Lazarus Group Evolved Their Infection Chain with Old and New Malware

Sojun Ryu

GReAT, Kaspersky

whoami

Sojun Ryu

11+ years experience in malware analysis & incident response

Security Researcher @ Global Research and Analysis Team, Kaspersky

Interested in

Reverse Engineering, Incident Reponse, Threat Intelligence, APTs, Cybercrimes

Focus on

Tracking Korean-speaking threat actors

Tracking threat actors targeting APAC region

Talks at FIRST

#FIRSTCTI22

#FIRSTCON23

Gwisin: A Spooky Ransomware Only Targets South Korea

Hyeok-Ju Gwon, Kyoung-Ju Kwak, Jungyun Lim, Sojun Ryu (S2W Inc., KR)

KILLNET: Quantity Over Quality

Sojun Ryu (S2W Inc., KR)


LAZARUS
LAZARUS GROUP

Lazarus group profile

Adversary

- Lazarus group (aka. Diamond Sleet, TEMP.Hermit)
- Published by Novetta in 2016
- Since at least 2009

Victim

- Over the world
- Cryptocurrency, Government, Defense, Software, IT, Automobile, etc.

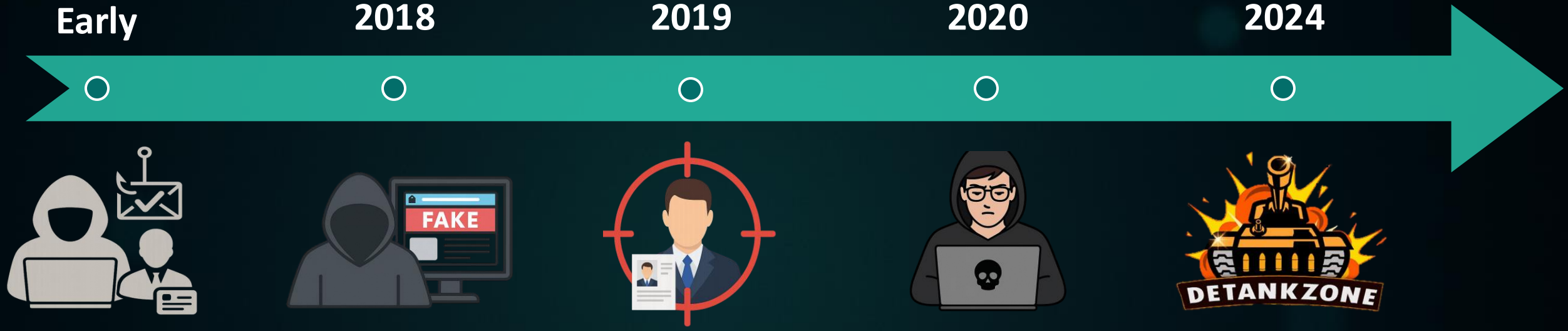
Capability

- Social engineering
- Multi-stage malware
- In-memory implants

Infrastructure

- Compromised web servers
- Controllable VPS servers
- Multi-Stage Channels

Evolution of social engineering techniques



Traditional
Spear-phishing

AppleJeus
Fake web site

Operation Dream Job
Fake job recruiter

Targeting security researchers
Fake security researcher

Targeting crypto investor
Fake DeFi game with AI generated image

Changes in the initial vector of Operation Dream Job

Channel

- Spear-phishing mail
  - Malicious attachment
  - Fake job seeker platform
- From job seeker platforms to
  - E-mail
  - WhatsApp
  - etc

Delivery

- Job description/offer
  - Malicious Word files
  - Trojanized PDF Viewer (Sumatra PDF/MuPDF/SecurePDF)
- Skill assessment
  - PuTTY/KiTTY
  - TightVNC/UltraVNC
  - Coding challenge

Summary of our research

3

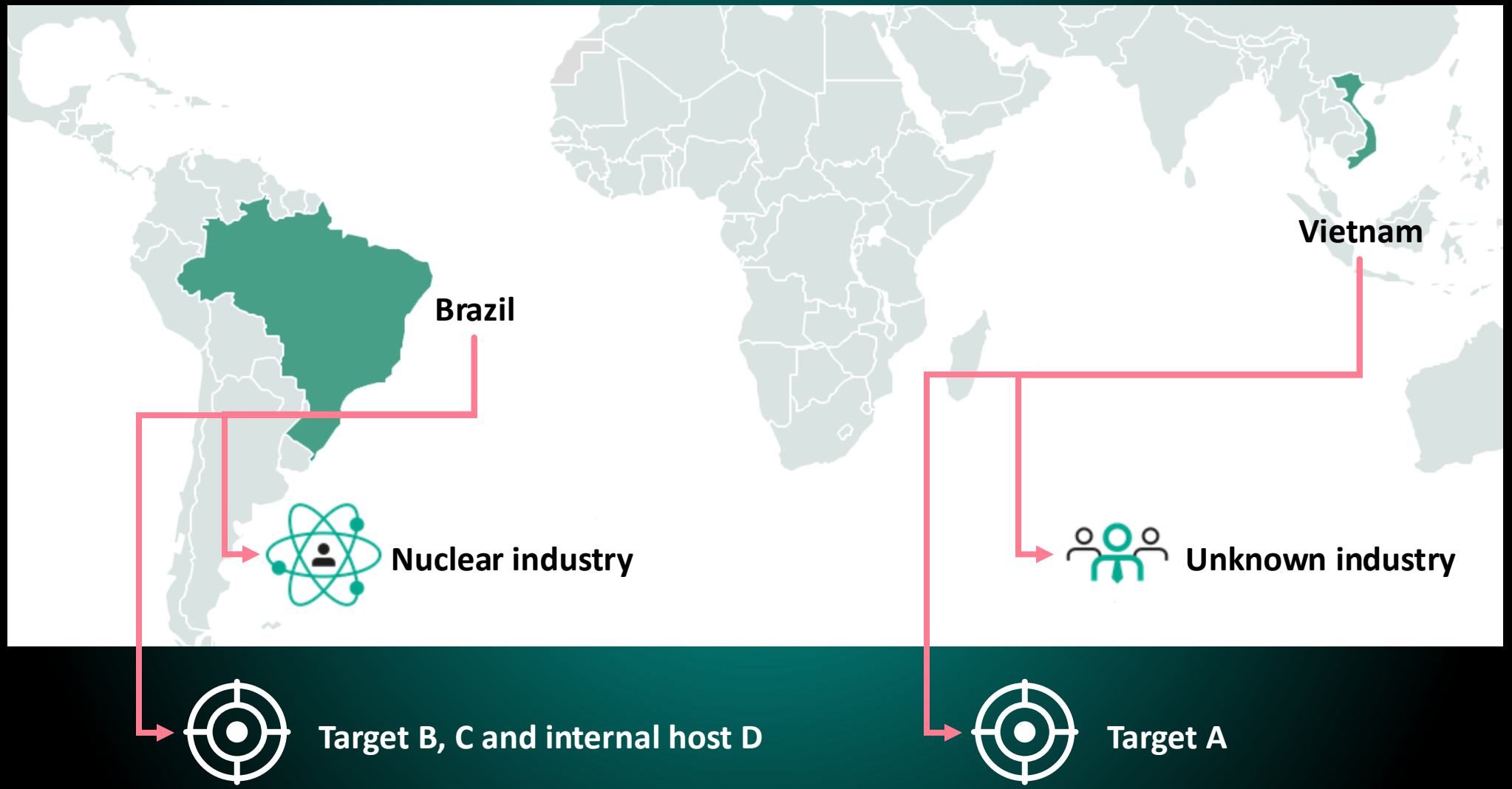
Number of initial targets

Lure theme

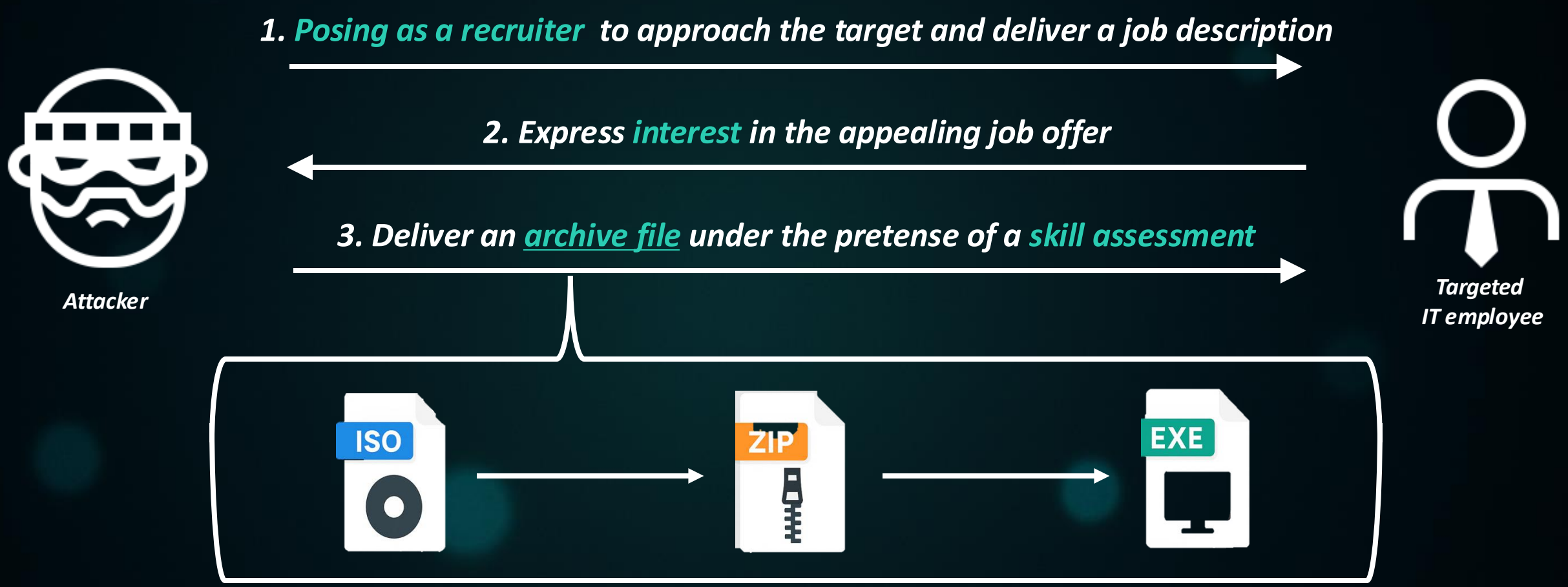
15

Number of malware families

Targets

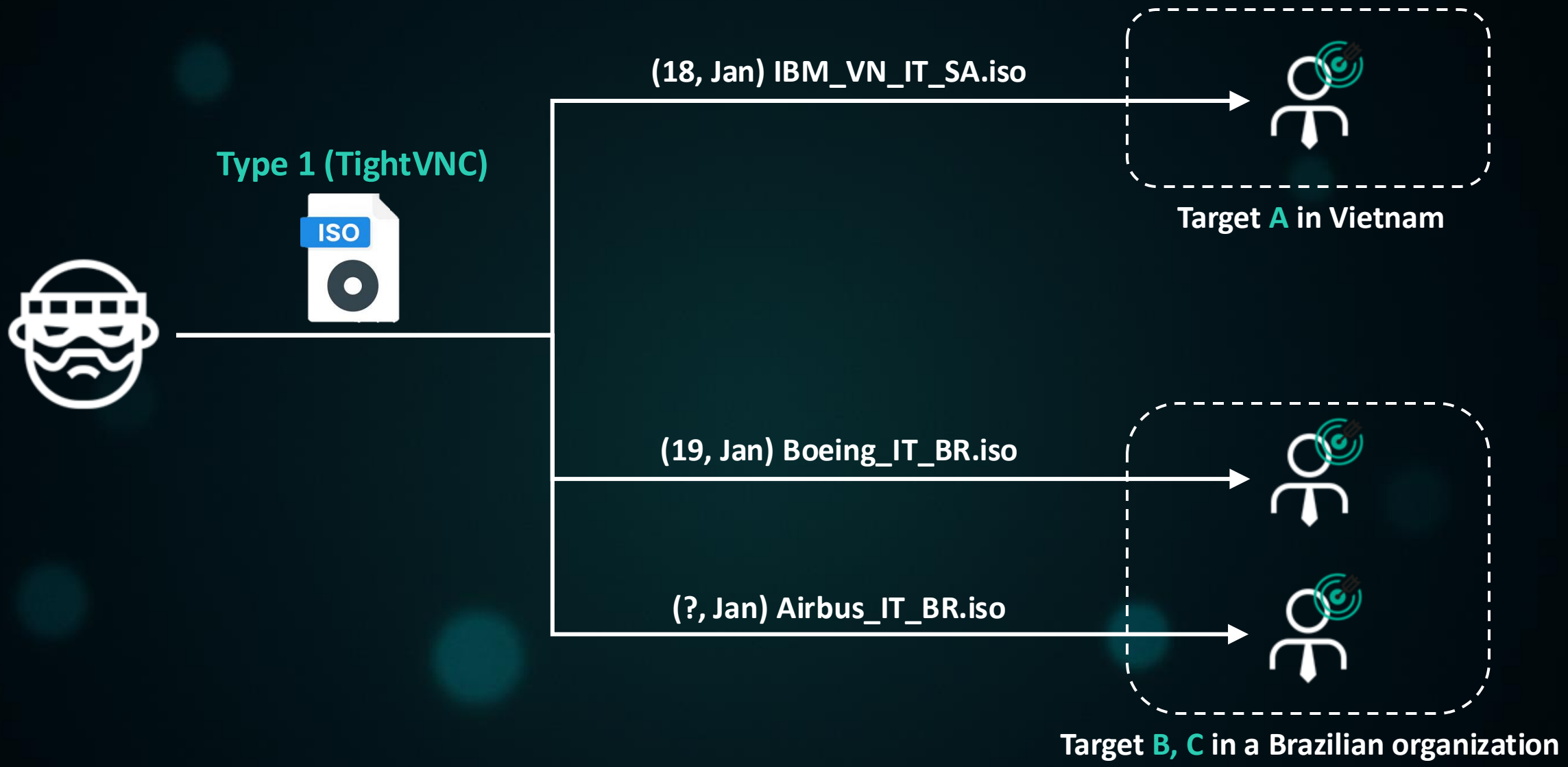

Brazil
Vietnam
Nuclear industry
Unknown industry
Target B, C and internal host D
Target A

Initial vector

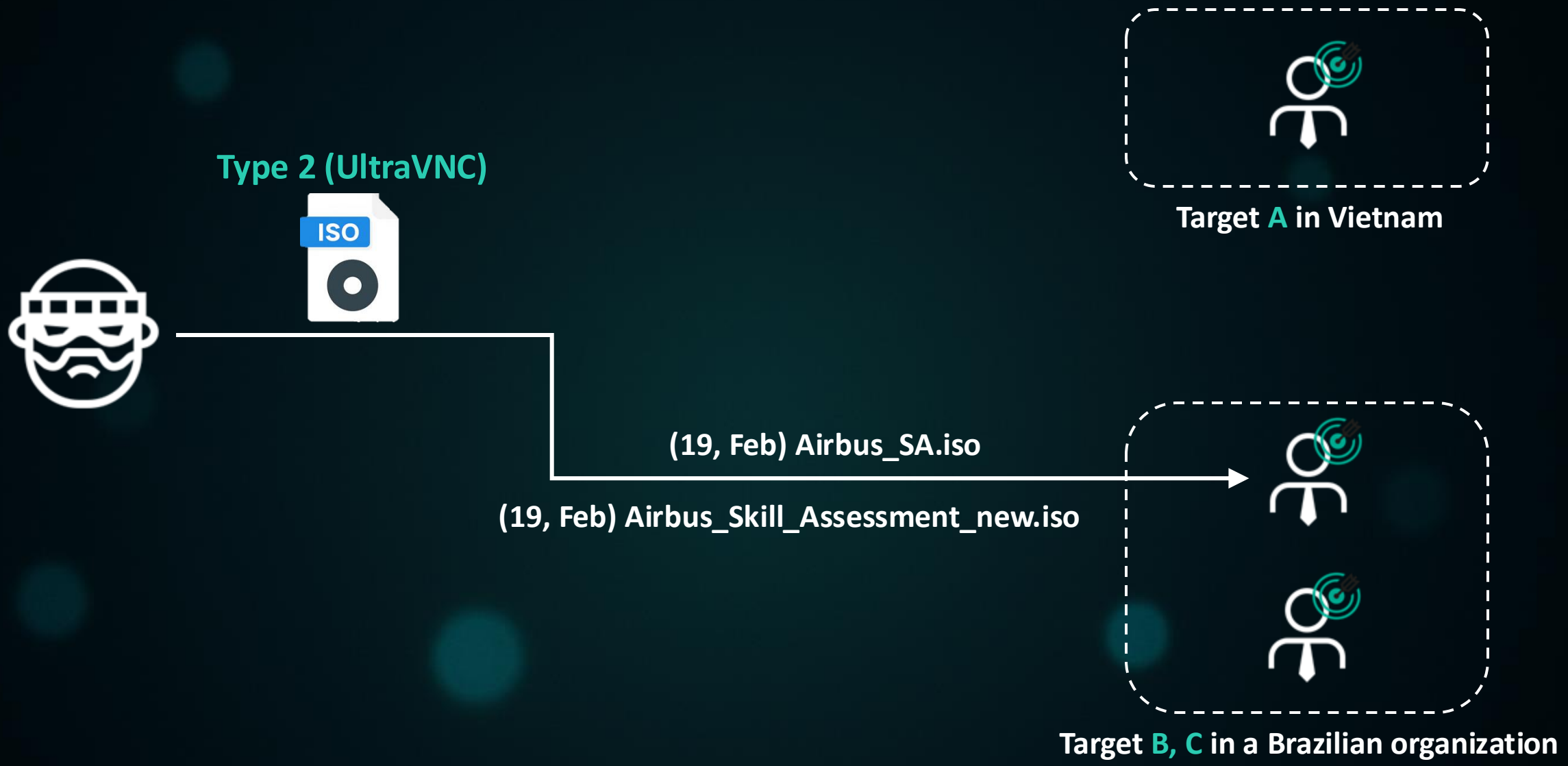


Lure the target to connect via a VNC application under the guise of a skill assessment

Initial access (Jan, 2024)

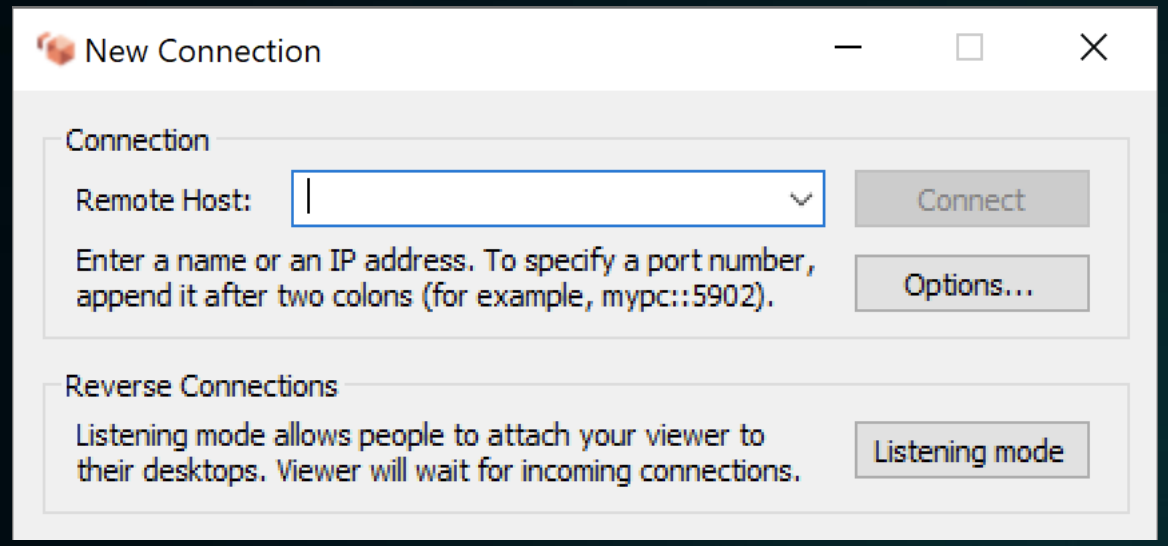


Initial access (Feb, 2024)

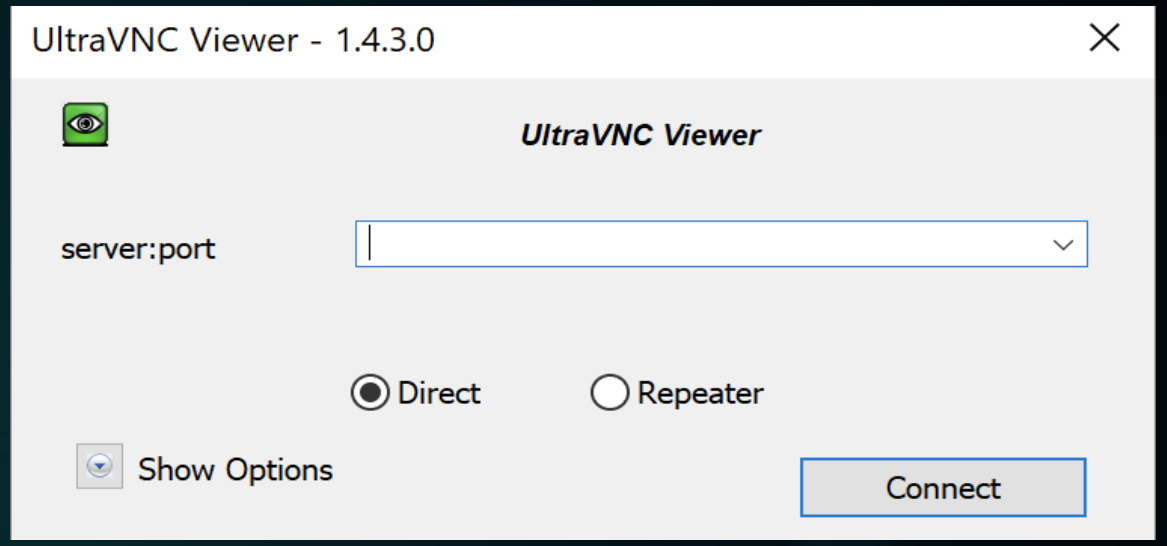


Initial access – VNC apps

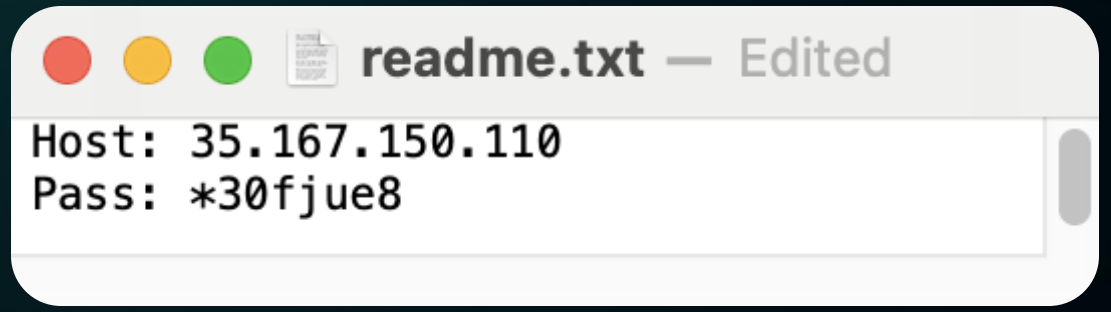
Type 1: EXE + TXT



Type 2: EXE + TXT + DLL

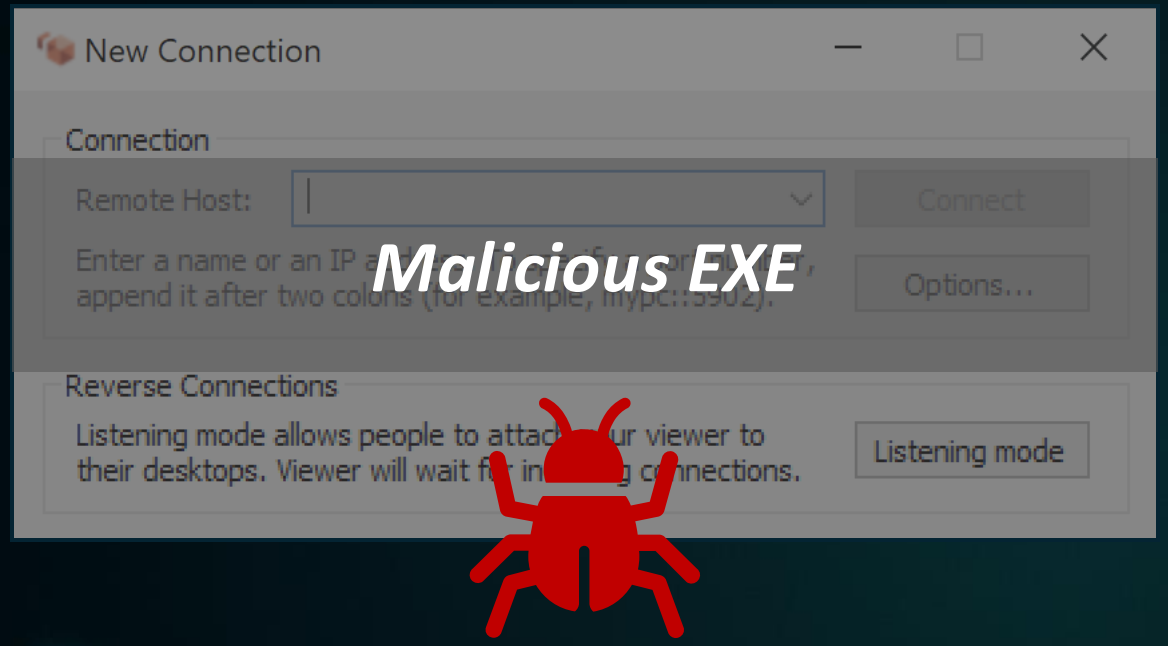


readme.txt

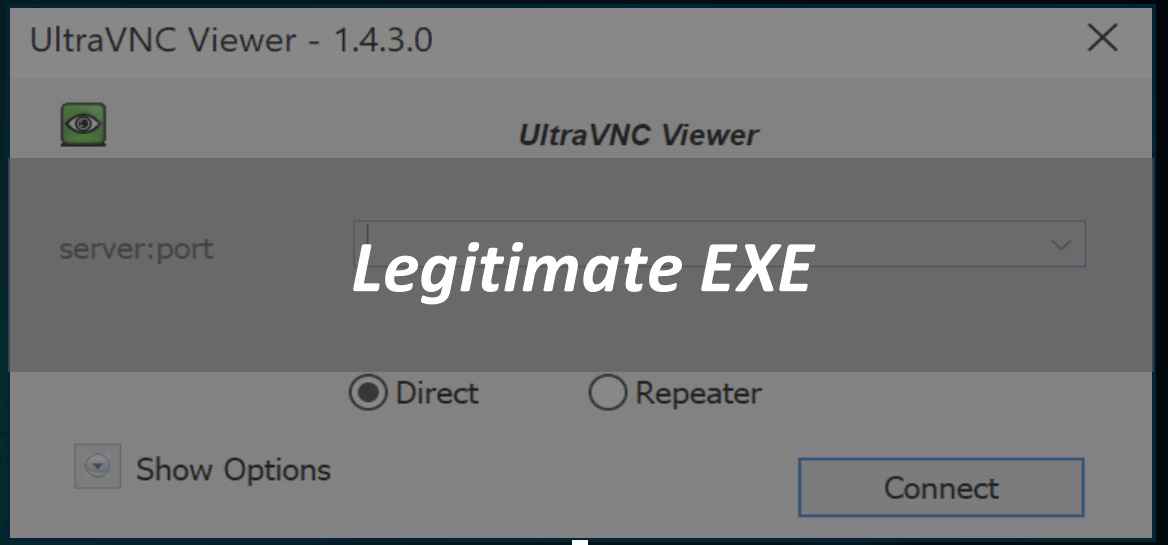


Initial access – VNC apps

Type 1: EXE + TXT



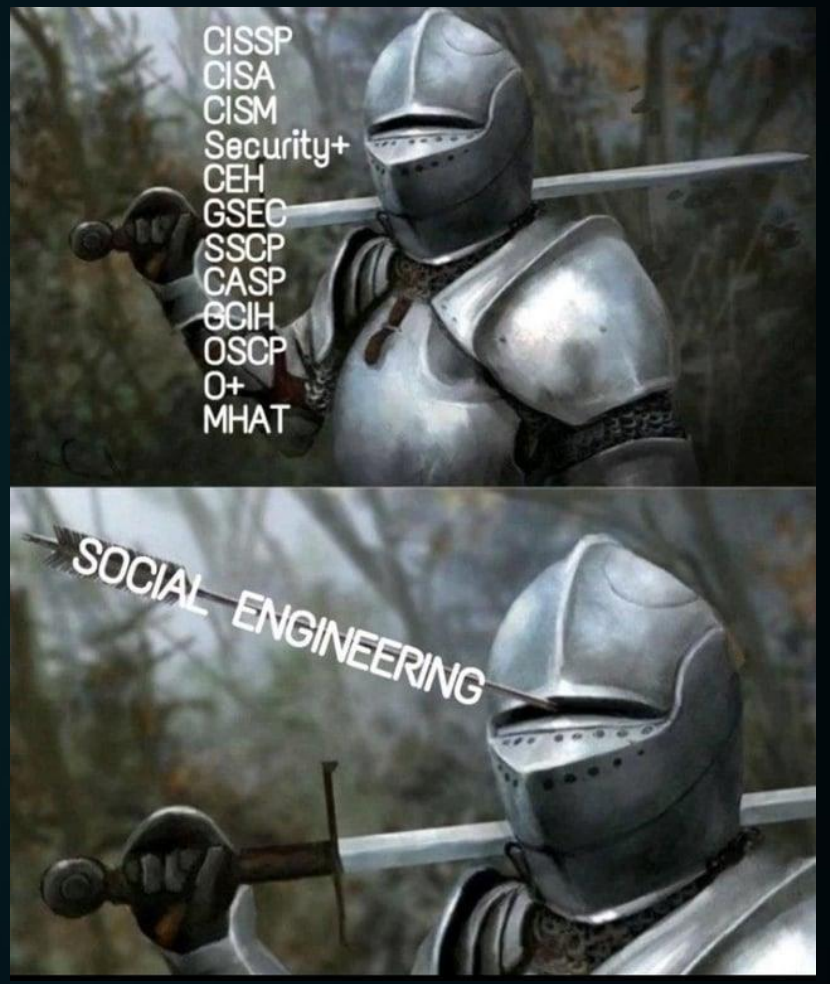
Type 2: EXE + TXT + DLL



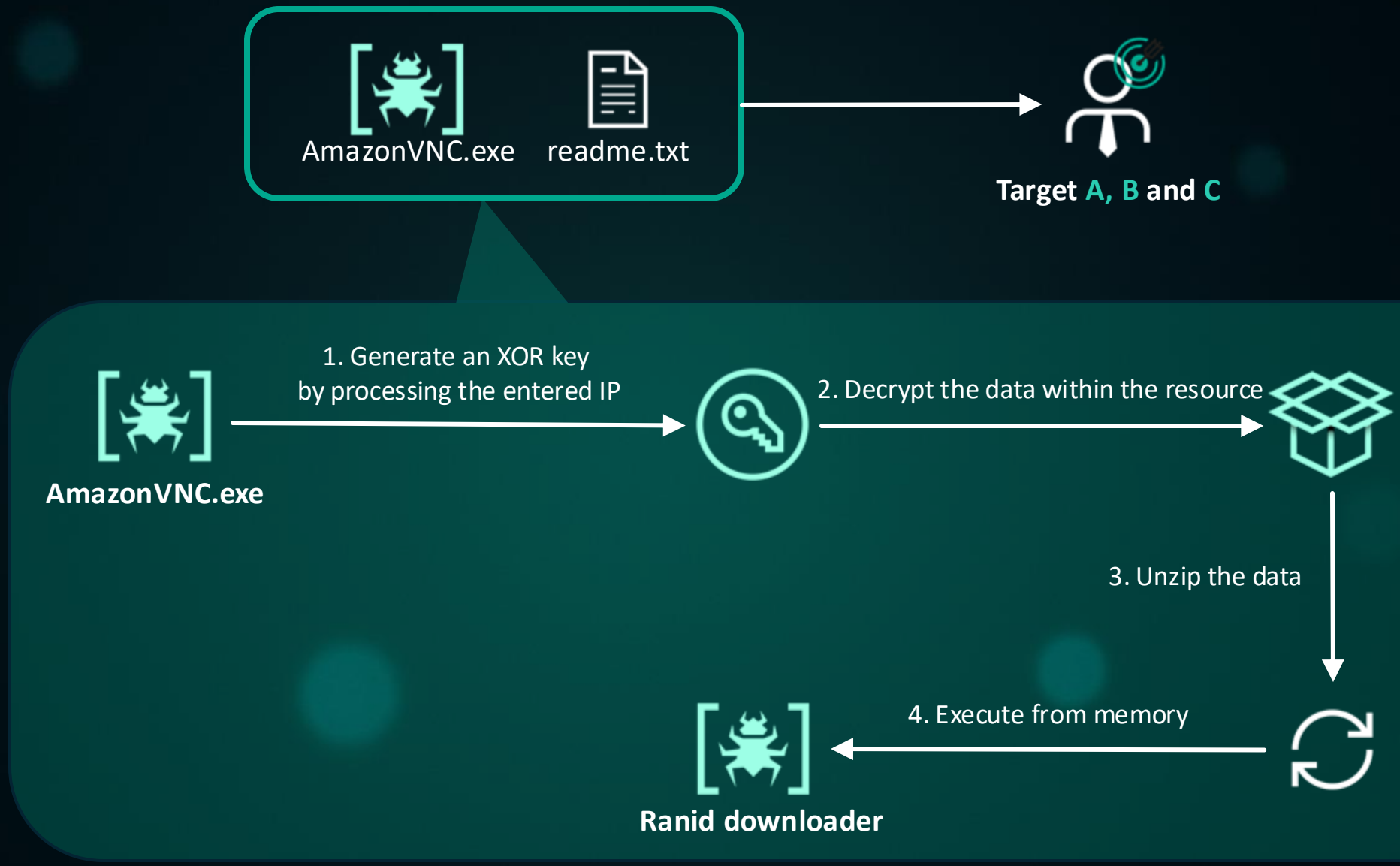
DLL Side-Loading

Malicious DLL
(vnclang.dll)

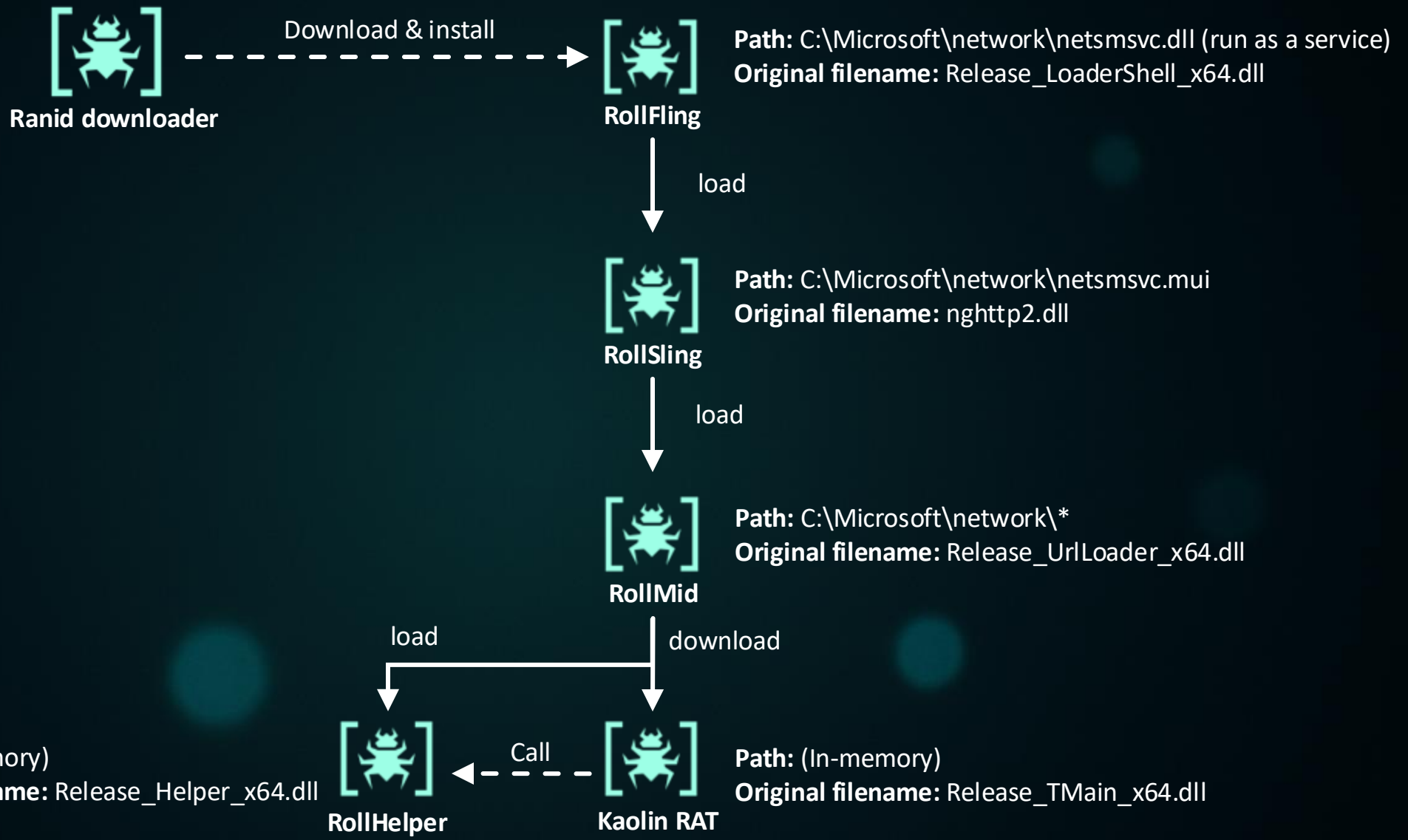
Execution


CISSP
CISA
CISM
Security+
CEH
GSEC
SSCP
CASP
GCIH
OSCP
O+
MHAT
SOCIAL ENGINEERING

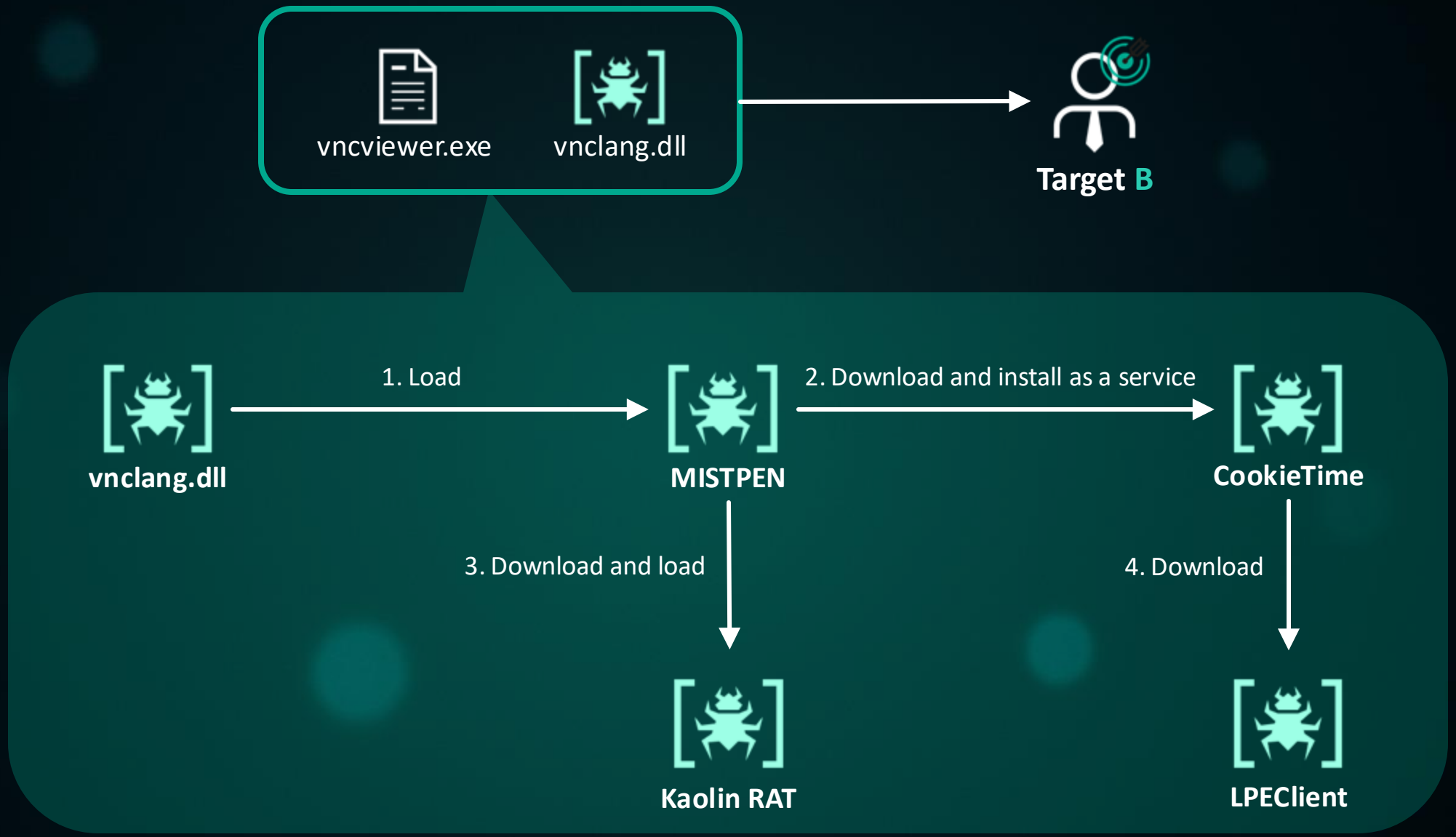
Execution (Type 1 in January)



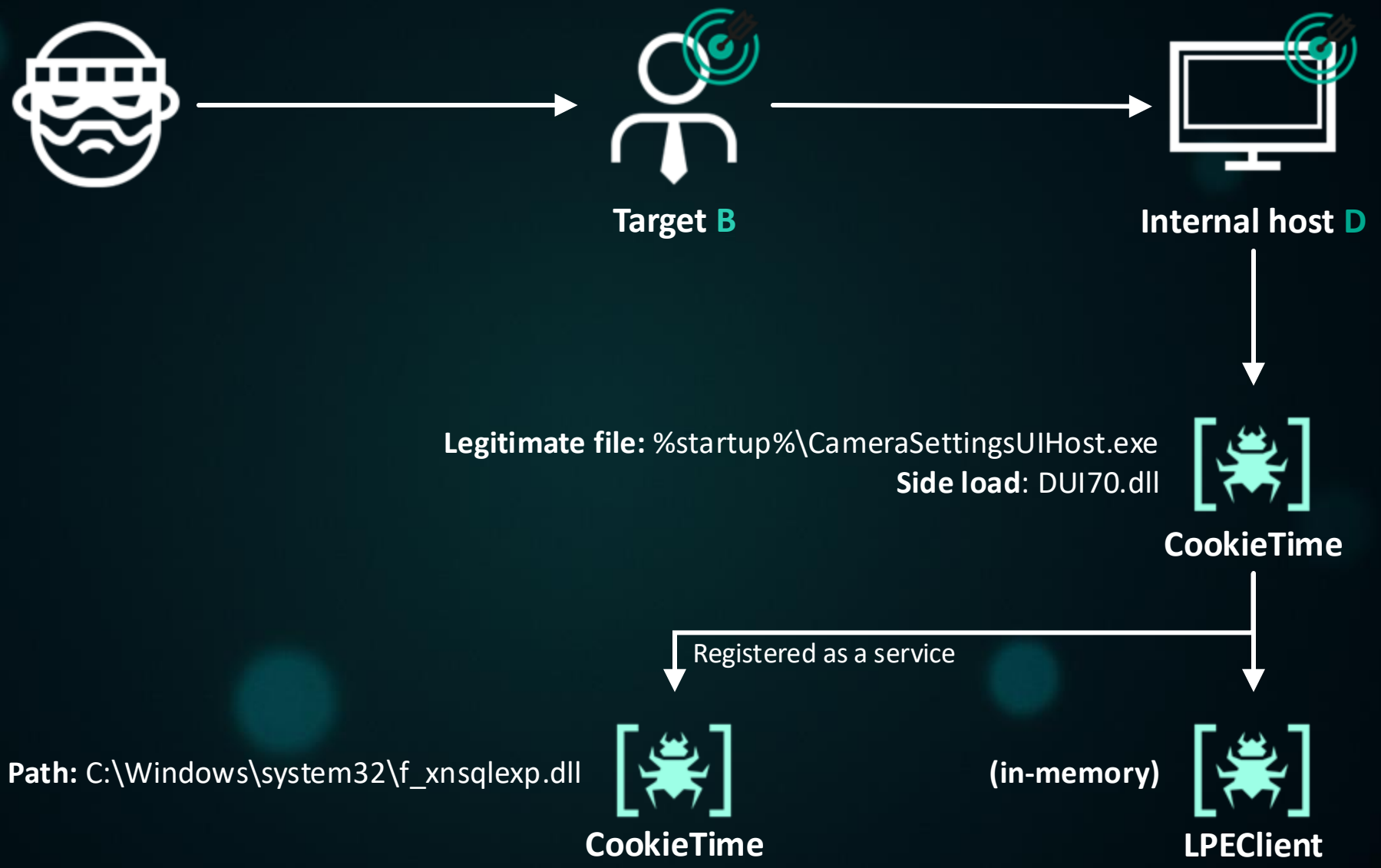
Execution (Type 1 in January)



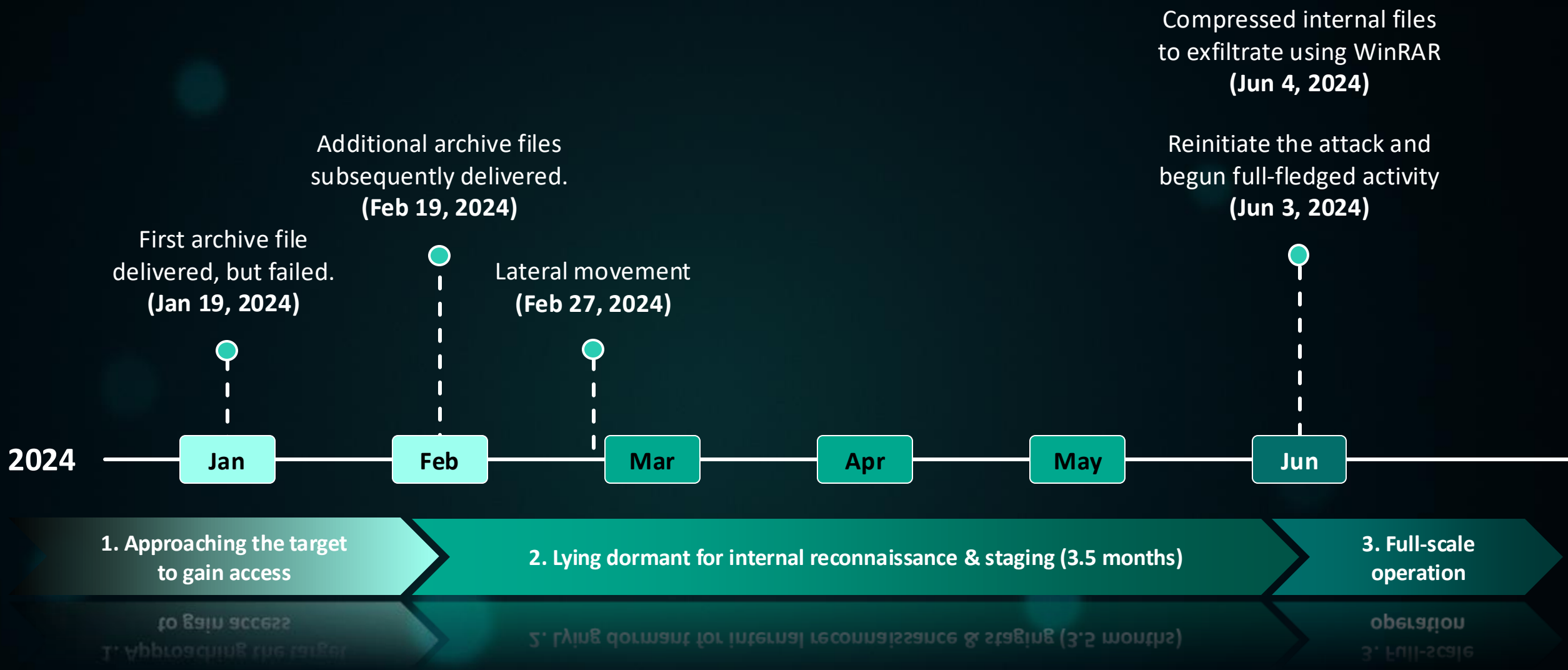
Execution (Type 2 in February)



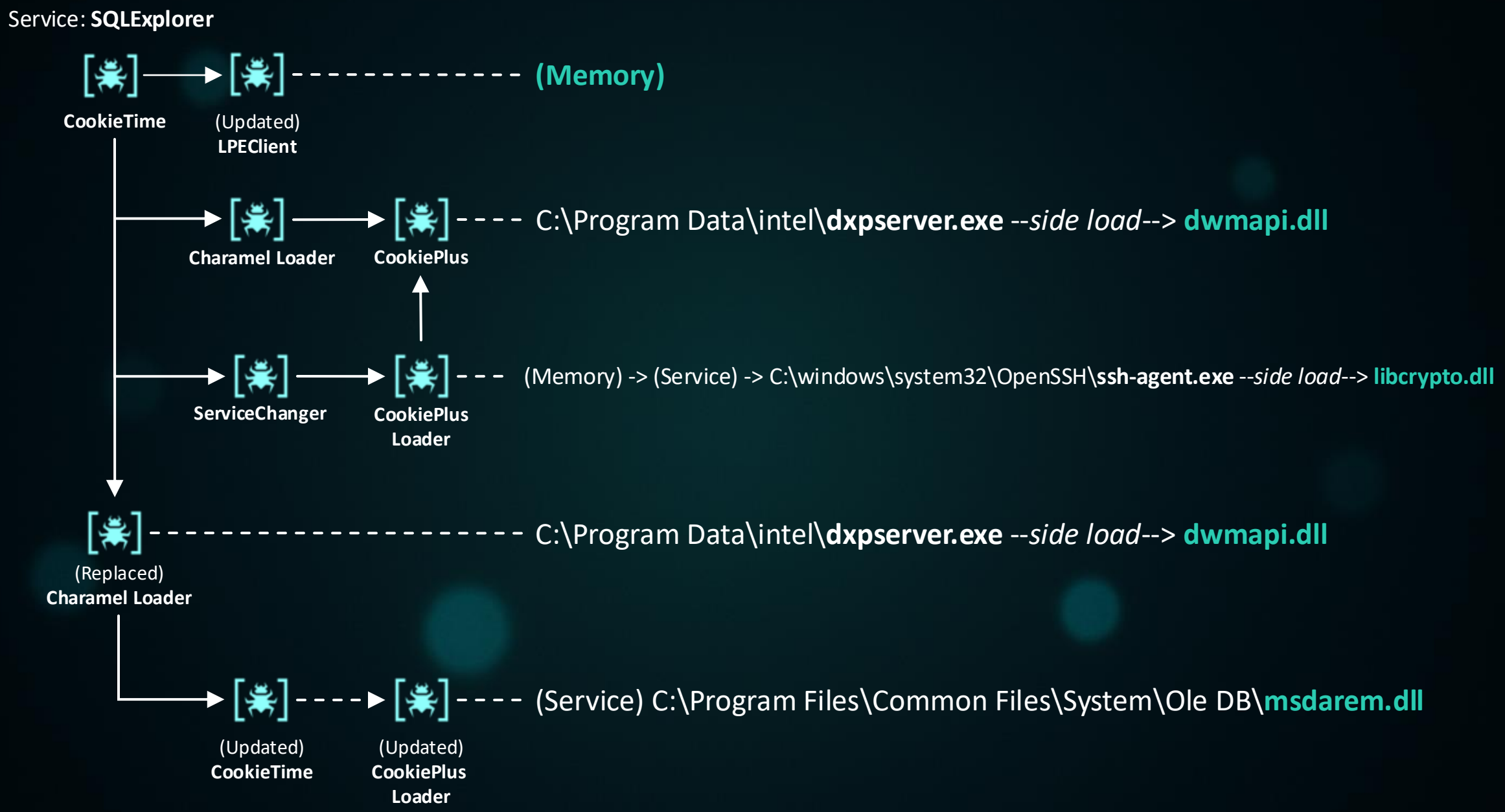
Lateral movement & Persistence



Timeline


First archive file delivered, but failed. (Jan 19, 2024)
Additional archive files subsequently delivered. (Feb 19, 2024)
Lateral movement (Feb 27, 2024)
Compressed internal files to exfiltrate using WinRAR (Jun 4, 2024)
Reinitiate the attack and begun full-fledged activity (Jun 3, 2024)
2024
Jan
Feb
Mar
Apr
May
Jun
1. Approaching the target to gain access
2. Lying dormant for internal reconnaissance & staging (3.5 months)
3. Full-scale operation

Overall infection structure on Host D



CookieTime

- a.k.a. LCPDot
- Since August, 2020 **(Old)**
- Using steganography to fetch additional command files

In this case,

- Commonly used for **persistence and re-entry**
- Primarily used to **download and execute additional payloads**
- Support multiple loading techniques – as a service/DLL side-loading
- C2 updated twice during the attack
  - Initial memory-staged, file update, in-memory patching

CookieTime

Num	Path	Legitimate file (Launcher)	Malicious DLL	Execution Type	Main function	Host installed
1	C:\ProgramData\Adobe	CameraSettingsUIHost.exe	DUI70.dll	DLL Side-Loading	InitThread	Target B, Host D
2	C:\Windows\System32	svchost.exe	f_xnsqlexp.dll	As a Service	ServiceMain	Target B, Host D
3	%startup%	CameraSettingsUIHost.exe	DUI70.dll	DLL Side-Loading	InitThread	Host D
4	C:\ProgramData\Intel	dxpserver.exe	dwmapi.dll	DLL Side-Loading	DllMain	Host D

LPEClient

- Since 2020 **(Old)**
- Collect extensive information from infected devices
- Widely used too by Lazarus, observed across multiple cases

In this case,

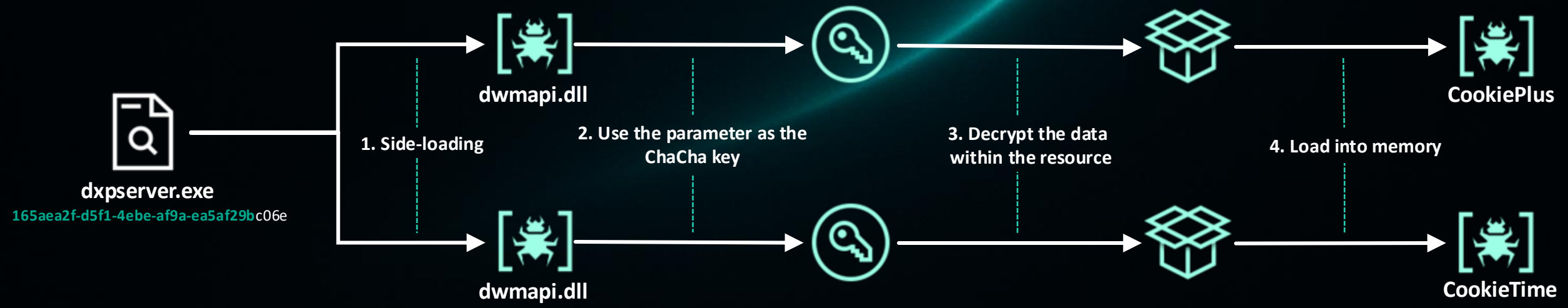
- Loaded by CookieTime
- **Updated variant** that has been observed since 2023 was used
- Same 1st C2 server used in both February and June
  - 2nd C2 server changed in June
- Primarily used for **profiling the infected device** rather than downloading

Charamel Loader

- Since 2024 **(New)**
- Accepts a ChaCha20 decryption key as a parameter
- In cases other than this one, it loads ForestTiger malware

In this case,

- Loaded by CookieTime
- Loads CookiePlus & CookieTime



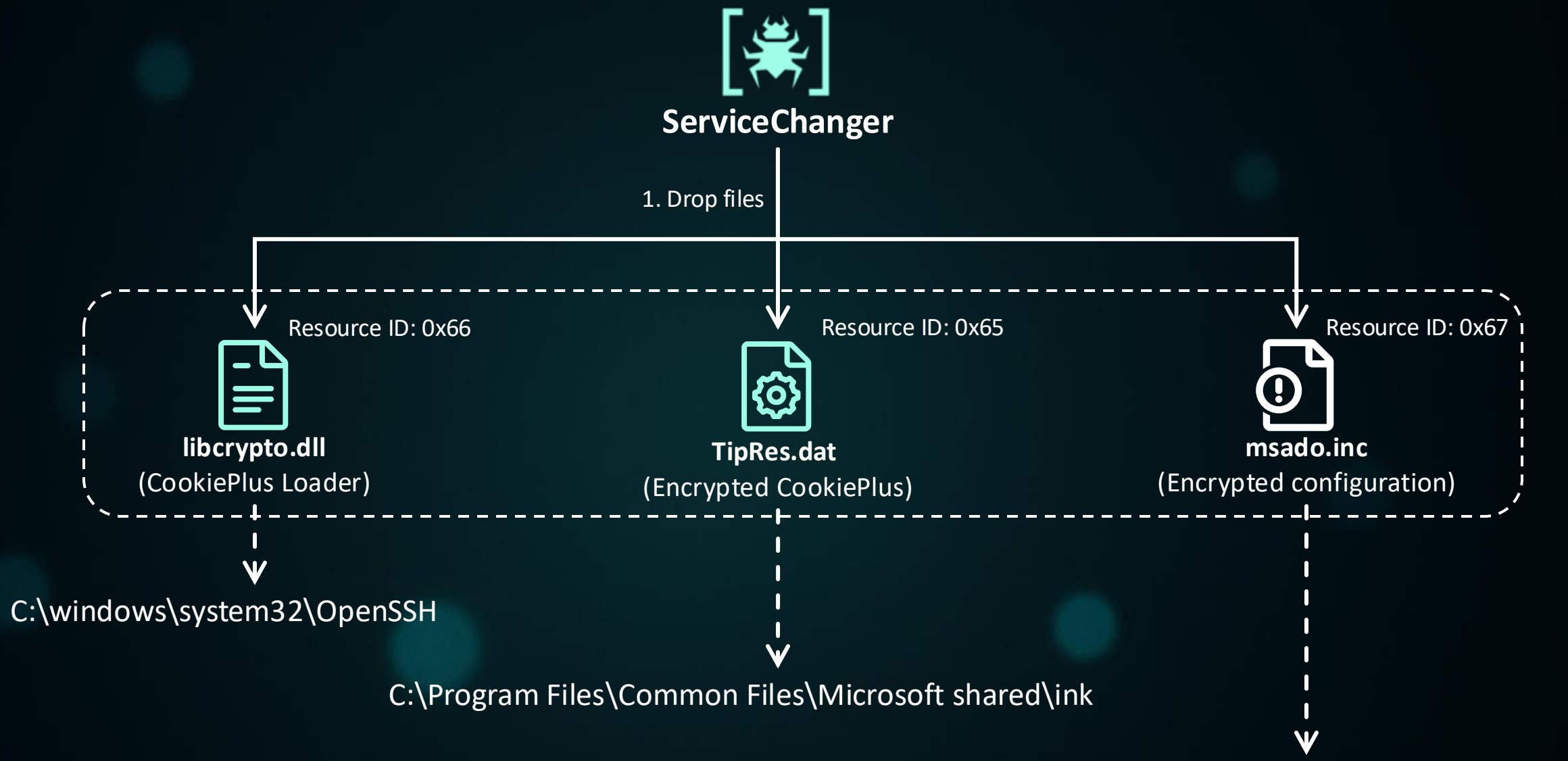
ServiceChanger

- Since 2024 **(New)**
- Executed in memory, and abuses legitimate service to trigger DLL side-loading
- The loader, payload, and configuration embedded within the resource

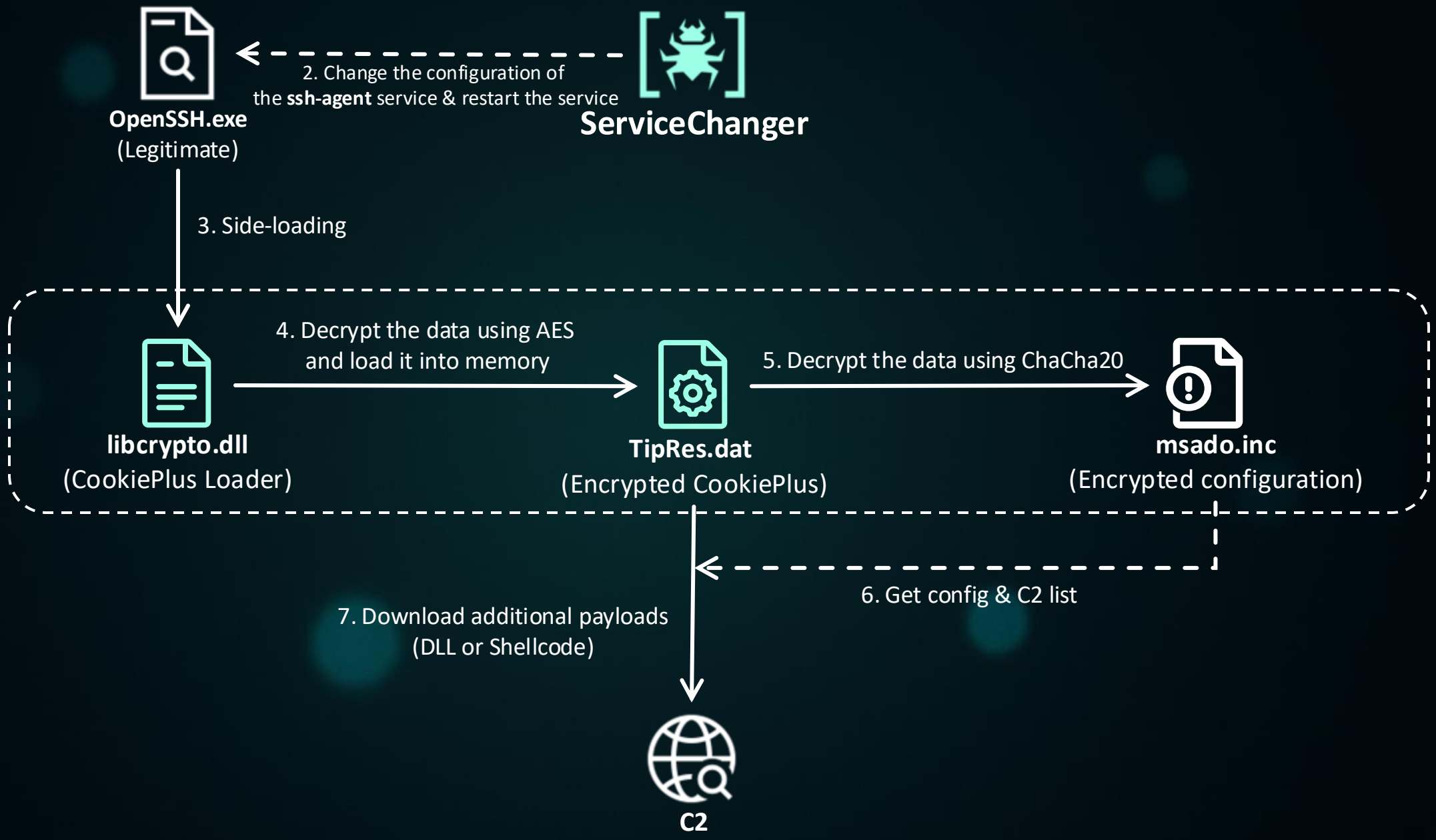
In this case,

- Loaded by CookieTime
- Abuses **ssh-agent** service by placing **libcrypto.dll** to trigger side-loading
- Leads to final loading of **CookiePlus**

ServiceChanger



ServiceChanger



CookiePlus

- Since 2024 **(New)**
- Lightweight malware designed to load a DLL and shellcode, rather than embedding all functionality
- Delivered as a set of components: Loader, Configuration, and Payload(s)

In this case,

- Two types observed: one using **external** configuration files, and another embedding the configuration **internally**
- **Three distinct plugins** are installed by the CookiePlus
- Masquerades as ComparePlus, the file comparison plugin for Notepad++

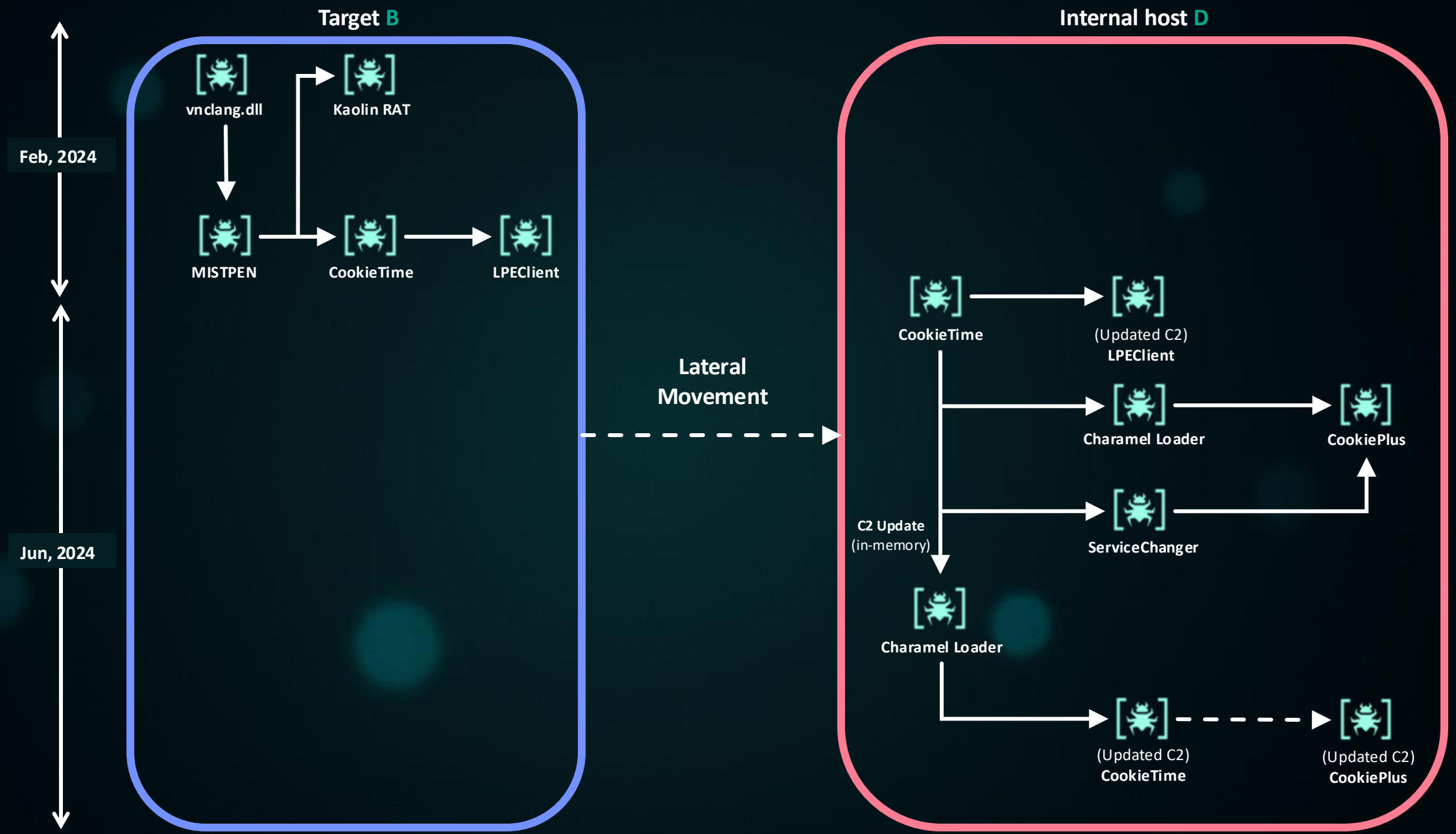
CookiePlus

Type	Loaded by	Encrypted Payload	Encrypted Configuration
1	Charamel Loader	Embedded in Charamel Loader’s resource	Inside of payload resources
2-1	ssh-agent service	C:\Program Files\Common Files\microsoft shared\ink**TipRes.dat**	C:\Program Files\Common Files\System **\ado\msado.inc**
2-2	netsvcs-registered service	C:\Program Files\Common Files\microsoft shared\ink**ThirdParty.dat**	C:\Program Files\Common Files\System **\msadc\msadc.inc**

CookiePlus plugin

Num	Description	Original filename	Parameters
1	Collects computer name, PID, current file path, current work path.	TBaseInfo.dll	None
2	Makes the main CookiePlus module sleep for the given number of minutes.	sleep.dll	Number
3	Writes the given number to set the execution time to the configuration file specified by the second parameter (e.g. msado.inc).	hiber.dll	Number, Config file path

Overall structure



Malware families derived from the Type 1

Ranid downloader

- First documented by Kaspersky (December, 2024)
- Since at least August, 2023 **(Relatively new)**

RollSling, RollFling, RollMid, Kaolin RAT

- RollSling – First documented by Microsoft (October, 2023)
- RollFling, RollMid, Kaolin RAT - First documented by Avast (April, 2024)
- Since at least January, 2023 **(Relatively new)**

MISTPEN

- First documented by Mandiant (September, 2024)
- Since at least February, 2024 **(New)**

Collection using WinRAR (ver. 5.80.2)

```
C:\ProgramData\Adobe\Adobe.db     // Path to the WinRAR
a                                 // Add to an archive
-hp1q2w3e4                        // Encrypt file and headers - pwd('1q2w3e4')
-m5                               // Set compression method  - best
-v2000000k                        // Split archive into around 2GB (2000000k)
C:\ProgramData\Adobe\Adobe060.CHK // Destination path
[Target path]                     // Source path to be archived
```

Collection using WinRAR (past cases)

From HvS-Consulting AG in 2020:

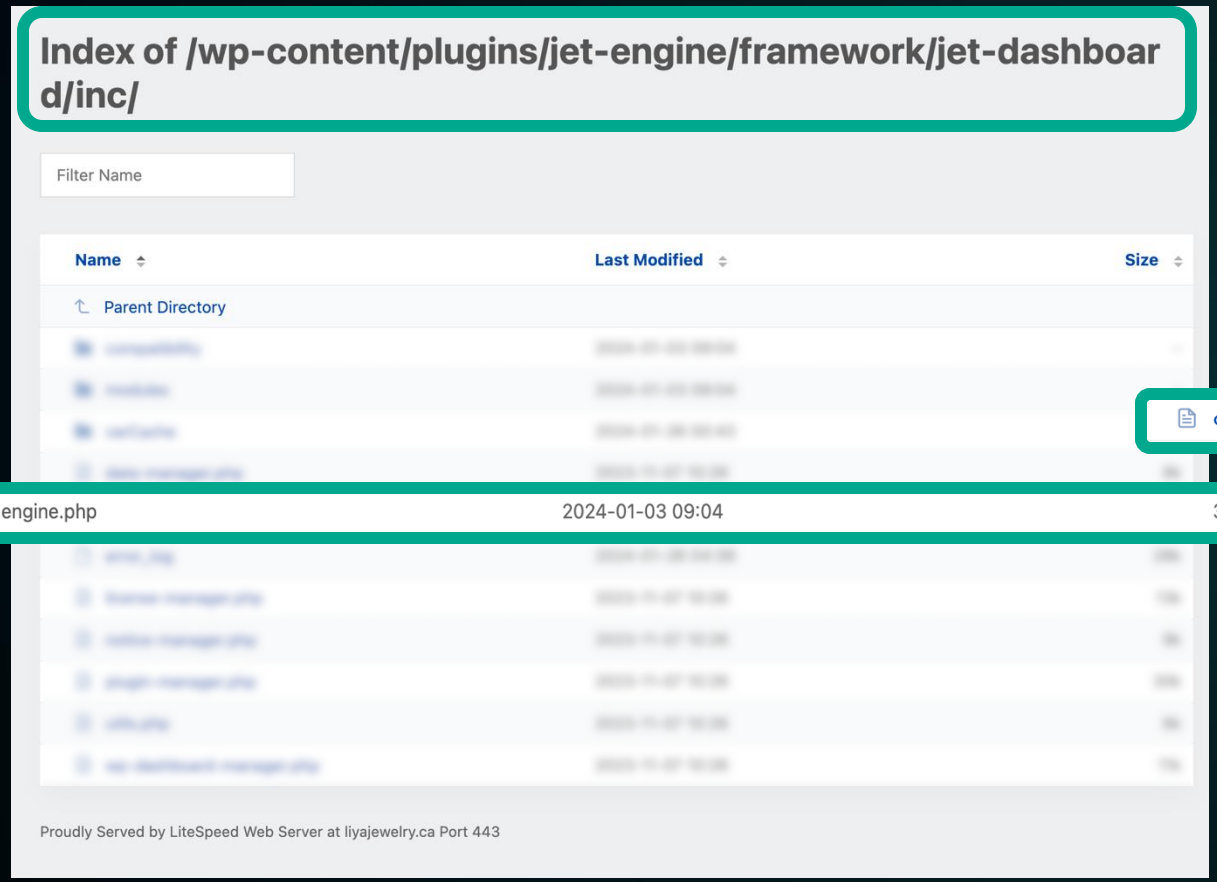
~DF123.TMP **a -hp1q2w3e4 -m5**
C:\ProgramData\IBM\restore002.dat [Target path]

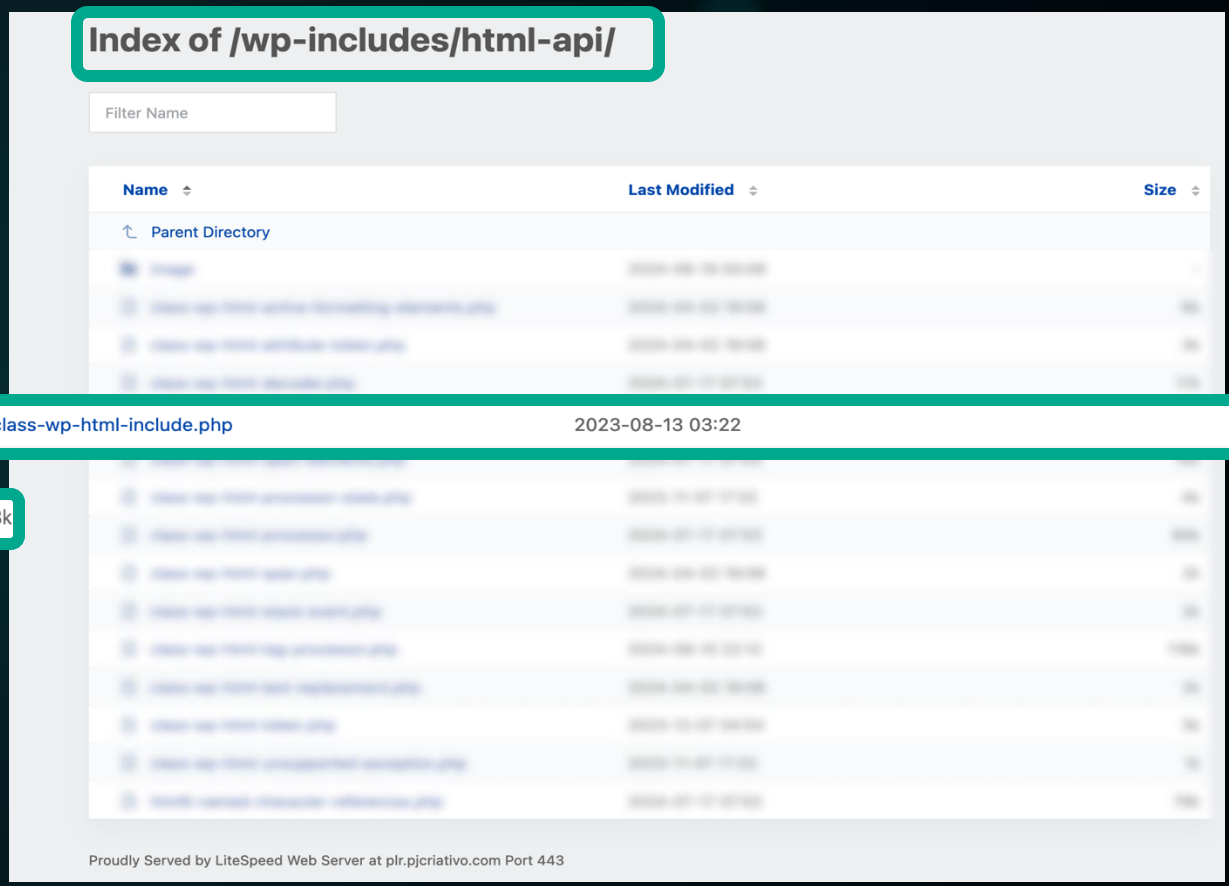
From our research in 2022:

adobearm.exe **a -hp1q2w3e4 -m5 -v2000000k**
“%LocalAppData%\Adobe\SYSVOL800.CHK [Target path]

Infrastructure

- C2 server mostly operated on **Wordpress**
  - Ranid downloader, MISTPEN, Kaolin RAT, CookieTime, CookiePlus





Infrastructure

- LPEClient is directly managed malware, suspecting 2nd C2 server is exclusively registered by the Lazarus group

Num	Domain	Created on	Expires on	IP Address	Organization	ASN	Registrar
1	www.resquery.com	2023-09-11	2024-09-11	146.70.88[.]45 (FR)	M247 Europe SRL	9009	Namecheap
2	www.gbresellers.com	2023-02-07	2025-02-07	46.17.103[.]97 (NL)	HOSTKEY B.V.	57043	Namecheap

Who’s background?

Same initial vector &
Overlapped malware set

Overlapped infrastructure

Overlapped infrastructure

Same initial vector &
Overlapped malware set

Wrap up – Malware

- **Full-fledged RAT**
  - Kaolin RAT
- **Modular RAT**
  - CookiePlus
- **Downloader**
  - Ranid downloader, RollMid
  - CookieTime, LPEClient, MISTPEN
- **Loader**
  - RollFling, RollSling
  - Charamel Loader, ServiceChanger

Wrap up – DLL Side-Loading

dxpserver.exe	dwmapi.dll
ssh-agent.exe	libcrypto.dll
CameraSettingsUIHost.exe	DUI70.dll

Wrap up – Paths

- C:\Users\[username]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

- C:\ProgramData\Adobe
- C:\ProgramData\Intel

- C:\Windows\System32\OpenSSH
- C:\Windows\System32

- C:\Program Files\Common Files\microsoft shared\ink
- C:\Program Files\Common Files\System\ado
- C:\Program Files\Common Files\System\msadc
- C:\Program Files\Common Files\System\Ole DB

Conclusion

- **Operation Dream Job is still active**
  - Old lure is still working today
- **Deploying their new malware**
  - CookiePlus, the most latest, is lightweight and modular
- **Along with their modernized legacy malware**
  - Still remain a key player
- **Operated by Lazarus APT (Advanced Persistent Threat)**
  - They don’t give up to achieve their goals

Thank you!

More info:
hypen1117@gmail.com

x: @hypen1117

GREAT

kaspersky