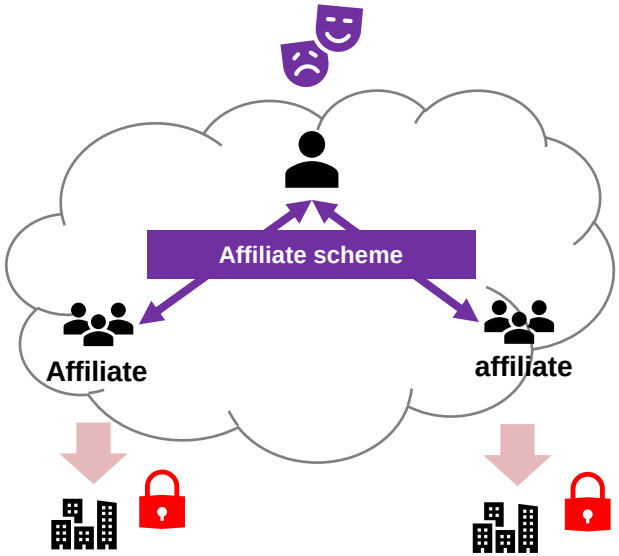
- Speculated to be Pakistani APT group
- Targets are organizations in India and Afghanistan
- Some security vendors explicitly says that the group is Pakistani

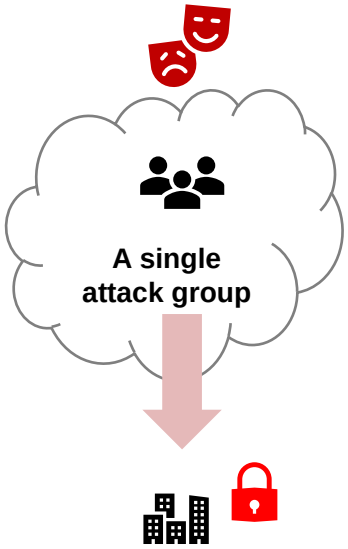
The whole picture of attribution

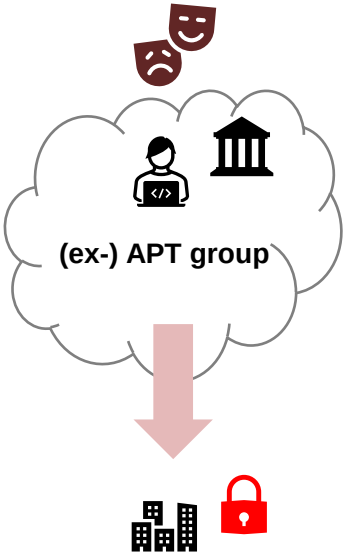


Is that actor really a ransomware gang?

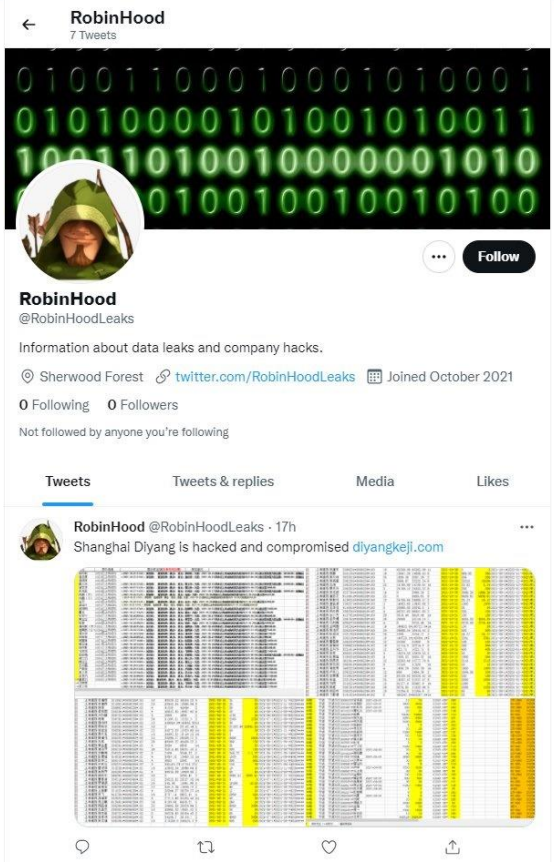
- Although RaaS, affiliate schemes, and the involvement of Russian and Eastern European criminals have received more attention, there have actually been a number of ransomware attacks by a single unidentified attack group or APT group (or groups that conducted APT campaigns in the past).
- Not all actors are operating as a part of RaaS, even in cases where well-known ransomware is identified from builder leaks, etc.
- However, in many cases, recovery is the priority in ransomware attack incident response, and thus analysis is not fully conducted until the cause of the attack, the ransomware used, and the attacker are identified.
- In addition, there is a tendency that accurate analysis is not conducted due to first responders' lack of incident experience and insufficient knowledge of ransomware attack response.







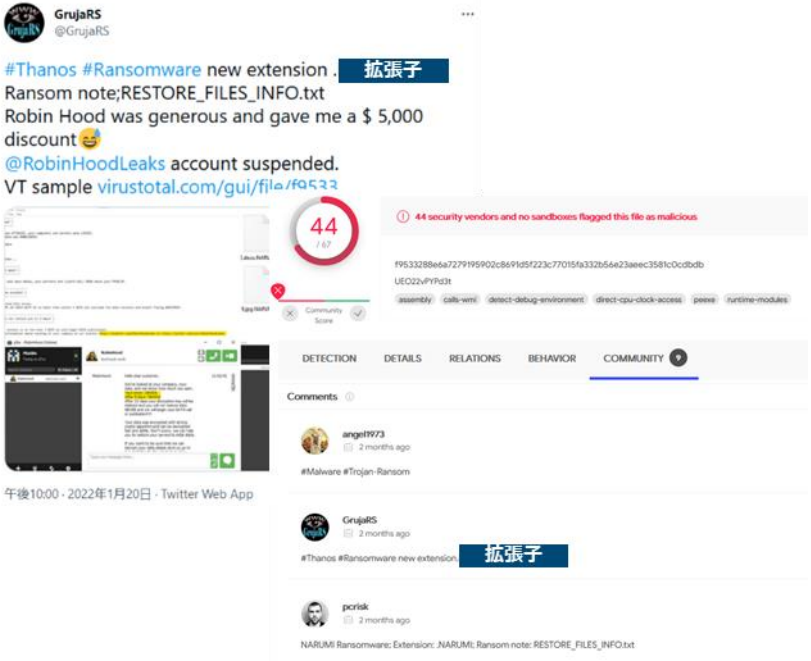
Case 1: Robinhood Leaks



- Active since at least October 2021.
- It was unclear whether the actor was Raas or a single attack group, but around the same time, another attack by the same group using a different ransomware (brand) was confirmed. It was believed that the same group was doing a fake “rebranding.”
- The group has targeted a wide range of companies in the past, including a European P&C insurance company, an African marketing firm, a Chinese manufacturer, and a U.S. software developer.
- Uses a variant of Thanos ransomware (possibly using Thanos Builder)
- File extensions after encryption appear to be abbreviated names of the affected organizations (different extensions are used for each victim)
- The X account was suspended in January 2022. Since then, the group has been using a Gettr account. Other SNS have also been used in the past. In some cases, they direct people to Tox chat.
- In the past, they have leaked some of the stolen data on SNS, but they stopped doing so.
- They are likely to exploit vulnerabilities in SSL-VPN products (or previously leaked credentials) in penetration

Identification by the characteristics of samples

- There were multiple samples with the same characteristics on VirusTotal.
- The target organization and region were inferred from the file extension after encryption, which is the abbreviated name of the target organization



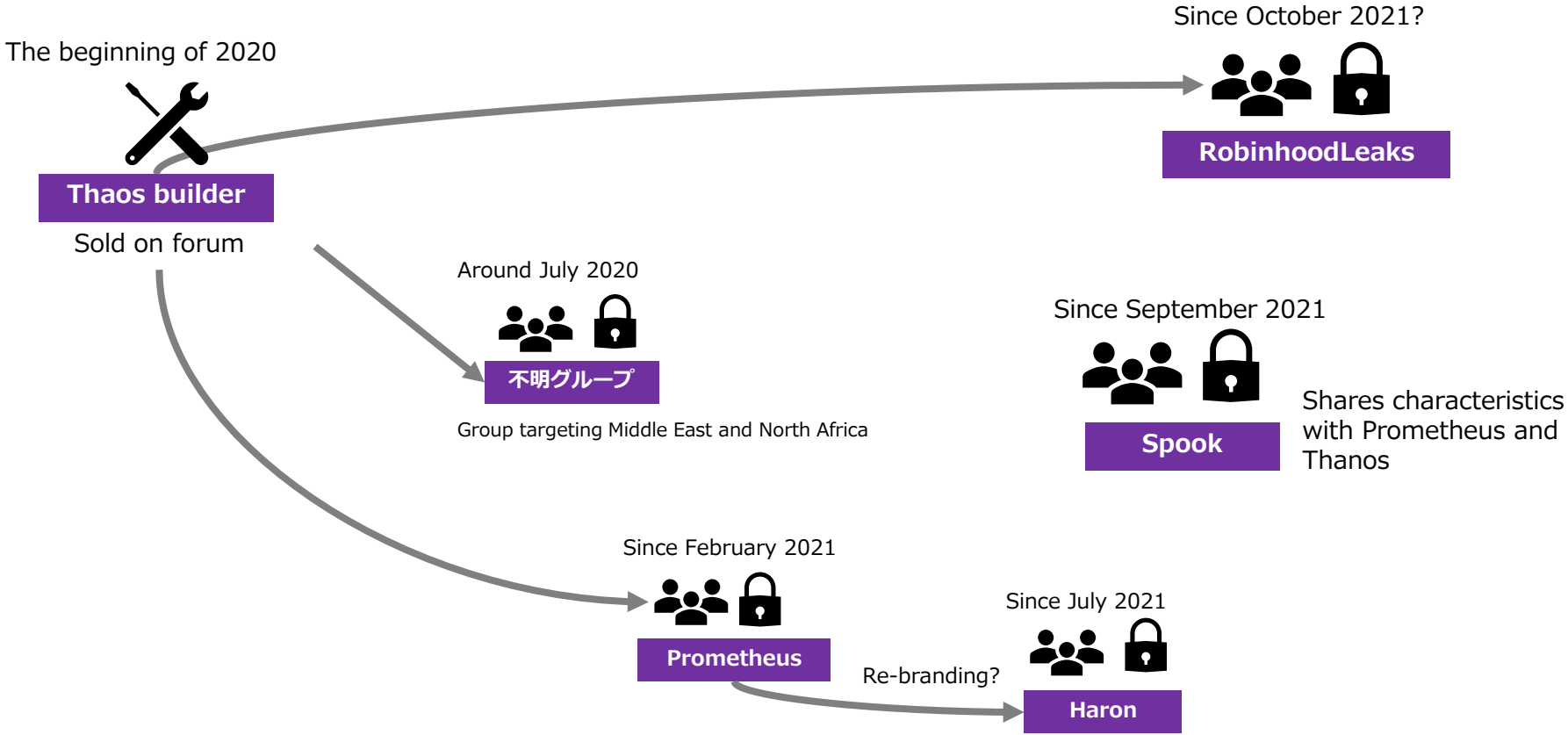
https://twitter.com/GrujaRS/status/1484148716479172608

Modification events

PID	Process	Operation	Key	Name	Value
744	UEO22vPYPd3t.exe	write	HKEY_CURRENT_USER\Software\KEYID\myKeyID	ID1	Qd40YXw8kcYgXQd8uyg7S1D2xyVN7jog+er3R0ijR9ZLDO16fPboz56yxZK+88CjaUuM7N4245+cH/g20pU8HQi+7deLM/FEdaUG7uYHFeT2ZlzvdmMBqsJp1FGQUkAz6ZZRF/wIG3j8IkPUCmJv /HUYu4mbOZku9wO73vEkr3GzoVyg34XFxEIEPfSmJs8YaTC8mnh+6eO4aASXg6wnu5TEYrv9XtYHgi+ndwLsVGHjyr29GuDDddohsEzCGpzBsvPTNfKLH2kptueqnfX7griBDol8kFQHDuBxf49hvlz Yyusmv99SY6w63serD3iKUe6Rd2l0CLxGxTdmKMRoli/CtqBoVFy6WZjrb3TnkckKQivY0QkbwwTNGu+iyJS6t1uGYeA1Xj2qqcbiWUFlF4AnLmo0u /8W1KGUIXSllgUB7SUXJhWmKNnYAhxEojNHiLbYuQH0K5K0UgmU64k757IITC2sr28BwJaDQ1SIe6S1Oe5XZzkEu9xeAWLZQ3CQqZNvFdvU5YNRg1sE /HUCgjDvm5Brd9pRPtz9MgKuFUGqToyP8f1IgtvrG36IUqKNjipPxPBy6c7g6ep+rRM97IeKfm9c25Epm01D7qmBAkZ3rkhav8yB9Og5fDf2R6+OJFCF2kLVxUj /TmnrMuwABN7XlKicxbBkXApWEMbZ0rWM=
744	UEO22vPYPd3t.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	LegalNoticeCaption	YOUR COMPANY IS HACKED AND COMPROMISED
744	UEO22vPYPd3t.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	LegalNoticeText	Your network was ATTACKED, your computers and servers were LOCKED, Your private data was DOWNLOADED: - Contracts - Customers data - Finance - HR - Databases - And more other... If you do not contact us in the next 3 DAYS we will begin DATA publication. We will post information about hacking of your company on our twitter https://twitter.com/RobinHoodLeaks or https://parler.com/user/RobinHoodLeaks You can find full details in the file RESTORE_FILES_INFO
744	UEO22vPYPd3t.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies \System	legalnoticecaption	YOUR COMPANY IS HACKED AND COMPROMISED
744	UEO22vPYPd3t.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies \System	legalnoticetext	Your network was ATTACKED, your computers and servers were LOCKED, Your private data was DOWNLOADED: - Contracts - Customers data - Finance - HR - Databases - And more other... If you do not contact us in the next 3 DAYS we will begin DATA publication. We will post information about hacking of your company on our twitter https://twitter.com/RobinHoodLeaks or https://parler.com/user/RobinHoodLeaks You can find full details in the file RESTORE_FILES_INFO
744	UEO22vPYPd3t.exe	write	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\FileSystem	LongPathsEnabled	1
744	UEO22vPYPd3t.exe	write	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	ProxyBypass	1
744	UEO22vPYPd3t.exe	write	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	IntranetName	1
744	UEO22vPYPd3t.exe	write	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	UNCAsIntranet	1
744	UEO22vPYPd3t.exe	write	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	AutoDetect	0

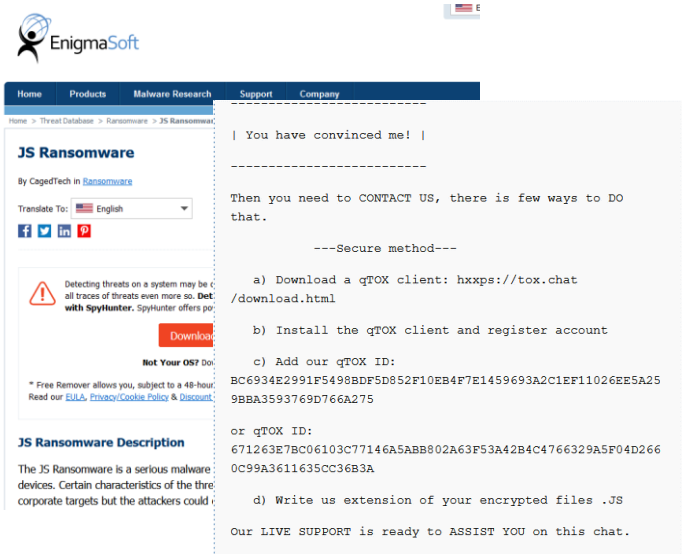
https://any.run/report/f9533288e6a7279195902c8691d5f223c77015fa332b56e23aeec3581c0cdbdb/ba082576-c0a4-4f18-9966-4b5e6da6108f

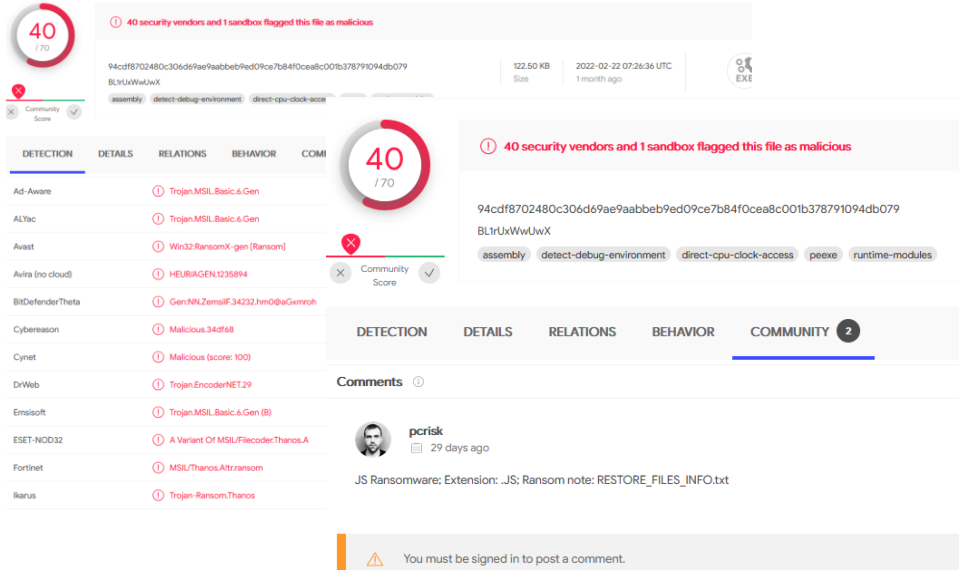
Ransomware actor that uses Thanos builder



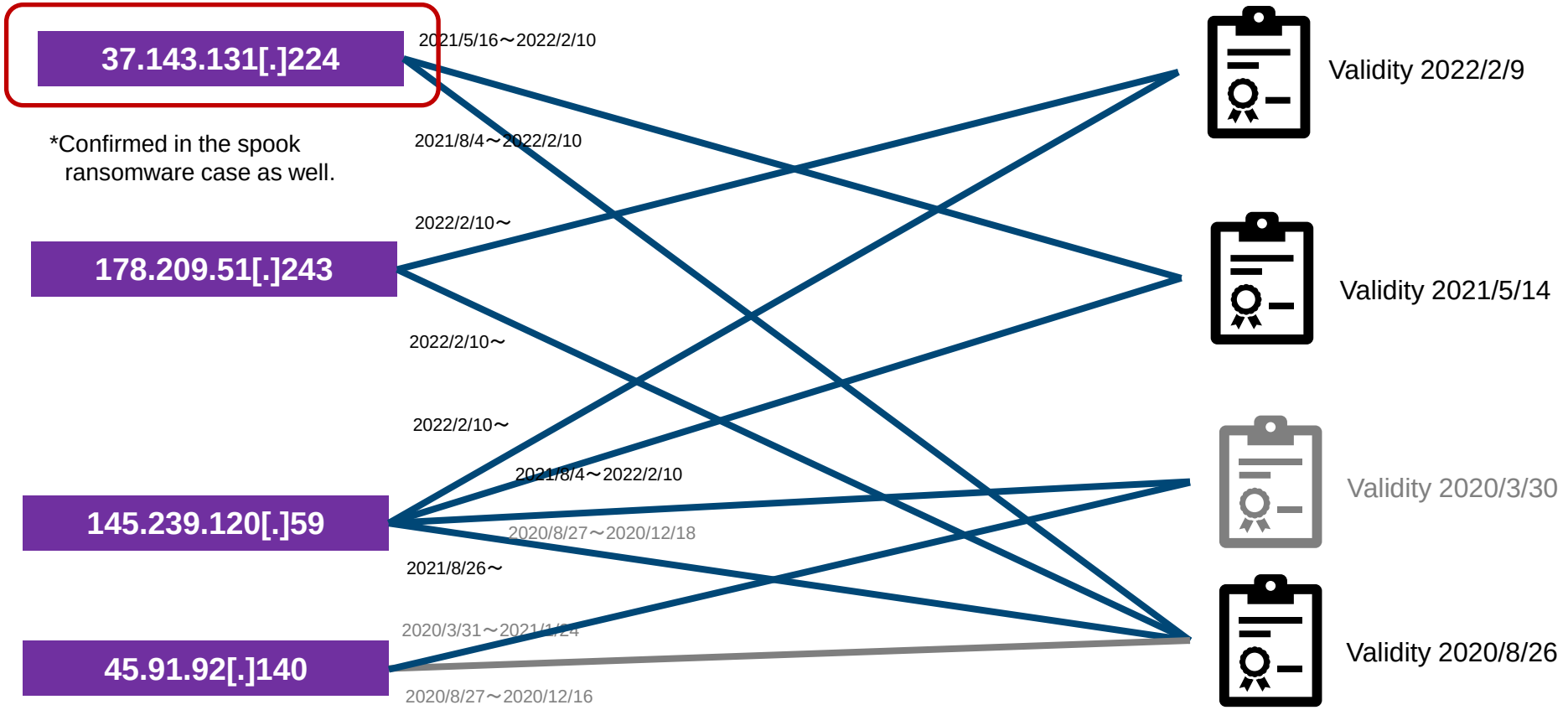
Identification by negotiation methods and used media

- Two Tox IDs found in the terminal side ransom note
  - BC6934E2991～
  - 671263E7BC0～
- Some vendors have labeled the sample that displays a ransom note with the same Tox ID as “JS Ransomware.” However, it appears to be the Thanos variant used by RobinhoodLeaks.





Identification through attack infrastructure



Common characteristics among the cases

	Spook ransom case	Case #1	Case #2	Case #3
SSL-VPN Product	Fortigate • Not listed on the Nov. 2020 Fortifuck list • OS version remains vulnerable	Sonicwall • Vulnerable version used • Notified by JPCERT/CC via DC in 2021	Sonicwall • Vulnerable version used • Notified by JPCERT/CC via ISP in 2021	Fortigate • Listed on the Nov. 2020 Fortifuck list • Multiple other suspect infrastructures
Unauthorized access to SSL-VPN	From the same IP address			
File extension	.spook	Abbreviated name of the target organization		
Contact information on the ransom note (device)		Tox ID	Not confirmed	Not confirmed
Contact information on the ransom note (server)		None	X account Gettr account	X account Gettr account

Case 2: Attack group that uses HUI loader

JPCERT CC

JPCERT/CC Eyes

Top > List of "Malware" > Analysis of HUI Loader

朝長 秀誠 (Shusei Tomonaga) May 19, 2022

Analysis of HUI Loader

Email

To conceal malware's features, attackers sometimes encode the malware and decode it only when they execute it. In such cases, the encoded malware is loaded and executed by a program called loader. In this way, an attacker can split the malware into a loader and encoded malware. Minimizing the loader's features and hiding important features of the malware make detection on infected hosts more difficult. Among such loaders, this article discusses HUI Loader, which has been used since around 2015.

Overview of HUI Loader

At JSAC2022, it was pointed out that several attack groups use HUI Loader [1], and JPCERT/CC has also confirmed attacks using this loader since around 2015. Figure 1 shows the changes in HUI Loader as well as the attack groups using it.

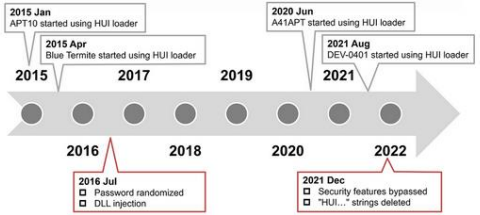


Figure 1. Changes in HUI Loader

Analysis of HUI Loader - JPCERT/CC Eyes
https://blogs.jpcert.or.jp/en/2022/05/HUILoader.html

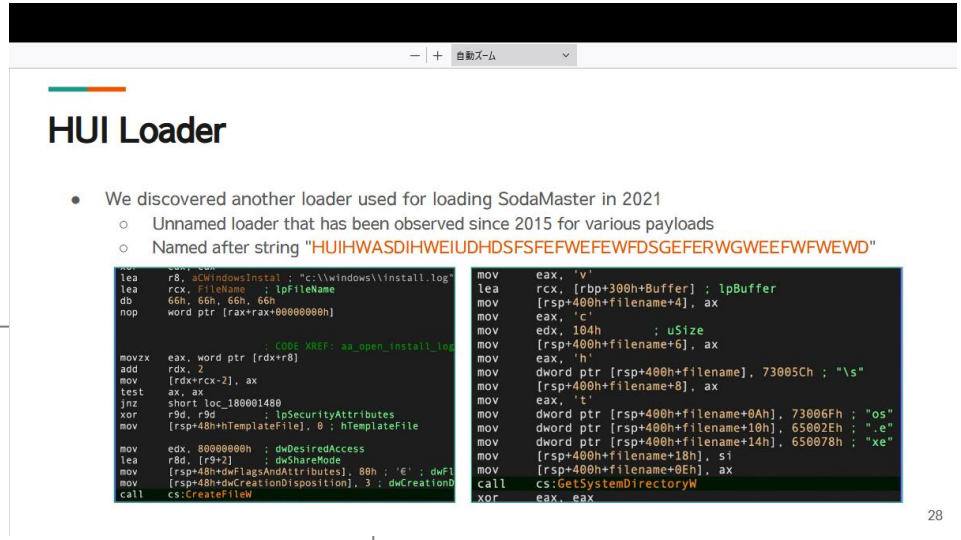
- HUI Loader was identified in an incident response to an targeted ransomware attack.
- Originally used by various targeted cyber attack groups
  - APT10 (Since 2015)
  - Blue Termite (Since 2015)
  - A41APT (Since 2020)
  - **DEV-0401** (Since 2021)

```
push    0               ; lpName
push    0               ; dwMaximumSizeLow
push    0               ; dwMaximumSizeHigh
push    4               ; flProtect
mov     esi, eax
push    0               ; lpFileMappingAttributes
push    esi             ; hFile
call    ds:CreateFileMappingW
mov     edi, eax
test    edi, edi
jnz     short loc_10002464
push    eax             ; Code
call    _exit

                        ; CODE XREF: StartAddress+10C↑j
lea     edx, [ebp+Buffer]
push    offset aHuihwasdihweiu ; "HUIHWASDIHWEIUDHDSFSFEFWEFEWFDSGEFERWGW"...
push    edx             ; Buffer
call    _swprintf
add     esp, 8
push    0               ; lpFileSizeHigh
push    esi             ; hFile
call    ds:GetFileSize
push    esi             ; hObject
mov     nSize, eax
call    ds:CloseHandle
push    0               ; dwNumberOfBytesToMap
push    0               ; dwFileOffsetLow
push    0               ; dwFileOffsetHigh
push    4               ; dwDesiredAccess
push    edi             ; hFileMappingObject
call    ds:MapViewOfFile
```

Features of HUI Loader

- Used mainly in targeted cyber attacks since around 2015
- Samples contain a distinctive string




```
Tuesday
Monday
Sunday
(null)
USER32.DLL
((((( H
h(((( H
H
CONOUT$
HUIHWASDIHWEIUDHDSFSFEFWEFEWFDSGEFERWGWEEFWFWEWD
tna.conf
```

https://jsac.jpcert.or.jp/archive/2022/pdf/JSAC2022_9_yanagishita-tamada-nakatsuru-ishimaru_en.pdf

DEV-0401

- All confirmed attacks since 2021 that used Lockfile, AtomSilo, Rook, NightSky, or Pandora ransomware are suspected to be performed by the same attack group, which Microsoft calls “DEV-0401.” Microsoft, SecureWorks, and others make the same argument.
- According to Microsoft, Lockbit2.0 has been used as ransomware payloads since April. Sygnia says Cheercrypt is also a fake rebrand of DEV-0401. Secureworks pointed out its connection to APT10.
- Exploits ProxyShell, Confluence vulnerability (CVE-2021-26084), Log4j vulnerability in VMwareHorizon, and ManageEngine ADSelfService Plus vulnerability (CVE-2021-40539) for initial penetration instead of compromising via SSL-VPN.
- No case of compromise via SSL-VPN was confirmed by JPCERT/CC.


DEV-0401: China-based lone wolf turned LockBit 2.0 affiliate

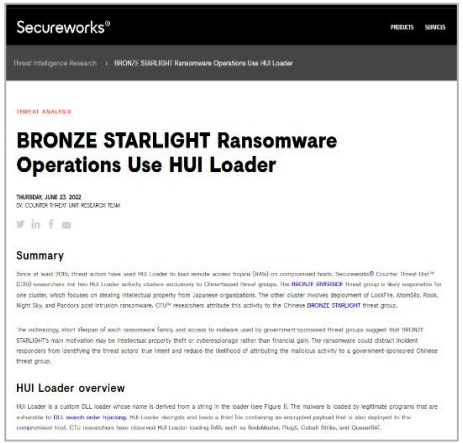
Differing from the other RaaS developers, affiliates, and access brokers profiled here, DEV-0401 appears to be an activity group involved in all stages of their attack lifecycle, from initial access to ransomware development. Despite this, they seem to take some inspiration from successful RaaS operations with the frequent rebranding of their ransomware payloads. Unique among human-operated ransomware threat actors tracked by Microsoft, DEV-0401 is confirmed to be a China-based activity group.

DEV-0401 differs from many of the attackers who rely on purchasing access to existing malware implants or exposed RDP to enter a network. Instead, the group heavily utilizes unpatched vulnerabilities to access networks, including vulnerabilities in Exchange, Manage Engine ADSelfService Plus, Confluence, and Log4j 2. Due to the nature of the vulnerabilities they preferred, DEV-0401 gains elevated credentials at the initial access stage of their attack.

Once inside a network, DEV-0401 relies on standard techniques such as using Cobalt Strike and WMI for lateral movement, but they have some unique preferences for implementing these behaviors. Their Cobalt Strike Beacons are frequently launched via DLL search order hijacking. While they use the common Impacket tool for WMI lateral movement, they use a customized version of the wmiexec.py module of the tool that creates renamed output files, most likely to evade static detections. Ransomware deployment is ultimately performed from a batch file in a share and Group Policy, usually written to the NETLOGON share on a Domain Controller, which requires the attackers to have obtained highly privileged credentials like Domain Administrator to perform this action.

DEV-0401 ransomware payloads over time

Microsoft
https://www.Microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/


Secureworks

Threat Intelligence Research › BRONZE STARLIGHT Ransomware Operations Use HUI Loader

THREAT ANALYSIS

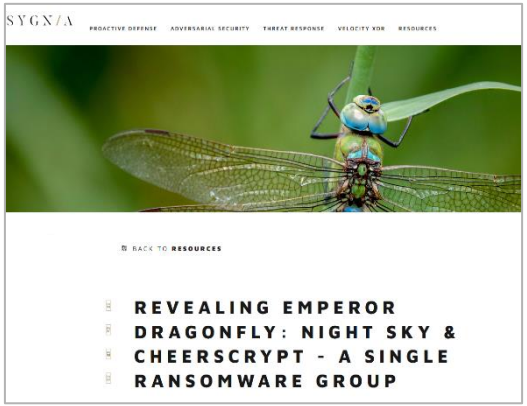
BRONZE STARLIGHT Ransomware Operations Use HUI Loader

THURSDAY, JUNE 23, 2022
BY COUNTER THREAT UNIT RESEARCH TEAM

Summary

HUI Loader overview

Secureworks
https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader



SYGNIA
https://blog.sygnia.co/revealing-emperor-dragonfly-a-chinese-ransomware-group

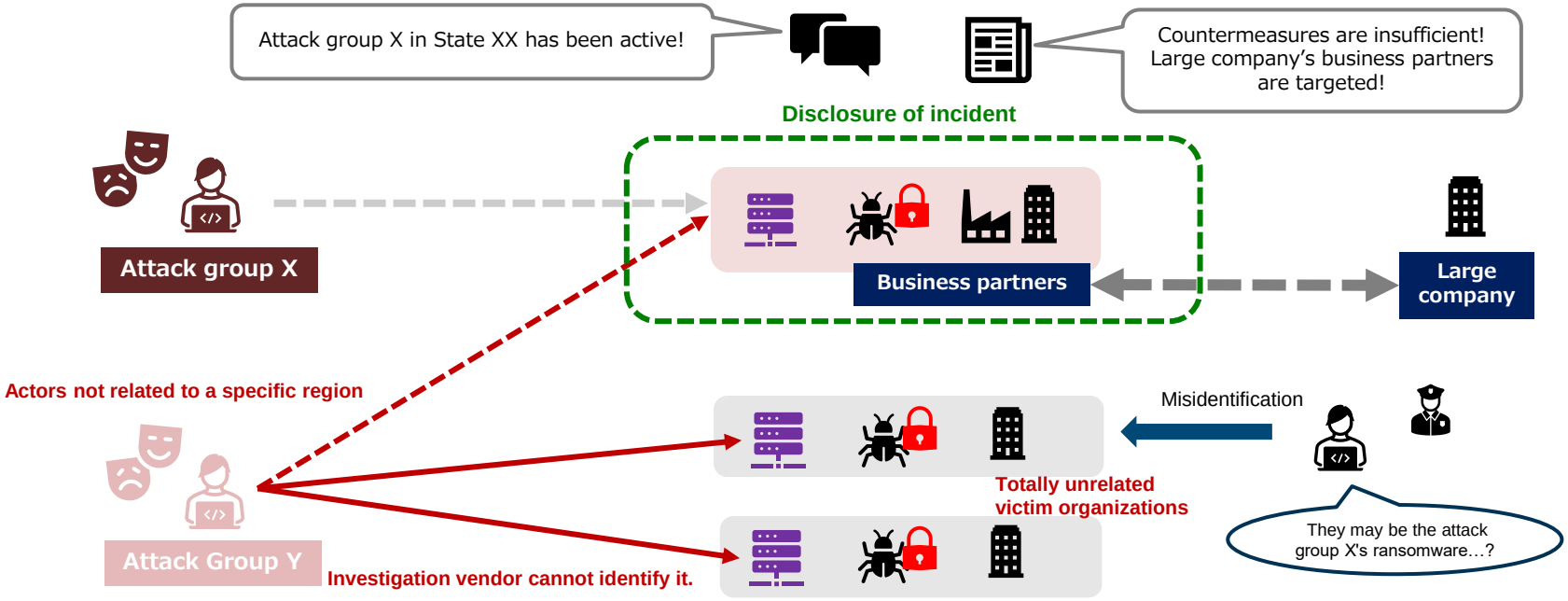
Tracking DEV-0401 that uses HUI Loader

- Lockile, Atom Silo, and Rook are similar to Babuk, whose source code leaked in September 2021.
- NightSky is similar to Rook, and the packer is also identical.
- Pandora and Rook contain the same code partially, and the packer is same as that of Nightsky‘s.
- TTP between each ransom case is also similar.

Ransomware used	LockFile	AtomSilo	Rook	Nightsky	Pandora	The case SecureWorks responded
Active	Since Aug. 2021	Since Sep. 2021	Since Nov. 2021	Since Dec. 2021	Since Feb. 2022	During Feb. 2022
Initial Penetration	Proxyshell vulnerability	Confluence vulnerability (CVE-2021-26084)	ManageEngine ADSelfService Plus vulnerability (CVE-2021-40539) was possibly exploited.	VMWare Horizon Log4j vulnerability		ManageEngine ADSelfService Plus vulnerability (CVE-2021-40539)
DLL side loading	Used KuGou Active Desktop legitimate file	Used KuGou Active Desktop legitimate file		Used MacAfee product legitimate file	Used MacAfee product legitimate file	
HUI Loader	✓	✓	✓	✓	✓	✓
Ransomware sample	Similar		Similar	Similar		
C2 infrastructure		Similar to NightSly case		Similar to Atomsilo case		

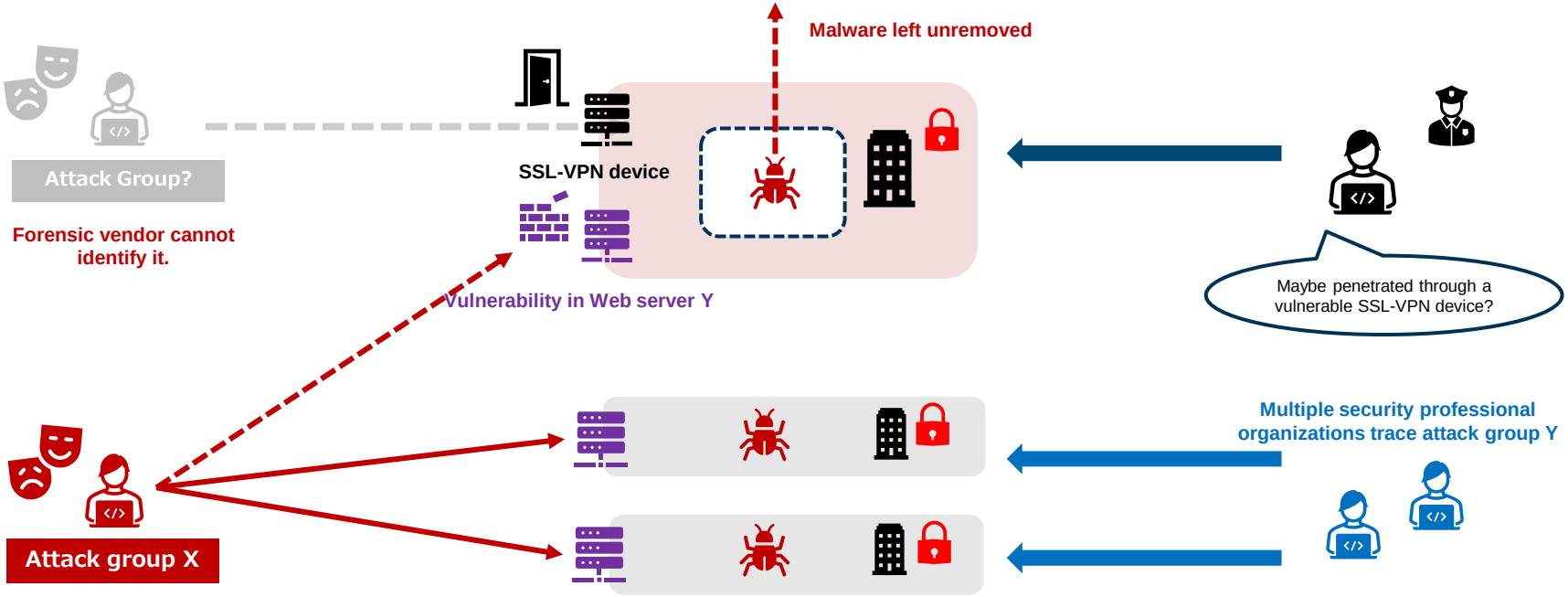
Cases where incident response fails due to insufficient actor identification #1

- As international tensions increase, people's speculations associate attacks and actors with specific regions, or relate the motivation for the attacks and the reasons for being targeted to international affairs and supply chain relationships.
- In reality, the attacks were conducted by actors completely unrelated to any particular region or supply chain, using known ransomware. They had been active since before the international situation changed. In some cases, the ransomware types were even misidentified, linking it to an unrelated attack group.



Cases where incident response fails due to insufficient actor identification #2

- We identified communications due to a certain type of malware infection and contacted the organization, and it turned out that it was due to the malware left unremoved in the ransomware attack over a year ago.
- The forensic vendor at the time had failed to identify the attack group. The vulnerable Web server, which was the initial access route used by the attack group at the time, was not investigated, and preventive measures were not properly implemented.



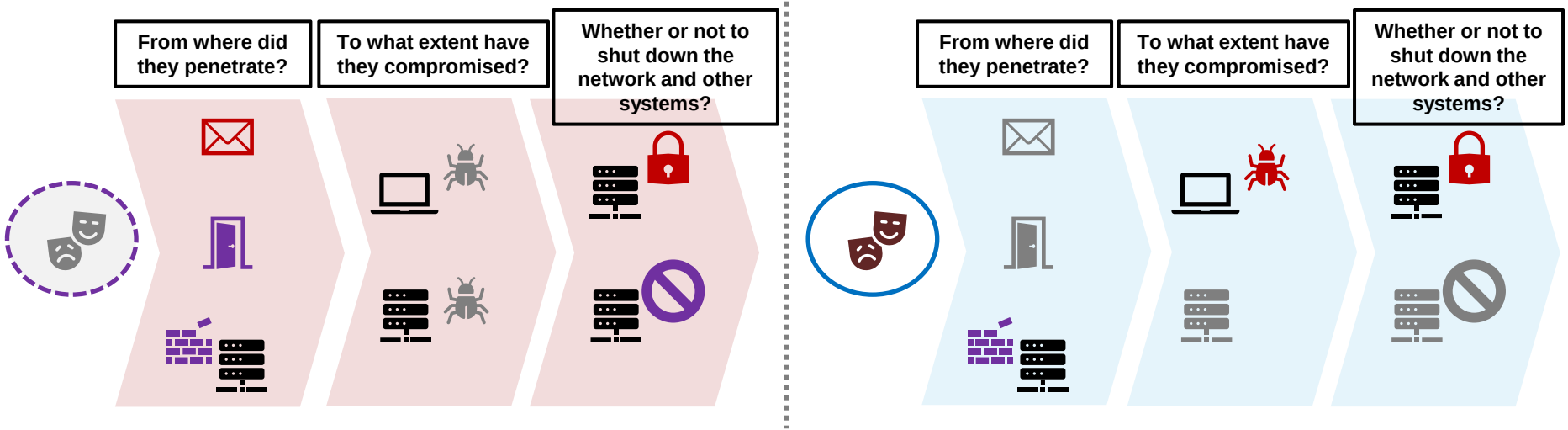
Why should ransomware attack actors be identified?

- To ensure that initial response is appropriate, prompt, and at low cost
  - Identify the cause of Initial Access.
  - Reduce unnecessary network shutdowns and forensics in the initial response by narrowing down the possible attack methods used.
- To ensure that APT actors conducting ransomware attacks are not missed.
- To contain the ransomware threat and select effective countermeasures for each actor.

Ensuring fast and efficient initial response

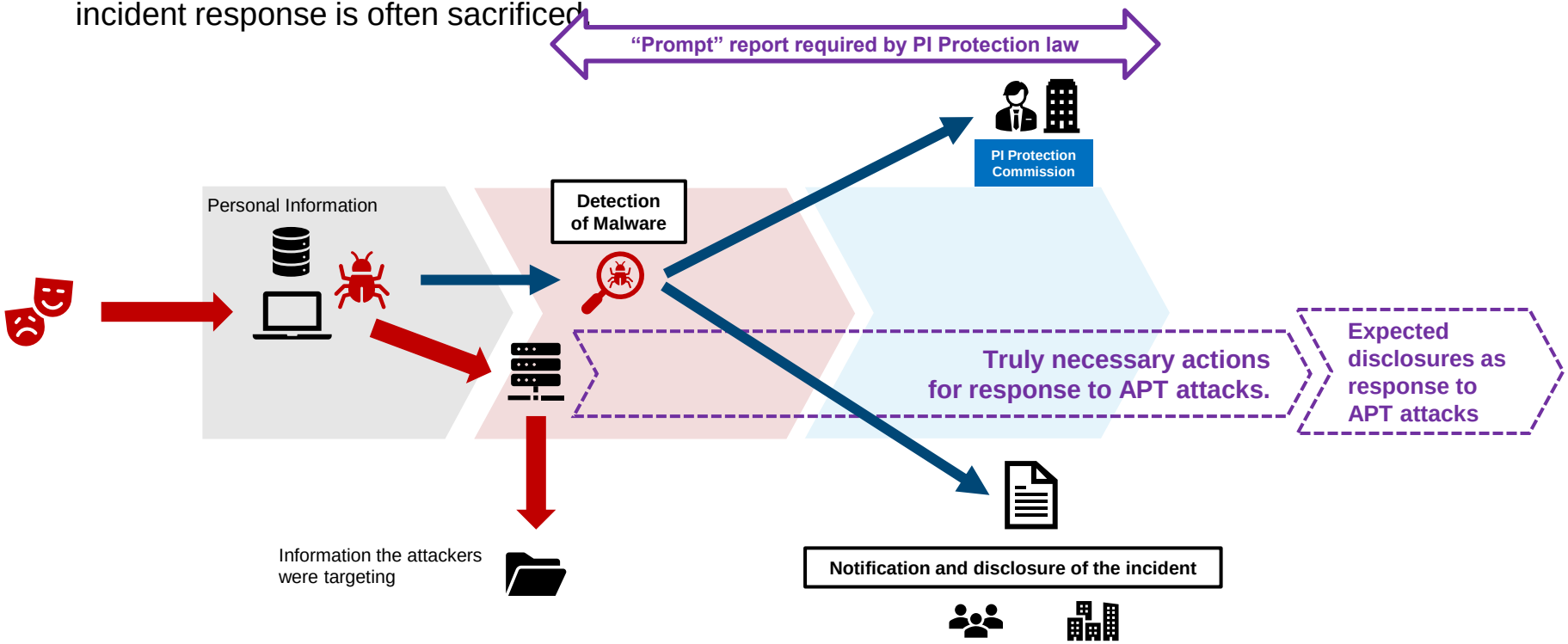
- Identify and narrow down the ransomware type and actor to infer the TTPs used
  - Narrow down the initial access and lateral movement routes and determining the priorities of investigation
  - Reduce unnecessary network and system shutdowns as much as possible

...but in reality, the staffs are asked to investigate "all systems" and "whether any information has leaked."



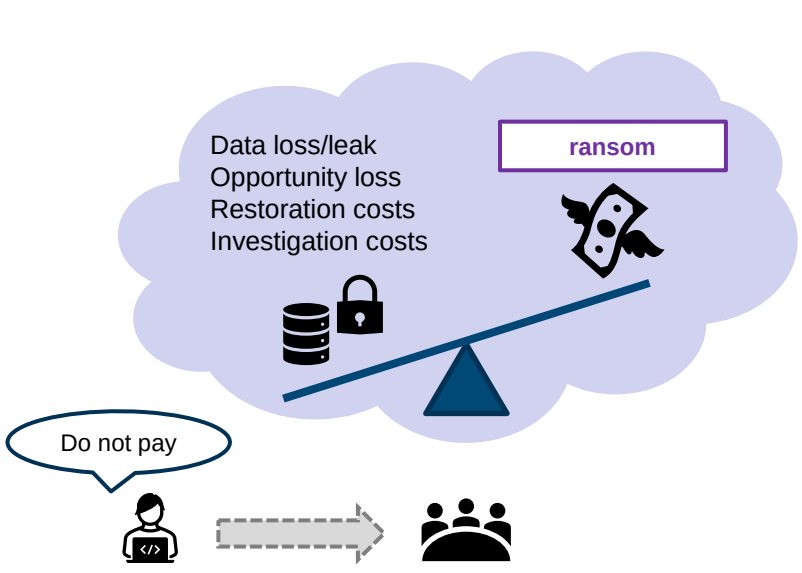
Why is the investigation of personal information leaks often prioritized?

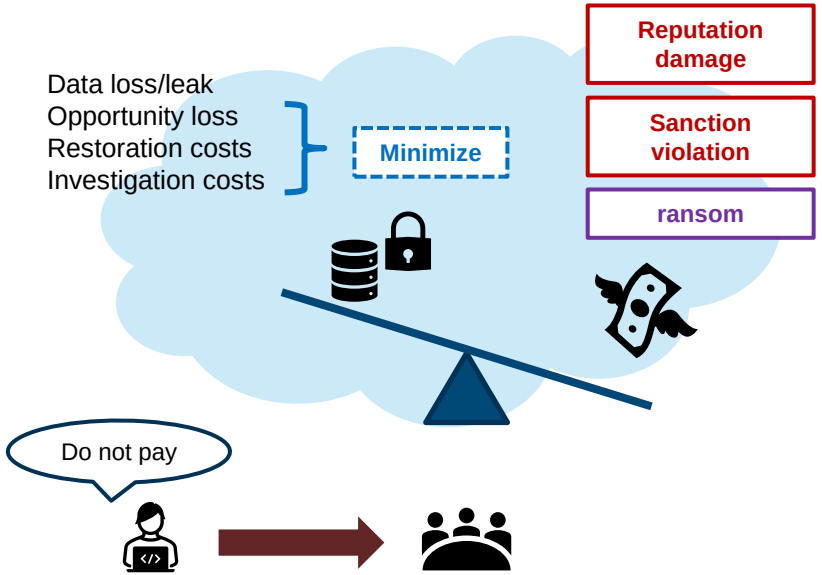
- Victim organizations often get overwhelmed by the “prompt” reports and notifications to affected individuals, which is required by the Personal Information Protection Law, and the resource for incident response is often sacrificed.



For a rational decision to refuse to pay ransom

- Trend toward restricting ransom payments in various countries, including statements made at the Counter Ransomware Initiative meeting lead by the U.S.
- Depending on the actor, ransom payment can be considered sanction violation.
- However, simply saying, “Do not pay ransom,“ does not provide a reasonable basis for decision making.
- Efficient initial response minimizes additional “damage“ as much as possible.

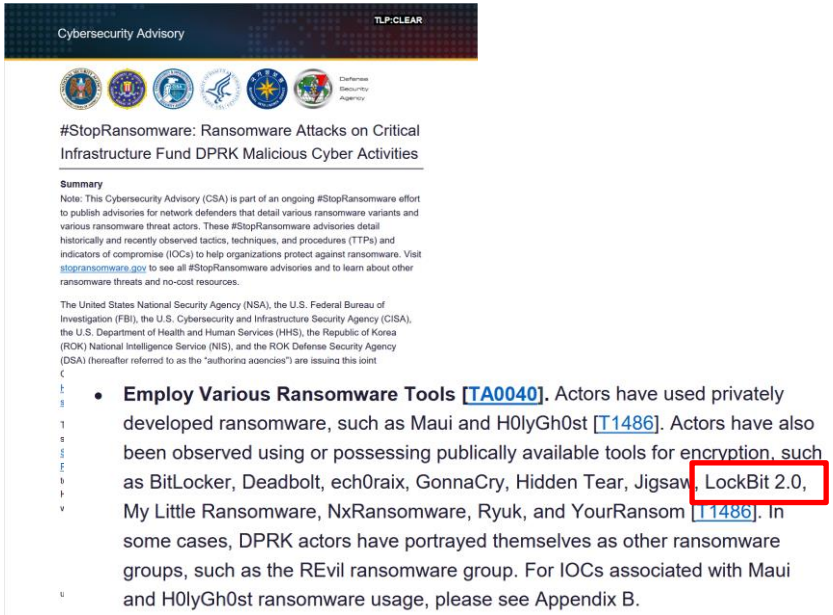




To trace and counter APT actors

- We may be missing APT attacks blended in numerous Lockbit 2.0 infection cases.

Subgroup of Lazarus



Cybersecurity Advisory TLP:CLEAR

#StopRansomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities

Summary

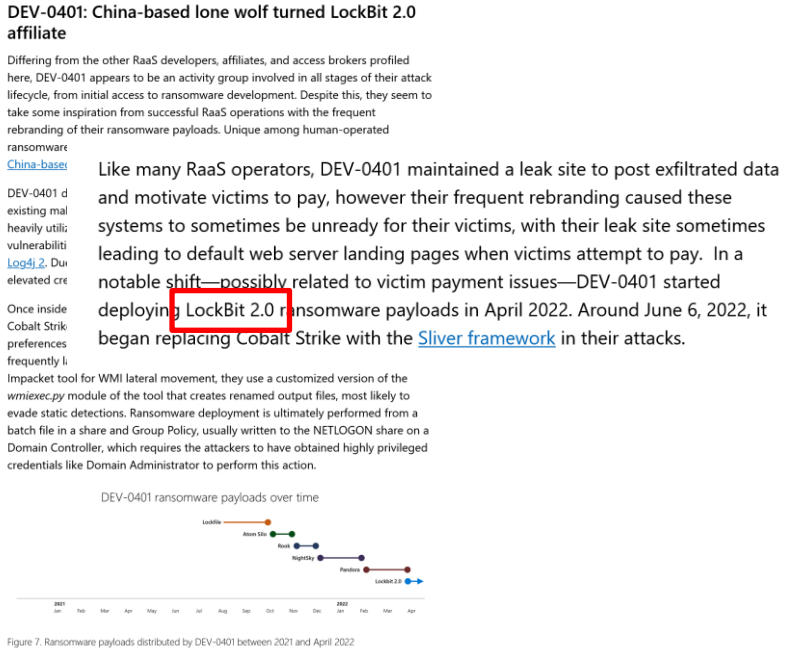
Note: This Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and various ransomware threat actors. These #StopRansomware advisories detail historically and recently observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and to learn about other ransomware threats and no-cost resources.

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 U.S. Department of Health and Human Services (HHS), the Republic of Korea (ROK) National Intelligence Service (NIS), and the ROK Defense Security Agency (DSA) (hereafter referred to as the "authoring agencies") are issuing this joint

- **Employ Various Ransomware Tools [TA0040].** Actors have used privately developed ransomware, such as Maui and H0lyGh0st [T1486]. Actors have also been observed using or possessing publically available tools for encryption, such as BitLocker, Deadbolt, ech0raix, GonnaCry, Hidden Tear, Jigsaw, LockBit 2.0, My Little Ransomware, NxRansomware, Ryuk, and YourRansom [T1486]. In some cases, DPRK actors have portrayed themselves as other ransomware groups, such as the REvil ransomware group. For IOCs associated with Maui and H0lyGh0st ransomware usage, please see Appendix B.

https://media.defense.gov/2023/Feb/09/2003159161/-1/-1/0/CSA_RANSOMWARE_ATTACKS_ON_CI_FUND_DPRK_ACTIVITIES.PDF

DEV-0401



DEV-0401: China-based lone wolf turned LockBit 2.0 affiliate

Differing from the other RaaS developers, affiliates, and access brokers profiled here, DEV-0401 appears to be an activity group involved in all stages of their attack lifecycle, from initial access to ransomware development. Despite this, they seem to take some inspiration from successful RaaS operations with the frequent rebranding of their ransomware payloads. Unique among human-operated ransomware

China-base

DEV-0401 d
existing mal
heavily utili
vulnerabiliti
Log4j 2. Du
elevated cre

Like many RaaS operators, DEV-0401 maintained a leak site to post exfiltrated data and motivate victims to pay, however their frequent rebranding caused these systems to sometimes be unready for their victims, with their leak site sometimes leading to default web server landing pages when victims attempt to pay. In a notable shift—possibly related to victim payment issues—DEV-0401 started deploying LockBit 2.0 ransomware payloads in April 2022. Around June 6, 2022, it began replacing Cobalt Strike with the Sliver framework in their attacks.

Once inside
Cobalt Strik
preferences
frequently l

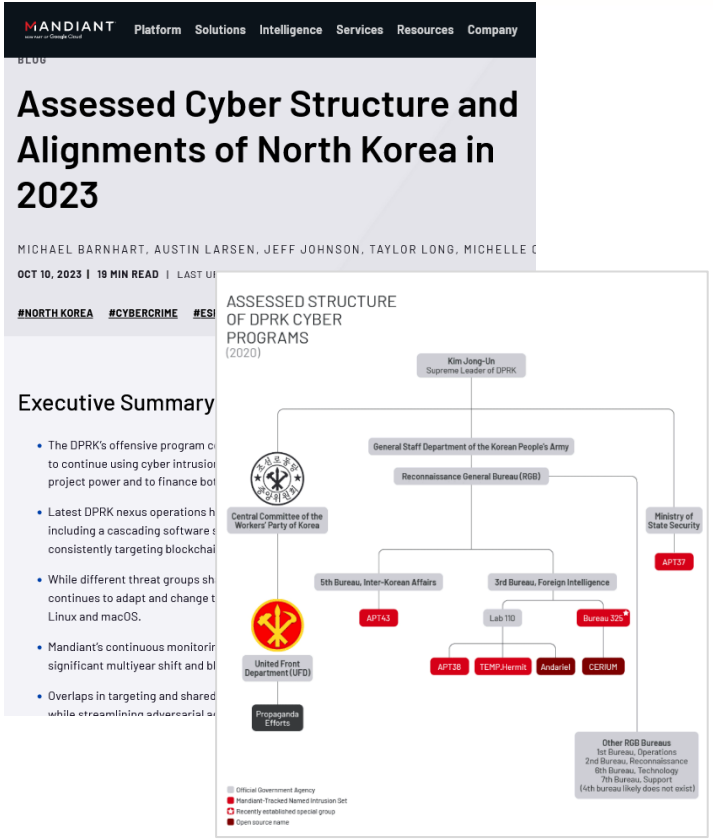
Impacket tool for WMI lateral movement, they use a customized version of the *wmiexec.py* module of the tool that creates renamed output files, most likely to evade static detections. Ransomware deployment is ultimately performed from a batch file in a share and Group Policy, usually written to the NETLOGON share on a Domain Controller, which requires the attackers to have obtained highly privileged credentials like Domain Administrator to perform this action.

DEV-0401 ransomware payloads over time

Figure 7. Ransomware payloads distributed by DEV-0401 between 2021 and April 2022

https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

Lazarus subgroups self-finance their activities



https://www.mandiant.com/resources/blog/north-korea-cyber-structure-alignment-2023

- APT43 (newly classified and tracked by Mandiant) is considered to be conducting attack campaigns targeting crypto assets for the purpose of self-funding its activities.
- Andariel, which includes Stonefly and several other subgroups, uses Maui, Lockbit 2.0, and other types of malware, according to a February 2023 joint advisory from U.S. officials. This is also considered to be intended for self-financing of its activities

Dangerous Password, etc.

Intended attacks targeting crypto assets

APT43

Intended cyber attack

+

Attacks targeting crypto assets for Self-finance

Andariel

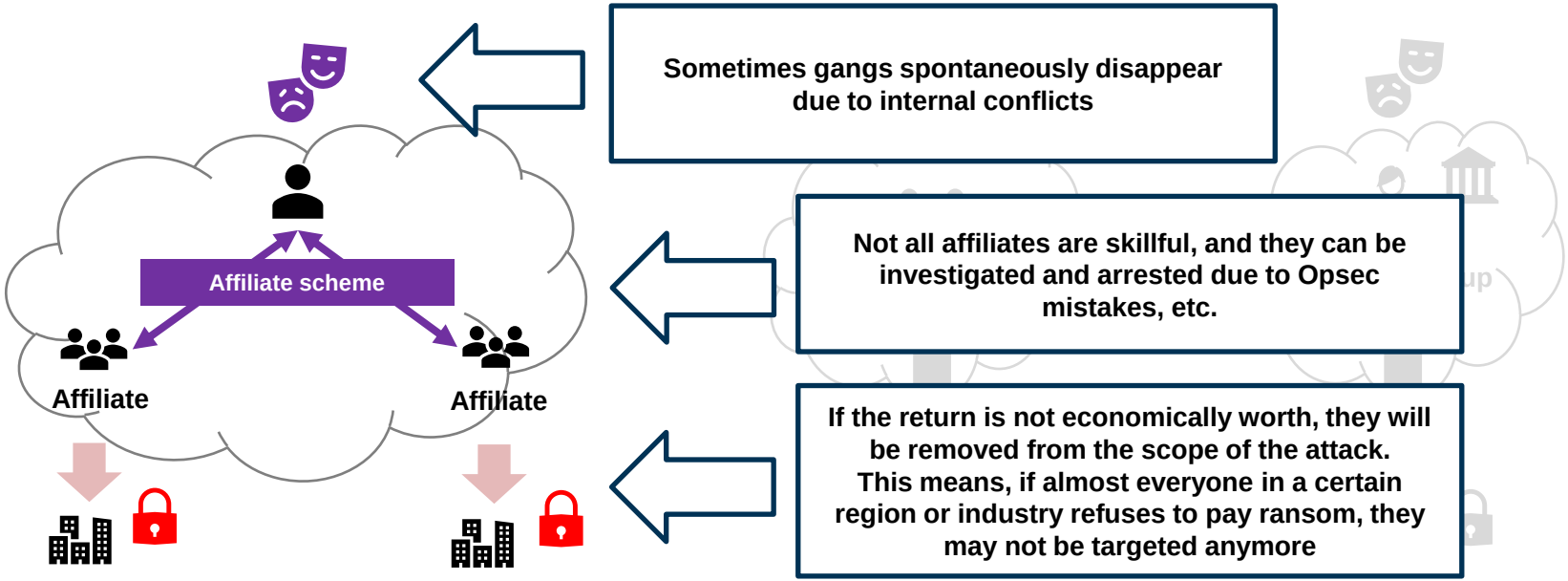
Intended cyber attack

+

Ransomware attacks for Self-finance

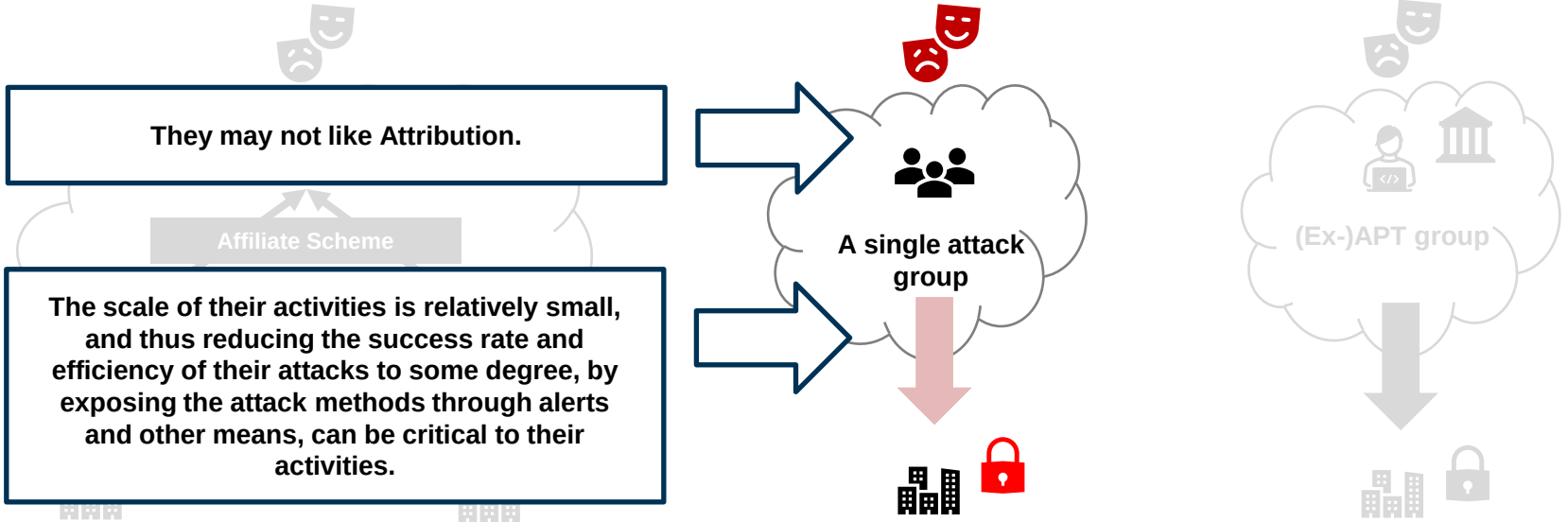
Case: countermeasures against affiliate scheme actors

- In some cases, affiliate schemes disappeared due to internal conflicts, and in other cases, the activities were ceased by the arrest of those involved.



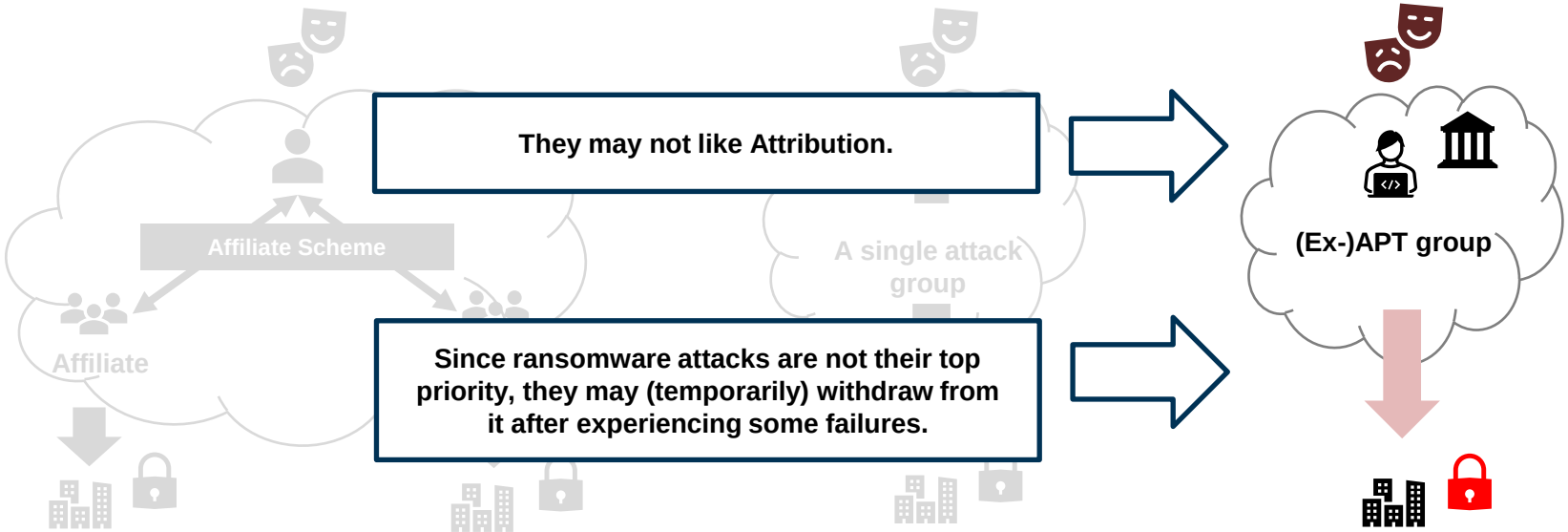
Case: countermeasures against a single attack group

- Hypothesis: Attackers use fake rebranding because they may not like attribution for some reason.
  - Exposing attack methods through alerts and analysis reports may deter attackers' activities to some degree, even when they are not arrested.
- The scale of their activities is relatively small compared to affiliate schemes. Therefore, reducing the success rate and efficiency of their attacks to some degree, through alerts and other means, can be critical to their activities.



Case: Countermeasures against APT Group

- Since many APT actors have ceased or changed their activities due to public attribution or have changed their activities and techniques as a result of alerts and analytical reports in the past, similar countermeasures and deterrence may be effective.
- Since ransomware attacks are only a "side business" to them, they may temporarily or permanently withdraw from ransomware attacks after experiencing some continued failures



Summary: Why ransomware attack group should be identified

- To ensure that initial response is appropriate, prompt, and at low cost
- To ensure that APT actors conducting ransomware attacks are not missed
- To contain the ransomware threat and select effective countermeasures for each actor.

⇒ Victims will be less inclined to pay ransom if the burden on them during ransomware attack incident response can be reduced.

⇒ Appropriate countermeasures for each type of actors would reduce the number of ransom-actor involved ?