

Toneshell Backdoor Used to Target Attendees of the IISS Defence Summit

Published: 2024-09-03 · Archived: 2026-04-02 12:26:47 UTC

The ToneShell backdoor, frequently associated with **Mustang Panda** (also known as Stately Taurus and Earth Preta, among other monikers), has been consistently deployed against government organizations, mainly in Southeast and East Asia, for cyber espionage.

Recently, this malware has resurfaced, likely targeting attendees of the 2024 **International Institute for Strategic Studies (IISS) Defence Summit** in Prague.

This campaign illustrates how cyber espionage and international strategy often intertwine as nations seek to infiltrate sensitive security and defense discussions to gain a strategic edge amid global conflicts, from the Russia-Ukraine war to rising tensions in the South China Sea.

While combing through files on Hatching Triage, one name stood out, prompting us to investigate further and share our findings in this article.

This blog post will explore our findings, including the malware's execution techniques, capabilities, and the [command and control \(C2\) infrastructure](#) that facilitates its operations.

The IISS Defence Summit: An Attractive Target for Cyber Espionage

The IISS Prague Defence Summit, scheduled for November 8-10, 2024, is a new event modeled after the successful Shangri-La and Manama Dialogues. The summit is poised to become a central forum for discussing defense and security within the Euro-Atlantic region.

Attendees include senior political leaders, defense ministers, policymakers, and industry executives from Europe, the United States, and allied nations. Discussions include defense capacity-building, strategic stability, and emerging threats.

This summit is a prime target for cyber espionage due to the participation of high-level officials discussing sensitive issues like military strategy, defense cooperation, and responses to geopolitical tensions. Accessing these discussions offers adversaries a strategic edge by exposing major global players' defense plans and policies.

File Discovery In Triage & ANY.RUN

During routine analysis on Hatching Triage, we discovered an executable file, "**IISS PRAGUE DEFENCE SUMMIT (8 – 10 November 2024).exe**," uploaded on 16 August. Given its relevance to an upcoming high-profile event, we decided to investigate further.

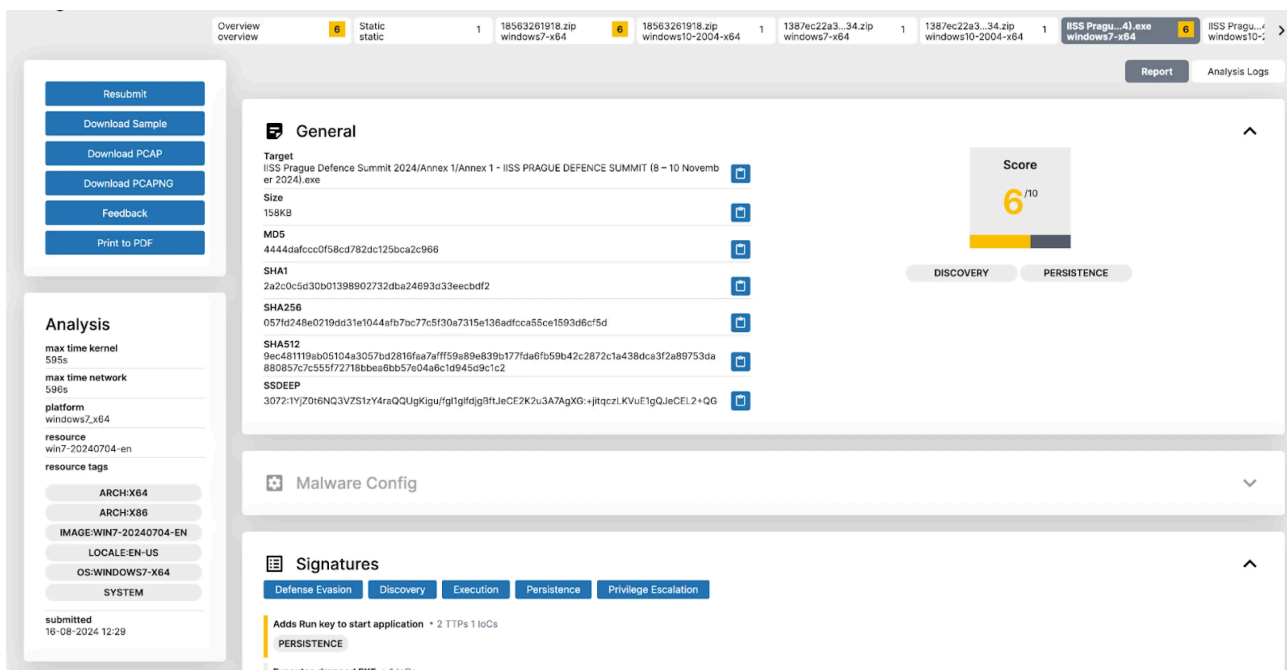


Figure 1: Hatching Triage Sandbox Analysis of suspicious EXE (Source/Link: [Triage](#))

To further solidify our suspicions, a review of the PCAP containing network traffic confirmed the malware communicating with its C2 server using the familiar magic bytes 17 03 03.

These bytes often appear in posts and reports as indicators of Toneshell and PubLoad activity.

We found the same executable file on [ANY.RUN](#), where it exhibited similar TTPs.

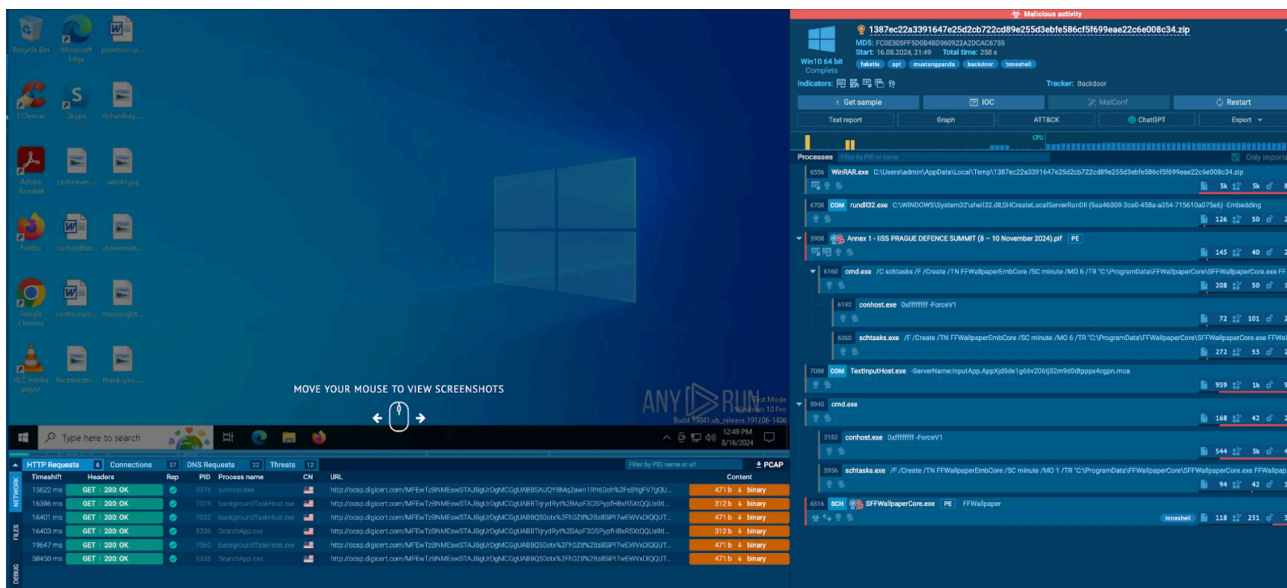


Figure 2: ANY.RUN analysis of the IISS-themed executable. (Source/Link: [ANY.RUN](#))

Decoy Document Analysis

Before diving into the malware itself, let's first examine the decoy PDF used in this attack. Upon extracting the archive, the user is presented with two folders: **Annex 1** and **Annex 2**.

The first folder contains the executable file mentioned above, while the second, contains the document seen in Figure 3 titled “Annex 2 - IISS PRAGUE DEFENCE SUMMIT (8 – 10 November 2024) - Copy.pdf.”



Figure 3: Document posing as an agenda for the upcoming IISS Defence Summit

The PDF is an exact copy of a legitimate document available on the IISS official website, with only its name altered. This tactic is designed to reassure the target by displaying a genuine agenda for the summit, reducing suspicion while the malware silently operates in the background.

Uncovering Malware Behavior and Execution

As previously mentioned, the extracted ZIP file reveals two folders. We'll now turn our attention to the suspicious file that caught our eye.

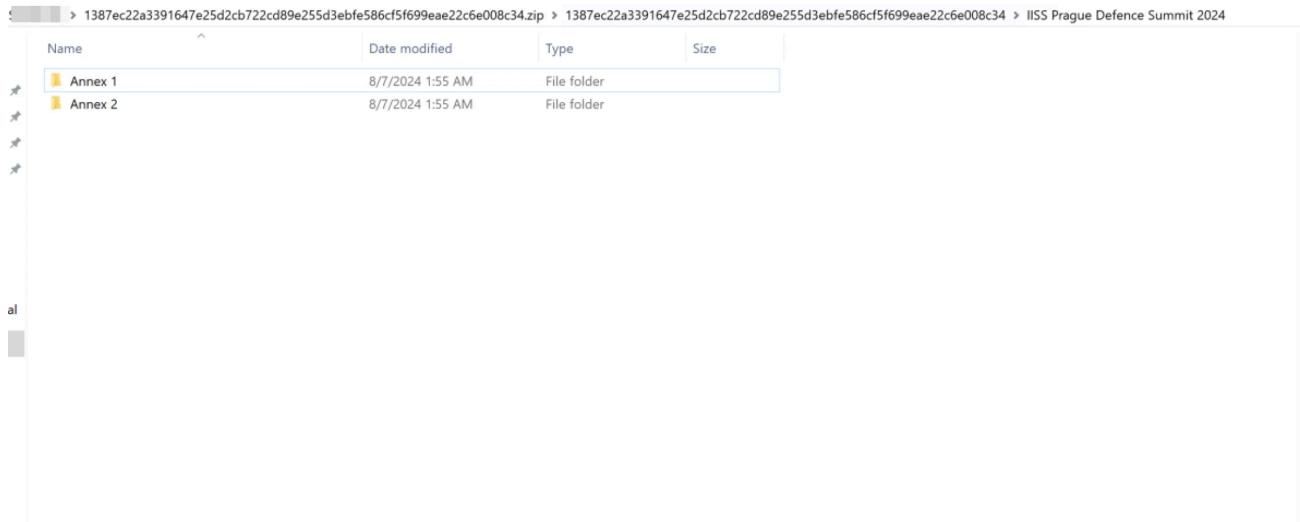


Figure 4: Annex 1 & 2 folders after extracting the zip contents

Inside the Annex 1 folder (Figure 5), we see a file name matching that of what we found in Triage. For the keen-eyed, you may have noticed the file type is "Shortcut to MS-DOS Program," which suggests it is a program information file (PIF).

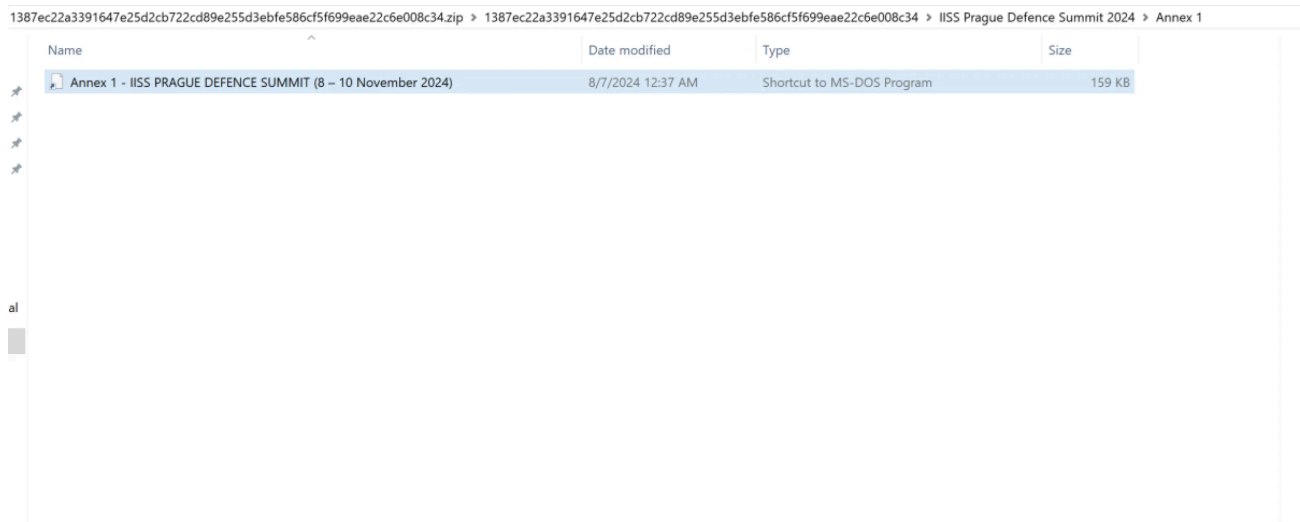


Figure 5: PIF-file masquerading as IISS agenda file

PIF files are shortcuts designed to provide metadata like a config file for MS-DOS programs. However, threat actors can use them as an alternative to .exe files to execute malicious code.

The PIF file acts as a dropper, which we'll soon see, and is signed by the "Hefei Nora Network Technology Co." A screenshot of the code signing certificate is below.

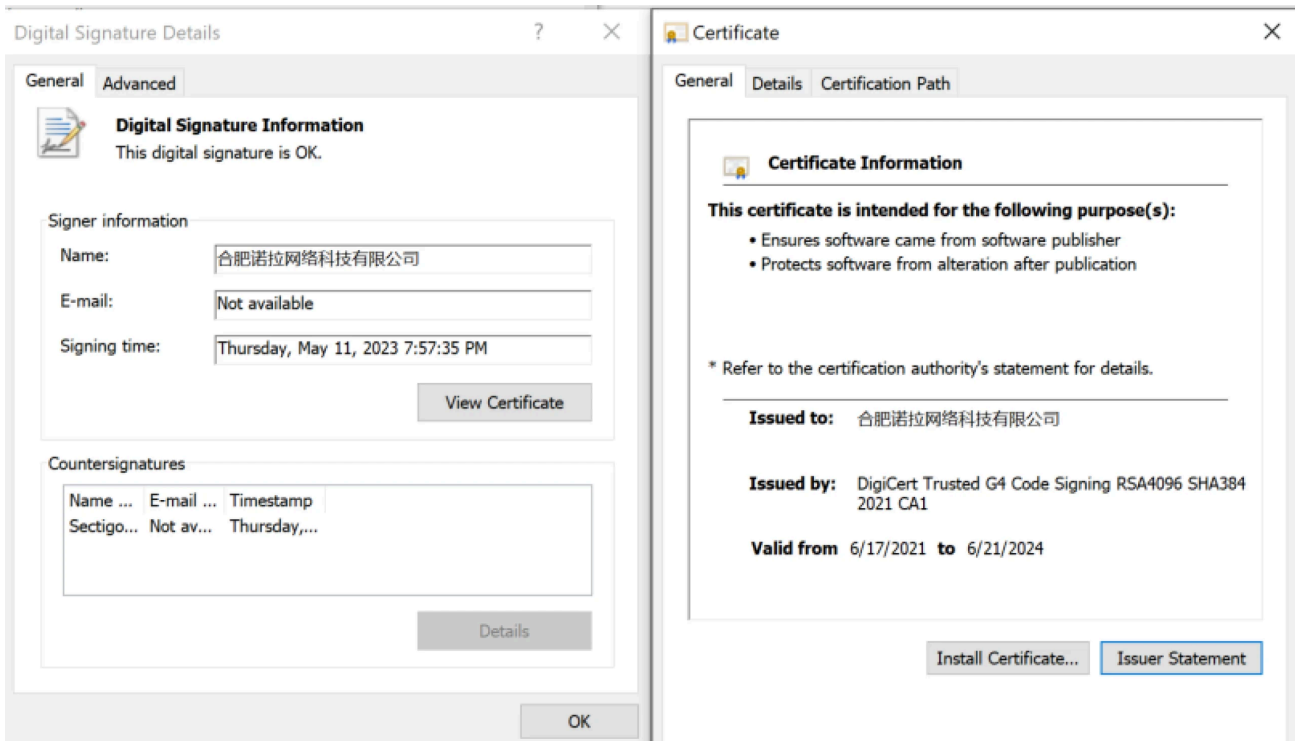


Figure 6: Codesigning certificate used for the malicious PIF-file

Analyzing the file in VirusTotal reveals the PIF-file has two aliases: **fhbemb.exe** and **SFFWallpaperCore.exe**.

This file also contains a PDB path of:

G:\CLIENT\fhbemb\src\bin\Release_NL\fhbemb.pdb

In our research, we were unable to locate information suggesting either of the above file names (fhbemb.exe and SFFWallpaperCore.exe) are legitimate Windows programs.

An April 2024 blog post by [secrss](#) uncovered a suspected **APT-Q-27** (aka Golden Eye Dog, Dragon Breath) operation that also used 'fhbemb.exe' to side load 'libemb.dll' to execute a modified version of Gh0st RAT.

[Sophos](#) has also previously reported similar DLL sideloading techniques by this group.

Figure 7 illustrates the malware execution flow as detailed in the Secrss post.

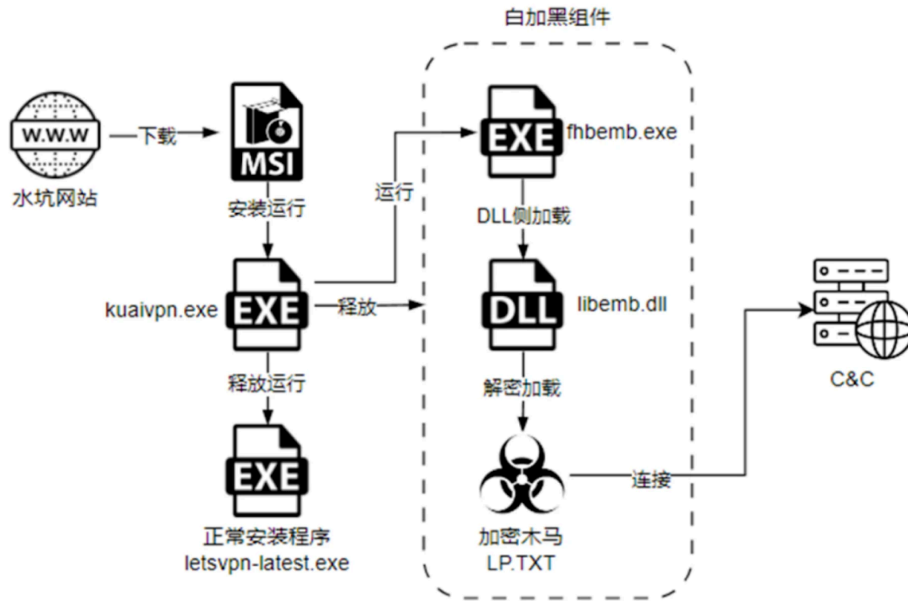


Figure 7: Secrss attack process diagram using similarly named files (Source: [Secrss](#))

Returning to the malicious PIF, upon execution, it checks for the presence of the FFWallpaperCore directory in C:\ProgramData. If the directory is absent, it drops SFFWallpaperCore.exe and libemb.dll, likely to verify whether the system has already been compromised.

Persistence is established by adding a registry run key and creating a scheduled task.

- Registry run key:

```
cmd.exe /C schtasks /F /Create /TN FFWallpaperEmbCore /SC minute /MO 6 /TR
"C:\ProgramData\FFWallpaperCore\SFFWallpaperCore.exe FFWallpaper"
```

- Creation of scheduled task

```
schtasks /F /Create /TN FFWallpaperEmbCore /SC minute /MO 6 /TR
"C:\ProgramData\FFWallpaperCore\SFFWallpaperCore.exe FFWallpaper"
```

The overall execution flow (**Figure 8**) follows a rather standard pattern commonly seen in malware operations.

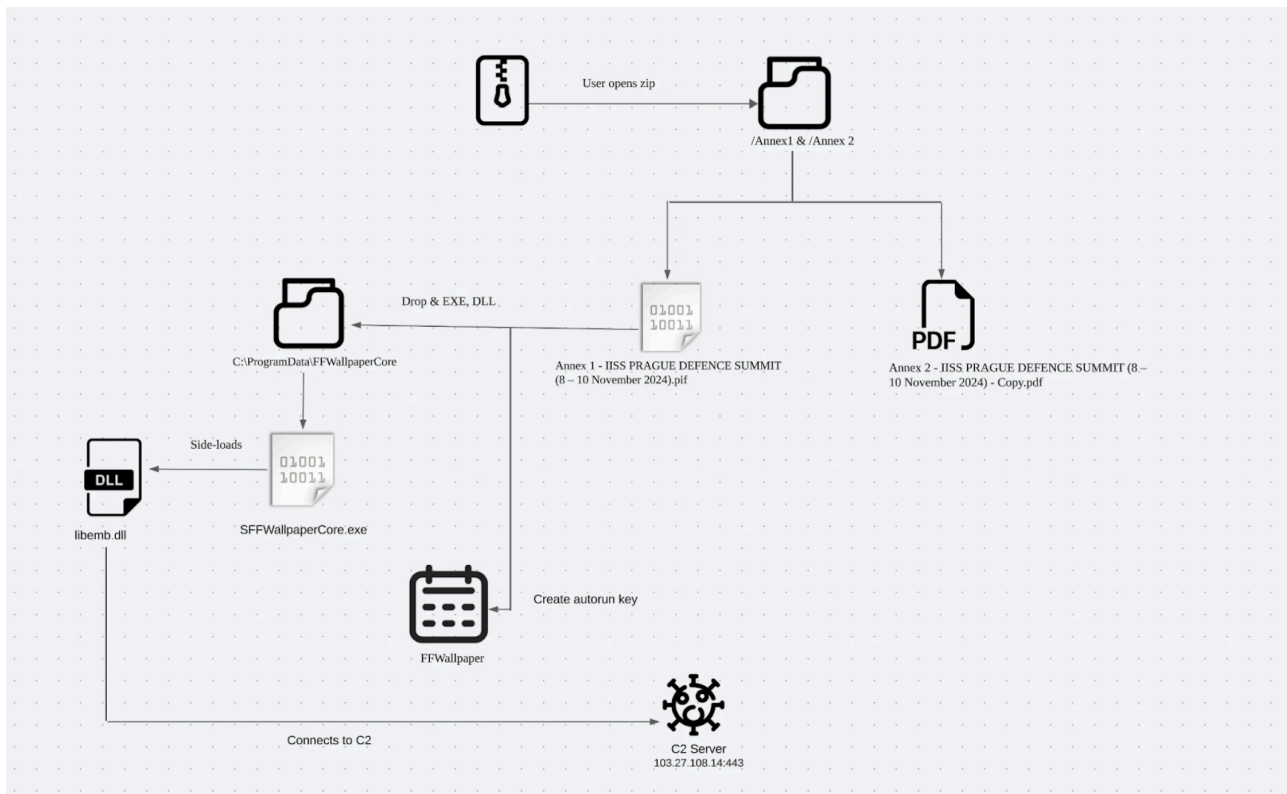


Figure 8: PIF event flow (Created using Lucidchart)

libemb.dll, written in C++, is signed by the same company as the EXE, but, as shown in Figure 9, the certificate is not trusted.

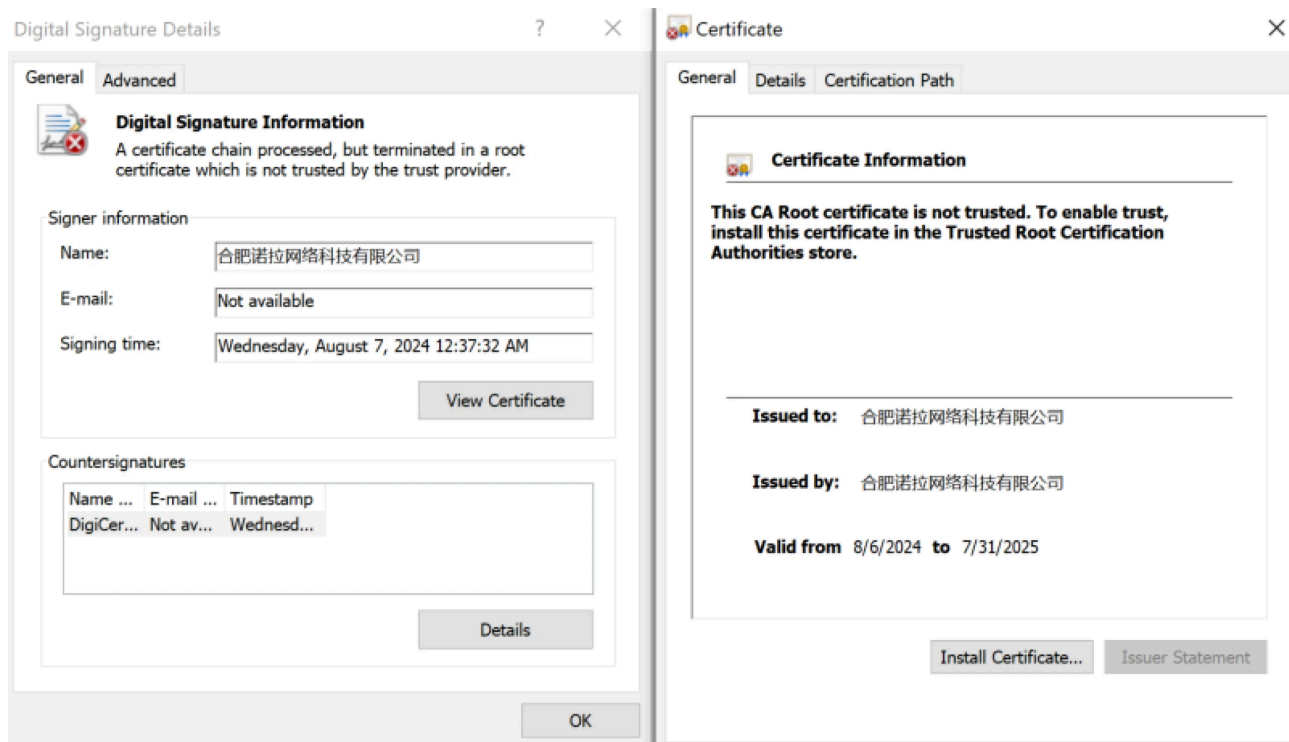


Figure 9: Untrusted codesigning certificate for libemb.dll

The DLL contains unique debug strings, which have become a hallmark of Mustang Panda malware. Within the file, we found two references to Twitter/X accounts: @Rainmaker1973 and @techyteachme, the latter belonging to Zack Allen,

who also runs a great Detection Engineering newsletter if you're interested.

```
1
2 undefined4 SetupAndEnumWindowProps(void)
3
4 {
5     SIZE_T _Size;
6     PROPENUMPROCEXW lpEnumFunc;
7     HWND hwnd;
8     void *local_c;
9     SIZE_T local_8;
10
11     local_c = (void *)0x0;
12     local_8 = 0;
13     ValidateAndProcessData(&local_c,&local_8);
14     _printf("Start...buitengebieden\n");
15     DisplayTimedDebugMessages();
16     _printf("ZackAllen.....techyteachme Ok\n");
17     _Size = local_8;
18     lpEnumFunc = (PROPENUMPROCEXW)VirtualAlloc((LPVOID)0x0,local_8,0x3000,0x40);
19     if (lpEnumFunc != (PROPENUMPROCEXW)0x0) {
20         FID_conflict:_memcpy(lpEnumFunc,local_c,_Size);
21         hwnd = GetTopWindow((HWND)0x0);
22         EnumPropsExW(hwnd,lpEnumFunc,0);
23     }
24     return 0;
25 }
26
```

Figure 10: Unique strings including the X account name for Zack Allen. Also notice the string before “buitengebieden,” which is Dutch for “outlying areas.”

```
1
2 void DisplayTimedDebugMessages(void)
3
4 {
5     int iVar1;
6     clock_t cVar2;
7     clock_t cVar3;
8     int iVar4;
9     |
10    iVar4 = 0;
11    do {
12        iVar1 = iVar4 + 1;
13        _printf("Massimo %d Jmpv...\n",iVar1);
14        cVar2 = _clock();
15        do {
16            cVar3 = _clock();
17        } while (cVar3 < cVar2 + 5000);
18        _printf("Rainmaker1973 %d c?\n",iVar1);
19        if (iVar4 < 3) {
20            _printf("\n");
21        }
22        iVar4 = iVar1;
23    } while (iVar1 < 4);
24    return;
25 }
26
```

Figure 11: Debug strings for X user Rainmaker1973

A network connection is established with the C2 server at 103.27.108.]14 on port 443. The traffic uses raw TCP but mimics TLS to evade detection.

This approach has been observed in multiple reports on Mustang Panda activity, specifically linked to ToneShell and Pubload malware.

Below is a PCAP screenshot from the initial communication with the C2 server.

```
00000000 17 03 03 00 1d 5f 5f ae 98 46 d7 c9 5c 65 36 11 ....._.F..\e6.
00000010 77 54 10 66 29 47 7f 30 36 4a 24 01 1a 1e 7f 24 wT.f)G.0 6J$....$
00000020 1b 6c .l
00000000 17 03 03 2c 29 53 24 5e 73 7e 24 c2 9c c1 09 8c ...,)S$^ s~$. ....
00000010 8d 49 d0 4b 63 00 33 7c 7c 06 60 01 7b 7a 12 4d .I.Kc.3| |.`. {z.M
00000020 75 6c 4e 03 59 55 2d 5e 73 7e 07 50 18 20 13 6f ulN.YU-^ s~.P. .o
00000030 4b 79 c0 8d 46 96 28 12 d2 0b 89 e6 f8 c0 c9 8d Ky..F.(. ....
00000040 52 59 87 fa bc cb 8b 87 b6 41 30 a8 f5 43 04 b1 RY..... .A0..C..
00000050 7d db e8 b8 ef b0 b7 e9 d3 54 f0 7f 07 e6 f3 ed }..... .T.....
00000060 6f 0e d0 5f b6 27 65 73 d3 64 65 e2 44 cf 8e 55 o...'.es .de.D..U
00000070 2e 26 fc e1 59 90 20 c2 f8 6c 49 df 85 42 82 91 .&..Y. . .lI..B..
00000080 9e e4 26 2a 73 70 3a 32 db 25 de 5e b8 3a 9e 83 ..&*sp:2 .%.^.:...
00000090 5f 69 75 8a 8a e5 a0 2e ad eb bf bf 8b 82 16 9b _iu.....
000000A0 5b 3e de 4a e7 5a 81 3a f4 5b 00 10 b0 1c 9d bb [>.J.Z.: .[.....
000000B0 4e cd 65 51 ef dc 5c 73 78 37 75 63 e5 26 64 78 N.eQ..\s x7uc.&dx
000000C0 1d 0e ce dd 30 42 41 7d cd fa e6 9b 8b 86 38 7d ....0BA} .....8}
000000D0 08 20 0d de 21 5d c8 26 e3 92 dc 0c df ee 4f ae . .!.].& .....0.
000000E0 2f 7f ac bf 54 f9 49 03 88 d0 56 b5 ab 2f c1 ca /...T.I. ..V../..
000000F0 34 55 01 d0 90 37 e2 61 9b 9d 32 50 a6 a1 25 84 4U...7.a ..2P..%.
00000100 68 eb 50 26 4e 39 85 05 aa 5d 6f aa 7a be a0 f2 h.P&N9... ]o.z...
00000110 71 1c 4d 3f 72 eb 91 ec 5f b8 e4 84 b6 9c bc 1f q.M?r... _.....
00000120 e5 c6 b5 6b 7f 7c 07 f0 21 ee 24 49 d1 2d 82 dd ...k.|.. !.$.I.-...
00000130 81 c2 92 7c 54 c1 26 9b e7 5c bb dc a0 2f 9e 27 ...|T.& .\.../.'
00000140 4c 42 6b 53 40 33 6b 51 df e6 5a 87 b2 8b 17 e0 LBkS@3kQ ..Z.....
00000150 d3 c6 a7 d8 35 d1 4b 57 4b c7 7d e6 e0 28 cb 8c ....5.KW K.}..(..
00000160 66 5b 9f 0a be c6 7f 03 54 15 95 7b 00 54 c6 e8 f[..... T..{.T..
00000170 fa de 9f 7e a5 d1 0f 42 90 ab 0f dd fc bb fb 54 ...~...B .....T
00000180 a8 49 51 6f f1 ba b1 36 4a 58 42 2c 63 b2 50 9b .IQo...6 JXB,c.P.
00000190 32 fc 73 b8 f2 5c dc 0e 34 2b c0 1b 19 e4 d7 e5 2.s..\.. 4+.....
000001A0 27 69 43 93 8d fb 7f 09 15 30 83 9d 74 f6 0c 4d 'iC..... .0..t..M
000001B0 4b 38 fe cf 82 ab a0 2e 2e 96 43 bf 72 1e ea 65 K8..... ..C.r...e
000001C0 24 c1 57 65 1b b9 84 33 a5 d0 3f ec b0 d3 1d ea $.We...3 ..?.....
```

Figure 12: Request header containing the magic bytes “17 03 03”

Network Infrastructure

The command and control server is hosted on Topway Global Limited’s ASN in Hong Kong, with ports **80**, **443**, and **3389** accessible. Interestingly, the IP briefly presented a self-signed RDP certificate at the start of August, carrying the common name “**WIN-USLKI5BA743**.”

Using RDP certificates has been a reliable method for tracking Mustang Panda’s infrastructure in the past, but recent variations suggest the threat actors are aware of this detection technique and are adjusting accordingly.

This particular certificate was issued on **Wednesday, August 25, 2021, at 03:36:30**—a detail that may prove significant in our investigation.

Below is a screenshot from Hunt showing this certificate, along with historical TLS data, to aid in identifying related activity.

Home > SSL History for 103.27.108.14

103.27.108.14 - Overview

Info Domains History (Beta) Associations **SSL History** SSH History JARM Port History Signals Activity

ASN AS132883	ASN Name TOPWAY GLOBAL LIMITED	Company Wah Tat Industrial Centre,Block C, 8-10 Wah Sing Road,Kwai Chung,Kowloon,HK	Region Kwai Tsing	Country HK
-----------------	-----------------------------------	--	----------------------	---------------

Last Seen	First Seen	IP	Ports	SubjectCommonName	IssuerOrganization
2024-08-01 3 weeks ago	2024-08-01 3 weeks ago	103.27.108.14	3389	WIN-USLK15BA743	Certificate Details Certificate IPs
2024-04-03 4 months ago	2024-03-30 4 months ago	103.27.108.14	443		Certificate Details Certificate IPs
2022-10-26 1 year ago	2022-10-26 1 year ago	103.27.108.14	8080	wiza.stark.io	Wiza-Stark Certificate Details Certificate IPs

Figure 13: SSL History data in Hunt showing the short-lived RDP certificate

With no additional domains or certificates to pivot on, we turn to Hunt's Advanced Search feature to identify servers using the same certificate, focusing specifically on the 'Not Before' date and time.

By applying the query shown in **Figure 14**, we narrowed the results to just seven servers—suggesting a potential link to the associated infrastructure. Notably, three of these servers were first observed only a few days ago, indicating recent and potentially active use at the time of writing.

Advanced Search ?

Certificates ▼ Search

Examples: [CobaltStrike in the past 7 days](#) ↔

Total count: **7**

IP	Ports	Sha256 Hash	SeenFirst	SeenLast
137.220.251.44	3389	60286C8A1E495AEC7062DE8E8EB644CE39CA30C4D9B5B117C12A1F486C0C3FF7(15)	2024-08-17 03:49:37	2024-08-17 03:49:37
45.115.236.142	3389	60286C8A1E495AEC7062DE8E8EB644CE39CA30C4D9B5B117C12A1F486C0C3FF7(15)	2024-07-17 02:10:28	2024-08-26 03:36:28
43.246.209.139	3389	60286C8A1E495AEC7062DE8E8EB644CE39CA30C4D9B5B117C12A1F486C0C3FF7(15)	2024-02-24 16:56:12	2024-08-26 13:33:15
103.27.109.206	3389	60286C8A1E495AEC7062DE8E8EB644CE39CA30C4D9B5B117C12A1F486C0C3FF7(15)	2024-08-27 12:33:38	2024-08-27 12:33:38
103.27.109.52	3389	60286C8A1E495AEC7062DE8E8EB644CE39CA30C4D9B5B117C12A1F486C0C3FF7(15)	2024-08-27 12:37:01	2024-08-27 12:37:01
103.43.16.65	3389	60286C8A1E495AEC7062DE8E8EB644CE39CA30C4D9B5B117C12A1F486C0C3FF7(15)	2024-03-16 18:11:13	2024-08-26 03:48:38
45.115.236.143	3389	60286C8A1E495AEC7062DE8E8EB644CE39CA30C4D9B5B117C12A1F486C0C3FF7(15)	2024-07-11 02:05:03	2024-08-17 03:44:37

1 of 1

Figure 14: Results of the search for servers hosting RDP certificates bearing the same not before date

IPs sharing the same certificate:

IP Address	ASN	Location
43.246.209.139	Topway Global Limited	HK
45.115.236.142	Topway Global Limited	HK
45.115.236.143	Topway Global Limited	HK
103.27.109.52	Topway Global Limited	HK
103.27.109.206	Topway Global Limited	HK
103.43.16.65	Topway Global Limited	HK
137.220.251.144	Topway Global Limited	JP

As shown in the table above, nearly all the IP addresses reside on the same ASN as the C2 server, with one exception. Additionally, the proximity of these IPs to each other strengthens our assessment that these servers may be controlled by the same threat actor or group and hosted within a similar or adjacent range to maintain operational control and flexibility.

Notably, the C2 IP has not yet been flagged as malicious by any vendors on VirusTotal.

Final Thoughts

While sandbox runs and dynamic analysis of the malware did not reveal the specific objectives of the threat actors once they gained access to infected systems, we can hypothesize that targeting a defense summit suggests an intent to gather intelligence on sensitive discussions.

To mitigate such threats, Hunt recommends conducting regular phishing awareness exercises for all users, closely verifying email senders and domain names before downloading files, and deploying an endpoint detection and response solution to identify malicious execution patterns.

If you'd like to stay ahead of threats like those uncovered in this post, [request a demo](#) today to see how our tools can enhance your defenses.

Network Observables

IP Address	ASN	Ports	Certificate Common Name	Notes
103.27.108.114	Topway Global Limited	80, 443, 3389	WIN-USLKI5BA743	C2

Host Observables

File Name	SHA-256 Hash	Notes
IISS Prague Defence Summit 2024.zip	1387ec22a3391647e25d2cb722cd89e255d3ebfe586cf5f699eae22c6e008c34	Lure document
Annex 1 - IISS PRAGUE DEFENCE SUMMIT (8 – 10 November 2024).pif	057fd248e0219dd31e1044afb7bc77c5f30a7315e136adfcca55ce1593d6cf5d	Legit, modified executable meant to trick users. Drops a PE and DLL containing ToneShell.
Annex 2 - IISS PRAGUE DEFENCE SUMMIT (8 – 10 November 2024) - Copy.pdf	901d713d4d12afbcee5e33603459ebc638afd6b4e2b13c72480c90313b796a66	Decoy PDF document.
SFFWallpaperCore.exe	057fd248e0219dd31e1044afb7bc77c5f30a7315e136adfcca55ce1593d6cf5d	Dropped immediately upon

File Name	SHA-256 Hash	Notes
		execution of Annex 1 - IISS PRAGUE DEFENCE SUMMIT (8 – 10 November 2024).pif
libemb.dll	f8e130e5cbbc4fb85d1b41e1c5bb2d7a6d0511ff3b224eb3076a175e69909b0d	Dropped immediately upon execution of Annex 1 - IISS PRAGUE DEFENCE SUMMIT (8 – 10 November 2024).pif

Source: <https://hunt.io/blog/toneshell-backdoor-used-to-target-attendees-of-the-iiss-defence-summit>