IIJ-SECT
IIJ Group Security Coordination Team

vb 2025
BERLIN
24-26 Sept 2025

Inside Pandora's Box

Dissecting the latest arsenal and tactics of APT27

Internet Initiative Japan Inc.
Naoki Takayama

About this talk

- This talk overviews the toolkit and malware used in an attack campaign done by APT27 observed in July 2025.
- In this attack campaign, threat actors leveraged several new techniques and tools, such as …
    - Use of a legitimate VPN server to achieve a persistent access.
    - Newly observed Cobalt Strike Beacon Downloaders.
    - An improved version of a rootkit observed in past attacking campaigns.
- I am going to describe the internals of these threats, alongside a detection methodology useful for defenders in each organization.

whoami

- Naoki Takayama
- Security researcher working at Internet Initiative Japan Inc. (AS2497)
  - Member of IIJ-SECT (private CSIRT of IIJ group).
  - https://sect.iij.ad.jp/en/
- Responsible for threat research and incident response.
  - Mainly researching tactics and malware used in targeted attacks.
- Spoken at BSides Tokyo 2023 in the past.
- X: @mopisec

Agenda

- Introduction
- Post-Exploitation Tools
  - EfsPotato
  - FRPS
  - frpModify
  - SoftEther VPN Server
- Malware
  - CS Beacon Downloaders
  - Rootkit + RAT
- Countermeasures
  - Detect BYOVD attack using event log
  - Microsoft Vulnerable Driver Blocklist
- Wrap-up
  - Conclusion
- Appendix
  - Malware Config & IoCs

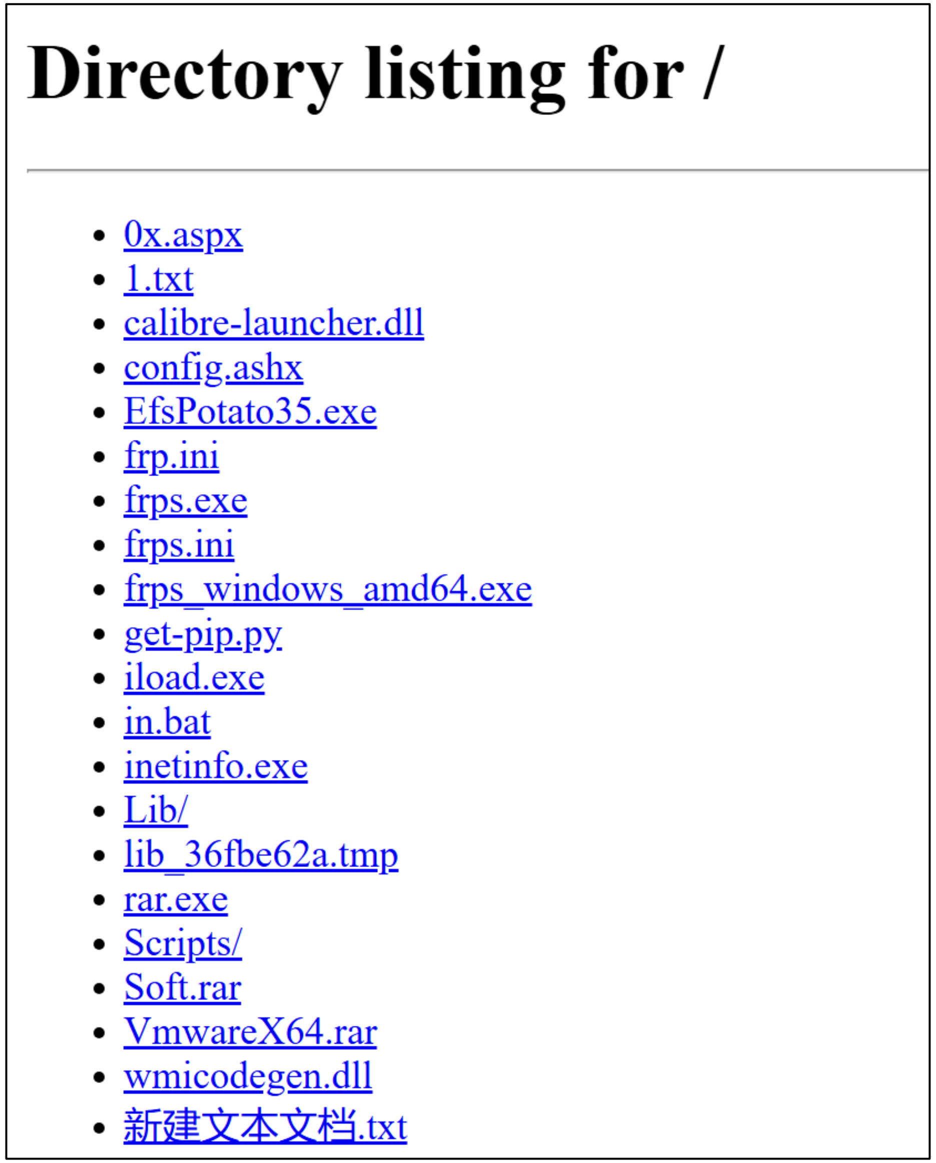
APT27 (LuckyMouse, Iron Tiger, ...)

Background	China-nexus APT group [1]
Activity	Since at least 2010 [2]
Recently Targeted Industries and Regions	- Gambling Company in Philippine (2019 - 2021) [3] - Entities in Europe (2024) [4]
Malware	Cobalt Strike Beacon, Hyperbro, NDISProxy, Pandora, PlugX, RShell, SysUpdate, and more ...

[1]: https://www.justice.gov/usao-dc/pr/chinese-nationals-ties-prc-government-and-apt27-charged-computer-hacking-campaign-profit
[2]: https://www.sekoia.io/en/glossary/apt27-luckymouse-emissarypanda/
[3]: https://www.trendmicro.com/en_us/research/21/d/iron-tiger-apt-updates-toolkit-with-evolved-sysupdate-malware-va.html
[4]: https://x.com/bfv_bund/status/1811364839656185985

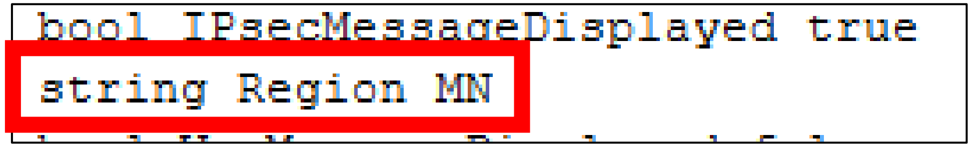
The Observed Campaign

- Victim: Mongolian (MN) Entity
- Compromised at least since June 2025
- A malicious server operated by threat actors exposed an open directory with:
  - Post-Exploitation Tools
  - Malware attributed to APT27
  - Exfiltrated files from victim hosts
- We analyzed those files and revealed the updates to their arsenal and tactics.



Directory listing for /

- 0x.aspx
- 1.txt
- calibre-launcher.dll
- config.ashx
- EfsPotato35.exe
- frp.ini
- frps.exe
- frps.ini
- frps_windows_amd64.exe
- get-pip.py
- iload.exe
- in.bat
- inetinfo.exe
- Lib/
- lib_36fbe62a.tmp
- rar.exe
- Scripts/
- Soft.rar
- VmwareX64.rar
- wmicodegen.dll
- 新建文本文档.txt



```
bool IPsecMessageDisplayed true
string Region MN
```

Arsenal

Post-Exploitation Tools

Privilege Escalation

- EfsPotato New

Port Forwarding

- FRPS
- frpModify New

Network Persistence

- SoftEther VPN Server New

Malware

Cobalt Strike Beacon Downloader

- Type A New
- Type B New

Rootkit + RAT

- Pandora Updated
- NDISProxy

Miscellaneous

Godzilla WebShell, ASP File Uploader

Arsenal

Post-Exploitation Tools

Privilege Escalation

- EfsPotato New

Port Forwarding

- FRPS
- frpModify New

Network Persistence

- SoftEther VPN Server New

Malware

Cobalt Strike Beacon Downloader

- Type A New
- Type B New

Rootkit + RAT

- Pandora Updated
- NDISProxy

Miscellaneous

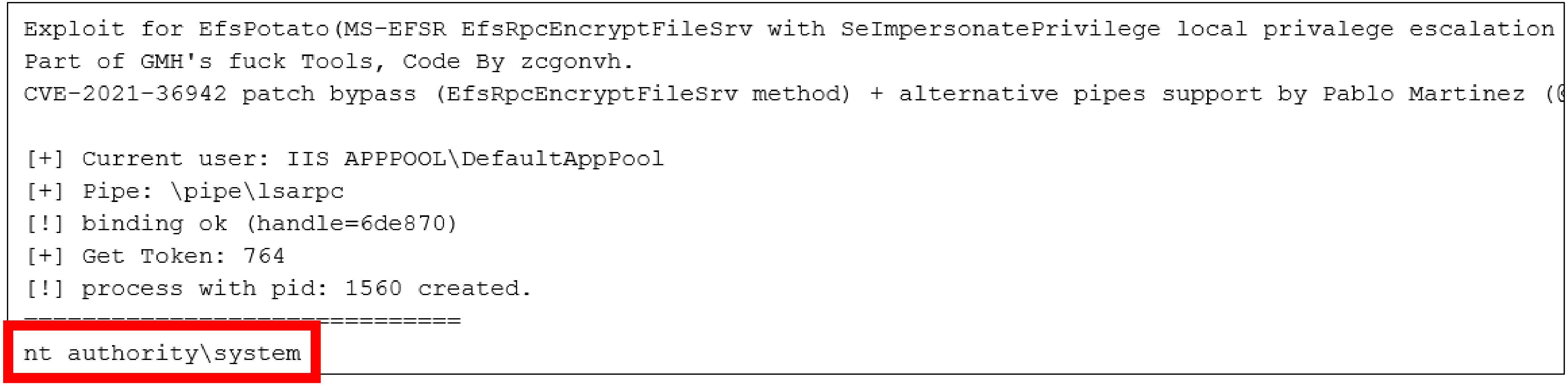
Godzilla WebShell, ASP File Uploader

New

Post-Exploitation Tools

EfsPotato

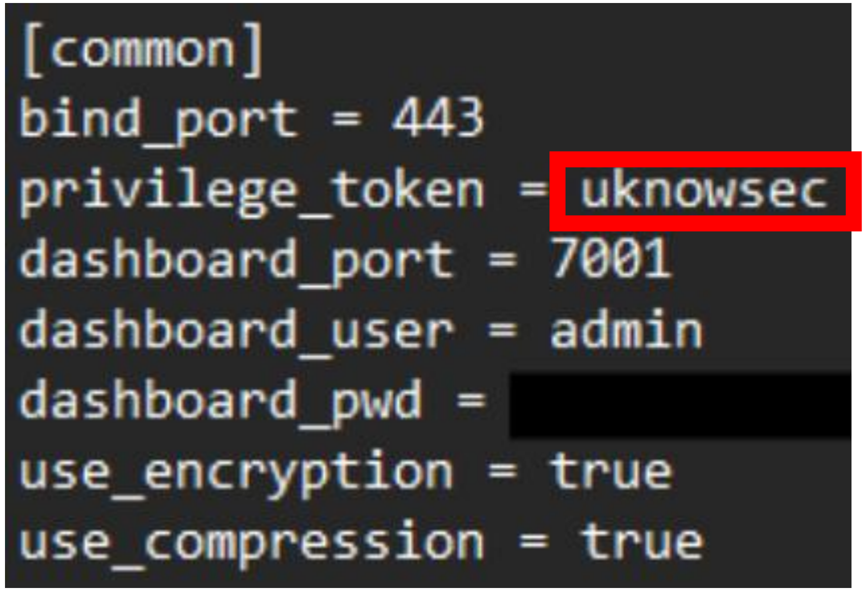
- Privilege escalation tool that abuses MS-EFSR (EfsRpcOpenFileRaw) to elevate service account with SeImpersonatePrivilege to SYSTEM.
- Supports until Windows 10/11/Server 2022 21H2.
- https://github.com/zcgonvh/EfsPotato



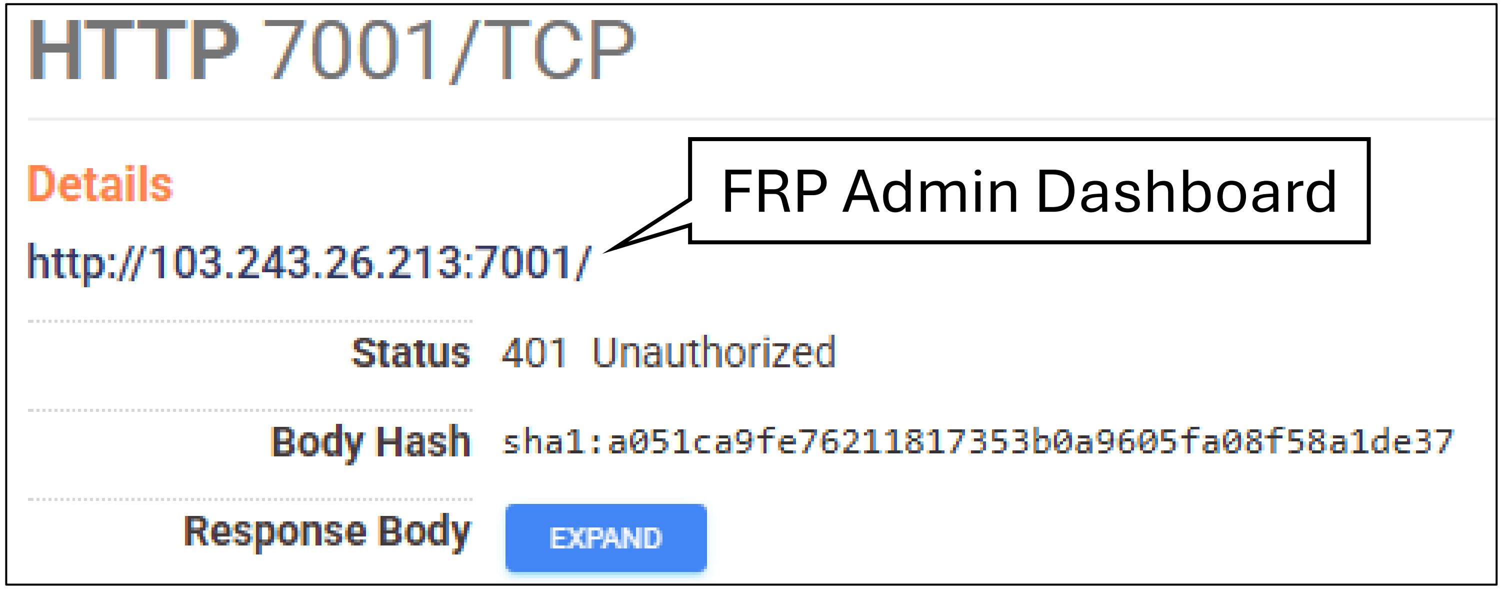
```
Exploit for EfsPotato(MS-EFSR EfsRpcEncryptFileSrv with SeImpersonatePrivilege local privalege escalation
Part of GMH's fuck Tools, Code By zcgonvh.
CVE-2021-36942 patch bypass (EfsRpcEncryptFileSrv method) + alternative pipes support by Pablo Martinez (@

[+] Current user: IIS APPPOOL\DefaultAppPool
[+] Pipe: \pipe\lsarpc
[!] binding ok (handle=6de870)
[+] Get Token: 764
[!] process with pid: 1560 created.
==============================
nt authority\system
```

FRPS

- Server-side program of FRP (Fast Reverse Proxy).
  - FRP is a legitimate open-source tool that can expose a local host behind a NAT or firewall to the internet.
- https://github.com/fatedier/frp



```
[common]
bind_port = 443
privilege_token = uknowsec
dashboard_port = 7001
dashboard_user = admin
dashboard_pwd = [redacted]
use_encryption = true
use_compression = true
```



HTTP 7001/TCP

Details

http://103.243.26.213:7001/

FRP Admin Dashboard

Status	401 Unauthorized
Body Hash	sha1:a051ca9fe76211817353b0a9605fa08f58a1de37
Response Body	EXPAND

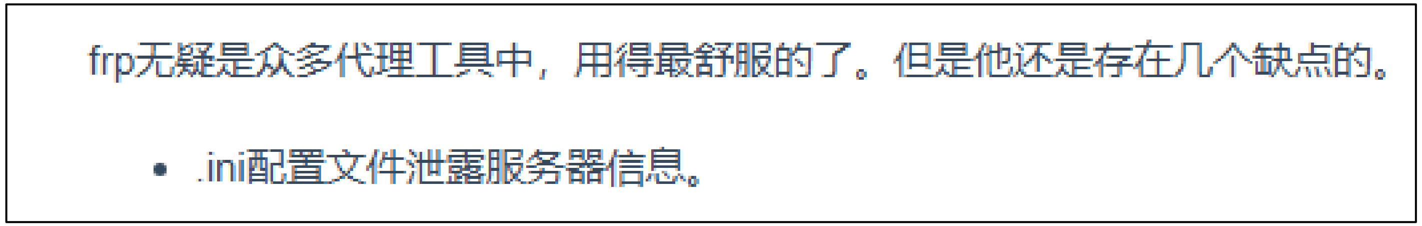
https://search.censys.io/hosts/103.243.26.213

Specifying Parameters

frpModify (Codename: frp指定参数)

- The modified version of FRP that does not require a configuration file.
  - frpModify receives parameters from command-line instead.
  - Digital forensic investigation might become harder, since the configuration parameters are not left on the file system.
- https://github.com/**uknowsec**/frpModify

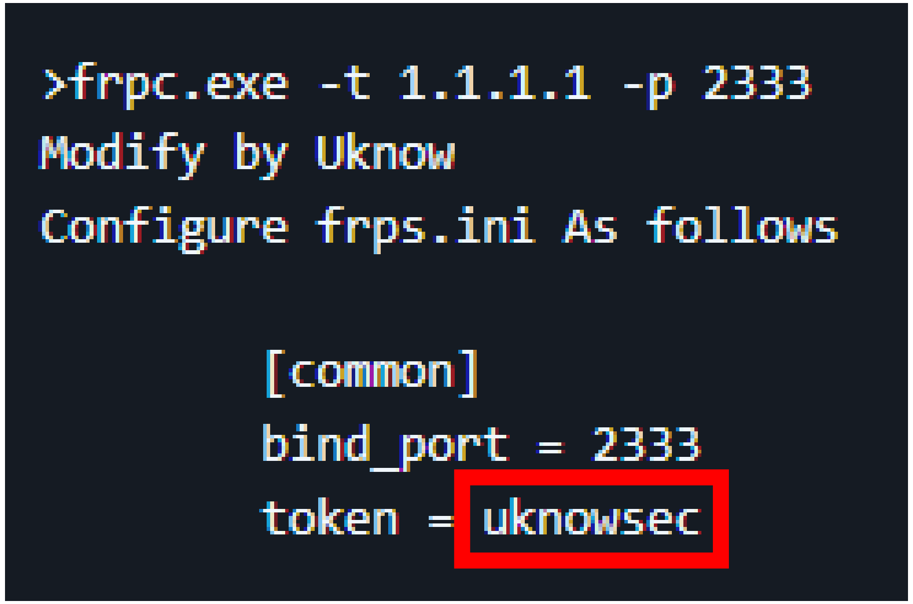
Author's Blog Post: https://uknowsec.cn/posts/notes/FRP改造计划.html



frp无疑是众多代理工具中，用得最舒服的了。但是他还是存在几个缺点的。

- .ini配置文件泄露服务器信息。

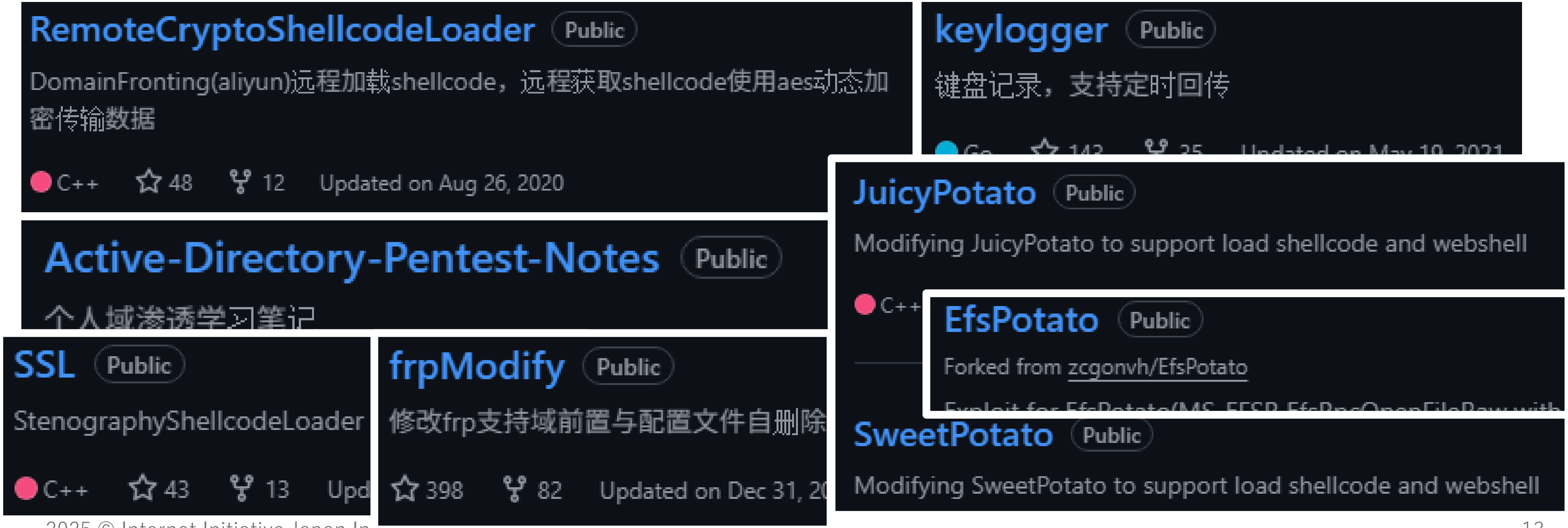
FRP is the most user-friendly proxy tool.
However, it still has several drawbacks.
- The .ini configuration file leaks server information.



```
>frpc.exe -t 1.1.1.1 -p 2333
Modify by Uknow
Configure frps.ini As follows

        [common]
        bind_port = 2333
        token = uknowsec
```

Other repositories from "uknowsec"

- Many infamous attacking tools (and even malware) were present there.
- https://github.com/uknowsec?tab=repositories



RemoteCryptoShellcodeLoader Public

DomainFronting(aliyun)远程加载shellcode，远程获取shellcode使用aes动态加密传输数据

● C++ ☆ 48 12 Updated on Aug 26, 2020

keylogger Public

键盘记录，支持定时回传

● Go ☆ 142 25 Updated on May 10, 2021

Active-Directory-Pentest-Notes Public

个人域渗透学习笔记

SSL Public

StenographyShellcodeLoader

● C++ ☆ 43 13 Upd

frpModify Public

修改frp支持域前置与配置文件自删除

☆ 398 82 Updated on Dec 31, 20

JuicyPotato Public

Modifying JuicyPotato to support load shellcode and webshell

● C++

EfsPotato Public

Forked from zcgonvh/EfsPotato

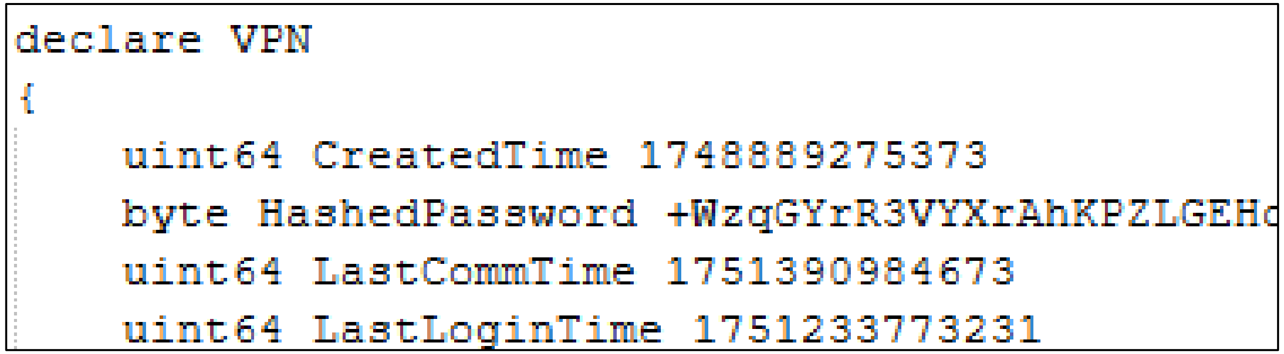
Exploit for EfsPotato(MS-EFSR EfsRpcOpenFileRaw with

SweetPotato Public

Modifying SweetPotato to support load shellcode and webshell

SoftEther VPN Server

- Legitimate VPN server software was abused for network persistence.
  - It listens on 50443/tcp of host "dc1" (= Domain Controller ?).
- As a spontaneous behavior, statistics data was found in configuration file (vpn_server.config).
  - Timestamps are recorded in UNIX time format.

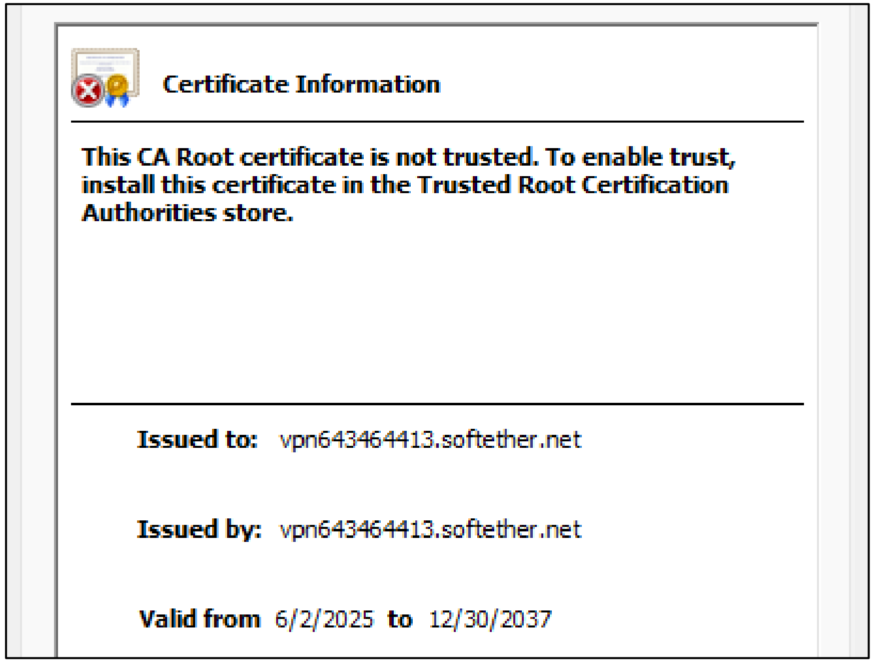


```
declare VPN
{
    uint64 CreatedTime 1748889275373
    byte HashedPassword +WzqGYrR3VYXrAhKPZLGEHc
    uint64 LastCommTime 1751390984673
    uint64 LastLoginTime 1751233773231
```

Created Time (UTC):
2025-06-02 (Mon) 18:34:35.373
Last Communication Time (UTC):
2025-07-01 (Tue) 17:29:44.673
Last Login Time (UTC):
2025-06-29 (Sun) 21:49:33.231

SoftEther VPN Server – Certificate

- OU = **vpn643464413.softether.net**
  O = **vpn643464413.softether.net**
  CN = **vpn643464413.softether.net**
- Unfortunately, the name resolution was not available at the point of investigation.
- There were no records on several reverse DNS lookup services as well.



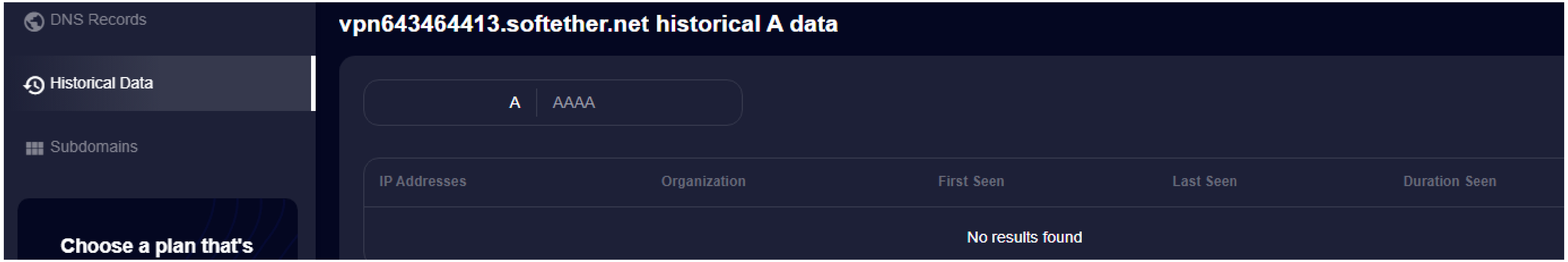
Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: vpn643464413.softether.net

Issued by: vpn643464413.softether.net

Valid from 6/2/2025 **to** 12/30/2037



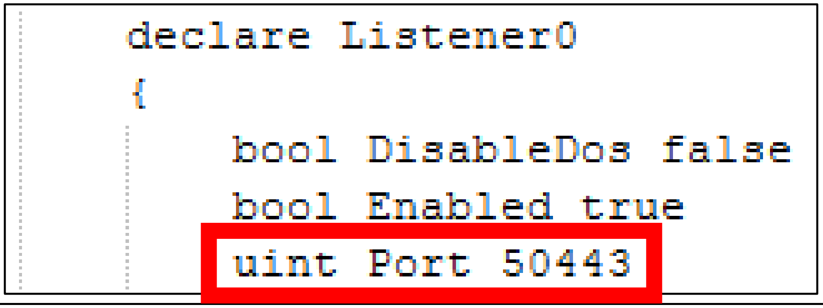
vpn643464413.softether.net historical A data

IP Addresses	Organization	First Seen	Last Seen	Duration Seen
No results found				

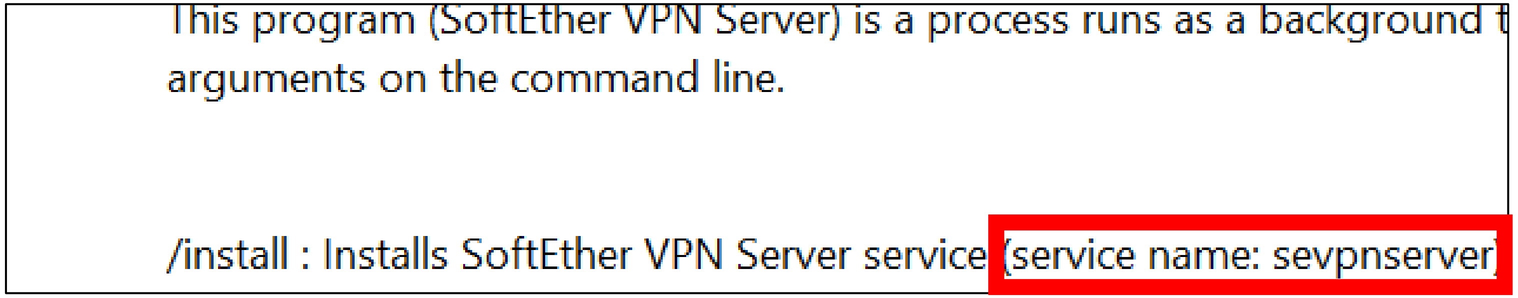
https://securitytrails.com/domain/vpn643464413.softether.net/history/a

SoftEther VPN Server – Indicators

- Indicators to detect running SoftEther VPN Server instance:

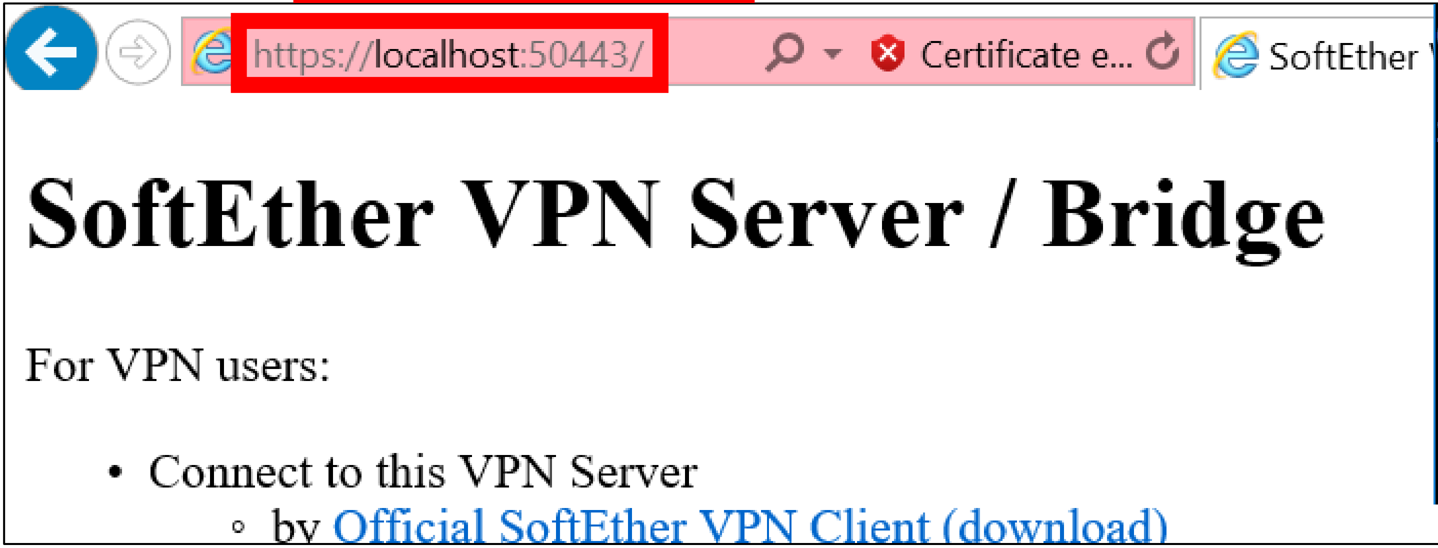


```
declare Listener0
{
    bool DisableDos false
    bool Enabled true
    uint Port 50443
```



This program (SoftEther VPN Server) is a process runs as a background t
arguments on the command line.

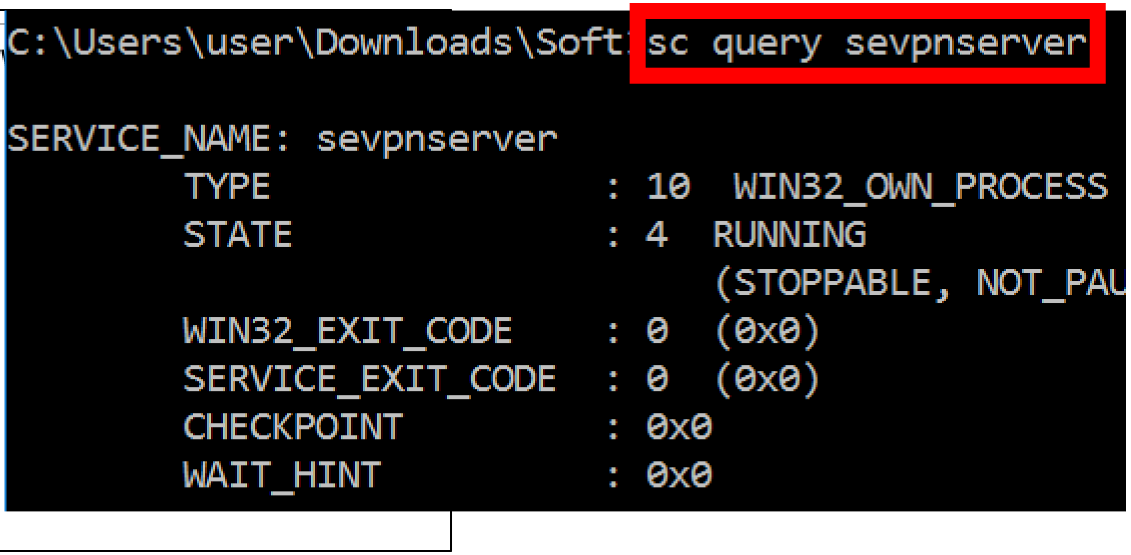
/install : Installs SoftEther VPN Server service (service name: sevpnserver)



SoftEther VPN Server / Bridge

For VPN users:

- Connect to this VPN Server
  - by Official SoftEther VPN Client (download)



```
C:\Users\user\Downloads\Soft sc query sevpnserver

SERVICE_NAME: sevpnserver
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAU
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

Arsenal

Post-Exploitation Tools

Privilege Escalation

- EfsPotato New

Port Forwarding

- FRPS
- frpModify New

Network Persistence

- SoftEther VPN Server New

Malware

Cobalt Strike Beacon Downloader

- Type A New
- Type B New

Rootkit + RAT

- Pandora Updated
- NDISProxy

Miscellaneous

Godzilla WebShell, ASP File Uploader

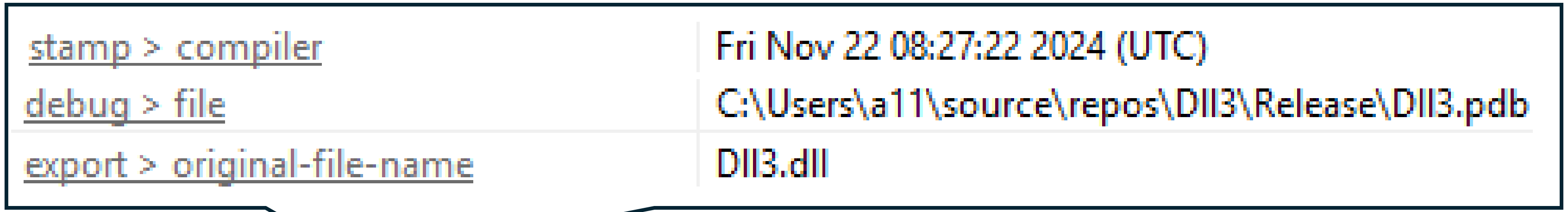
New

Cobalt Strike Beacon Downloaders

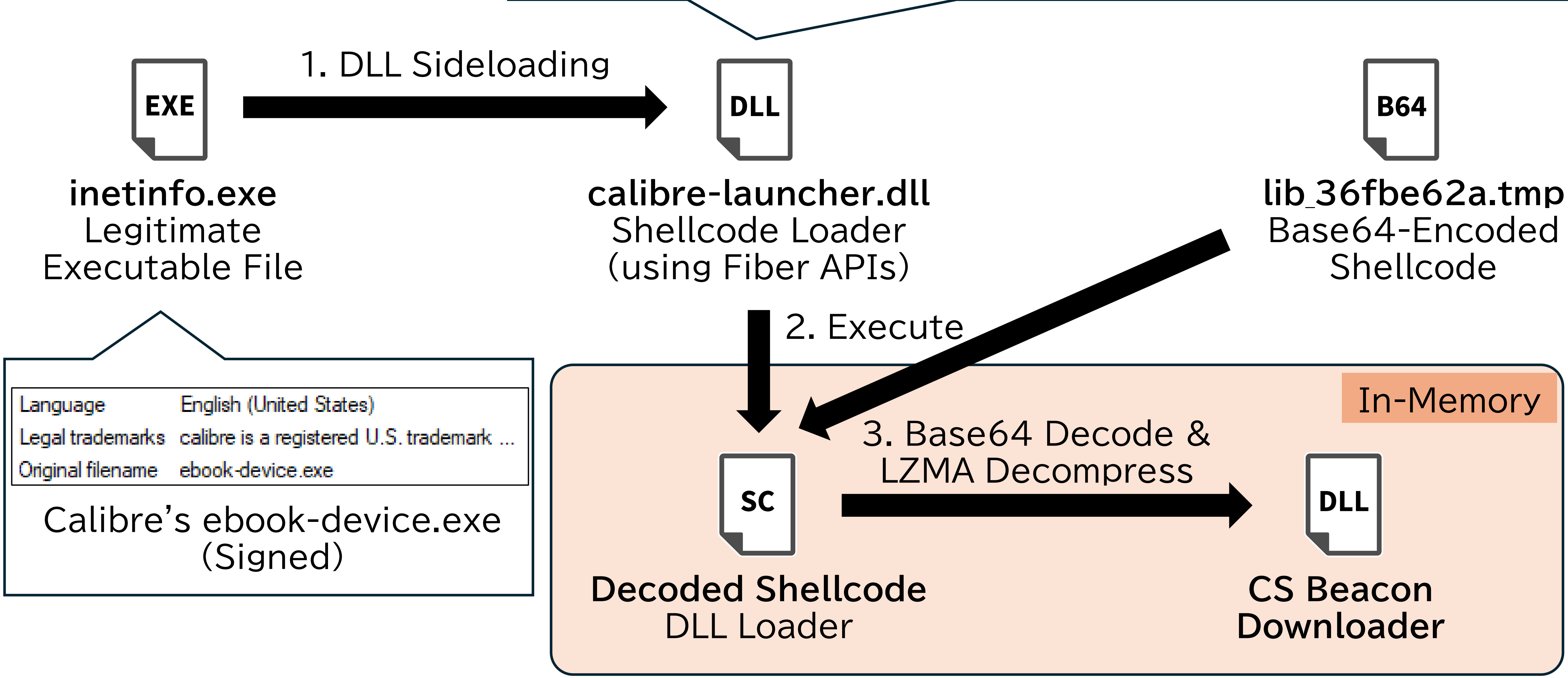
Cobalt Strike Beacon Downloaders

- Two different types of Cobalt Strike Beacon Downloaders were observed in this attack campaign.
  - Both connect to the same endpoint (URL).
- For convenience, we call each of them Type A and Type B.

Type A



stamp > compiler	Fri Nov 22 08:27:22 2024 (UTC)
debug > file	C:\Users\a11\source\repos\Dll3\Release\Dll3.pdb
export > original-file-name	Dll3.dll



1. DLL Sideloading

EXE
inetinfo.exe
Legitimate Executable File

Language	English (United States)
Legal trademarks	calibre is a registered U.S. trademark ...
Original filename	ebook-device.exe

Calibre’s ebook-device.exe (Signed)

DLL
calibre-launcher.dll
Shellcode Loader (using Fiber APIs)

B64
lib_36fbe62a.tmp
Base64-Encoded Shellcode

2. Execute

In-Memory

SC
Decoded Shellcode
DLL Loader

3. Base64 Decode & LZMA Decompress

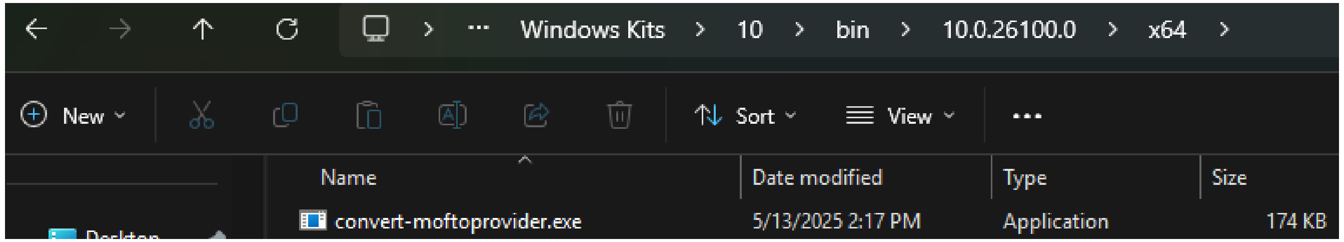
DLL
CS Beacon Downloader

Type B – Infection Flow

EXE

convert-moftoprovider.exe
Legitimate Executable File

This executable file is included in Windows SDK like this:



Windows Kits > 10 > bin > 10.0.26100.0 > x64 >

Name	Date modified	Type	Size
convert-moftoprovider.exe	5/13/2025 2:17 PM	Application	174 KB

1. DLL Sideloading

DLL

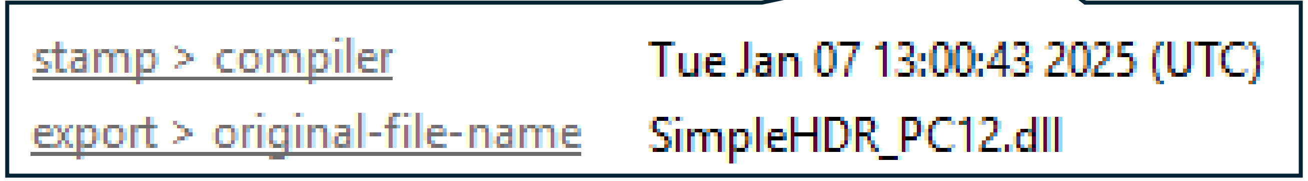
wmicodegen.dll
Shellcode Loader

2. Decrypt & Execute

In-Memory

SC

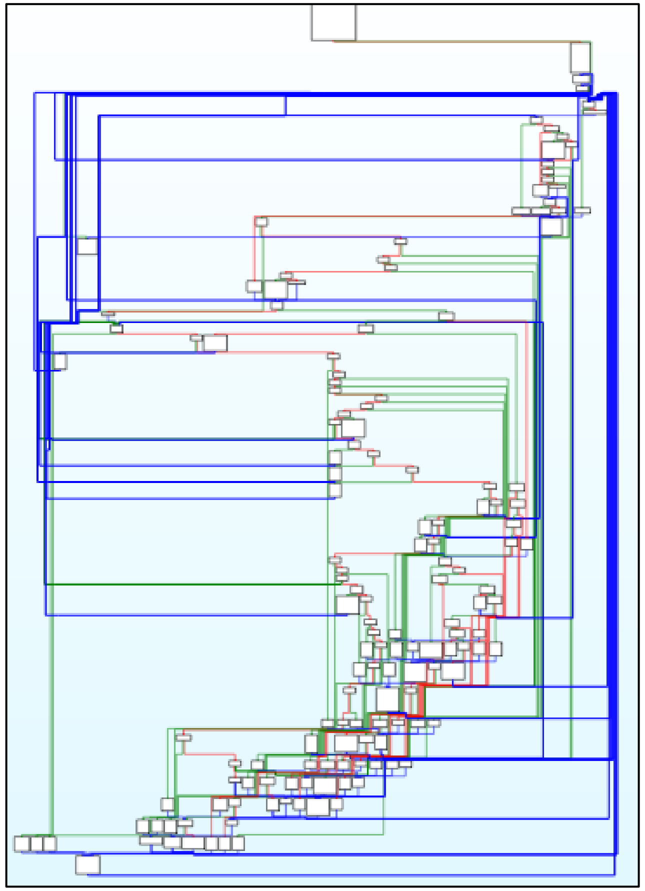
CS Beacon Downloader

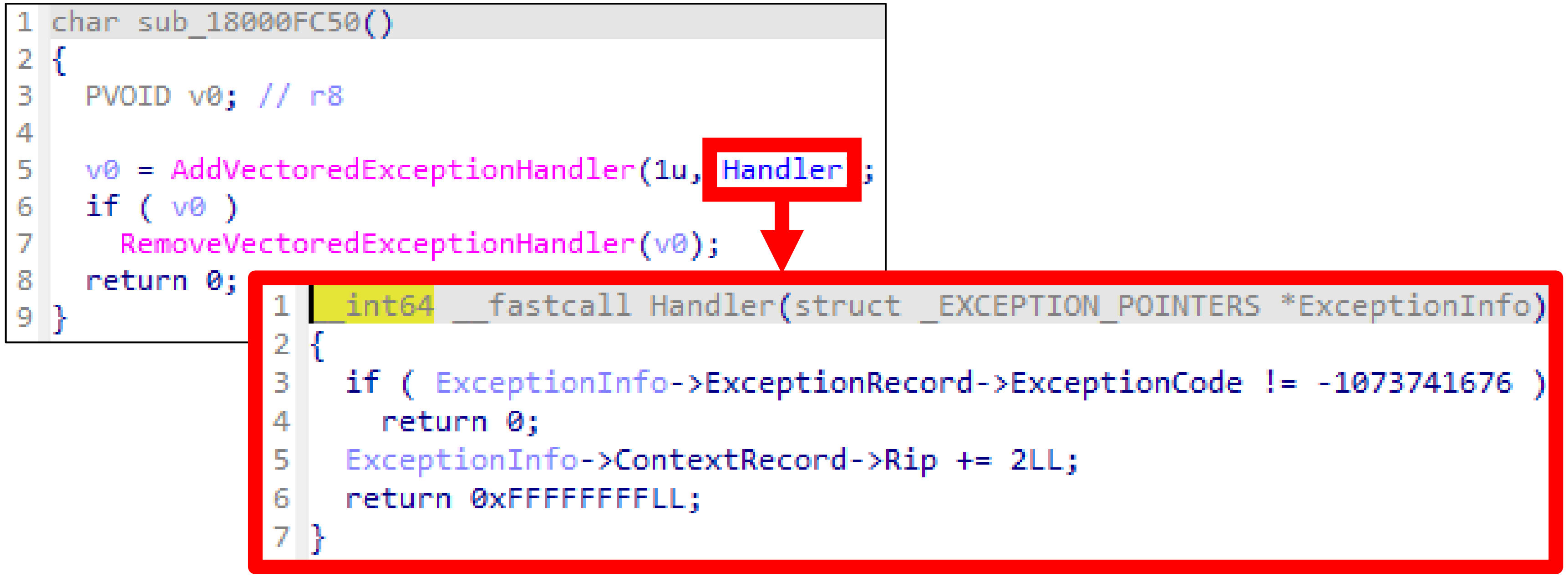


stamp > compiler	Tue Jan 07 13:00:43 2025 (UTC)
export > original-file-name	SimpleHDR_PC12.dll

Type B – Binary Obfuscation

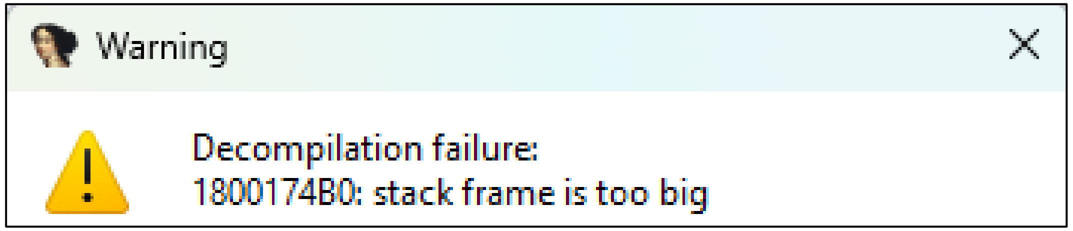
- The loader was heavily obfuscated using CFF and exception handler.





```
char sub_18000FC50()
{
  PVOID v0; // r8

  v0 = AddVectoredExceptionHandler(1u, Handler);
  if ( v0 )
    RemoveVectoredExceptionHandler(v0);
  return 0;
}
```

```
__int64 __fastcall Handler(struct _EXCEPTION_POINTERS *ExceptionInfo)
{
  if ( ExceptionInfo->ExceptionRecord->ExceptionCode != -1073741676 )
    return 0;
  ExceptionInfo->ContextRecord->Rip += 2LL;
  return 0xFFFFFFFFLL;
}
```

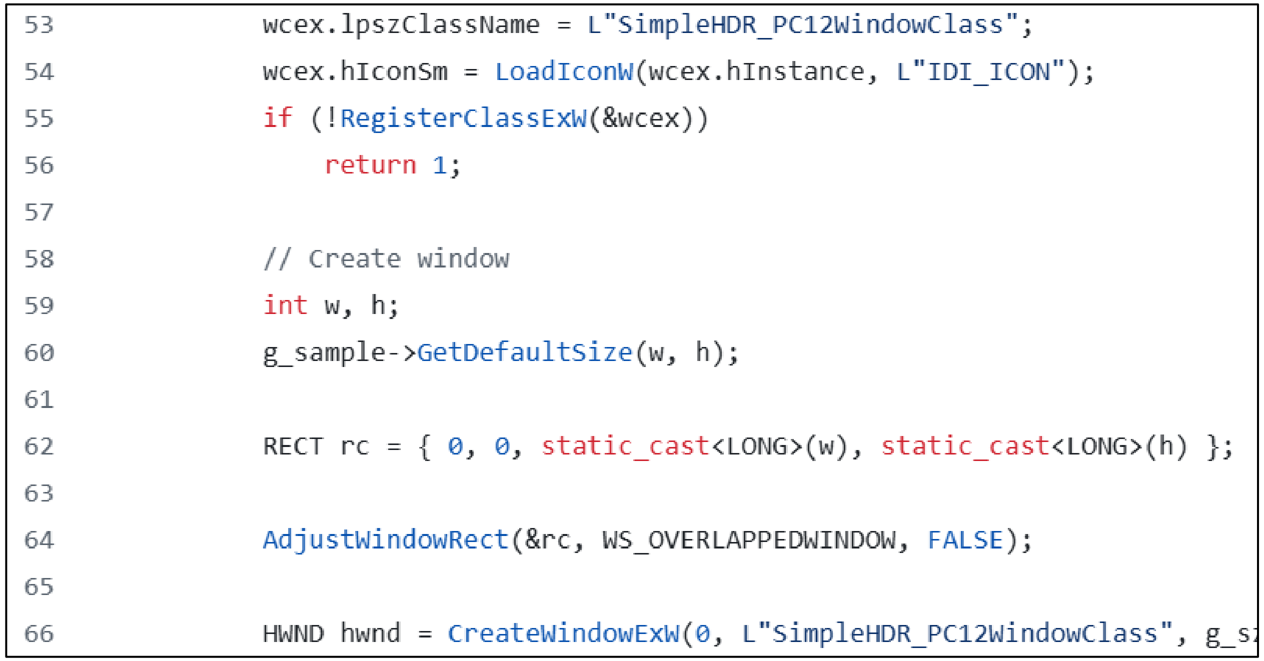


Warning

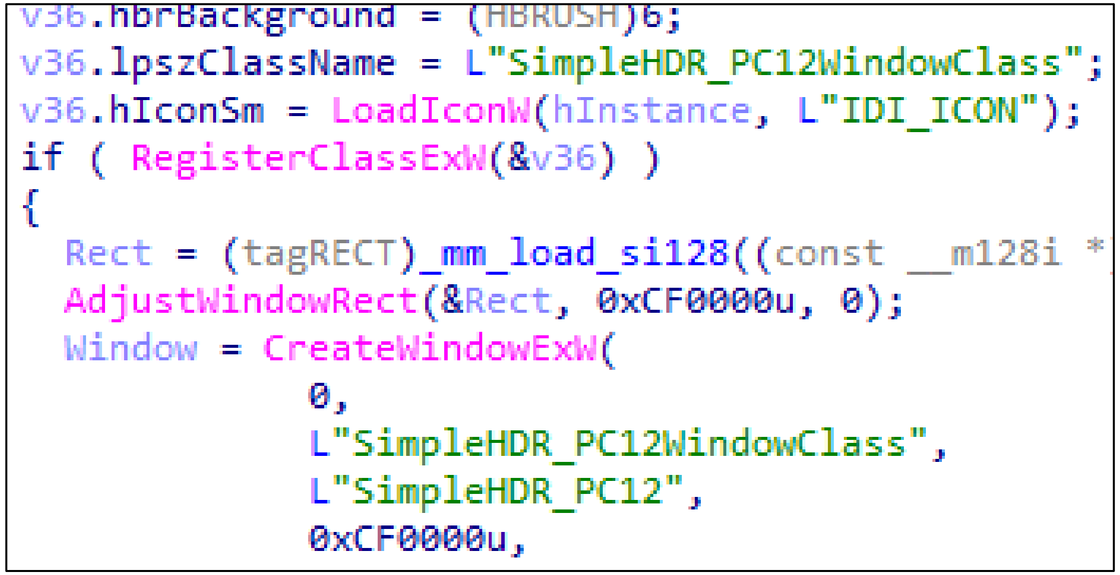
Decompilation failure:
1800174B0: stack frame is too big

Type B – Use of a Code Sample

- This loader was developed based on the code sample of the computer game published by Xbox ATG below (SimpleHDR_PC12).
- https://github.com/microsoft/Xbox-ATG-Samples/tree/main/PCSamples/Graphics/SimpleHDR_PC12



```
        wcex.lpszClassName = L"SimpleHDR_PC12WindowClass";
        wcex.hIconSm = LoadIconW(wcex.hInstance, L"IDI_ICON");
        if (!RegisterClassExW(&wcex))
            return 1;

        // Create window
        int w, h;
        g_sample->GetDefaultSize(w, h);

        RECT rc = { 0, 0, static_cast<LONG>(w), static_cast<LONG>(h) };

        AdjustWindowRect(&rc, WS_OVERLAPPEDWINDOW, FALSE);

        HWND hwnd = CreateWindowExW(0, L"SimpleHDR_PC12WindowClass", g_s
```



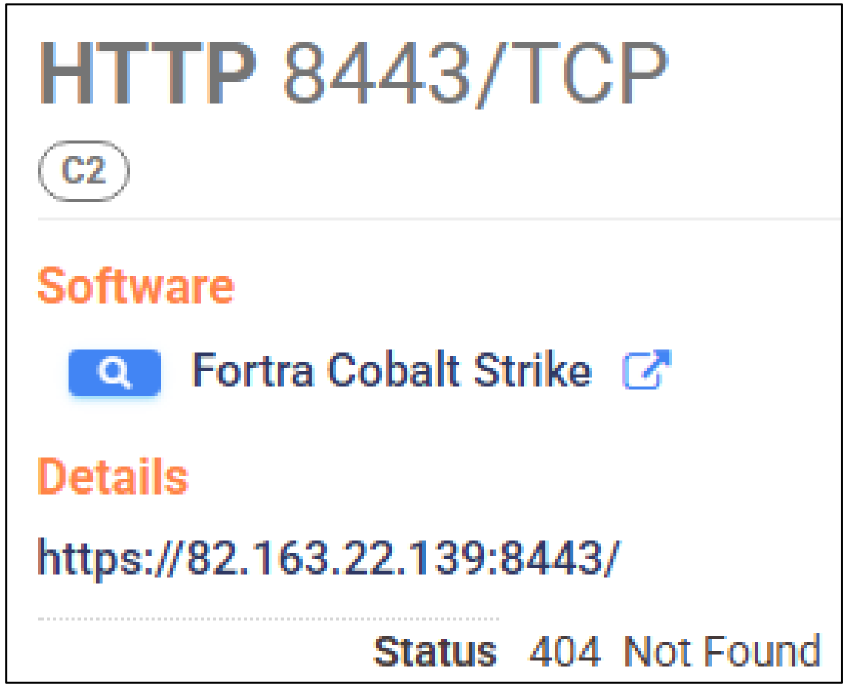
```
v36.hbrBackground = (HBRUSH)6;
v36.lpszClassName = L"SimpleHDR_PC12WindowClass";
v36.hIconSm = LoadIconW(hInstance, L"IDI_ICON");
if ( RegisterClassExW(&v36) )
{
  Rect = (tagRECT)_mm_load_si128((const __m128i *
  AdjustWindowRect(&Rect, 0xCF0000u, 0);
  Window = CreateWindowExW(
             0,
             L"SimpleHDR_PC12WindowClass",
             L"SimpleHDR_PC12",
             0xCF0000u,
```

Type B – Similarity

- In July 2025, Kaspersky identified the loader of stealer malware used in an attack campaign conducted by APT41.
  - The SOC files: Rumble in the jungle or APT41’s new target in Africa https://securelist.com/apt41-in-africa/116986/
- We have medium confidence that the Type B loader I found is related to that sample, because both are:
  - Renamed to "wmicodegen.dll" and used with the same legitimate executable file "convert-moftoprovider.exe" for DLL sideloading.
  - Developed based on the same sample code (SimpleHDR_PC12).
  - Compiled and used for an attack campaign within 2025.

Endpoint that Downloaders Accesses

- hxxps://cdn.windowserrorapis[.]com:8443/v5/owa/rYpKZYehSa0sW1gFbbaVg4KB1m.cab
- Cobalt Strike C2 server was also observed on same address and port.



HTTP 8443/TCP

C2

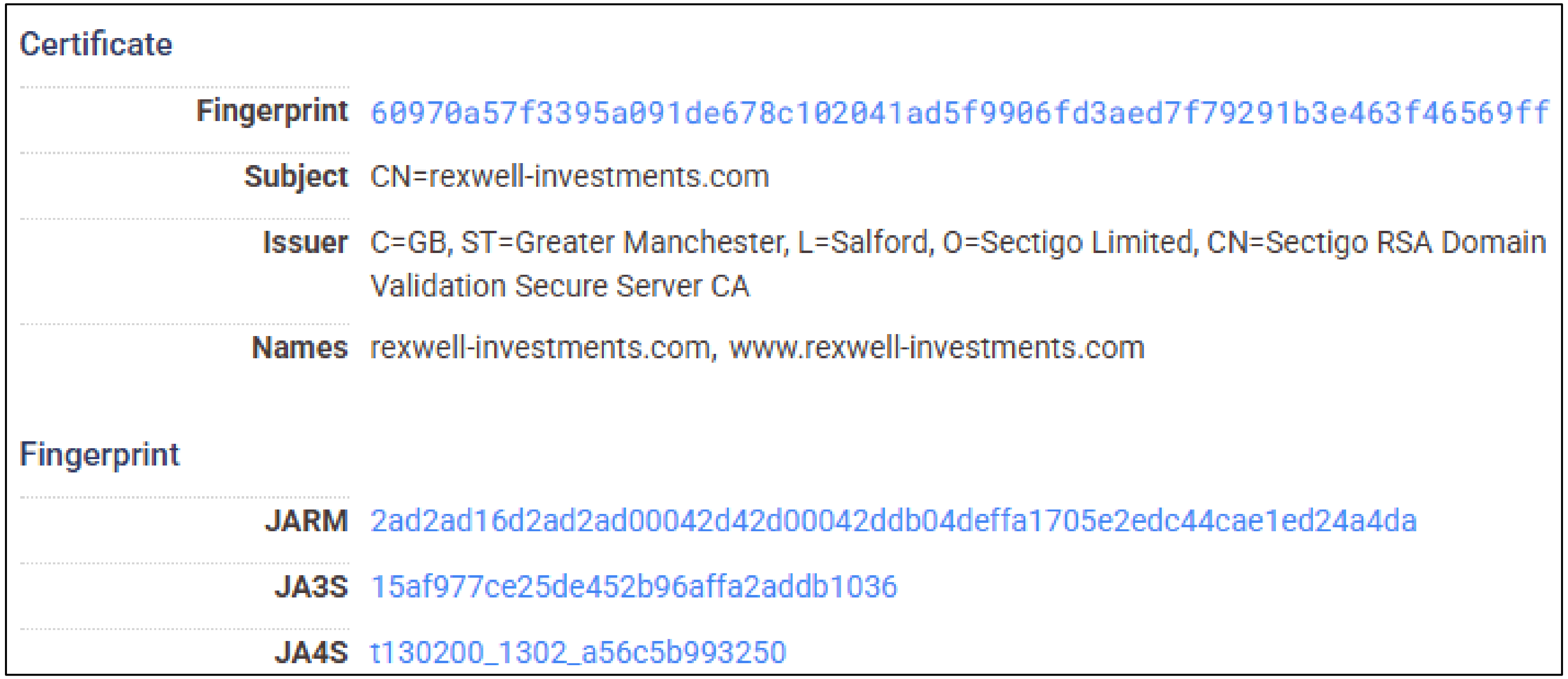
Software

Fortra Cobalt Strike

Details

https://82.163.22.139:8443/

Status 404 Not Found



Certificate

Fingerprint	60970a57f3395a091de678c102041ad5f9906fd3aed7f79291b3e463f46569ff
Subject	CN=rexwell-investments.com
Issuer	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
Names	rexwell-investments.com, www.rexwell-investments.com

Fingerprint

JARM	2ad2ad16d2ad2ad00042d42d00042ddb04deffa1705e2edc44cae1ed24a4da
JA3S	15af977ce25de452b96affa2addb1036
JA4S	t130200_1302_a56c5b993250

https://search.censys.io/hosts/82.163.22.139

Arsenal

Post-Exploitation Tools

Privilege Escalation

- EfsPotato New

Port Forwarding

- FRPS
- frpModify New

Network Persistence

- SoftEther VPN Server New

Malware

Cobalt Strike Beacon Downloader

- Type A New
- Type B New

Rootkit + RAT

- Pandora Updated
- NDISProxy

Miscellaneous

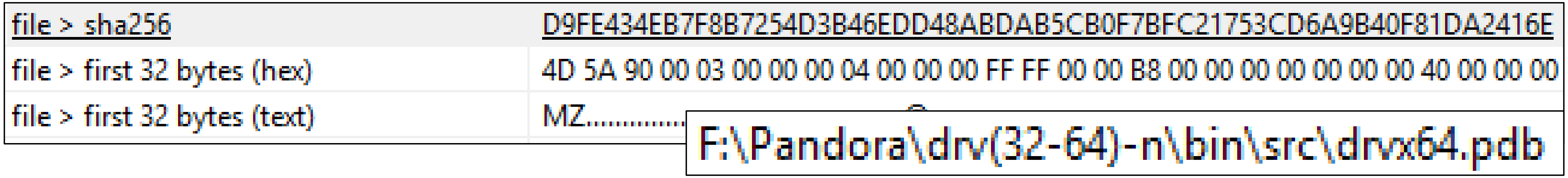
Godzilla WebShell, ASP File Uploader

Updated

Rootkit + RAT

Pandora

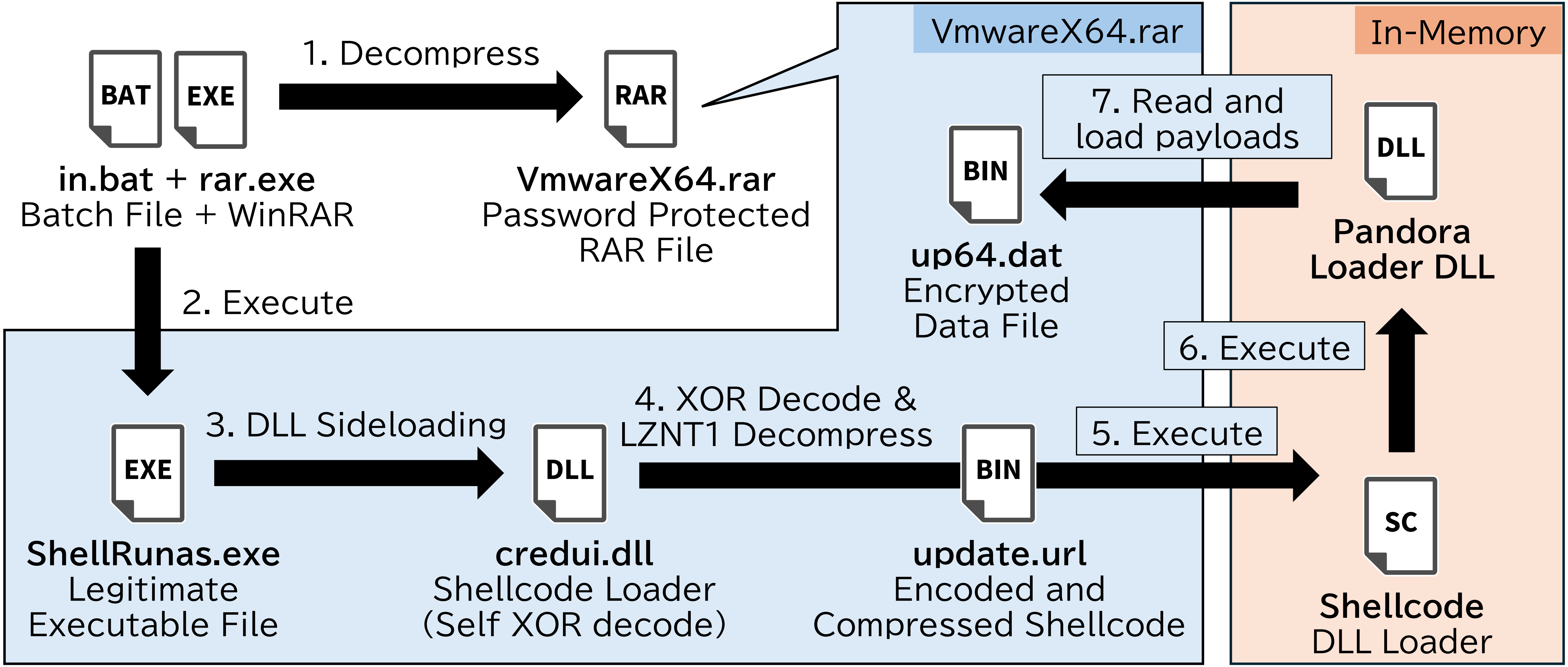
- Passive backdoor leveraged by APT27 (Iron Tiger).
  - Both rootkit and RAT modules of Pandora are developed using C++.
- Initially discovered by Trend Micro in 2021.
  - https://www.trendmicro.com/en_us/research/21/d/iron-tiger-apt-updates-toolkit-with-evolved-sysupdate-malware-va.html
  - We identified several updates from a sample described above.
- The sample observed in this campaign:



file > sha256	D9FE434EB7F8B7254D3B46EDD48ABDAB5CB0F7BFC21753CD6A9B40F81DA2416E
file > first 32 bytes (hex)	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00
file > first 32 bytes (text)	MZ............

F:\Pandora\drv(32-64)-n\bin\src\drvx64.pdb

Pandora – Infection Flow



Pandora Loader

- Pandora Loader is a payload that prepares and loads Pandora Rootkit.
- This Pandora Loader sample:
  - Creates a folder at C:¥Windows¥Help¥OEMex .
  - Moves the extracted files from the RAR file to the created folder.
  - Creates the service named "dsxdsex" for persistence.
  - Writes Pandora Rootkit and RAT to a certain registry key.
    - Originally stored in the "up64.dat" file with a DES encryption.
  - Injects the next-stage payload (see the next page) that executes Pandora Rootkit to "svchost.exe".

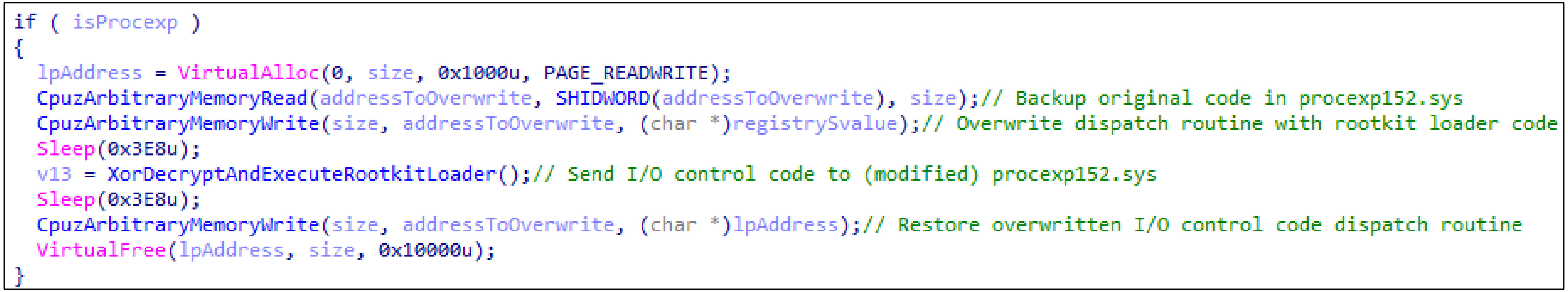
Pandora Loader – BYOVD

- To load the Pandora Rootkit payload, the next-stage payload firstly drops and loads two legitimate drivers, "cpuz141.sys" and "procexp152.sys".
- The former driver can be abused to achieve arbitrary memory read and write (CVE-2017-15303).
  - Loading a legitimate vulnerable driver for purposes like bypassing security features is a common technique among attackers.
  - This technique is called Bring Your Own Vulnerable Driver (BYOVD).
  - https://www.loldrivers.io/drivers/fab98aaa-e4e7-4c4a-af65-c00d35cf66e9

Updated

Pandora Loader – Load Rootkit

- Pandora Loader exploits this vulnerability to overwrite an IOCTL dispatch routine of the "procexp152.sys" to the code that executes Pandora Rootkit.
  - The sample in the past report bypasses the DSE with the different method and writes Pandora Rootkit to the filesystem to load.
  - The threat actors changed their approach to make fileless.



```
if ( isProcexp )
{
  lpAddress = VirtualAlloc(0, size, 0x1000u, PAGE_READWRITE);
  CpuzArbitraryMemoryRead(addressToOverwrite, SHIDWORD(addressToOverwrite), size);// Backup original code in procexp152.sys
  CpuzArbitraryMemoryWrite(size, addressToOverwrite, (char *)registrySvalue);// Overwrite dispatch routine with rootkit loader code
  Sleep(0x3E8u);
  v13 = XorDecryptAndExecuteRootkitLoader();// Send I/O control code to (modified) procexp152.sys
  Sleep(0x3E8u);
  CpuzArbitraryMemoryWrite(size, addressToOverwrite, (char *)lpAddress);// Restore overwritten I/O control code dispatch routine
  VirtualFree(lpAddress, size, 0x10000u);
}
```

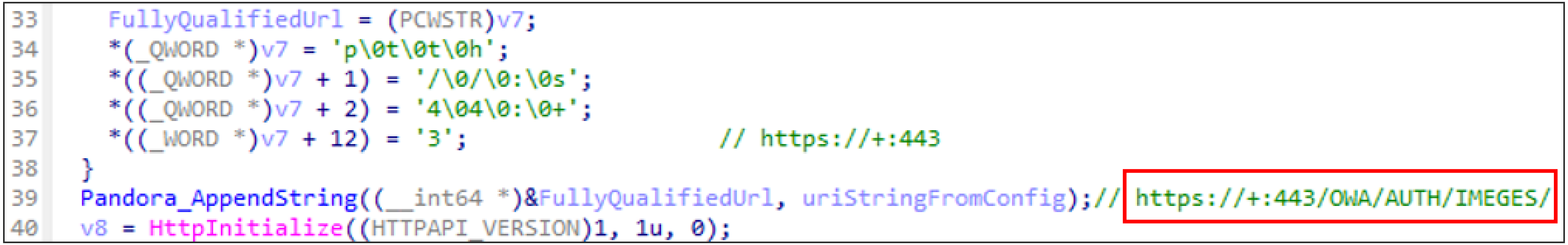
Pandora Rootkit

Updated

- This Pandora Rootkit sample can hide process, file, registry key, and attacker's access in kernel-level.
- As an update from sample in the past report, Pandora Rootkit embedded the code of an open-source rootkit named "Hidden.sys".
    - "Hidden.sys" was also used in past attack campaign to hide certain files and registry keys but separately used with Pandora Rootkit.
    - The threat actors integrated two different rootkits, possibly for decreasing the risk of detection by security products.
- Pandora Rootkit executes Pandora RAT by injecting it to "lsass.exe".

Pandora RAT

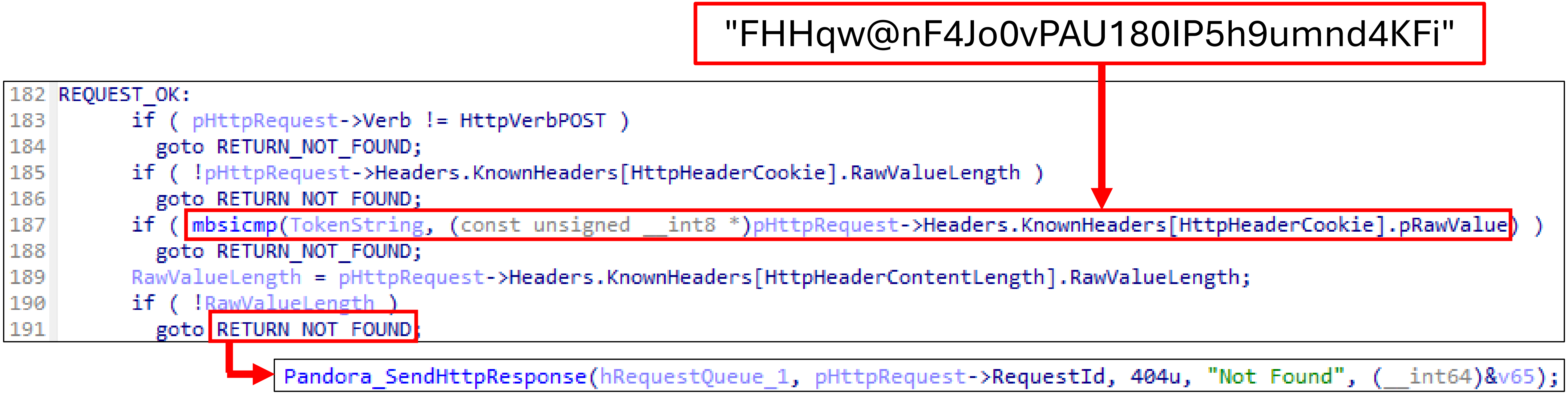
- Pandora RAT functions as a HTTPS server, receiving connections on TCP port 443 and processing requests sent to the specific path defined in the configuration data.
- For the sample we analyzed, the path was set to "/OWA/AUTH/IMEGES/".



```
    FullyQualifiedUrl = (PCWSTR)v7;
    *(_QWORD *)v7 = 'p\0t\0t\0h';
    *((_QWORD *)v7 + 1) = '/\0/\0:\0s';
    *((_QWORD *)v7 + 2) = '4\04\0:\0+';
    *((_WORD *)v7 + 12) = '3';                  // https://+:443
  }
  Pandora_AppendString((__int64 *)&FullyQualifiedUrl, uriStringFromConfig);// https://+:443/OWA/AUTH/IMEGES/
  v8 = HttpInitialize((HTTPAPI_VERSION)1, 1u, 0);
```

Pandora RAT – Cookie

- The server checks whether a request comes from attackers or not by verifying that the HTTP method is POST and that the 'Cookie' header contains the specific value below.



"FHHqw@nF4Jo0vPAU180IP5h9umnd4KFi"

```
REQUEST_OK:
      if ( pHttpRequest->Verb != HttpVerbPOST )
        goto RETURN_NOT_FOUND;
      if ( !pHttpRequest->Headers.KnownHeaders[HttpHeaderCookie].RawValueLength )
        goto RETURN_NOT_FOUND;
      if ( mbsicmp(TokenString, (const unsigned __int8 *)pHttpRequest->Headers.KnownHeaders[HttpHeaderCookie].pRawValue) )
        goto RETURN_NOT_FOUND;
      RawValueLength = pHttpRequest->Headers.KnownHeaders[HttpHeaderContentLength].RawValueLength;
      if ( !RawValueLength )
        goto RETURN_NOT_FOUND;
```

```
Pandora_SendHttpResponse(hRequestQueue_1, pHttpRequest->RequestId, 404u, "Not Found", (__int64)&v65);
```

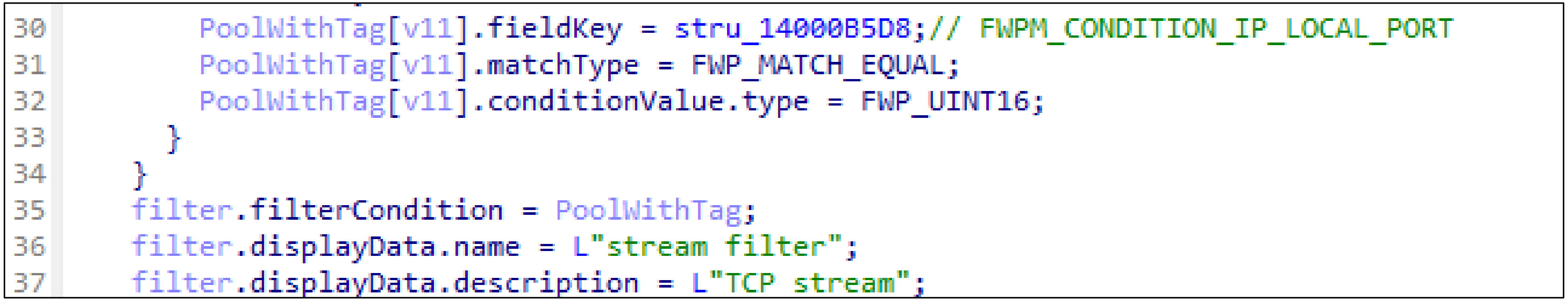
Pandora RAT – Commands

- The 1st byte of the HTTP request body represents a command ID, and the rest of the data is treated as its arguments (e.g., sub-command ID).

ID	RTTI Name	Description
0x14	CMUnload	Output debug message "[test] uninstall" but does nothing.
0x1F	-	Enable / Disable SOCKS5 proxy.
0x22	-	Does nothing.
0x23	-	Relay an HTTP request to a host also infected with Pandora.
0x28	CMFile	File manipulation (upload, download, rename, and etc...)
0x29	CMProcess	Process manipulation (enumeration, termination).
0x2A	CMServices	Service manipulation (create, stop, delete, and etc...)
0x2C	CMCmd	Start a remote shell.

Pandora Rootkit – WFP

- In addition to handling incoming connections on TCP port 443, Pandora RAT can also handle RAT commands via TCP streams filtered using the Windows Filtering Platform (WFP) in the Pandora rootkit.
  - It is implemented based on the sample code available on GitHub.
    https://github.com/microsoft/windows-driver-samples/tree/main/network/trans/stmedit
- Filtered port numbers are shown in the Appendix section.



```
        PoolWithTag[v11].fieldKey = stru_14000B5D8;// FWPM_CONDITION_IP_LOCAL_PORT
        PoolWithTag[v11].matchType = FWP_MATCH_EQUAL;
        PoolWithTag[v11].conditionValue.type = FWP_UINT16;
      }
    }
    filter.filterCondition = PoolWithTag;
    filter.displayData.name = L"stream filter";
    filter.displayData.description = L"TCP stream";
```

Pandora Rootkit – IOCTL Code

- Rootkit and RAT communicates through specific IOCTL code.

IOCTL Code	Description
0x222400	Initialize WFP (Windows Filtering Platform).
0x222404	Retrieve a filtered TCP stream* into a buffer.
0x222408	Get the size of a filtered TCP stream*.
0x22240C	Send a response to the sender of a filtered TCP stream*.
0x222414	Register a port number to monitor and filter TCP streams*.
0x222418	Register an additional validation key used as the Cookie header to distinguish C2 communications from others.
0x22241C	Retrieve an error code.
0x222420	Disable the PPL of a process identified by a specified PID.

* Filtered TCP streams, which are dropped packets by WFP, can be used to handle RAT commands from attackers.

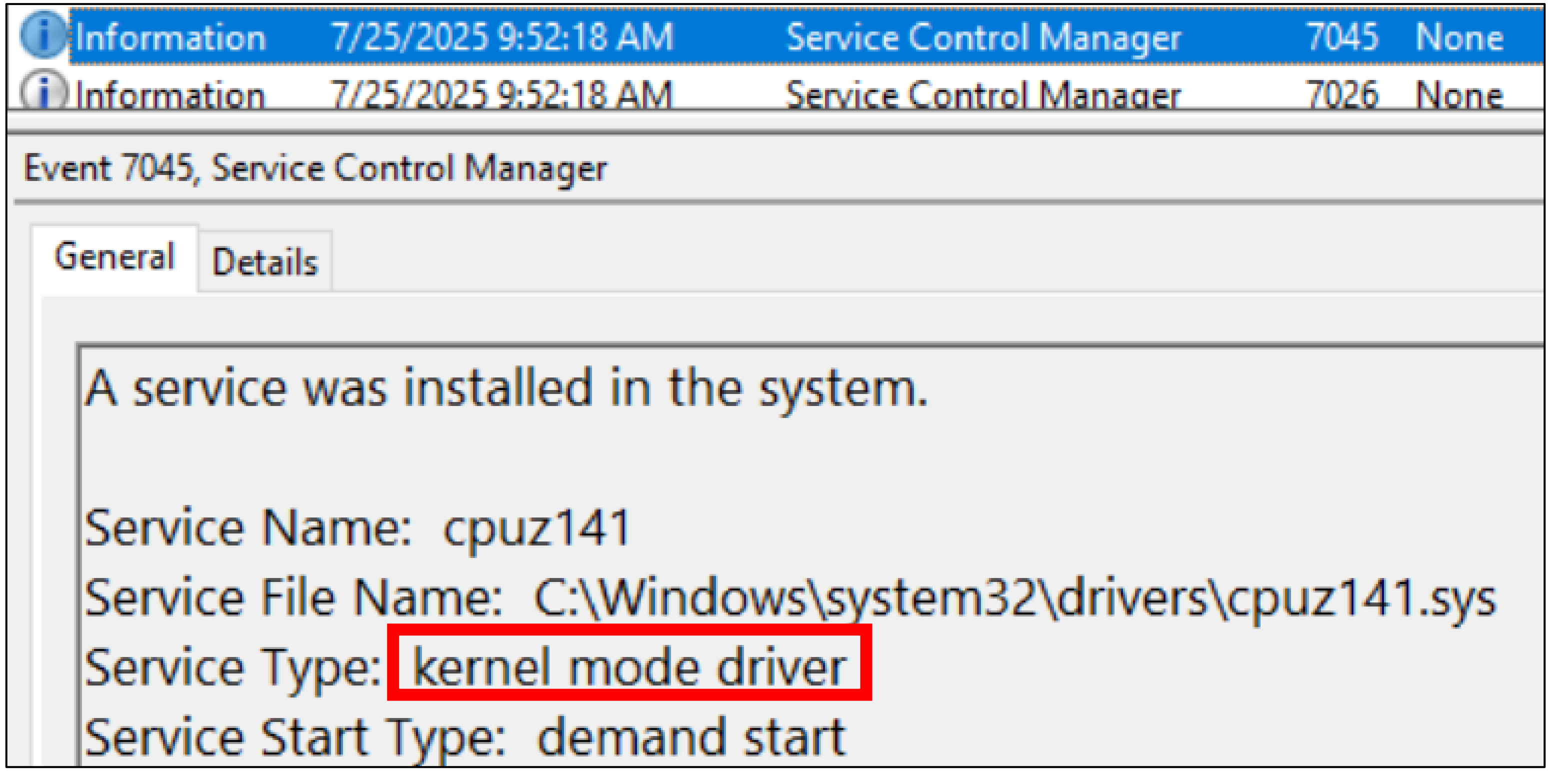
NDISProxy

- Another passive backdoor leveraged by APT27.
  - Similar but less functionality compared to Pandora.
  - Same payload described in past report has been observed.
- Detailed analysis report is published by Kaspersky.
  - LuckyMouse signs malicious NDISProxy driver with certificate of Chinese IT company - SecureList
    https://securelist.com/luckymouse-ndisproxy-driver/87914/

Countermeasures

Detecting BYOVD attack

- Several events are logged when drivers are installed on the system.
- System.evtx – Event ID: 7045 (**Recorded in default environment**)



```
Information   7/25/2025 9:52:18 AM   Service Control Manager   7045   None
Information   7/25/2025 9:52:18 AM   Service Control Manager   7026   None
```

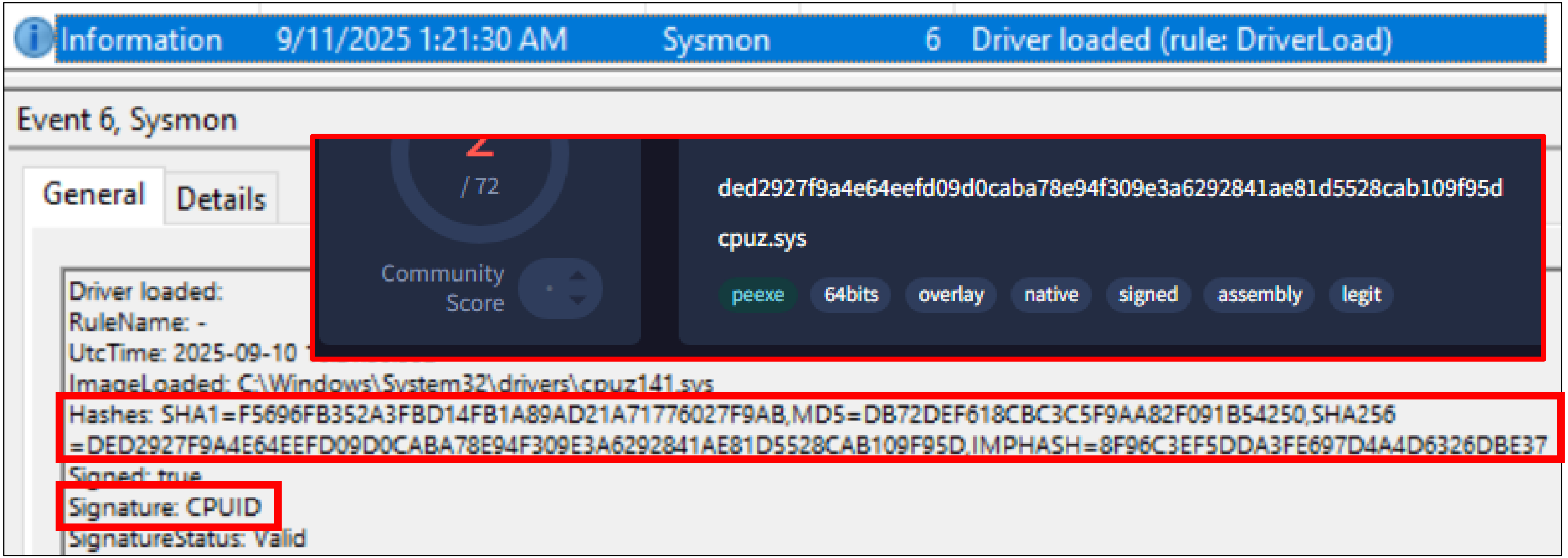
Event 7045, Service Control Manager

A service was installed in the system.

Service Name: cpuz141
Service File Name: C:\Windows\system32\drivers\cpuz141.sys
Service Type: kernel mode driver
Service Start Type: demand start

Detecting BYOVD attack

- Sysmon.evtx – Event ID: 6



```
Information    9/11/2025 1:21:30 AM    Sysmon    6    Driver loaded (rule: DriverLoad)
```

Event 6, Sysmon

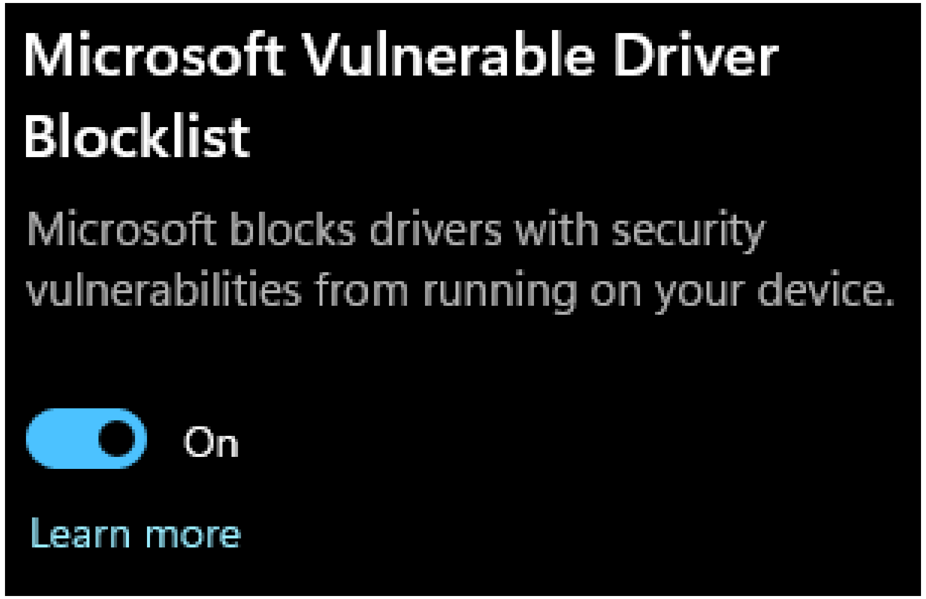
```
Driver loaded:
RuleName: -
UtcTime: 2025-09-10
ImageLoaded: C:\Windows\System32\drivers\cpuz141.sys
Hashes: SHA1=F5696FB352A3FBD14FB1A89AD21A71776027F9AB,MD5=DB72DEF618CBC3C5F9AA82F091B54250,SHA256
=DED2927F9A4E64EEFD09D0CABA78E94F309E3A6292841AE81D5528CAB109F95D,IMPHASH=8F96C3EF5DDA3FE697D4A4D6326DBE37
Signed: true
Signature: CPUID
SignatureStatus: Valid
```

ded2927f9a4e64eefd09d0caba78e94f309e3a6292841ae81d5528cab109f95d

cpuz.sys

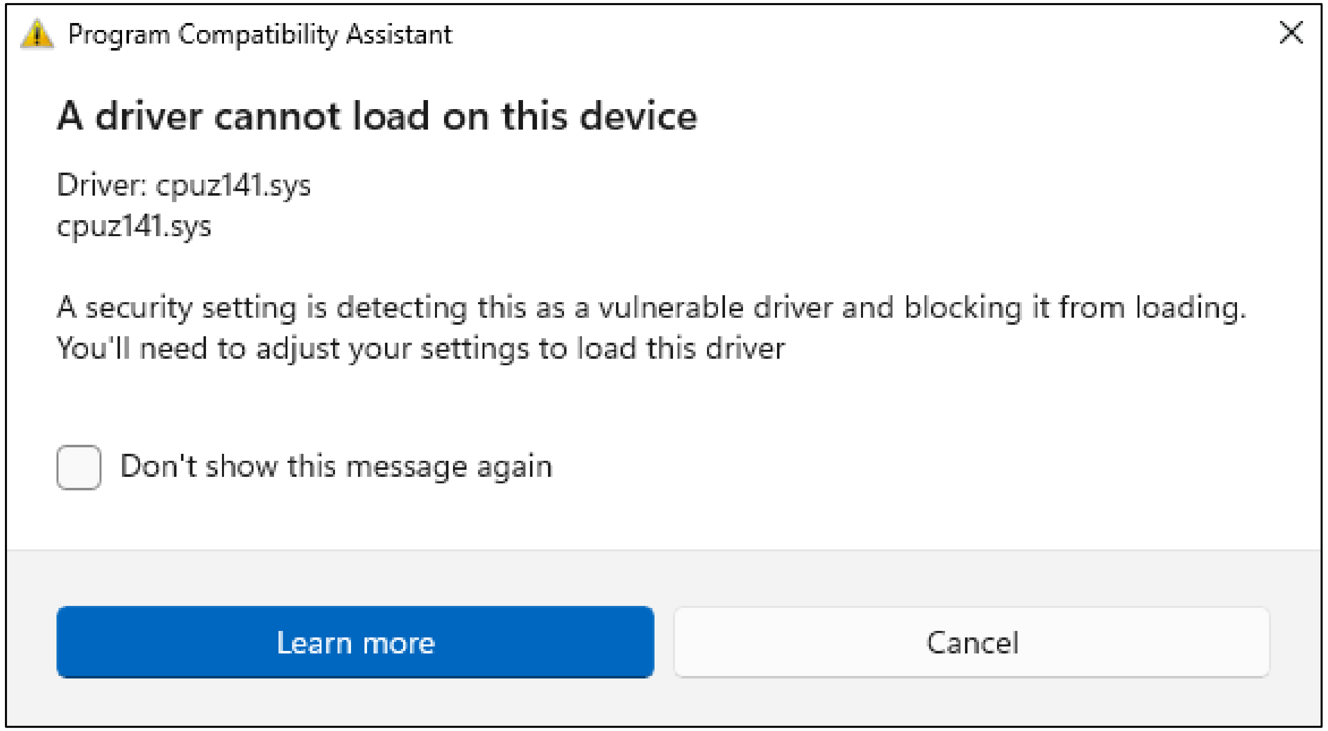
Microsoft Vulnerable Driver Blocklist

- A security feature within WDAC (Windows Defender Application Control) that blocks known vulnerable drivers to be loaded.
- Available on Windows 10/11 22H2 or later.



Microsoft Vulnerable Driver Blocklist

Microsoft blocks drivers with security vulnerabilities from running on your device.



A driver cannot load on this device

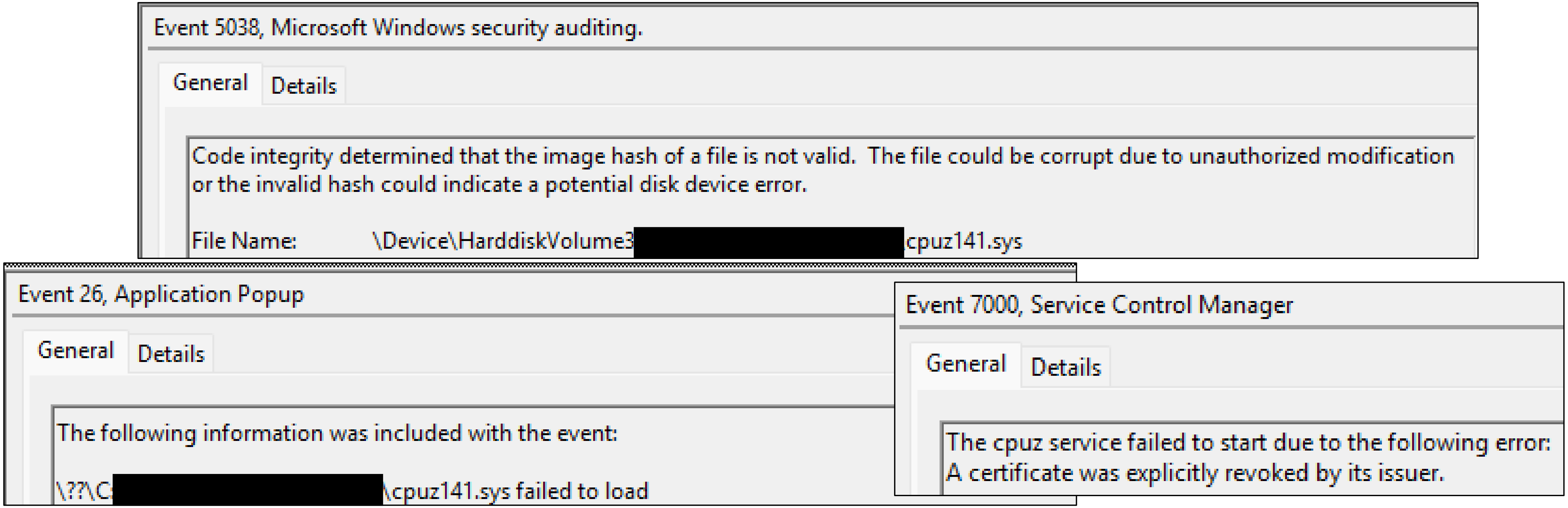
Driver: cpuz141.sys
cpuz141.sys

A security setting is detecting this as a vulnerable driver and blocking it from loading. You'll need to adjust your settings to load this driver

□ Don't show this message again

Other Event Logs

- Event logs recorded when system blocked the driver load.
- System.evtx – Event ID: 26, 7000 / Security.evtx – Event ID: 5038



Event 5038, Microsoft Windows security auditing.

Code integrity determined that the image hash of a file is not valid. The file could be corrupt due to unauthorized modification or the invalid hash could indicate a potential disk device error.

File Name: \Device\HarddiskVolume3[redacted]cpuz141.sys

Event 26, Application Popup

The following information was included with the event:

\??\C[redacted]\cpuz141.sys failed to load

Event 7000, Service Control Manager

The cpuz service failed to start due to the following error:
A certificate was explicitly revoked by its issuer.

Wrap-up

Conclusion

- APT27 started to abuse a legitimate VPN server software to achieve persistent access against compromised hosts.
- They also deployed rootkits, enabling threat actors to stealthily control infected hosts.
- Detecting BYOVD using tools/features such as Sysmon and Microsoft Vulnerable Driver Blocklist is important.
- Scripts for analyzing similar malware samples is available on GitHub: https://github.com/mopisec/vb2025-inside-pandoras-box

Thank you for listening!

Any comments or questions are welcome!

X: @mopisec

Appendix

Pandora – Configuration Data

Name	Value
Cookie Value	FHHqw@nF4Jo0vPAU180IP5h9umnd4KFi
Path	/OWA/AUTH/IMEGES/
Mutex Name	Global¥dsxEnddsxdsex
Semaphore Name	Global¥dsxdsxdsex
Filtered Port Numbers	135, 80, 443, 445, 1433, 3306, 3389, 8080, 21, 389, 53, 444, 7001

NDISProxy – Configuration Data (1)

Name	Value
Service Name	ndisproxy-mn
Service Display Name	ndisproxy-mn Proxy Server Driver
Service Description	ndisproxy-mn Proxy Server Driver
Rootkit Filename	ndisproxy-mn.sys

NDISProxy – Configuration Data (2)

Name	Value
Cookie Value	qZ326NZxb%^u1YSj&E~6UwbmugYV02*&
Path	/mneges/
Mutex Name	Global¥DoorEND-ndisproxy-mn
Semaphore Name	Global¥Door-ndisproxy-mn
Filtered Port Numbers	80, 135, 443, 445, 995, 1433, 1723, 3389, 8080

IoCs (Cobalt Strike Beacon Downloader)

- Type A
- calibre-launcher.dll
  c5f522b43c30019679efe0628dfdf3877b17f78889c0bb38855bb831e68b1f37
- lib_36fbe62a.tmp
  10991eaf16d57a33ddd441e45e48171381faa319cda8dc5f7852b67569a80441

- Type B
- wmicodegen.dll
  414bcdcf1706f803704f28e8a23d30d162f03c6d3cd588686a93f72e36255c94

IoCs (Pandora + NDISProxy)

- in.bat (Pandora)
  a7e35eb1235274284196af91a5c24811b90777dcb4cdc7429672cc3c9d98138b
- VmwareX64.rar (Pandora)
  abafc8d0214eeebcb9bea8d42de21408fe556de2f56bac4cc18b281c629e6766
- credui.dll (Pandora)
  8df614fb32ac6a53809297ac1ffad6ceb1efacce3637e449592a42af29505b8c
- update.url (Pandora)
  6108049cf2bfae1615292f25286f23e801e3e8ecd7006e46a0d5e9bdd092e0c3
- up64.dat (Pandora)
  27bb87aeefd7a68fe5de9004a8f37817376ef3cd47c9bf2e7096b01ecf997e38
- iload.exe (NDISProxy)
  d67e183a051d07b0d9b1001d357f436d217ac7c76c403965094d98afd18052df

IoCs (Network)

- Cobalt Strike C2 Server
  - cdn.windowserrorapis[.]com
  - 82.163.22[.]139
- Others (FRPS, Open Directory, and more...)
  - 103.243.26[.]213

IoCs (Others)

- Folder (Pandora)
  - C:¥Windows¥Help¥OEMex
- Service (Pandora)
  - dsxdsex
- Registry Key (Pandora)
  - HKLM¥Software¥Classes¥dsxUpdate
- Registry Key (NDISProxy)
  - HKLM¥Software¥Classes¥64ndisproxy-mn