ToneShell Backdoor Used to Target Attendees of the IISS Defence Summit

hunt.io/blog/toneshell-backdoor-used-to-target-attendees-of-the-iiss-defence-summit

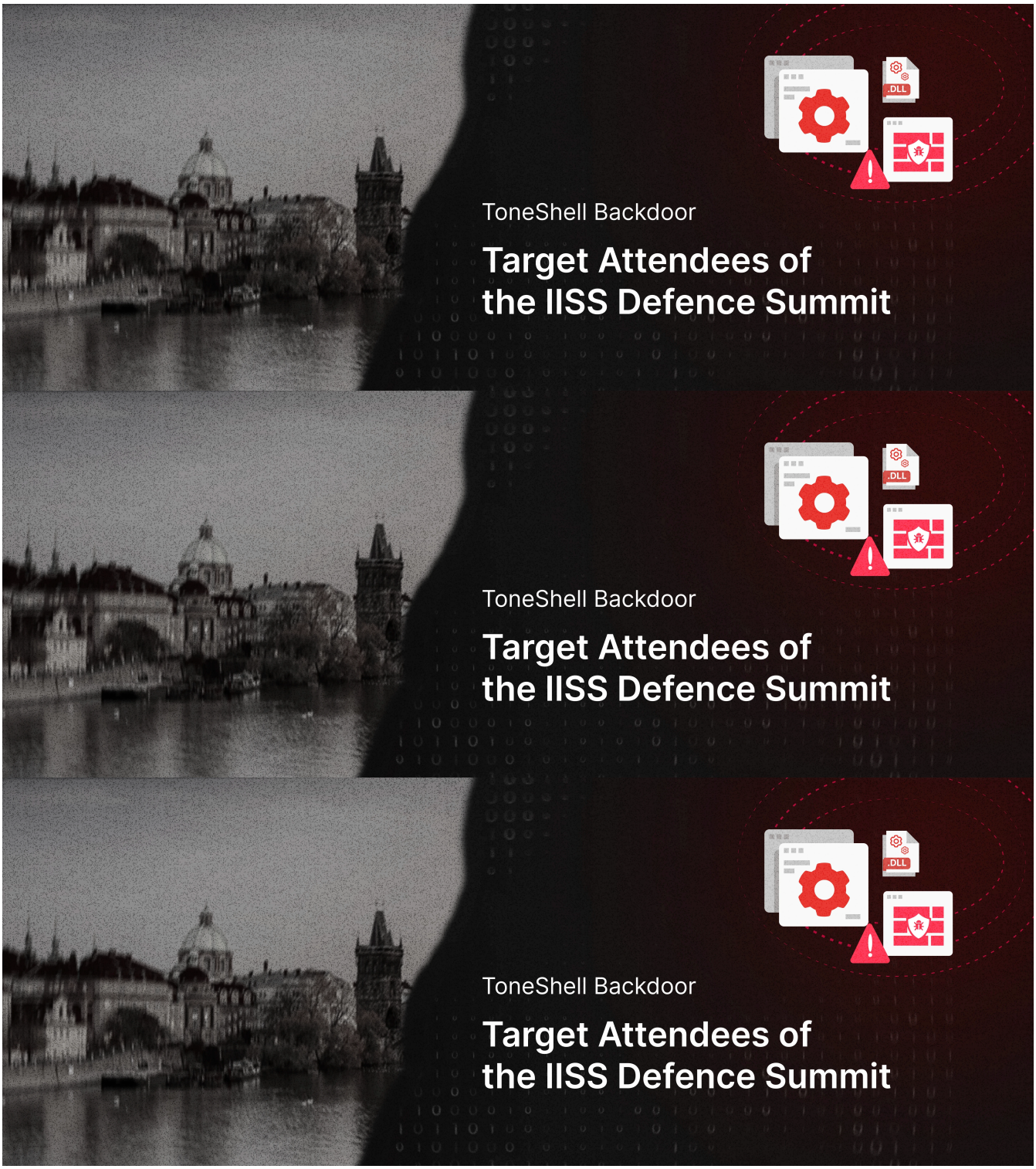

TABLE OF CONTENTS

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.

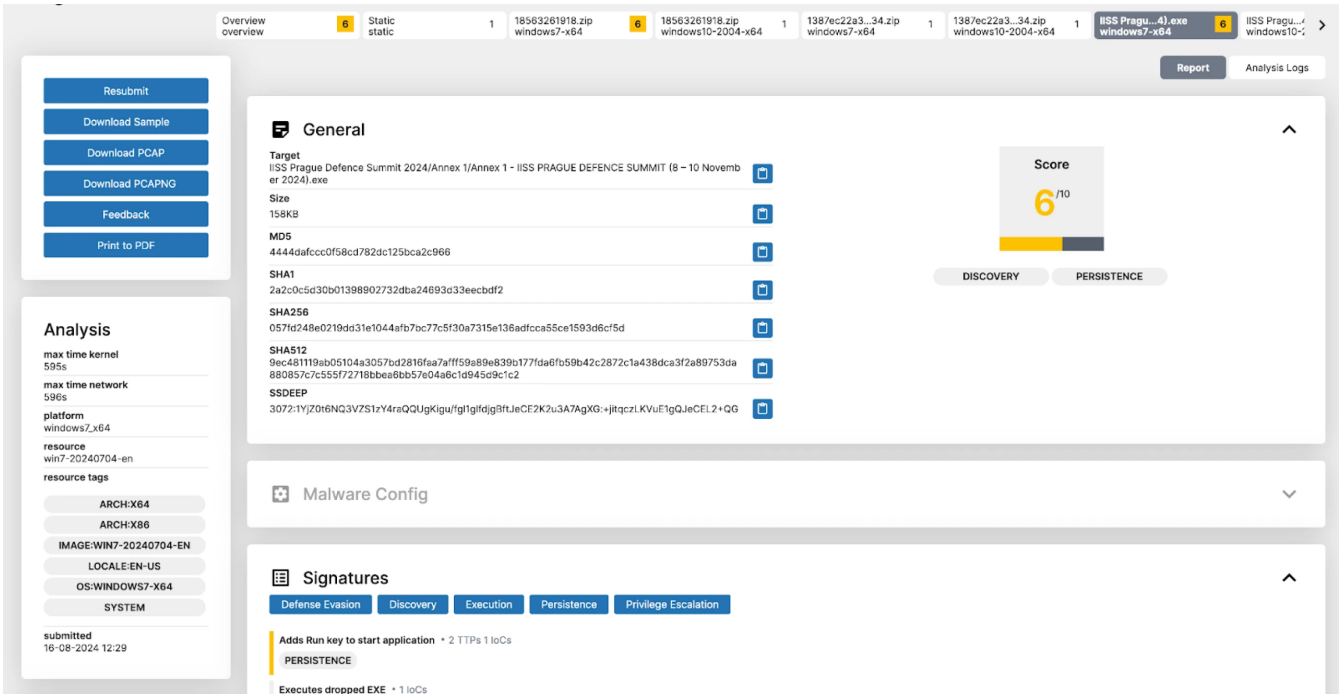

Figure 1: Hatching Triage Sandbox Analysis of suspicious EXE (Source/Link: Triage)

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.

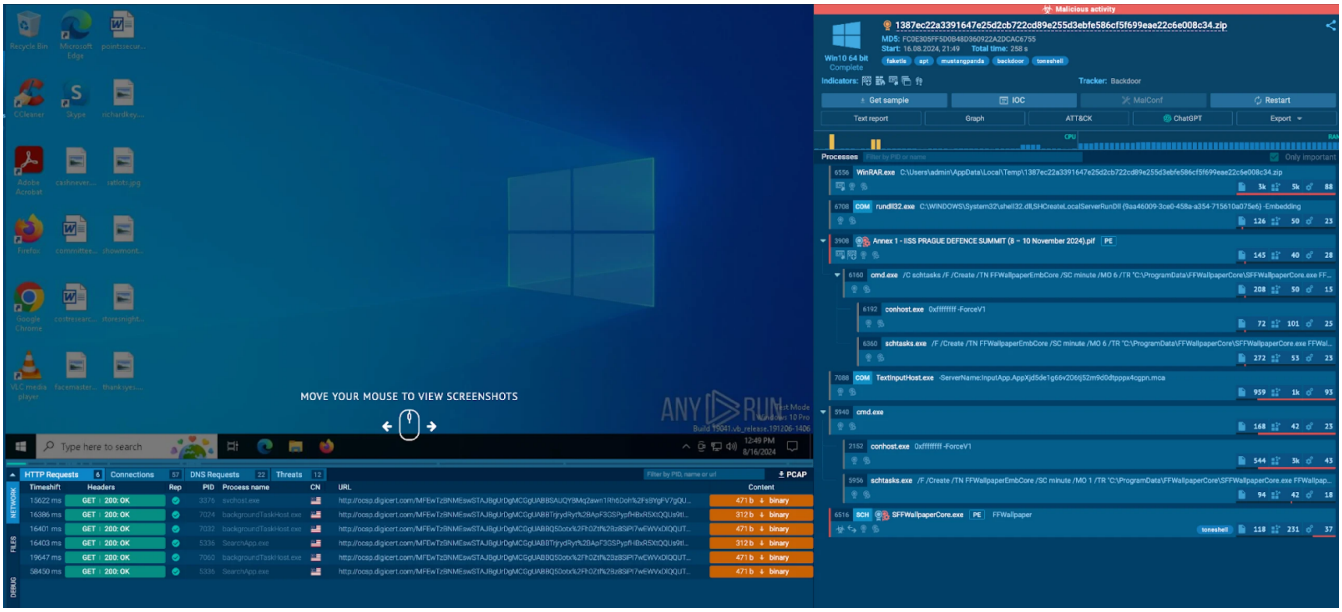

Figure 2: ANY.RUN analysis of the IISS-themed executable. (Source/Link: ANY.RUN)

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."

IISS PRAGUE DEFENCE SUMMIT
8 – 10 November 2024

As at 13 June 2024

OUTLINE AGENDA

All events will take place at the Prague Marriott Hotel,
V Celnici 8, 110 00 Prague, Czech Republic,
except for dinner on Saturday evening, which will be held at the Žofín Palace

All sessions will be on-the-record

FRIDAY 8 NOVEMBER

All day	BILATERAL MEETINGS BETWEEN GOVERNMENT DELEGATIONS
14:30 – 15:30	PRESENTATION OF IISS PRAGUE DEFENCE SUMMIT RESEARCH REPORT
16:00 – 17:30	SIMULTANEOUS SPECIAL SESSIONS
	Session I: **PROCURING FOR NATIONAL REQUIREMENTS**
	Session II: **INNOVATING AT SPEED**
	Session III: **DEFENCE PLANNING AND OPERATIONAL NEEDS**
18:30 – 19:30	WELCOME RECEPTION
	MINISTERIAL RECEPTION (BY INVITATION ONLY)
19:30 – 21:30	KEYNOTE ADDRESS & OPENING DINNER

SATURDAY 9 NOVEMBER

08:55 – 09:00	OPENING OF THE SUMMIT AND WELCOME REMARKS
09:00 – 10:30	FIRST PLENARY SESSION **RETHINKING EUROPEAN DEFENCE REQUIREMENTS AND CAPACITY**
10:30 – 11:00	*Refreshment Break*
11:00 – 12:30	SECOND PLENARY SESSION **TOWARDS A NEW ERA OF TECHNOLOGY SHARING**
12:30 – 14:00	DELEGATE LUNCH

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.

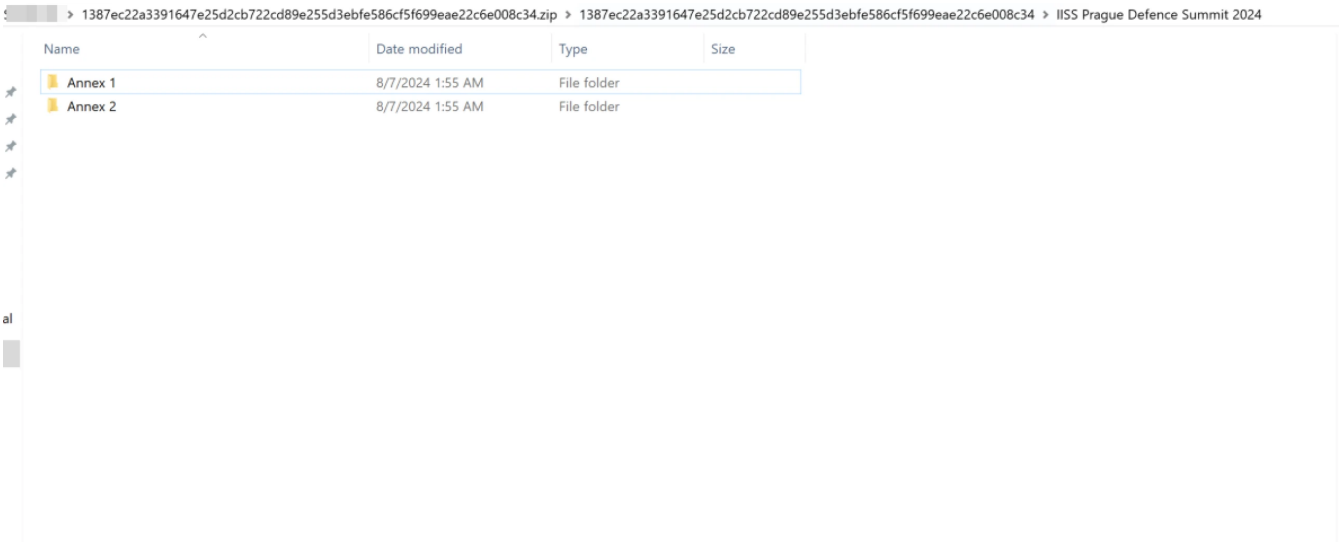

Figure 4: Annex 1 & 2 folders after extracting the zip contents

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).

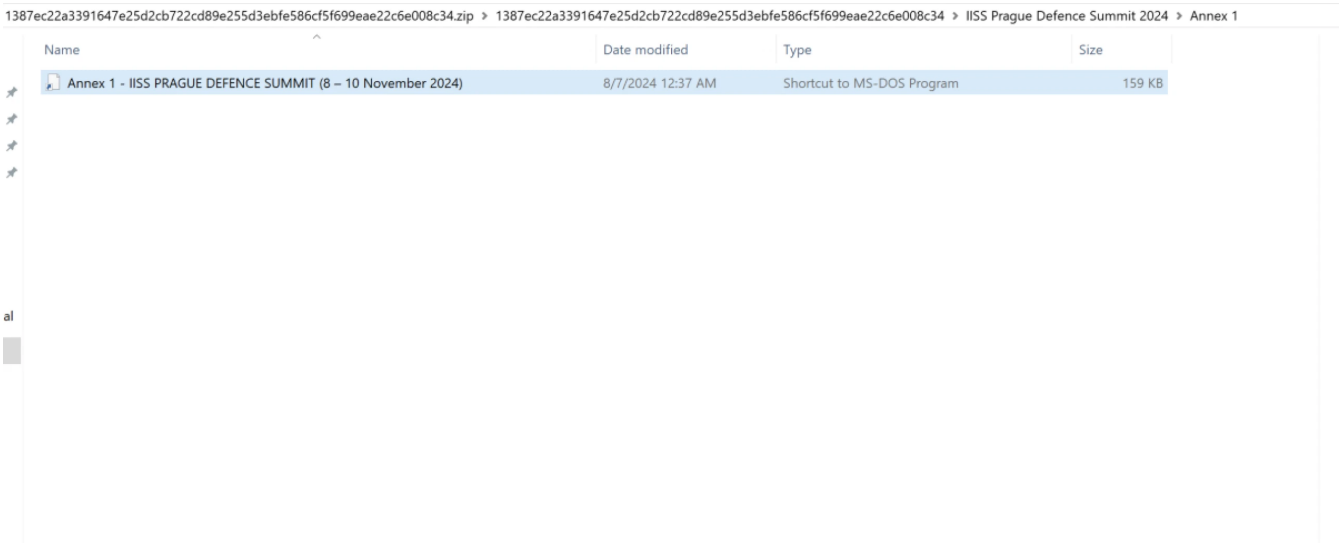

Figure 5: PIF-file masquerading as IISS agenda file

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.

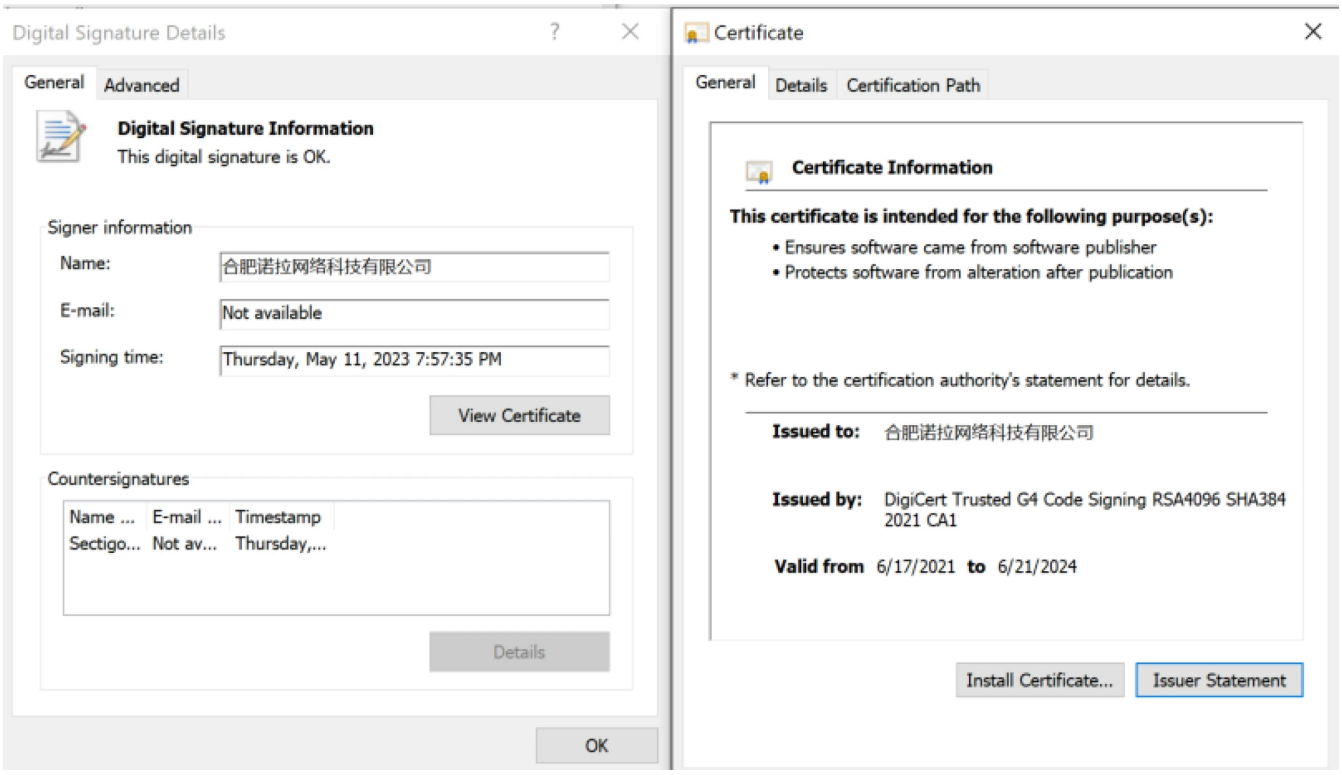

Figure 6: Codesigning certificate used for the malicious PIF-file

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.

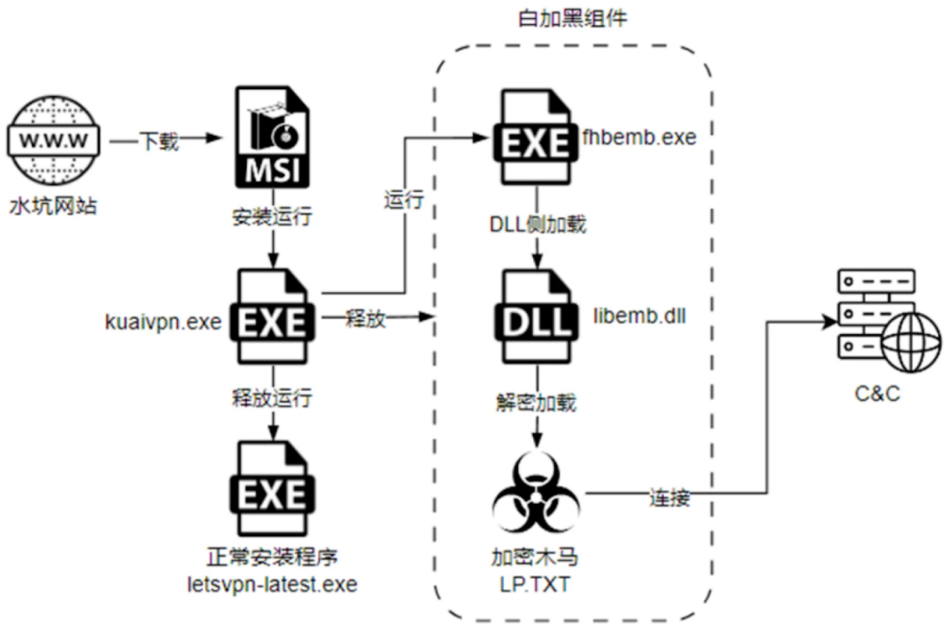

Figure 7: Secrss attack process diagram using similarly named files (Source: Secrss)
Returning to the malicious PIF, upon execution, it checks for the presence of the FFWallpaperCore directory in C:\ProgramData. If the directory is absent, it drops SFFWallpaperCore.exe and libemb.dll, likely to verify 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.

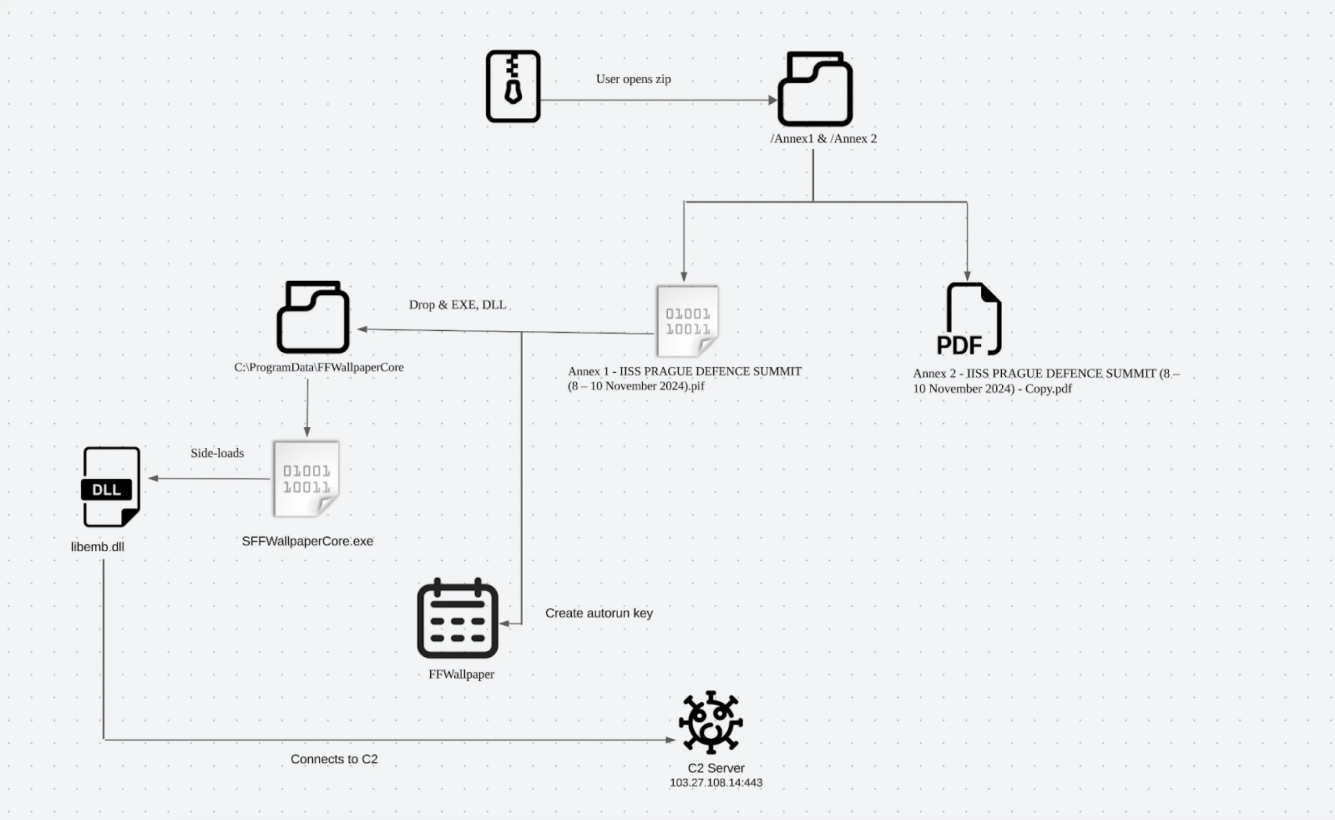

Figure 8: PIF event flow (Created using Lucidchart)

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.

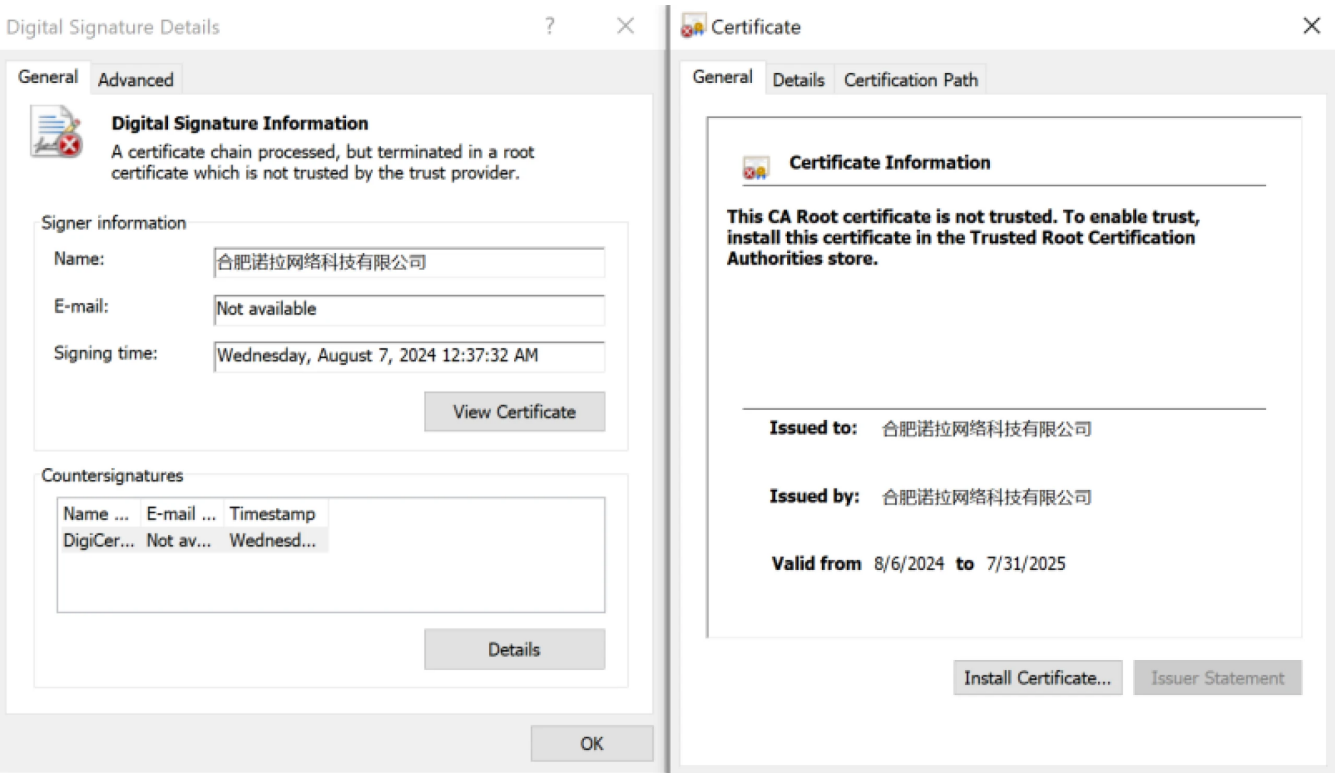

Figure 9: Untrusted codesigning certificate for libemb.dll

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.

```
undefined4 SetupAndEnumWindowProps(void)

{
  SIZE_T _Size;
  PROPENUMPROCEXW lpEnumFunc;
  HWND hWnd;
  void *local_c;
  SIZE_T local_8;

  local_c = (void *)0x0;
  local_8 = 0;
  ValidateAndProcessData(&local_c,&local_8);
  _printf("Start...buitengebieden\n");
  DisplayTimedDebugMessages();
  _printf("ZackAllen......techyteachme Ok\n");
  _Size = local_8;
  lpEnumFunc = (PROPENUMPROCEXW)VirtualAlloc((LPVOID)0x0,local_8,0x3000,0x40);
  if (lpEnumFunc != (PROPENUMPROCEXW)0x0) {
    FID_conflict:_memcpy(lpEnumFunc,local_c,_Size);
    hWnd = GetTopWindow((HWND)0x0);
    EnumPropsExW(hWnd,lpEnumFunc,0);
  }
  return 0;
}
```

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

```
void DisplayTimedDebugMessages(void)

{
  int iVar1;
  clock_t cVar2;
  clock_t cVar3;
  int iVar4;

  iVar4 = 0;
  do {
    iVar1 = iVar4 + 1;
    _printf("Massimo %d Jmpv...\n",iVar1);
    cVar2 = _clock();
    do {
      cVar3 = _clock();
    } while (cVar3 < cVar2 + 5000);
    _printf("Rainmaker1973 %d c?\n",iVar1);
    if (iVar4 < 3) {
      _printf("\n");
    }
    iVar4 = iVar1;
  } while (iVar1 < 4);
  return;
}
```

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.

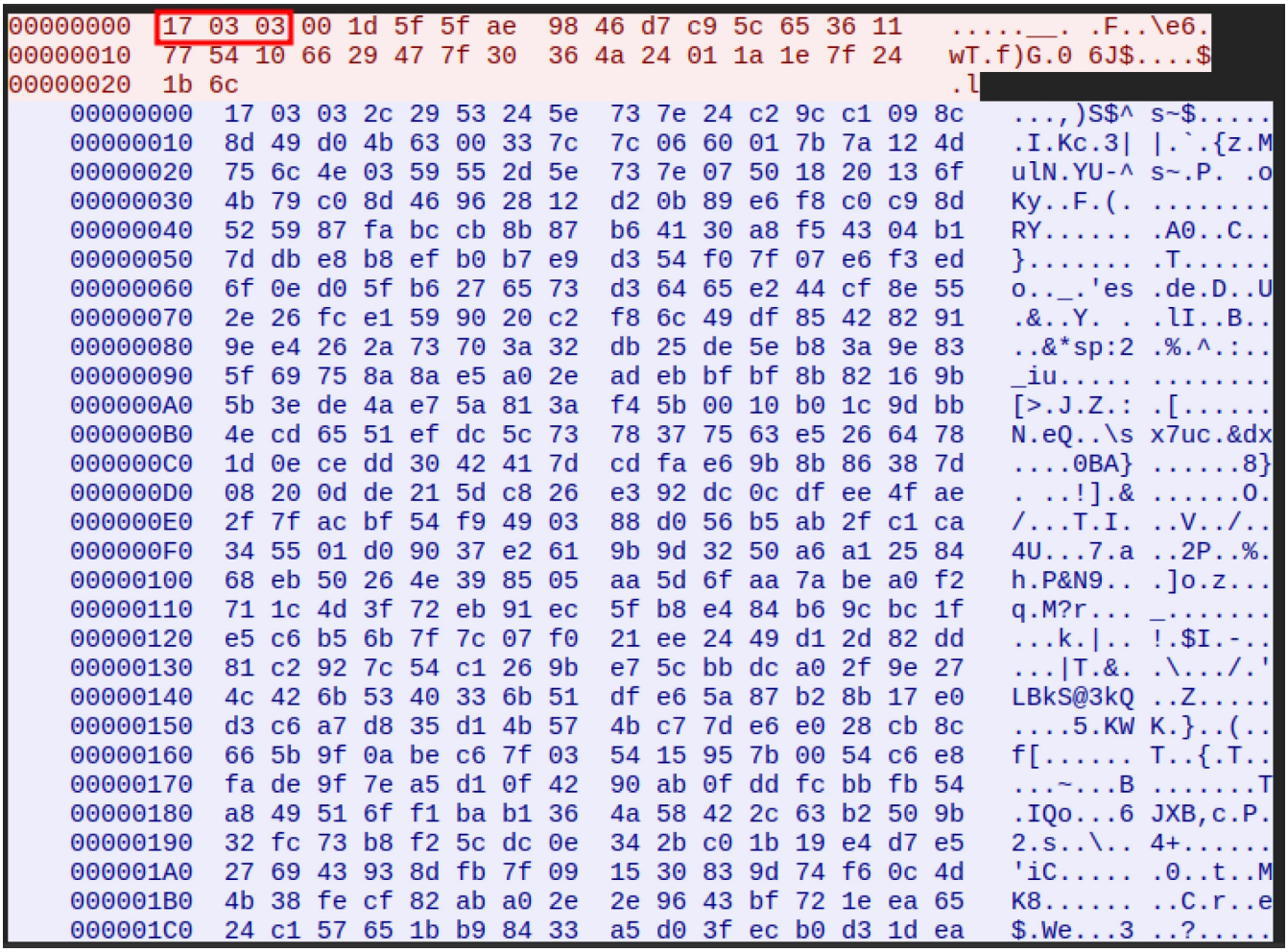

Figure 12: Request header containing the magic bytes “17 03 03”

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.

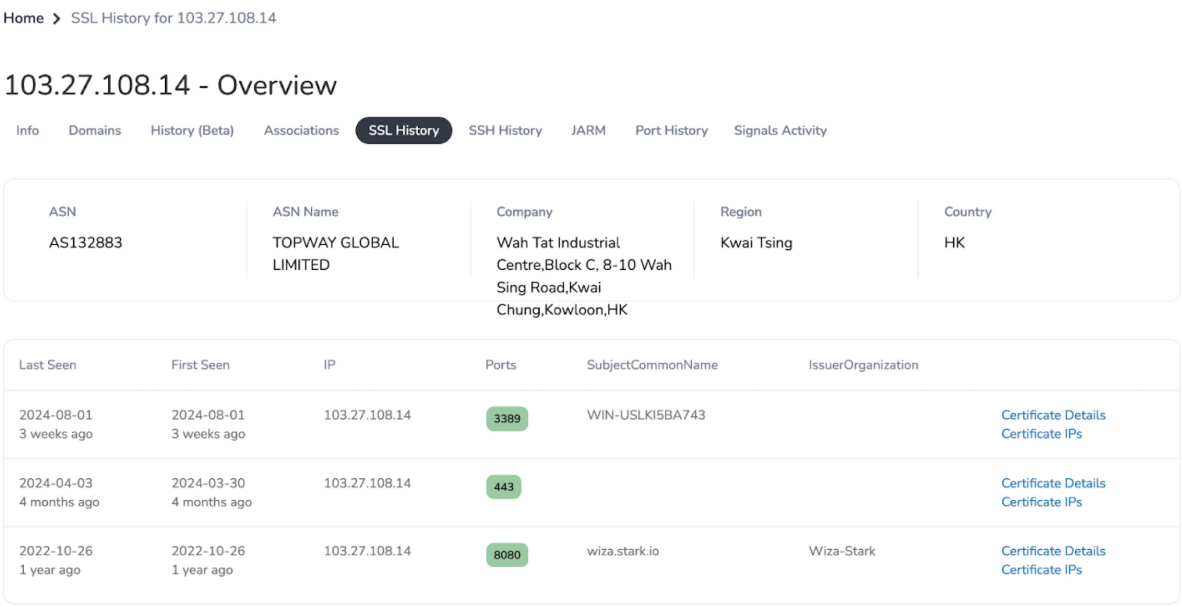

Figure 13: SSL History data in Hunt showing the short-lived RDP certificate

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.

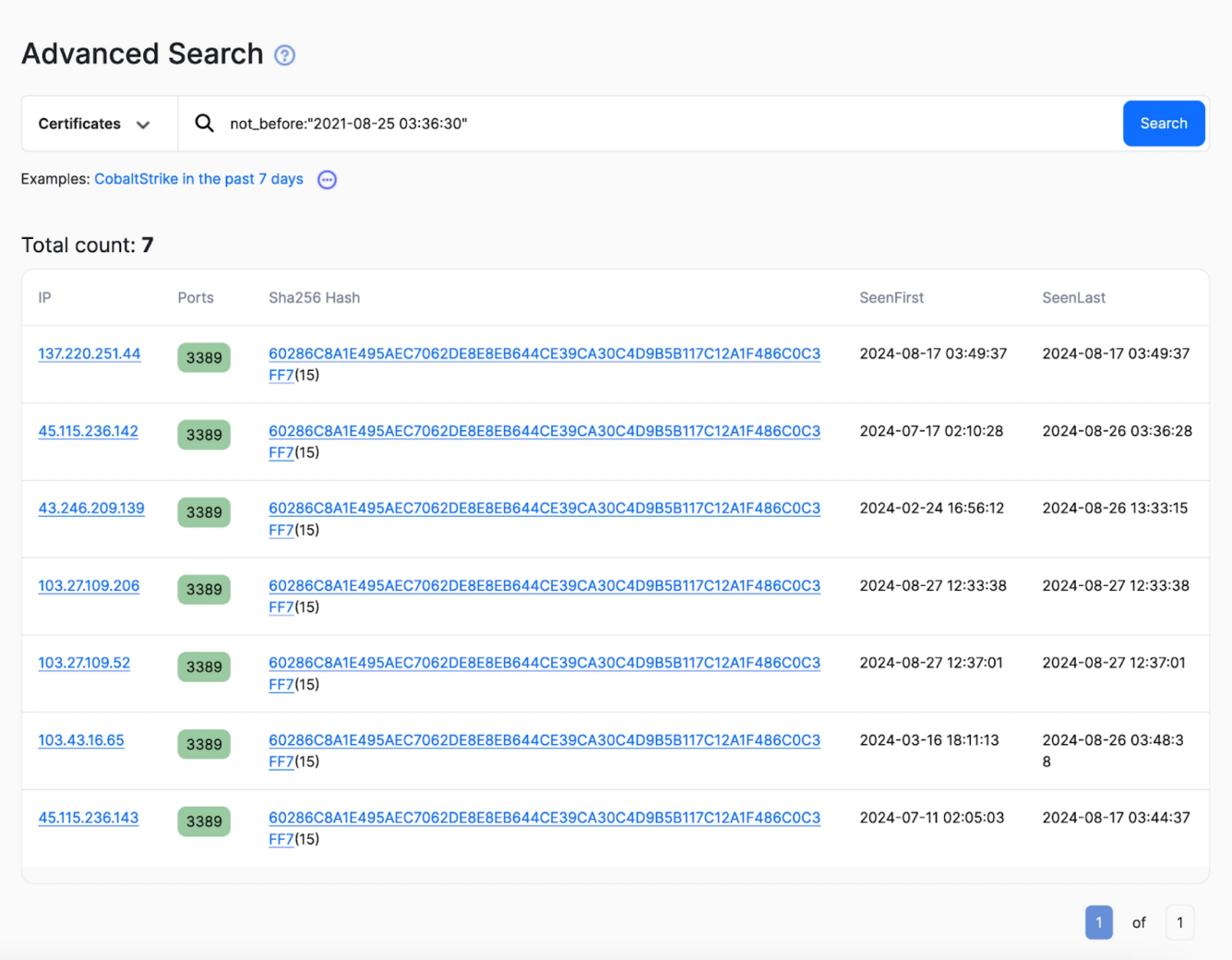

Figure 14: Results of the search for servers hosting RDP certificates bearing the same not before date

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.]44	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.]14	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 execution of Annex 1 - IISS PRAGUE DEFENCE SUMMIT (8 – 10 November 2024).pif

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

TABLE OF CONTENTS

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.

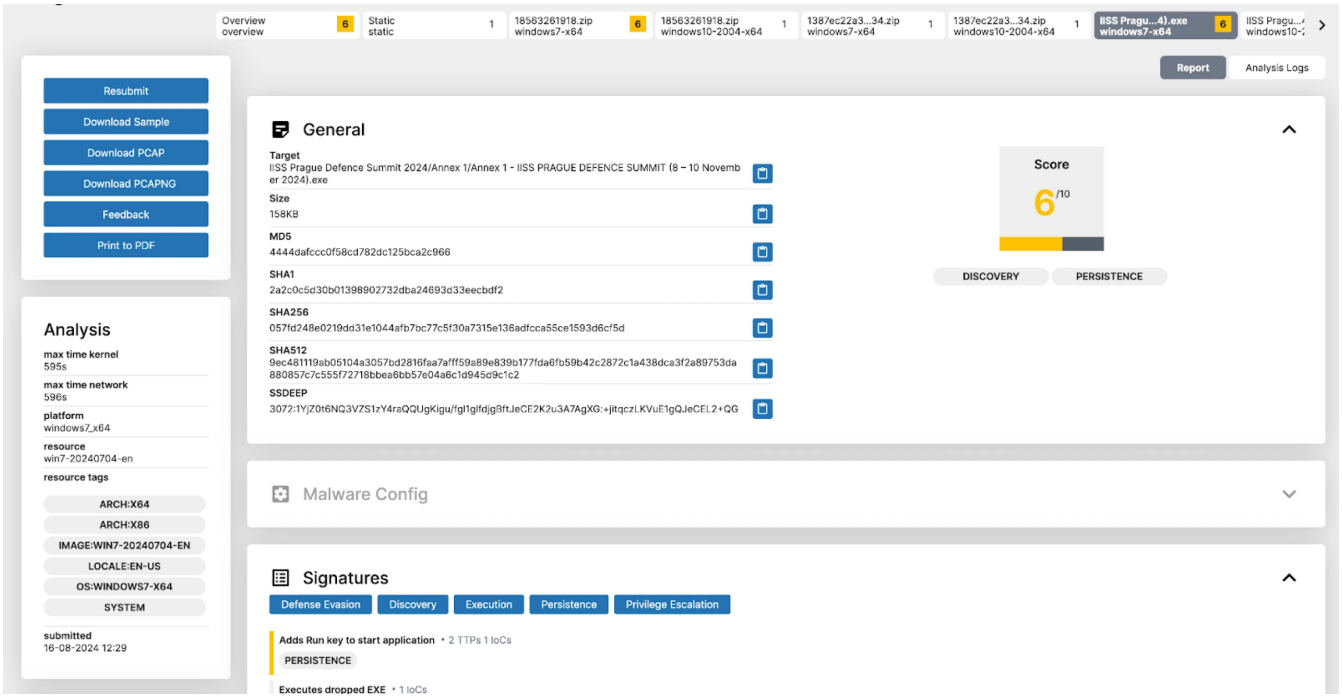

Figure 1: Hatching Triage Sandbox Analysis of suspicious EXE (Source/Link: Triage)

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.

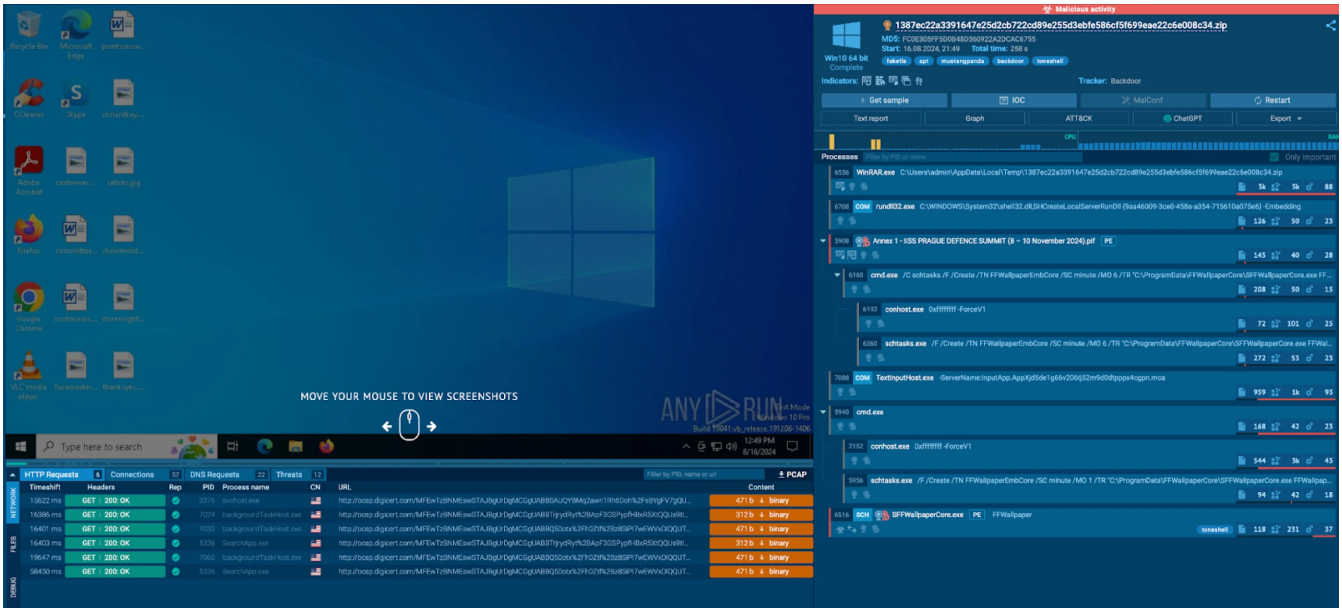

Figure 2: ANY.RUN analysis of the IISS-themed executable. (Source/Link: ANY.RUN)

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."

IISS PRAGUE DEFENCE SUMMIT
8 – 10 November 2024

As at 13 June 2024

OUTLINE AGENDA

All events will take place at the Prague Marriott Hotel,
V Celnici 8, 110 00 Prague, Czech Republic,
except for dinner on Saturday evening, which will be held at the Žofín Palace

All sessions will be on-the-record

FRIDAY 8 NOVEMBER

All day	BILATERAL MEETINGS BETWEEN GOVERNMENT DELEGATIONS
14:30 – 15:30	PRESENTATION OF IISS PRAGUE DEFENCE SUMMIT RESEARCH REPORT
16:00 – 17:30	SIMULTANEOUS SPECIAL SESSIONS
	Session I: **PROCURING FOR NATIONAL REQUIREMENTS**
	Session II: **INNOVATING AT SPEED**
	Session III: **DEFENCE PLANNING AND OPERATIONAL NEEDS**
18:30 – 19:30	WELCOME RECEPTION
	MINISTERIAL RECEPTION (BY INVITATION ONLY)
19:30 – 21:30	KEYNOTE ADDRESS & OPENING DINNER

SATURDAY 9 NOVEMBER

08:55 – 09:00	OPENING OF THE SUMMIT AND WELCOME REMARKS
09:00 – 10:30	FIRST PLENARY SESSION **RETHINKING EUROPEAN DEFENCE REQUIREMENTS AND CAPACITY**
10:30 – 11:00	*Refreshment Break*
11:00 – 12:30	SECOND PLENARY SESSION **TOWARDS A NEW ERA OF TECHNOLOGY SHARING**
12:30 – 14:00	DELEGATE LUNCH

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.

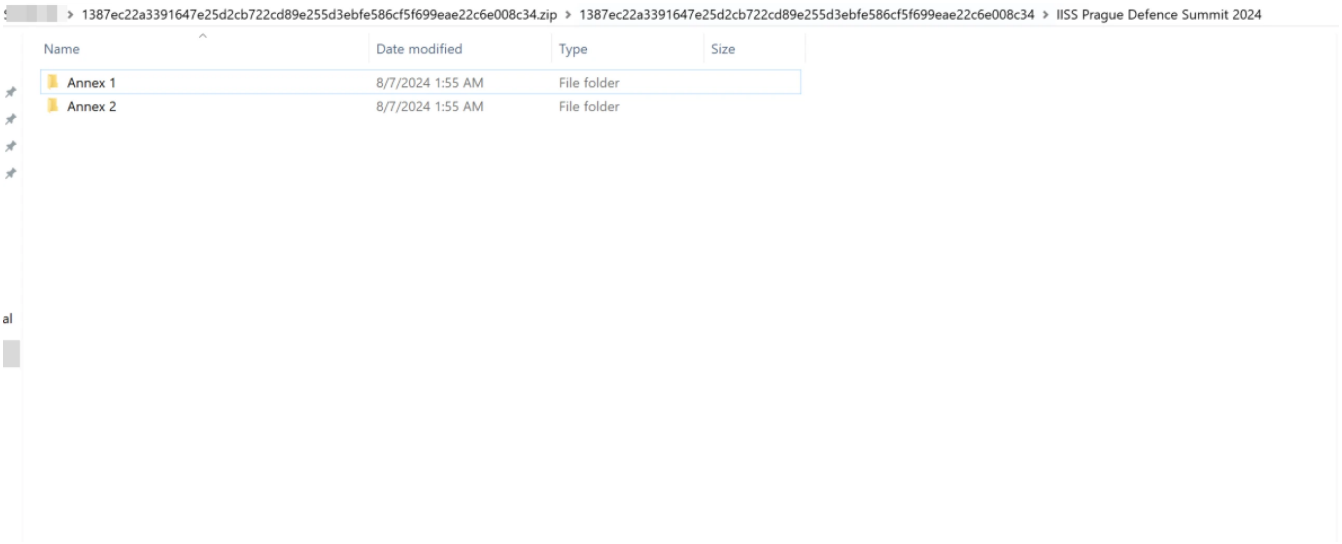

Figure 4: Annex 1 & 2 folders after extracting the zip contents

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).

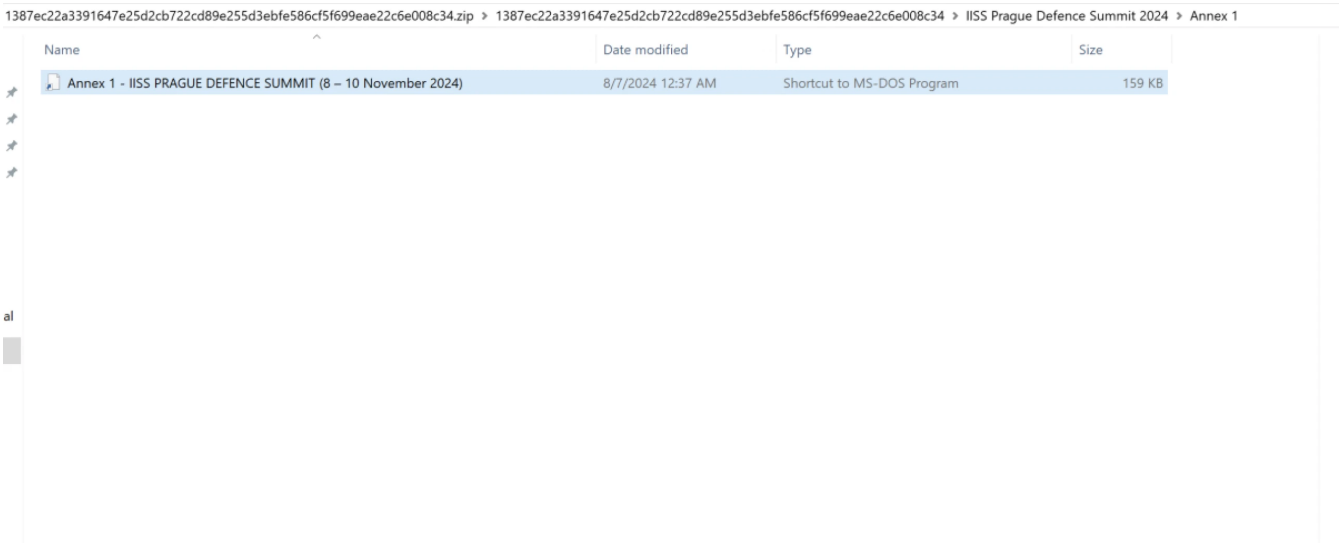

Figure 5: PIF-file masquerading as IISS agenda file

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.

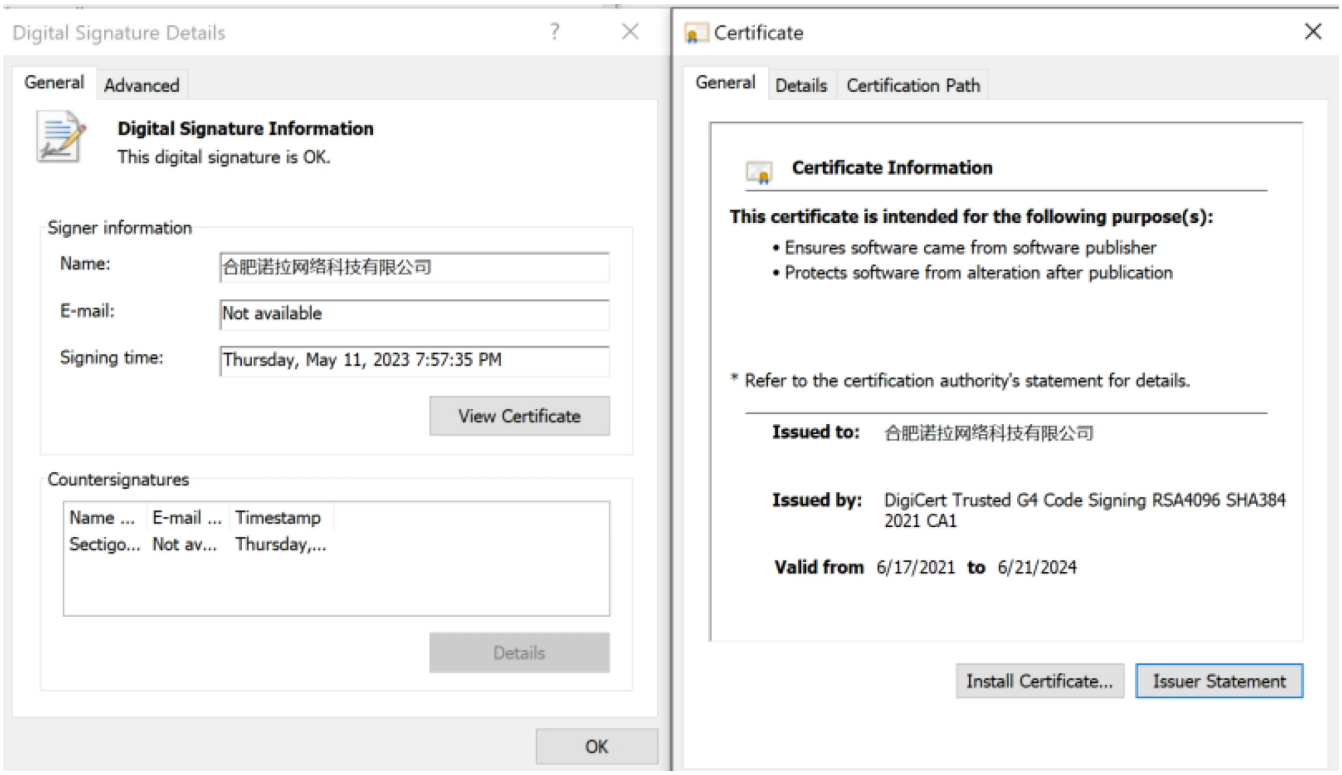

Figure 6: Codesigning certificate used for the malicious PIF-file

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.

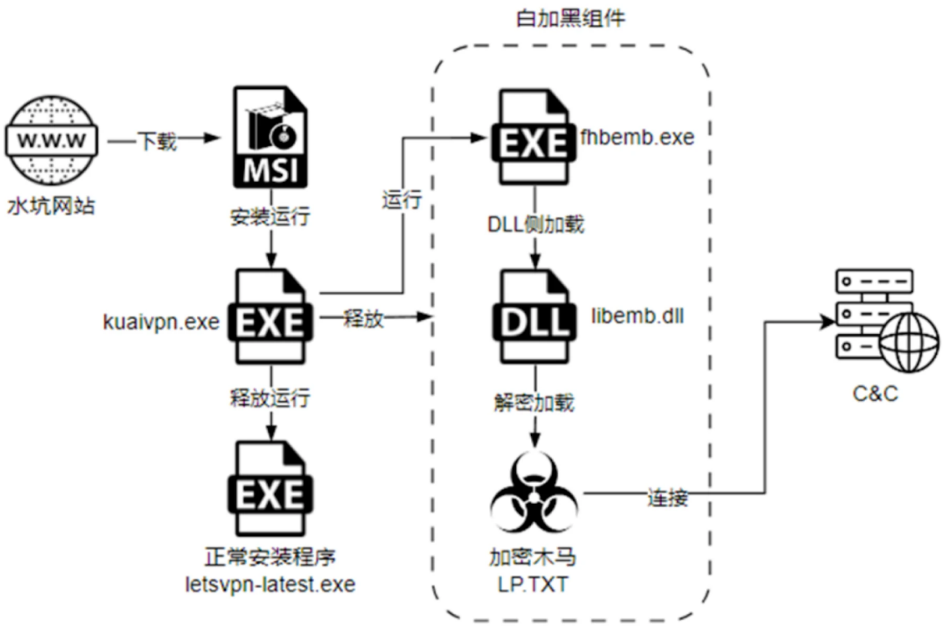

Figure 7: Secrss attack process diagram using similarly named files (Source: Secrss)
Returning to the malicious PIF, upon execution, it checks for the presence of the FFWallpaperCore directory in C:\ProgramData. If the directory is absent, it drops SFFWallpaperCore.exe and libemb.dll, likely to verify 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.

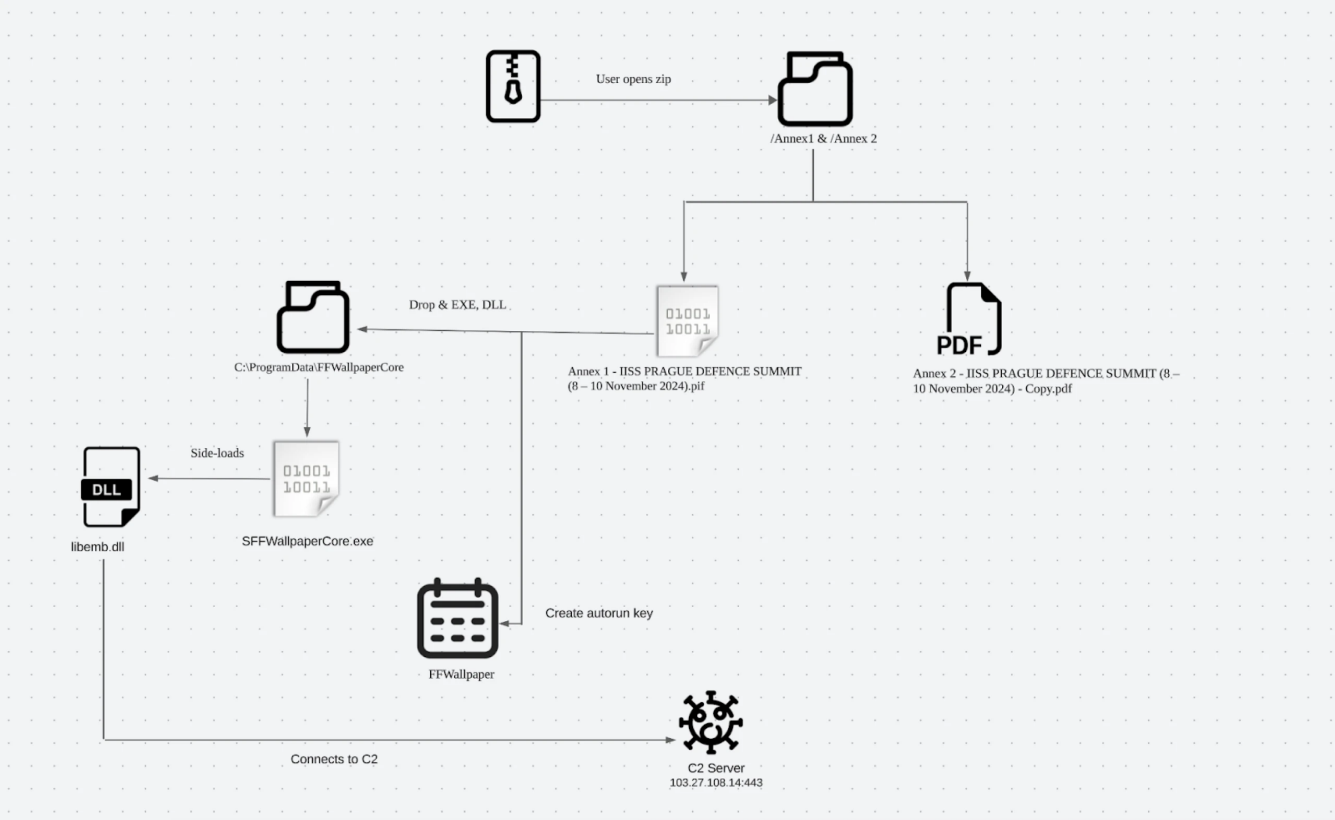

Figure 8: PIF event flow (Created using Lucidchart)

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.

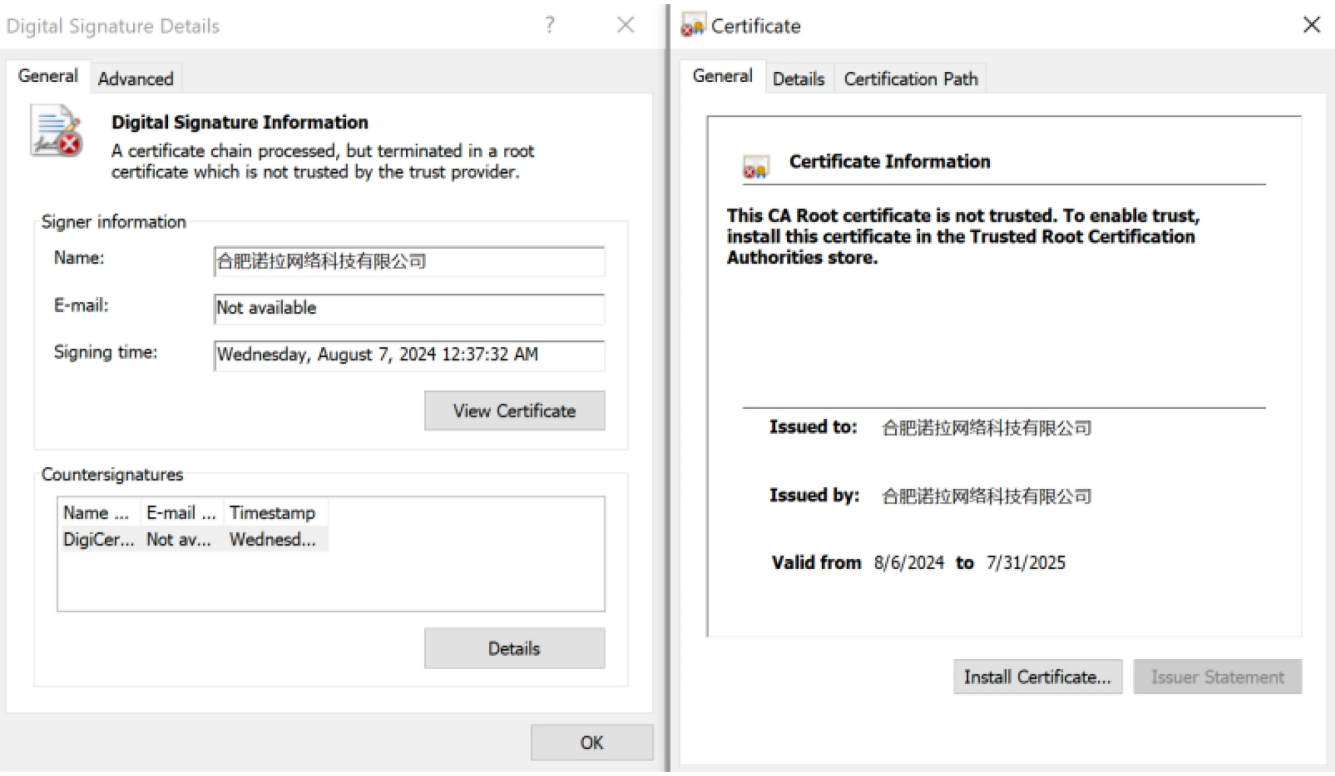

Figure 9: Untrusted codesigning certificate for libemb.dll

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.

```
undefined4 SetupAndEnumWindowProps(void)

{
  SIZE_T _Size;
  PROPENUMPROCEXW lpEnumFunc;
  HWND hWnd;
  void *local_c;
  SIZE_T local_8;

  local_c = (void *)0x0;
  local_8 = 0;
  ValidateAndProcessData(&local_c,&local_8);
  _printf("Start...buitengebieden\n");
  DisplayTimedDebugMessages();
  _printf("ZackAllen......techyteachme Ok\n");
  _Size = local_8;
  lpEnumFunc = (PROPENUMPROCEXW)VirtualAlloc((LPVOID)0x0,local_8,0x3000,0x40);
  if (lpEnumFunc != (PROPENUMPROCEXW)0x0) {
    FID_conflict:_memcpy(lpEnumFunc,local_c,_Size);
    hWnd = GetTopWindow((HWND)0x0);
    EnumPropsExW(hWnd,lpEnumFunc,0);
  }
  return 0;
}
```

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

```
void DisplayTimedDebugMessages(void)

{
  int iVar1;
  clock_t cVar2;
  clock_t cVar3;
  int iVar4;

  iVar4 = 0;
  do {
    iVar1 = iVar4 + 1;
    _printf("Massimo %d Jmpv...\n",iVar1);
    cVar2 = _clock();
    do {
      cVar3 = _clock();
    } while (cVar3 < cVar2 + 5000);
    _printf("Rainmaker1973 %d c?\n",iVar1);
    if (iVar4 < 3) {
      _printf("\n");
    }
    iVar4 = iVar1;
  } while (iVar1 < 4);
  return;
}
```

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.

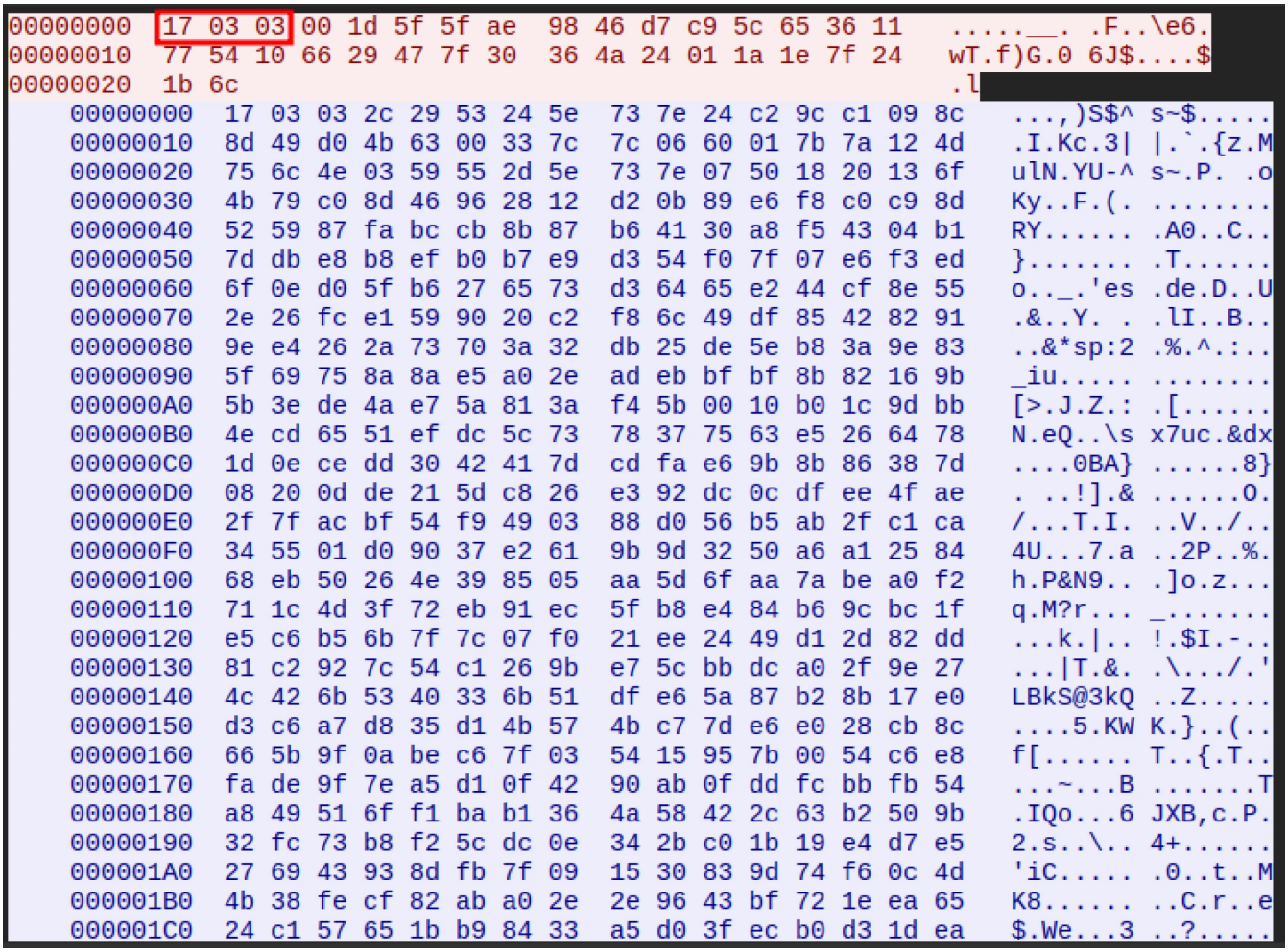

Figure 12: Request header containing the magic bytes “17 03 03”

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.

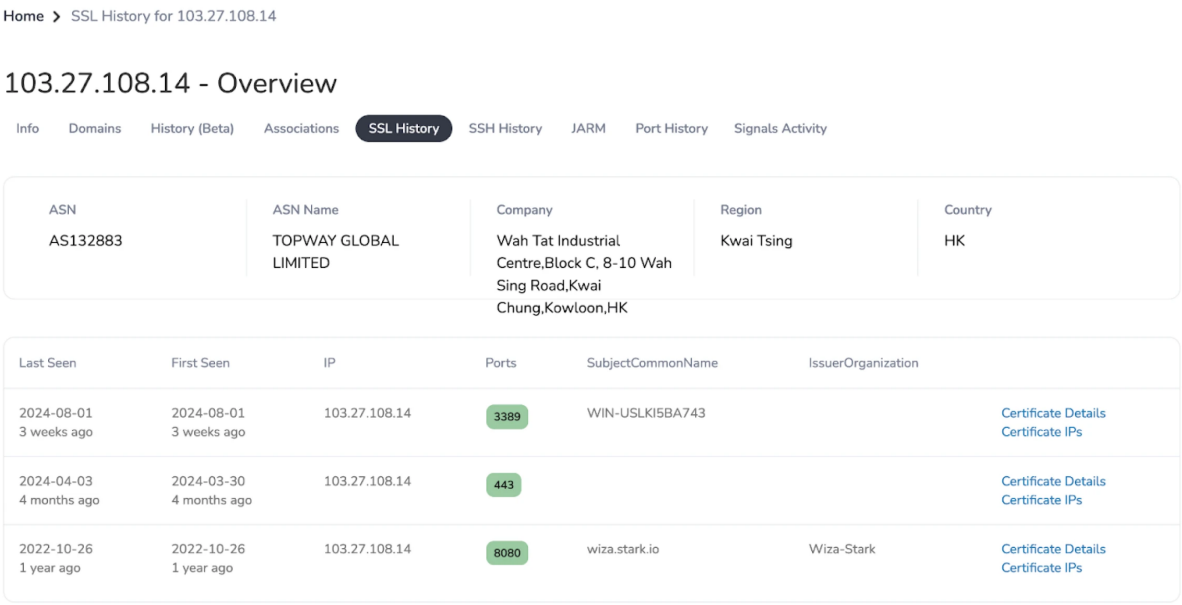

Figure 13: SSL History data in Hunt showing the short-lived RDP certificate

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.

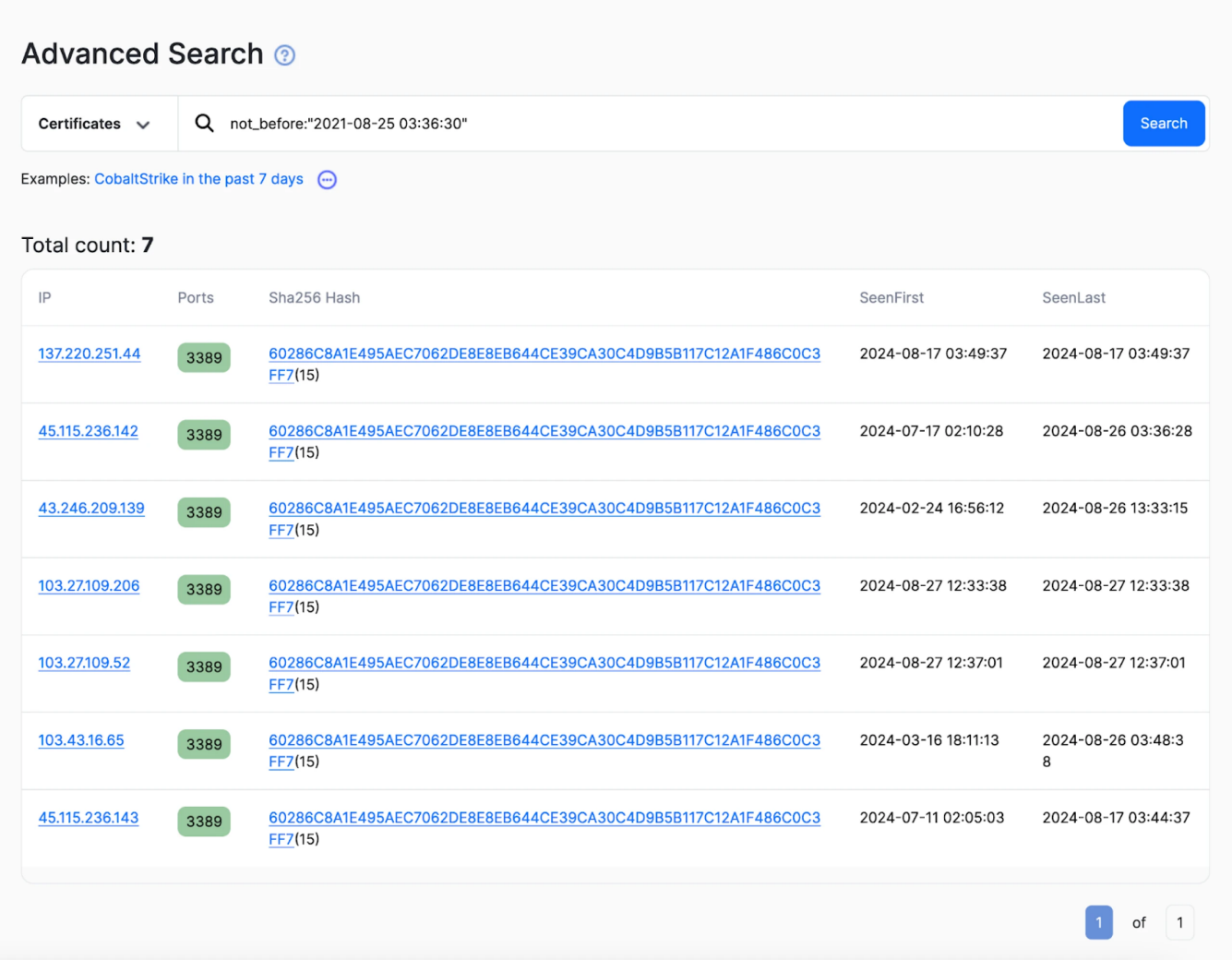

Figure 14: Results of the search for servers hosting RDP certificates bearing the same not before date

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.]44	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.]14	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 execution of Annex 1 - IISS PRAGUE DEFENCE SUMMIT (8 – 10 November 2024).pif

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