

Converging Interests: Analysis of Threat Clusters Targeting a Southeast Asian Government

Executive Summary

Unit 42 researchers uncovered a series of cyberespionage campaigns targeting a government organization in Southeast Asia. Our initial investigation began with tracking Stately Taurus activity between June 1–Aug. 15, 2025. This activity involves USB-propagated malware called USBFect (aka HIUPAN), which deploys a PUBLOAD backdoor. Our investigation led to the discovery of two additional, distinct activity clusters we’re tracking as CL-STA-1048 and CL-STA-1049.

The attackers behind CL-STA-1048 used an espionage toolkit comprising several components:

- EggStremeFuel backdoor
- Masol remote access Trojan (RAT)
- EggStreme Loader (which delivered the comprehensive Gorem RAT with keylogging)
- A simple data theft tool we internally label TrackBak stealer

In contrast, CL-STA-1049’s operations involved using a novel loader, which we named Hypnosis loader, to deploy the FluffyGh0st RAT payload.

These activity clusters overlap with publicly reported campaigns aimed at establishing persistent access. Significant overlap in tactics, techniques and procedures (TTPs) with known China-aligned campaigns suggests the clusters and threat group have a common target of interest, potentially coordinating their effort.

Palo Alto Networks customers are better protected from the threats discussed in this article through the following products and services:

- [Advanced WildFire](#)
- [Advanced URL Filtering](#) and [Advanced DNS Security](#)
- [Cortex XDR](#) and [XSIAM](#)

If you think you might have been compromised or have an urgent matter, contact the [Unit 42 Incident Response team](#).

Related Unit 42 Topics	Malware
Threat Groups or Activity Clusters Discussed	Cluster Bravo, Cluster Charlie, Crimson Palace, Earth Estries, Stately Taurus, Unfading Sea Haze, CL-STA-1048, CL-STA-1049
Remote Access Trojans Discussed	FluffyGh0st, Gh0st, Gorem, Masol
Loaders Discussed	ClaimLoader, CoolClient, EggStreme, Hypnosis
Stealers Discussed	TrackBak
Backdoors Discussed	Backdr-NQ, EggStremeFuel, PUBLOAD, RawCookie

Southeast Asian Government Targeting

This investigation revealed a persistent espionage campaign targeting a government organization in Southeast Asia.

Our analysis identified three distinct clusters of activity in parallel within the victim’s network, each with different tools and methods but likely working toward this common objective:

- **Stately Taurus:** We attributed one of the activity clusters with high confidence to this threat actor, which leveraged USB-based malware to deploy the [PUBLOAD](#) backdoor, a consistent TTP for this group.
- **CL-STA-1048:** This cluster includes attacks using a toolkit of espionage payloads, deploying multiple RATs like [MasolRAT](#) and the RawCookie backdoor. The use of diverse and sometimes noisy tooling suggests a determined effort to establish a foothold. This activity shows links to publicly reported China-affiliated actors like [Earth Estries](#) and those behind the [Crimson Palace](#) Campaign.
- **CL-STA-1049:** This cluster features stealth and persistence, with attackers using the novel Hypnosis loader to deploy the FluffyGh0st RAT. This activity overlaps with the China-aligned group known as [Unfading Sea Haze](#).

The convergence of these three distinct, China-aligned clusters against a single, high-value government target illustrates a complex and well-resourced operation. Figure 1 provides a visual overview of the relationships between these activity clusters, the tools used in the attacks and previously reported threat groups.

- ProgramData\Intel_EVENT.dll
- ProgramData\intel_u2ec.dll
- ProgramData\intel_UsbConfig.exe
- Libraries\Dialogui\EVENT.dll

The malware stages these files to execute and propagate its payload via USB devices.

ClaimLoader

ClaimLoader (EVENT.dll) is a shellcode loader, documented by Japanese IT security company [LAC in 2022](#), that loads the PUBLOAD backdoor in memory. The sample identified in this activity largely had the same capabilities, but with slight variations. The malware copies its components to a working directory (e.g., C:\Users\Public\Libraries\Dialogui). These components include:

- A legitimate parent process
- ClaimLoader itself

The loader then registers the copied legitimate application in a Windows registry autorun key to establish persistence.

ClaimLoader then uses an XOR key to decrypt an embedded shellcode payload and executes the shellcode by using the CryptEnumOIDInfo API. This technique, shown below in Figure 2, is similar to the one described in LAC’s report.

```

strncpy(key, "cba8d3c116aa0177a5e749c24eff427e7638d5f7");
j = 0;
key_len = strlen(key);
for ( i = 0; i < 0x1C0F; ++i )
{
    byte_71760468[i] ^= key[j++];           // decode the shellcode by XOR
    if ( j > key_len )
        j = 0;
}
buf = VirtualAlloc(0, 0x1C0Fu, 0x3000u, 0x40u);
if ( buf )
{
    memcpy_0(buf, byte_71760468, 0x1C0Fu);
    return CryptEnumOIDInfo(0, 0, 0, buf);  // run the shellcode via Callback
}
return buf;

```

Figure 2. Shellcode decryption and execution by ClaimLoader.

The shellcode is PUBLOAD, first documented by [Cisco Talos in 2022](#). Variants of PUBLOAD use either HTTP or TCP for command-and-control (C2) communications. The sample we observed is a variant that uses TCP.

PUBLOAD encrypts data from the infected host, including:

- Volume info
- Computer name
- Username
- Tick count

The malware accomplishes this by using multiple XOR loops and sends the information with a fake TLS header (17 03 03) over TCP.

Once PUBLOAD receives a response from the C2 server, it decodes and executes the final payload in memory. During our analysis, we did not identify any further stages of tooling.

In November 2024, we analyzed similar activity from Stately Taurus, including an identical [PUBLOAD sample](#). This sample maintained consistent configurations and aligned with [Trend Micro's research](#) on the group.

CoolClient

During the same time period, on Aug. 4, 2025, at 08:50:15 UTC, we detected the two suspicious DLL files listed in Table 1 on an agent without PUBLOAD activity.

SHA256	File Path
835795aa494021752f21fbef63c81227c1b934437a02aa1f2a258c9f60b0b7a3	C:\ProgramData\GoogleUpdate\libvlc.dll
851d57a2bf514202f54dafa1eb83a862653be7512b6e9535914b8d1d719d495f	C:\Users\USER\AppData\LocalLow\Brother\Prtnr\angforvpnlbcrypt1_1.dll

Table 1. CoolClient loader DLL files.

Our analysis of the samples revealed they were CoolClient loaders. CoolClient loader is a shellcode loader that heavily implements anti-disassembly techniques. Without countering these techniques, analysis tools can produce incorrectly disassembled code, as shown in Figure 3 below.

```

jmp     short loc_100011DF
-----
dd 584CEAEh, 8068006Ah, 6A000000h, 6A006A03h, 68016A00h
dd offset aCProgramdataGo ; "c:\\programdata\\GoogleUpdate\\loader.j"...
db 0FFh, 15h
dd offset CreateFileA      aCProgramdataGo db 'c:\\programdata\\GoogleUpdate\\loader.ja',0
dw 4589h                                     ; DATA XREF: .text:10
dd 0EA14EBFCh, 0EA0BEB50h                                     ; .rdata:10012B7C1o
dd 0EB2444D6h, 4CEAEEDh, 0FC5D8B58h, 0FFFFB83h, 13085h
dd 0EA14EB00h, 0EA0BEB50h, 1A8C48Bh, 0BEB0674h, 0F66DDEAh
dd 0EB2444D6h, 4CEAEEDh, 0F4858D58h, 68FFFFFFEh, 104h
dd 0E850006Ah, 1234h, 0EB0CC483h, 0EB50EA14h, 0C48BEA0Bh
dd 67401A8h, 0DDEA0BEBh, 44D60F66h, 0EEEBEB24h, 8D584CEAh
dd 0FFFEF485h, 10468FFh, 6A500000h
db 0, 0FFh, 15h
dd offset GetModuleFileNameA
db 0EBh
dd 0EB50EA14h, 0C48BEA0Bh, 67401A8h, 0DDEA0BEBh, 44D60F66h
dd 0EEEBEB24h, 8D584CEAh, 0FFFEF485h, 505C6AFFh, 0E27E8h
dd 8C48300h, 0EB0000C6h, 0EB50EA14h, 0C48BEA0Bh, 67401A8h
dd 97EA0BEBh, 44D60F66h, 0EEEBEB24h, 8D584CEAh, 0FFFEF4BDh
dd 478A4FFFh, 17F8D01h, 0F675C084h
db 66h, 0A1h
dd offset word_10012B84
dw 8D8Dh
dd 0FFFFFFEF4h, 49078966h, 401F0Fh, 8D01418Ah, 0C0840149h
db 75h, 0F6h, 0A1h
dd offset dword_10012AE4
db 89h
db 1, 0A1h
dd offset dword_10012AE8
dw 4189h
db 4, 66h, 0A1h
dd offset dword_10012AEC
db 66h
dd 0EB084189h, 0EB50EA14h, 0C48BEA0Bh, 67401A8h, 97EA0BEBh
dd 44D60F66h, 0EEEBEB24h, 8D584CEAh, 0FFFEF485h, 68006AFFh
dd 80h, 6A036Ah, 16A006Ah
db 50h, 0FFh, 15h
dd offset CreateFileA
db 8Bh
dd 53006AD8h
db 0FFh, 15h
dd offset GetFileSize
dw 406Ah
dd 100068h, 57F88B00h, 15FF006Ah
dd offset VirtualAlloc
dd 458DF08Bh, 50006AF8h, 89535657h, 15FFFC75h
dd offset ReadFile
db 53h, 0FFh, 15h
dd offset CloseHandle
db 57h
dd 65E8D68Bh, 83FFFFFFDh, 14EB04C4h, 0BEB50EAh, 0A8C48BEAh
dd 0EB067401h, 6698EA0Bh, 2444D60Fh, 0EAEEEBEBh, 458B584Ch

```

Figure 3. An incorrectly disassembled CoolClient loader due to anti-disassembly techniques.

These DLL files load payloads from an encrypted file located at:

c:\\programdata\\GoogleUpdate\\loader.ja

We were unable to obtain this file during our investigation. However, it likely overlaps with the loader.ja file [reported by Trend Micro](#) that loads the final CoolClient payload.

CoolClient was first reported by [Sophos in 2022](#) and observed in Stately Taurus activity by [Trend Micro in 2023](#). This threat is built on the open-source C++ library HP-Socket to support multiple C2 protocols and a client/server two-way connection. Figure 4 shows HP-Socket's class information embedded in a CoolClient sample.

Example of the embedded class information

CTrojanClient	CTrojanClient:
CircleQueue	CircleQueue:
CMyHttpClient	CMyHttpClient: CTrojanClient;
CMyHttpClient	CHttpClientListener: IHttpClientListener, IHttpListenerT<class DualInterface<class IHttpRequester,class ITcpClient>>;
CMyHttpClient	ITcpClientListener: IClientListenerT<class ITcpClient>, ISocketListenerT<class ITcpClient>;
CMyHttpsClient	CMyHttpsClient: CTrojanClient;
CMyHttpsClient	CHttpClientListener: IHttpClientListener, IHttpListenerT<class DualInterface<class IHttpRequester,class ITcpClient>>;
CMyHttpsClient	ITcpClientListener: IClientListenerT<class ITcpClient>, ISocketListenerT<class ITcpClient>;
IComplexSocket	IComplexSocket:
ISocketListenerT<class ITcpServer>	ISocketListenerT<class ITcpServer>:
CTcpServerListener	CTcpServerListener: ITcpServerListener, IServerListenerT<class ITcpServer>, IComplexSocketListenerT<class ITcpServer>;
CTcpServer	CTcpServer: ITcpServer, IServer, IComplexSocket;
CMyTcpServer	CMyTcpServer: CTrojanClient;
CMyTcpServer	CTcpServerListener: ITcpServerListener, IServerListenerT<class ITcpServer>, IComplexSocketListenerT<class ITcpServer>;
IArqClient	IArqClient:
ISocketListenerT<class IUdpClient>	ISocketListenerT<class IUdpClient>:
CUdpClientListener	CUdpClientListener: IUdpClientListener, IClientListenerT<class IUdpClient>, ISocketListenerT<class IUdpClient>;
CUdpClient	CUdpClient: IUdpClient, IClient;
CArqSessionT<class CUdpArqClient,class CUdpArqClient>	CArqSessionT<class CUdpArqClient,class CUdpArqClient>:
CUdpArqClient	CUdpArqClient: IArqClient;
CUdpArqClient	CUdpClient: IUdpClient, IClient;
CMyUdpClient	CMyUdpClient: CTrojanClient;
CMyUdpClient	CUdpClientListener: IUdpClientListener, IClientListenerT<class IUdpClient>, ISocketListenerT<class IUdpClient>;

Identical class structure as HP-Socket's source code

名称: UDP 户端 Socket 监听器抽象基类 描述: 定义某些事件的默认处理方法 (忽略事件)
class CUdpClientListener : public IUdpClientListener
名称: UDP 客户端 Socket 监听器接口 描述: 定义 UDP 客户端 Socket 监听器的所有事件
class IUdpClientListener : public IClientListenerT<IUdpClient>
名称: 客户端 Socket 监听器接口 描述: 定义客户端 Socket 监听器的所有事件
template<class T> class IClientListenerT : public ISocketListenerT<T>

Figure 4. HP-Socket's class information embedded in CoolClient.

CoolClient supports the following capabilities:

- Uploading and deleting a file
- Tunneling packets
- Starting keylogging
- Sending port map information

The lack of arbitrary code execution in CoolClient suggests it is designed as a tunneling tool or stealer that attackers could use to gather information for further lateral movement.

CoolClient activity was distinct from PUBLOAD infections. However, we confirmed that the specific anti-disassembly technique used by the CoolClient loader samples we found is identical to that used by USBFect/HIUPAN. This supports our attribution of CoolClient activity to Stately Taurus, suggesting it was another attempt by the group to secure access.

CL-STA-1048 - Espionage Toolkit

The activity, tracked under CL-STA-1048, deployed a wide variety of tools with similar functionality. This pattern suggests that the threat actor behind CL-STA-1048 actively sought a payload that could bypass XDR. In the process of doing so, they inadvertently exposed a significant portion of their toolkit to our analysis.

On Aug. 9, 2025, we observed alerts originating from a Microsoft Edge process. Our investigation of this alert identified a DLL named mscorsvc.dll (SHA256: 1aa37a477c539edf25656a300002a28d4246ec83344422dd705b42d3443a2623) being loaded into memory via mscorsvw.exe.

We identified this DLL as a lightweight, TCP-based backdoor written in C, which we determined was [EggStremeFuel](#). While the initial execution vector for EggStremeFuel remains unknown, the subsequent activity was highly revealing, including the attempted deployment of several tools.

The following sections detail our analysis of these tools, starting with the initial identification of EggStremeFuel.

EggStremeFuel

During its initialization, EggStremeFuel encrypts embedded C2 configurations using RC4 and stores them in %APPDATA%\Microsoft\Windows\Cookies\Cookies.dat.

The configuration is structured as a key-value pair separated by two pound (#) symbols. An example of this is shown below:

```
dm:laichingte[.]net##ip:58.69.38[.]83##st:30##mp:443##mp:443##bp:5228##
```

EggStremeFuel imports this C2 configuration from Cookies.dat upon each execution, allowing for dynamic updates. It then starts its C2 communication with an initial check-in, sending the C2 server a random 16-byte session key and its MD5 hash.

The backdoor then encrypts and decrypts all C2 communication using RC4 with this session key. The backdoor supports the following capabilities:

- Uploading or downloading files
- Listing files or directories
- Starting or terminating a reverse shell
- Sending the current global IP address
- Getting, updating or overwriting the C2 configuration

Masol RAT

Twenty minutes after we observed the EggStremeFuel deployment, Cortex XDR detected another malicious payload on the same agent at the following path C:\Windows\System32\AxInstSVs.dll (SHA256 hash: 05995284b59ad0066350f43517382228f7eee63cd297e787b2a271f69ecf2dfc). We identified the second sample as Masol RAT, an HTTP-based Windows backdoor previously documented by [Sophos](#) and [Trend Micro](#) in 2024.

The sample recovered during this incident contained an embedded program database (PDB) path identical to the one Sophos and Trend Micro referenced: E:\Masol_https190228\x64\Release\Masol.pdb.

Masol RAT also has several overlaps with the Linux backdoor known as Backdr-NQ, which [Sophos reported in 2022](#). Both backdoors share a similar code flow, the same configuration decryption algorithm and the same backdoor commands.

The Masol RAT we observed in this incident is designed to be executed as a Windows service DLL and is not packed or obfuscated.

It communicates with its C2 servers over HTTP POST, encrypted by AES. Masol RAT features backdoor commands for the following activities:

- Executing arbitrary commands
- Getting or updating C2 configurations
- Uploading or downloading a file

EggStreme Loader

Concurrent with the deployment of Masol RAT, we detected other malware identified as [EggStreme loader](#) (aka EggStreme Agent or Goreme RAT) at C:\Windows\System32\XblAuthManagers.dll (SHA256: 6caa78943939bd7518f5e7eaa44fa778d0db8b822e260d7fe281cf45513f82d9). This finding aligns with [a Bitdefender blog post](#) detailing similar activity in Southeast Asia.

EggStreme loader is a multi-layered loader designed to launch a payload, Goreme RAT. EggStreme loader leverages multiple publicly available tools, such as [DarkLoadLibrary](#) and [libpeconv](#), to achieve an in-memory payload execution. Although Cortex XDR prevented the final payload from executing, our analysis suggests attackers attempted to deploy Goreme RAT, shown below in Figure 5.

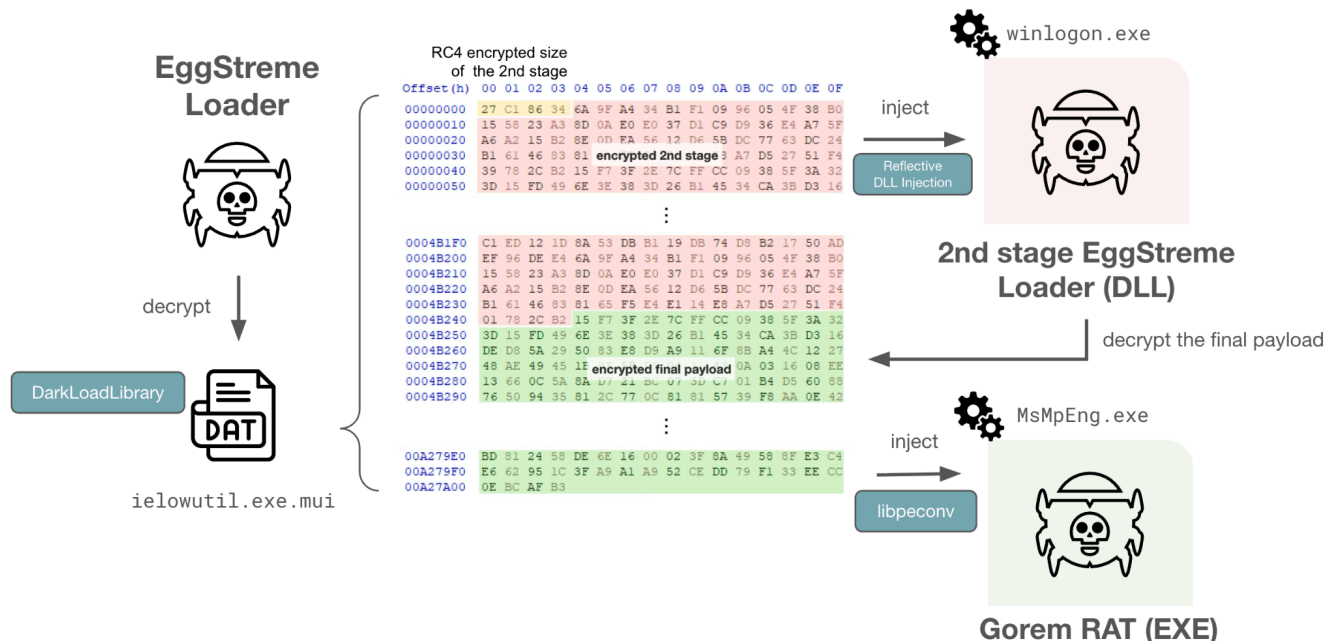


Figure 5. An overview of EggStreme Loader's execution flow.

This malware uses Google Remote Procedure Call (gRPC) for C2 communication. This method provides the malware with a wide array of functionalities through its backdoor commands. Furthermore, it acts as a launcher for a user-mode keylogger module.

The keylogger module performs the following activities:

- Capturing keystrokes, window titles, clipboard contents and network information
- Saving the output to the following path: %LOCALAPPDATA%\Microsoft\Windows\Explorer\thumbcache.dat

Gorem RAT incorporates a total of 59 backdoor commands, enabling various functionalities. Most backdoor commands are identical to the command Bitdefender reported. However, we observed a variant of Gorem RAT that implements a new feature to upload or download over Dropbox.

TrackBak

Finally, 40 minutes after the attackers attempted to deploy Masol RAT, we observed a malicious payload we have named TrackBak based on its log output filename. This payload masquerades as an MS Edge log file to track user activity history. (SHA256: 84e37e42312b9a502c40cf1f3fc181e3ebd4f3e35c58bbf182740dfe38d3b6b9)

TrackBak is an infostealer that performs the following activities:

- Collecting key logs
- Exfiltrating clipboard data
- Gathering network information
- Collecting files from drives

Attribution

There are a number of links between CL-STA-1048 and China-affiliated activity. In particular, the use of both [Masol RAT](#) and [EggStreme](#) was publicly reported in relation to China-affiliated activity, such as [Crimson Palace](#) and [Earth Estries](#).

Chinese threat groups often share tooling, as well as tactics, techniques and procedures (TTPs) with each other. As such, we cannot state with certainty whether these public reports relate to the same group.

CL-STA-1049 - Stealthy Loader and FluffyGh0st RAT Deployment

On Aug. 1, 2025, we identified yet another cluster of activity, which we track as CL-STA-1049. The attackers deployed a novel DLL loader to install [FluffyGh0st RAT](#). We named this malware Hypnosis loader.

FluffyGh0st RAT is associated with [Unfading Sea Haze](#) and overlaps with activity tracked by Sophos as [Crimson Palace](#).

Starting on Aug. 1, 2025, Cortex XDR generated multiple alerts related to suspicious files in the C:\Program Files\Common Files\Bitdefender\SetupInformation\ directory.

These alerts highlighted a DLL sideloading attack that used a legitimate Bitdefender executable, seccenter.exe. Alerts focused on three files associated with the Hypnosis loader activity that were dropped in the Bitdefender application directory are shown in Table 2.

SHA256 Hash	File Path	Malware
9d7c8d3bc4ac108fb2602424a1f4918c051c2443f0526bbb2c970c8e57dbd90d	C:\Program Files\Common Files\Bitdefender\SetupInformation\version.dll	Hypnosis loader
c774fd7373084f93383593f0a40f56c8a8b95b73e59cd4fc7117daa6b7441e73	C:\Program Files\Common Files\Bitdefender\SetupInformation\bdusersy.dll	Likely final payload
35ca351a831c67f0e0a658a186be0065043e0977cb70771c03a24b0523edcf30	C:\Program Files\Common Files\Bitdefender\SetupInformation\FILE_NAME\$.log	An additional malicious DLL masquerading as a log file

Table 2. Identified samples of malware from the Hypnosis loader activity.

Hypnosis Loader

Our analysis revealed that the malicious Hypnosis loader DLL is sideloaded by seccenter.exe. To prevent the seccenter.exe application that sideloaded the malicious Hypnosis loader DLL from crashing, all the DLL's exported functions are proxied to the legitimate version.dll file located in the Windows system directory.

Once side-loaded by the EXE, Hypnosis loader patches the DLL's host process entry point, redirecting execution to an infinite Sleep function. This ensures the main thread does not terminate while the malicious routine executes later, as shown in Figures 6 and 7.

```

v26 = *(unsigned int *)&modBaseAddr*(((int *)modBaseAddr + 0xF) + 0x28); // 0x28 = AddressOfEntryPoint
VirtualProtect(&modBaseAddr[v26], 0xCu, PAGE_EXECUTE_READWRITE, (PDWORD)&Buffer);
*(_QWORD *)&modBaseAddr[v26] = 0xB848;
*(_DWORD *)&modBaseAddr[v26 + 8] = 0xE0FF0000;
*(_QWORD *)&modBaseAddr[v26 + 2] = sub_7FF8F31A13E0;
VirtualProtect(&modBaseAddr[v26], 0xCu, (DWORD)Buffer.BaseAddress, (PDWORD)&Buffer);

```

Figure 6. Hypnosis loader's code to patch the DLL's host process entry point.

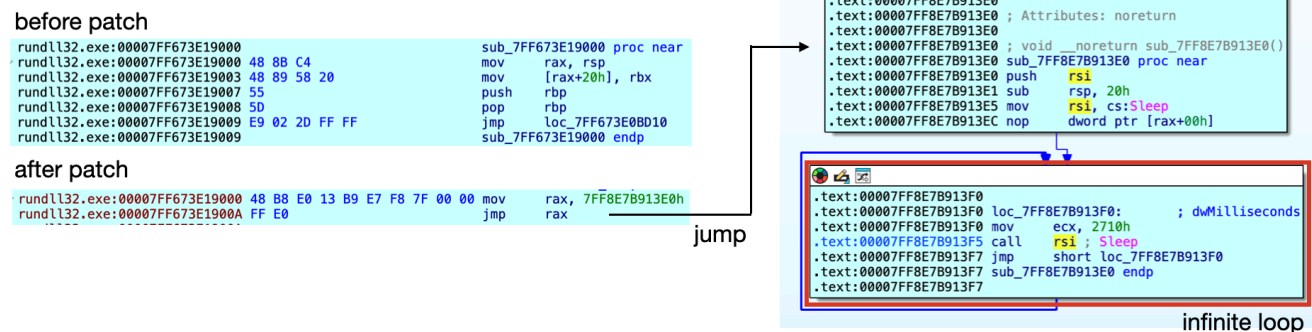


Figure 7. Disassembled instructions showing the patched DLL host process code.

After patching the DLL's host process, Hypnosis loader creates a new thread to decrypt the name of the final payload (bdusersy.dll) with an RC4 key and loads it using the LoadLibrary API.

Initial Analysis of the Final Payload

Based on our analysis of Hypnosis loader (version.dll), the file named bdusersy.dll is likely the final payload. However, we could not recover this sample. Our telemetry revealed the bdusersy.dll file communicated with a server at webmail.rpcthai[.]com. The base domain rpcthai[.]com appears to be used for the website of a legitimate Thai-based company, which implies that attackers hijacked the domain and created webmail.rpcthai[.]com to act as a C2 server.

Looking for other related samples communicating to this domain, we found a DLL file with the SHA256 hash

34bf325492614dd4d842ec24f22a402ab73908cb91a74846945eae4775290ff2. This DLL's imphash value 0bf0bd027fda34d4afa5f86b6340019 leads to two payloads on VirusTotal uploaded in 2024:

- SHA256 hash: [f07b2af21e3fab6af5166a44ca77ed0ebc7c9a3e623202a63d4c4492abce8d65](#)
- SHA256 hash: [58ed0463d4cb393cd09198a6409591b39cae06bb0ba5f5d760186de88410f6b8](#)

Our analysis revealed that these payloads were FluffyGh0st. Sophos referenced the second sample in a report on a [Chinese espionage campaign called Crimson Palace](#).

\$FILE_NAME\$.log and Its Relationship to the Final Payload

The file named \$FILE_NAME\$.log is a DLL file. Advanced WildFire analysis revealed this DLL file has an embedded network configuration pointing to webmail.homesmountain[.]com, which matches the domain structure of the C2 server that the likely final payload bdusersy.dll communicated with.

With its imphash value 511898b2f71f31932dfb3ee06e904289, we identified additional samples that we also attributed to FluffyGh0st:

- SHA256 hash: [4e26aa1bb28874f0897ab9a08e61d4b99caaa395fe63cbe4398f7297371e388c](#)
- SHA256 hash: [11c7728697d5ea11c592fee213063c6369340051157f71ddc7ca891f5f367720](#)

The 11c7728697d5ea11c592fee213063c6369340051157f71ddc7ca891f5f367720 sample is contained in a [ZIP archive file that was submitted to VirusTotal](#). This ZIP archive also contained a [sample of Hypnosis loader](#).

Given the overlaps of bdusersy.dll with FluffyGh0st and our discovery of the ZIP archive with both Hypnosis loader and FluffyGh0st, it is plausible that the bdusersy.dll discovered is FluffyGh0st.

FluffyGh0st

FluffyGh0st is a custom version of the publicly available Gh0st RAT, which [Bitdefender first reported in 2024 \[PDF\]](#). Bitdefender attributed this malware to a China-aligned threat actor that they call Unfading Sea Haze.

FluffyGh0st is designed to allow the attacker to manipulate the system via remote access, but its full capabilities require additional plugins. It downloads these plugins from C2 servers embedded in the sample, which are encrypted with RC4 and compressed using LZNT1, before attempting to execute the export function InstallPlugin.

Attribution

Although we did not observe direct evidence linking CL-STA-1049 with CL-STA-1048 during this incident, these clusters may be part of the Crimson Palace campaign. CL-STA-1049 is likely associated with the group Bitdefender called Unfading Sea Haze, and some of its tooling overlaps with [Cluster Bravo of Crimson Palace](#). CL-STA-1048 is potentially linked to [Cluster Charlie of Crimson Palace](#), based on its use of FluffyGh0st.

Conclusion

Between June and August 2025, attackers targeted a Southeast Asian government entity with a persistent cyberespionage campaign involving three distinct clusters of activity. One cluster we've attributed to Stately Taurus, and the other two we have designated as CL-STA-1048 and CL-STA-1049. The convergence of these activity clusters, all of which show links to known China-aligned actors, points to a coordinated effort to achieve a common strategic goal.

The attackers' methodology indicates they intended to gain long-term, persistent access to sensitive government networks, not just to cause disruption. These well-resourced adversaries used diverse tool sets, including Stately Taurus's USB propagation, CL-STA-1048's multi-payload strategy and CL-STA-1049's stealthy FluffyGh0st RAT. Their primary goal was to continuously locate and exfiltrate data, as evidenced by the deployment of infostealers and comprehensive backdoors.

Palo Alto Networks Protection and Mitigation

Palo Alto Networks customers are better protected from the threats discussed above through the following products and services:

- The [Advanced WildFire](#) machine-learning models and analysis techniques have been reviewed and updated in light of the indicators shared in this research.
- [Advanced URL Filtering](#) and [Advanced DNS Security](#) identify known domains and URLs associated with this activity as malicious.
- [Cortex XDR](#) and [XSIAM](#) can help prevent the threats described in this article by employing the [Malware Prevention Engine](#). This approach combines several layers of protection, including [Advanced WildFire](#), Behavioral Threat Protection and the Local Analysis module, designed to prevent both known and unknown malware from causing harm to endpoints.

If you think you may have been compromised or have an urgent matter, get in touch with the [Unit 42 Incident Response team](#) or call:

- North America: Toll Free: +1 (866) 486-4842 (866.4.UNIT42)
- UK: +44.20.3743.3660
- Europe and Middle East: +31.20.299.3130
- Asia: +65.6983.8730
- Japan: +81.50.1790.0200
- Australia: +61.2.4062.7950
- India: 000 800 050 45107
- South Korea: +82.080.467.8774

Palo Alto Networks has shared these findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the [Cyber Threat Alliance](#).

Indicators of Compromise

SHA256 Hashes

- 05995284b59ad0066350f43517382228f7eee63cd297e787b2a271f69ecf2dfc
- 07bd506d2a8db98c2478ac11bb6c46d84f1aa84f4a9af643804ed857ad7399c3
- 11c7728697d5ea11c592fee213063c6369340051157f71ddc7ca891f5f367720
- 1aa37a477c539edf25656a300002a28d4246ec83344422dd705b42d3443a2623
- 21fe238c462b2f22a7e97f1f06e4f12e8c6e5f3a6ffe671b671909b501fa537
- 2616dfadf8aa222303269eb7202c75e2a8fc5b05b6b63ae2cb7576b9a27733f9
- 29d4cc64c7c9b7ecd16d96e9c6dcde1fe22a4c2d202074aadf41cbcef494bc19
- 34bf325492614dd4d842ec24f22a402ab73908cb91a74846945eae4775290ff2
- 4b29b74798a4e6538f2ba245c57be82953383dc91fe0a91b984b903d12043e92
- 4e26aa1bb28874f0897ab9a08e61d4b99caaa395fe63cbe4398f7297371e388c
- 58ed0463d4cb393cd09198a6409591b39cae06bb0ba5f5d760186de88410f6b8
- 6745422717f0ccdf2ae3330d133945268d4cd21215adc982400d82b38ebeeca
- 6caa78943939bd7518f5e7eaa44fa778d0db8b822e260d7fe281cf45513f82d9
- 6f4f76c7a2638087a0da6002cd2c76d1673305b1e850a1f4068f14755f59d45b
- 74e7093615da36b28effb3aa6eef5a31e7ea59627bd619b488f087091e8d65e9
- 835795aa494021752f21fbef63c81227c1b934437a02aa1f2a258c9f60b0b7a3
- 83f06fa37f1136f765f799851812f11060ab34df3b34bc61777acc59a30b4c6e
- 84e37e42312b9a502c40cf1f3fc181e3ebd4f3e35c58bbf182740dfe38d3b6b9
- 851d57a2bf514202f54dafa1eb83a862653be7512b6e9535914b8d1d719d495f
- c47d55ad95a6c6ffac45c2b205e03bddadf5e36f55988599053b1fd0e49448a5
- d4d753c6ea5c86a44c9a65cd0d4eaeabb072b19e0ef68ef7da3a879f689772c9
- e1672dab0daf1c84f14f7bb827851c27753da067490e10cd6144fe7873892fec
- e61a1f4269e934481f6cb19576b3dbc434952b01445fd4e1ebc6906a1b449ef8
- e9b52577091c8e25e91c485216de34d5a26ab707a10b1e5cd31ed7aa055939d3
- f07b2af21e3fab6af5166a44ca77ed0ebc7c9a3e623202a63d4c4492abce8d65
- f62223c9750fb2edfd979a8cae204cb9ce5e0950b52a47b62f195cd05dd3e2fb

IPv4 Addresses

- 103.15.29[.]17
- 103.131.95[.]107
- 103.122.164[.]106
- 109.248.24[.]177
- 120.89.46[.]135

Domains

- distriyy[.]net
- fikksvex[.]com
- laichingte[.]net
- popnike-share[.]com
- shepinspect[.]com
- theuklg[.]com
- webmail.homesmountain[.]com
- webmail.rpcthai[.]com

Additional Resources

- [Deep Dive Into Unfading Sea Haze: A New Threat Actor in the South China Sea](#) – Bitdefender
- [Crimson Palace returns: New Tools, Tactics, and Targets](#) – Sophos
- [Stately Taurus Activity in Southeast Asia Links to Bookworm Malware](#) – Unit 42, Palo Alto Networks
- [Earth Preta Evolves its Attacks with New Malware and Strategies](#) – TrendMicro
- [HoneyMyte updates CoolClient and deploys multiple stealers in recent campaigns](#) – SecureList