ToneShell Backdoor Used to Target Attendees of the IISS Defence Summit

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

ToneShell Backdoor

Target Attendees of the IISS Defence Summit



ToneShell Backdoor

Target Attendees of the IISS Defence Summit





ToneShell Backdoor

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 <u>command</u> <u>and control (C2) infrastructure</u> 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.

	Overview 6	Static static	1 18563261918.zi windows7-x64	o <mark>6</mark>	18563261918.zip windows10-2004-x6	¹	1387ec22a334.zip windows7-x64	1 1387 wind	ec22a334.zip ows10-2004-x64	1 IISS Pragu4) windows7-x64	.exe 6 4	IISS Pragu. windows10
											Report	Analysis Lo
Resubmit Download Sample	General											~
Download PCAP	Target	C	1/4	CENCE OUR	111T (0 10 November 1	_			Score			
Download PCAPNG	er 2024).exe	Summit 2024/Anne	x I/Annex I - IISS PRAGUE DI	FENCE SUN	INIT (8 - TO Novemb	Û			00010			
Feedback	158KB					Ċ			6			
Print to PDF	MD5 4444dafccc0f58cd7	82dc125bca2c966				۵						
	SHA1 2a2c0c5d30b01398	302732dba24693d3	33eecbdf2			Ċ		DIS	COVERY	PERSISTENCE		
Analysis	SHA256 057fd248e0219dd31	e1044afb7bc77c5f3	30a7315e136adfcca55ce1593	3d6cf5d		Ċ						
nax time kernel 95s	SHA512 9ec481119ab05104a	3057bd2816faa7aff	f59a89e839b177fda6fb59b4	2c2872c1a4	38dca3f2a89753da	ŕ						
nax time network 96s	SSDEEP	SDDea6DD57e04a60	10945090102									
latform indows7_x64	3072:1YjZ0t6NQ3VZ	S1zY4raQQUgKigu/	fgl1glfdjgBftJeCE2K2u3A7Ag	(G:+jitqczl.K	VuE1gQJeCEL2+QG	Ľ)						
esource nin7-20240704-en												
source tags		0 1										
ARCH:X64	Malware	e Config										
ARCH:X86												
IMAGE:WIN7-20240704-EN												
LOCALE:EN-US	🗐 Signatu	roc										
OS:WINDOWS7-X64	i olghata	103										
SYSTEM	Defense Evasion	Discovery	Execution Persistend	e Priv	lege Escalation							
ubmitted 6-08-2024 12:29	Adds Run key to s	tart application * 2	TTPs 1 IoCs									

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

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 <u>ANY.RUN</u>, where it exhibited similar TTPs.

	参 Malicious activity
	9 1387ec22a3391647e25d2cb722cd89e255d3ebfe586cf5f699eae22c6e008c34.zip
Rande Ein Monande pointeans	MD5: FC0E305FF500B480360922A2DCAC6755
ingre al more privatenti	Start: 16.08.2024, 21.14 Total ume: 258.8 Win10 64.bit faketa at mustaropanda backdoor tomeshell
	Complete Indicators: 闷 誌 및 등 왕 Tracker: Backdoor
S E	± Get sample
a COlenner Stype nichanding	Text report Graph ATT&CK @ ChatGPT Export -
	ov
	Processes Filter by PD or name
	6159 WinRAR.exe C:\Users\admin\AppData\Loca\\Temp\1387ec22a3391647e25d2cb722cd89e255d3ebfe586cf5f699eae22c6e008c34.zip
Adda cránne, utistigg	Щ 9 8 2 3 4 d [*] 3 4 d [*]
	6708 COM rundi32.exe C:\WINDOWS\System32\shell32.dll,SHCreateLocalServerRunDil (9aa46009-3ce0-458a-a354-715610a075e6) -Embedding
	운 % 🗎 126 11 50 d'
	▼ 3108 @@ Annex 1 - IISS PRAGUE DEFENCE SUMMIT (8 - 10 November 2024).pif PE
Firefox convertee showmont.	□同 〒 6 145 計 40 ♂
	6160 ordere /C schtasks /F /Create /TN FFWallpaperFmbCore /SC minute /MD 6 /TR 'C\ProgramData\FFWallpaperCore\SFFWallpaperCore.exe F
	⊕
	6100 analysis and Defillified Exception
Google contresear	
Unterie	
	Solo Sunaskaler // / rear //
	NAME Tradewiddent are Describeration for beVidte 1 of AND Provide International and
VL meða facemater Harkiye	Com recomponence conversame input op september geovzoeg szimologi ppixed primes
above Your MOUSE TO VIEW SCREENSHOTS	
	▼ 5140 cmd.exe
	2 10 10 11 12
🖬 🔎 Type here to search 💦 🖓 🖬 😳 🔚 🥹 🕹 🕹	2152 conhost.exe 0xfffffff -ForceV1
A UTD Downeric & Connections 37 DBS Benurate 37 Threate 33	± 541 ± ± x σ
Timethy Headers Rep PID Processment CN URL Content	5956 schtasks.exe /F /Create /TN FFWallpaperEmbCore /SC minute /MO 1 /TR 'C\ProgramData\FFWallpaperCore\SFFWallpaperCore.exe FFWallpa
💈 15622 ms 🛛 💽 🚺 12602.0K 💿 3376 stohosteve 📑 http://oosp.djajcer.com/MFEx/T28HMEswSTAJBg/UDgACCgUA8BSAU(Y8Mq2xwn1Rh6both72/18YrgFV/7gU 🔰 471.b 🕹 brawy	£ % ■ 94 ± 42 d'
🖹 14086 ma 🚺 GET i 200: OK 👘 🕘 7024 background Taskkost ove 🐸 http://coep.digicert.com/MFExTzBNMExxSTAJBgJzDgMC0gJJABBTBygRyByBrBbrSteQQU90L 🚺 312 b 4 binary	6516 SCH @ SFFWalpaperCore.exe PE FFWalpaper
a 📴 🖞 🖓 🕹 🕹 🕹 🕹 🕹 🕹 🕹 🕹 🕹 🕹 🕹 🕹 🕹	분·5 문 5 (Beenhell) 🖹 118 12 231 d
P tokus ma UCI 1 200 OK S SUB-SUBCONDARS ME MARK MARK SUBSTANDARS AND	
1947 His OCT 200 CK O 200 Cking Contracts Later	

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							
Figure 3: Document posing as an agen	da 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.

1387ec22a3391647e25d2cb722cd89e255d3ebfe586cf5f699eae22c6e008c34.zip > 1387ec22a3391647e25d2cb722cd89e255d3ebfe586cf5f699eae22c6e008c34 > IISS Prague Defence Summit 2024

	Name	^	Date modified	Туре	Size
	📕 Annex 1		8/7/2024 1:55 AM	File folder	
A A	📕 Annex 2		8/7/2024 1:55 AM	File folder	
*					
d					
1					

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).

Name Date modified Type	Size 159 KB
	159 KB
Annex 1 - IISS PRAGUE DEFENCE SUMMIT (8 – 10 November 2024) 8/7/2024 12:37 AM Shortcut to MS-DOS Program	
al	

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.

Digital Signature Deta	ails	? ×	Certificate X
General Advanced			General Details Certification Path
Digital Sig This digital	nature Information signature is OK.		Certificate Information
Signer information			This certificate is intended for the following purpose(s):
Name:	合肥诺拉网络科技有限公司		Ensures software came from software publisher Protects software from alteration after publication
E-mail:	Not available		
Signing time:	Thursday, May 11, 2023 7:57:35 PM		* Refer to the certification authority's statement for details.
	View Cert	ificate	Issued to: 合肥诺拉网络科技有限公司
Countersignatures	Timestamp		Issued by: DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1
Sectigo Not av	Thursday,		Valid from 6/17/2021 to 6/21/2024
	Detai	IS OK	Install Certificate Issuer Statement

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 <u>secrss</u> 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 Secres post.



Figure 7: Secrss attack process diagram using similarly named files (Source: <u>Secrss</u>) 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.

Digital Signature Deta	ails ?	X General Details Certification Path
Digital Sig A certificat certificate Signer information Name:	gnature Information te chain processed, but terminated in a root which is not trusted by the trust provider.	Certificate Information This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.
E-mail: Signing time:	Not available Wednesday, August 7, 2024 12:37:32 AM View Certificate	Issued to: 合肥诺拉网络科技有限公司
Countersignatures Name E-mail DigiCer Not av	I Timestamp v Wednesd	Issued by: 合肥诺拉网络科技有限公司 Valid from 8/6/2024 to 7/31/2025
	Details OK	Install Certificate Issuer Statement

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.

```
2undefined4 SetupAndEnumWindowProps(void)
4 {
   SIZE_T _Size;
6 PROPENUMPROCEXW lpEnumFunc;
   HWND hWnd;
   void *local_c;
   SIZE_T local_8;
11
   local c = (void *)0x0;
   local_8 = 0;
   ValidateAndProcessData(&local_c,&local_8);
   _printf("Start...buitengebieden\n");
14
   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);
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."

```
2 void DisplayTimedDebugMessages(void)
4 {
 6 clock_t cVar2;
    clock_t cVar3;
    int iVar4;
12
      iVar1 = iVar4 + 1;
13
       _printf("Massimo %d Jmpv...\n",iVar1);
14
       cVar2 = _clock();
      do {
        cVar3 = _clock();
17
      } while (cVar3 < cVar2 + 5000);</pre>
      _printf("Rainmaker1973 %d c?\n",iVar1);
if (iVar4 < 3) {
18
         _printf("\n");
20
21
22
      iVar4 = iVar1;
23        } while (iVar1 < 4);</pre>
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			.\e6.
00000010	77	54	10 (66 2	29	47	7f	30	36	4a	24	01	1a :	1e -	7f :	24	wT	.f)G.0 6J\$	\$
00000020	1b	6c															.1		
0000	0000	17	03	03	2c	29	53	24	5e	73	7e	24	c2	9c	c1	09	8c	,)S\$^	s~\$
0000	0010	8d	49	d0	4b	63	00	33	7c	7c	06	60	01	7b	7a	12	4d	.I.Kc.3	.`.{z.M
0000	0020	75	6C	4e	03	59	55	2d	5e	73	7e	07	50	18	20	13	6f	ulN.YU-^	s~.Po
0000	0030	4b	79	c0	8d	46	96	28	12	d2	Θb	89	e6	f8	c0	c9	8d	KyF.(.	
0000	0040	52	59	87	fa	bc	cb	8b	87	b6	41	30	a8	f5	43	04	b1	RY	.A0C
0000	0050	7d	db	e8	b8	ef	b0	b7	e9	d3	54	f0	7f	07	e6	f3	ed	}	.T
0000	0060	6f	0e	d0	5f	b6	27	65	73	d3	64	65	e2	44	cf	8e	55	o'es	.de.DU
0000	0070	2e	26	fc	e1	59	90	20	c2	f8	6c	49	df	85	42	82	91	.&Y	.lIB
0000	0080	9e	e4	26	2a	73	70	3a	32	db	25	de	5e	b8	3a	9e	83	&*sp:2	.%.^.:
0000	0090	5f	69	75	8a	8a	e5	a0	2e	ad	eb	bf	bf	8b	82	16	9b	_iu	
0000	00A0	5b	3e	de	4a	e7	5a	81	Зa	f4	5b	00	10	b0	1c	9d	bb	[>.J.Z.:	.[
0000	00B0	4e	cd	65	51	ef	dc	5c	73	78	37	75	63	e5	26	64	78	N.eQ\s	x7uc.&dx
0000	0000	1d	0e	ce	dd	30	42	41	7d	cd	fa	e6	9b	8b	86	38	7d	0BA}	8}
0000	00D0	08	20	0d	de	21	5d	c8	26	e3	92	dc	0c	df	ee	4f	ae	!].&	0.
0000	00E0	2f	7f	ac	bf	54	- f9	49	03	88	d0	56	b5	ab	2f	c1	са	/T.I.	v/
0000	00F0	34	55	01	d0	90	37	e2	61	9b	9d	32	50	a6	a1	25	84	4U7.a	2P%.
0000	0100	68	eb	50	26	4e	39	85	05	aa	5d	6f	aa	7a	be	a0	f2	h.P&N9	.]o.z
0000	0110	71	1c	4d	3f	72	eb	91	ec	5f	b8	e4	84	b6	9c	bc	1f	q.M?r	
0000	0120	e5	C6	b5	6b	7f	7c	07	f0	21	ee	24	49	d1	2d	82	dd	k.	!.\$I
0000	0130	81	c2	92	7c	54	_c1	26	9b	e7	5c	bb	dc	a0	2f	9e	27	T.&.	.\/.'
0000	0140	4c	42	6b	53	40	33	6b	51	df	e6	5a	87	b2	8b	17	e0	LBkS@3kQ	
0000	0150	d3	C6	a7	d8	35	d1	4b	57	4b	c7	7d	e6	e0	28	cb	8c	5.KW	K.}(
0000	0160	66	5b	9f	0a	be	c6	7f	03	54	15	95	7b	00	54	c6	e8	f[T{.T
0000	0170	fa	de	9f	7e	a5	d1	0f	42	90	ab	0f	dd	fc	bb	fb	54	~B	T
0000	0180	a8	49	51	6f	f1	ba	b1	36	4a	58	42	2c	63	b2	50	9b	.IQ06	JXB, c.P.
0000	0190	32	fc	73	b8	f2	5c	dc	0e	34	2b	c0	1b	19	e4	d7	e5	2.s\	4+
0000	01A0	27	69	43	93	8d	fb	7f	09	15	30	83	9d	74	f6	0c	4d	'iC	.0tM
0000	01B0	4b	38	fe	cf	82	ab	a0	2e	2e	96	43	bf	72	1e	ea	65	K8	C.re
0000	01C0	24	c1	57	65	1b	b9	84	33	a5	d0	3f	ec	b0	d3	1d	ea	\$.We3	?

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) As	ssociations SSL History	SSH History	JARM Port Histor	y Signals A	ctivity						
ASN		ASN Name	Company		Region		Country					
AS132883	T L	TOPWAY GLOBAL LIMITED	Wah Tat Ir Centre,Blo Sing Road	ndustrial ock C, 8-10 Wah ,Kwai	Kwai Tsing		НК					
Chung,Kowloon,HK												
Last Seen	First Seen	IP	Ports	SubjectCommonNa	me	IssuerOrganization						
2024-08-01 3 weeks ago	2024-08-01 3 weeks ago	103.27.108.14	3389	WIN-USLKI5BA74	3		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 ③

Examples: CobaltStrike in the past 7 days 💮

Certificates 🗸

Q not_before:"2021-08-25 03:36:30"

Total count: 7

IP	Ports	Sha256 Hash	SeenFirst	SeenLast
<u>137.220.251.44</u>	3389	60286C8A1E495AEC7062DE8E8E8644CE39CA30C4D9B5B117C12A1F486C0C3 FF7(15)	2024-08-17 03:49:37	2024-08-17 03:49:37
45.115.236.142	3389	60286C8A1E495AEC7062DE8E8EB644CE39CA30C4D9B5B117C12A1F486C0C3 FF7(15)	2024-07-17 02:10:28	2024-08-26 03:36:28
<u>43.246.209.139</u>	3389	60286C8A1E495AEC7062DE8E8EB644CE39CA30C4D9B5B117C12A1F486C0C3 FF7(15)	2024-02-24 16:56:12	2024-08-26 13:33:15
103.27.109.206	3389	60286C8A1E495AEC7062DE8E8E8644CE39CA30C4D9B5B117C12A1F486C0C3 FF7(15)	2024-08-27 12:33:38	2024-08-27 12:33:38
<u>103.27.109.52</u>	3389	60286C8A1E495AEC7062DE8E8E8644CE39CA30C4D9B5B117C12A1F486C0C3 FF7(15)	2024-08-27 12:37:01	2024-08-27 12:37:01
103.43.16.65	3389	60286C8A1E495AEC7062DE8E8E8644CE39CA30C4D9B5B117C12A1F486C0C3 FF7(15)	2024-03-16 18:11:13	2024-08-26 03:48:3 8
<u>45.115.236.143</u>	3389	60286C8A1E495AEC7062DE8E8EB644CE39CA30C4D9B5B117C12A1F486C0C3 FF7(15)	2024-07-11 02:05:03	2024-08-17 03:44:37

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	НК
45.115.236.]143	Topway Global Limited	НК
103.27.109.]52	Topway Global Limited	НК
103.27.109.]206	Topway Global Limited	НК
103.43.16.]65	Topway Global Limited	НК
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.

Search

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, <u>request a demo</u> 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 <u>command</u> <u>and control (C2) infrastructure</u> 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.

	Overview	6 Static static	1 18563261918.zij windows7-x64	6	18563261918.zip windows10-2004-x64	1387ec22a334.zip windows7-x64	1 1387e windo	c22a334.zip 1 ws10-2004-x64	IISS Pragu4).exe windows7-x64	IISS Pragu windows10-:
									Report	Analysis Log
Resubmit Download Sample										
		Seneral								^
Download PCAP	Target IISS Prag	ue Defence Summit 2024/An	nex 1/Annex 1 - IISS PRAGUE DE	FENCE SUM	IMIT (8 – 10 Novemb 💼			Score		
Download PCAPNG	er 2024).	exe						/10		
Feedback	158KB							0		
Print to PDF	MD5 4444dafo	ccc0f58cd782dc125bca2c96	6		Ċ					
	SHA1 2a2c0c5d	d30b01398902732dba24693	3d33eecbdf2				DIS	COVERY	PERSISTENCE	
Analysis	SHA256 057fd248	3e0219dd31e1044afb7bc77c	5f30a7315e136adfcca55ce1593	d6cf5d						
nax time kernel 95s	SHA512 9ec48111	9ab05104a3057bd2816faa7	afff59a89e839b177fda6fb59b4	2c2872c1a4	38dca3f2a89753da					
nax time network	SSDEEP	/C5551/2/1800e86005/e048	6C1094509C1CZ							
latform indows7_x64	3072:1Yj7	Z0t6NQ3VZS1zY4raQQUgKig	u/fgl1glfdjgBftJeCE2K2u3A7Ag)	(G:+jitqczl.K	VuE1gQJeCEL2+QG					
esource vin7-20240704-en										
source tags										
ARCH:X64	E N	lalware Config								\sim
ARCH:X86										
IMAGE:WIN7-20240704-EN										
LOCALE:EN-US	E C	ignoturoo								
OS:WINDOWS7-X64	E 3	signatures								~
SYSTEM	Defens	se Evasion Discovery	Execution Persistence	e Privi	ilege Escalation					
ubmitted 6-08-2024 12:29	Adds R PERSI	tun key to start application =	2 TTPs 1 IoCs							

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

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 <u>ANY.RUN</u>, where it exhibited similar TTPs.

	参 Malicious activity
	9 1387ec22a3391647e25d2cb722cd89e255d3ebfe586cf5f699eae22c6e008c34.zip
Rande Ein Monande pointeans	MD5: FC0E305FF500B480360922A2DCAC6755
ingre al more privatenti	Start: 16.08.2024, 21.14 Total ume: 258.8 Win10 64.bit faketa at mustaropanda backdoor tomeshell
	Complete Indicators: 闷 誌 및 등 용 Tracker: Backdoor
S E	± Get sample
a COlenner Stype nichanding	Text report Graph ATT&CK @ ChatGPT Export -
	ov
	Processes Filter by PD or name
	6159 WinRAR.exe C:\Users\admin\AppData\Local\Temp\1387ec22a3391647e25d2cb722cd89e255d3ebfe586cf5f699eae22c5e008c34.zip
Adda cránne, utistigg	Щ 9 8 2 9 8 ² 9 8 2
	6708 COM rundi32.exe C:\WINDOWS\System32\shell32.dll,SHCreateLocalServerRunDil (9aa46009-3ce0-458a-a354-715610a075e6) -Embedding
	운 % 🗎 126 11 50 d'
	▼ 3108 @@ Annex 1 - IISS PRAGUE DEFENCE SUMMIT (8 - 10 November 2024).pif PE
Firefox convertee showmont.	□ 145 計 40 ♂
	6160 ordere /C schtasks /F /Create /TN FFWallpaperFmbCore /SC minute /MD 6 /TR 'C\ProgramData\FFWallpaperCore\SFFWallpaperCore.exe F
	© % 1208 ±2' 50 d'
	6100 analysis and Defillified Exception
Google contresear	
Unterie	
	Solo Sunaskaler // / rear //
	NAME Tradewiddent are Describeration for beVidte 1 of AND Provide International and
VL meða facemater Harkiye	Com recomponence conversame input op september geovzoeg szimologi ppixed primes
above Your MOUSE TO VIEW SCREENSHOTS	
	▼ 5140 cmd.exe
	2 10 10 11 12
🖬 🔎 Type here to search 💦 🖓 🖬 😳 🔚 🥹 🕹 🕹	2152 conhost.exe 0xfffffff -ForceV1
A UTD Downeric A Connections 37 DBS Benurate 37 Threate 33	± 541 ± ± x σ
Timethy Headers Rep PID Processment CN URL Content	5956 schtasks.exe /F /Create /TN FFWallpaperEmbCore /SC minute /MO 1 /TR 'C\ProgramData\FFWallpaperCore\SFFWallpaperCore.exe FFWallpa
💈 15622 ms 🛛 💽 🚺 12602.0K 💿 3376 stohosteve 📑 http://oosp.djajcer.com/MFEx/T28HMEsvSTAJBg/UDgACCgUA8BSAU(Y8Mq2xwn1Rh6both72/18YrgFV/7gU 🔰 471.b 🕹 brawy	£ % ■ 94 ± 42 d'
🖹 14086 ma 🚺 GET i 200: OK 👘 🕘 7024 background Taskkost ove 🐸 http://coep.digicert.com/MFExTzBNMExxSTAJBgJzDgMC0gJJABBTBygRyByBrBbrSteQQU90L 🚺 312 b 4 binary	6516 SCH @ SFFWalpaperCore.exe PE FFWalpaper
a 📴 🖞 🖓 🕹 🕹 🕹 🕹 🕹 🕹 🕹 🕹 🕹 🕹 🕹 🕹 🕹	분·5 문 5 (Beenhell) 🖥 118 12 231 d
P tokus ma UCI 1 200 OK S SUB-SUBCONDARS ME MARK MARK SUBSTANDARS AND	
1947 His OCT 200 OK O Statistical set statistic and History Contract Control of Statistic Con	

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

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							
Figure 3: Document posing as an agen	da 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.

1387ec22a3391647e25d2cb722cd89e255d3ebfe586cf5f699eae22c6e008c34.zip > 1387ec22a3391647e25d2cb722cd89e255d3ebfe586cf5f699eae22c6e008c34 > IISS Prague Defence Summit 2024

	Name	^	Date modified	Туре	Size
	📕 Annex 1		8/7/2024 1:55 AM	File folder	
A A	📕 Annex 2		8/7/2024 1:55 AM	File folder	
*					
d					
1					

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).

138	ec22a3391647e25d2cb722cd89e255d3ebfe586cf5f699eae22c6e008c34.zip > 13	87ec22a3391647e25d2cb722cd89e255d3eb	fe586cf5f699eae22c6e008c34 > IISS Pr	ague Defence Summit 2024
	Name	Date modified	Туре	Size
*	Annex 1 - IISS PRAGUE DEFENCE SUMMIT (8 – 10 November 2024)	8/7/2024 12:37 AM	Shortcut to MS-DOS Program	159 KB
*				
*				
aı				

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.

Digital Signature Deta	ails	? ×	Certificate X
General Advanced			General Details Certification Path
Digital Sig This digital	nature Information signature is OK.		Certificate Information
Signer information			This certificate is intended for the following purpose(s):
Name:	合肥诺拉网络科技有限公司		Ensures software came from software publisher Protects software from alteration after publication
E-mail:	Not available		
Signing time:	Thursday, May 11, 2023 7:57:35 PM		* Refer to the certification authority's statement for details.
	View Certi	ificate	Issued to: 合肥诺拉网络科技有限公司
Countersignatures Name E-mail	Timestamp		Issued by: DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1
Sectigo Not av	Thursday,		Valid from 6/17/2021 to 6/21/2024
	Detail	SOK	Install Certificate Issuer Statement

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 <u>secrss</u> 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 Secres post.



Figure 7: Secrss attack process diagram using similarly named files (Source: <u>Secrss</u>) 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.

Digital Signature Deta	ails ?	X General Details Certification Path
Digital Sig A certificat certificate Signer information	gnature Information re chain processed, but terminated in a root which is not trusted by the trust provider.	Certificate Information This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification
Name: E-mail: Signing time:	合肥诺拉网络科技有限公司 Not available Wednesday, August 7, 2024 12:37:32 AM	Authorities store.
	View Certifica	te Issued to: 合肥诺拉网络科技有限公司
Name E-mail	Timestamp	Issued by: 合肥诺拉网络科技有限公司
	Detrile	Valid from 8/6/2024 to 7/31/2025
	Details	OK Install Certificate Issuer Statement

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.

```
2undefined4 SetupAndEnumWindowProps(void)
4 {
   SIZE_T _Size;
6 PROPENUMPROCEXW lpEnumFunc;
   HWND hWnd;
   void *local_c;
   SIZE_T local_8;
11
   local c = (void *)0x0;
   local_8 = 0;
   ValidateAndProcessData(&local_c,&local_8);
   _printf("Start...buitengebieden\n");
14
   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);
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."



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			.\e6.
00000010	77	54 :	10 0	66 2	29	47	7f	30	36	4a	24	01	1a 🛛	1e 🛛	7f :	24	wT	.f)G.0 6J\$	\$
00000020	1b	6c															.1		
0000	9000	17	03	03	2c	29	53	24	5e	73	7e	24	c2	9c	c1	09	8c	,)S\$^	s~\$
00000	9010	8d	49	dΘ	4b	63	00	33	7c	7c	06	60	01	7b	7a	12	4d	.I.Kc.3	.`.{z.M
0000	9020	75	6C	4e	03	59	55	2d	5e	73	7e	07	50	18	20	13	6f	ulN.YU-^	s~.Po
00000	9030	4b	79	c0	8d	46	96	28	12	d2	0b	89	e6	f8	c0	c9	8d	KyF.(.	
00000	9040	52	59	87	fa	bc	cb	8b	87	b6	41	30	a8	f5	43	04	b1	RY	.A0C
00000	9050	7d	db	e8	b8	ef	b0	b7	e9	d3	54	f0	7f	07	e6	f3	ed	}	.T
00000	9060	6f	0e	d0	5f	b6	27	65	73	d3	64	65	e2	44	cf	8e	55	o'es	.de.DU
00000	9070	2e	26	fc	e1	59	90	20	c2	f8	6c	49	df	85	42	82	91	.&Y	.lIB
00000	9080	9e	e4	26	2a	73	70	3a	32	db	25	de	5e	b8	3a	9e	83	&*sp:2	.%.^.:
00000	9090	5f	69	75	8a	8a	e5	a0	2e	ad	eb	bf	bf	8b	82	16	9b	_iu	
0000	90A0	5b	3e	de	4a	e7	5a	81	3a	f4	5b	00	10	b0	1c	9d	bb	[>.J.Z.:	.[
0000	90B0	4e	cd	65	51	ef	dc	5c	73	78	37	75	63	e5	26	64	78	N.eQ\s	x7uc.&dx
0000	90C0	1d	0e	ce	dd	30	42	41	7d	cd	fa	e6	9b	8b	86	38	7d	0BA}	8}
0000	90D0	08	20	0d	de	21	5d	c8	26	e3	92	dc	0c	df	ee	4f	ae	!].&	0.
0000	90E0	2f	7f	ac	bf	54	- f9	49	03	88	d0	56	b5	ab	2f	c1	са	/T.I.	V/
0000	90F0	34	55	01	d0	90	37	e2	61	9b	9d	32	50	a6	a1	25	84	4U7.a	2P%.
0000	9100	68	eb	50	26	4e	39	85	05	aa	5d	6f	aa	7a	be	a0	f2	h.P&N9	.]o.z
0000	9110	71	1c	4d	3f	72	eb	91	ec	5f	b8	e4	84	b6	9c	bc	1f	q.M?r	
0000	9120	e5	C6	b5	6b	7f	7c	07	f0	21	ee	24	49	d1	2d	82	dd	k.	!.\$I
00000	9130	81	c2	92	7c	54	_c1	26	9b	e7	5c	bb	dc	a0	2f	9e	27	T.&.	.\/.'
00000	9140	4c	42	6b	53	40	33	6b	51	df	e6	5a	87	b2	8b	17	e0	LBkS@3kQ	Z
00000	9150	d3	C6	a7	d8	35	d1	4b	57	4b	c7	7d	e6	e0	28	cb	8c	5.KW	K.}(
00000	9160	66	5b	9f	0a	be	C6	7f	03	54	15	95	7b	00	54	C6	e8	f[T{.T
00000	9170	fa	de	9f	7e	a5	d1	0f	42	90	ab	0f	dd	fc	bb	fb	54	~B	T
00000	9180	a8	49	51	6f	f1	ba	b1	36	4a	58	42	2c	63	b2	50	9b	.IQ06	JXB,c.P.
00000	9190	32	fc	73	b8	f2	5c	dc	0e	34	2b	C0	1b	19	e4	d7	e5	2.s\	4+
00000	91A0	27	69	43	93	8d	fb	7f	09	15	30	83	9d	74	f6	0c	4d	'iC	.0tM
0000	91B0	4b	38	fe	cf	82	ab	a0	2e	2e	96	43	bf	72	1e	ea	65	K8	C.re
0000	91C0	24	c1	57	65	1b	b9	84	33	a5	d0	3f	ec	b0	d3	1d	ea	\$.We3	?

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) As	ssociations SSL History	SSH History	JARM Port Histor	y Signals A	ctivity					
ASN		ASN Name	Company		Region		Country				
AS132883	T L	TOPWAY GLOBAL LIMITED	Wah Tat Ir Centre,Blo Sing Road	ndustrial ock C, 8-10 Wah ,Kwai	Kwai Tsing		НК				
	Chung,Kowloon,HK										
Last Seen	First Seen	IP	Ports	SubjectCommonNa	me	IssuerOrganization					
2024-08-01 3 weeks ago	2024-08-01 3 weeks ago	103.27.108.14	3389	WIN-USLKI5BA74	3		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 ③

Examples: CobaltStrike in the past 7 days 💮

Certificates 🗸

Q not_before:"2021-08-25 03:36:30"

Total	count	7
Total	count:	1

IP	Ports	Sha256 Hash	SeenFirst	SeenLast
137.220.251.44	3389	60286C8A1E495AEC7062DE8E8EB644CE39CA30C4D9B5B117C12A1F486C0C3 FF7(15)	2024-08-17 03:49:37	2024-08-17 03:49:37
<u>45.115.236.142</u>	3389	60286C8A1E495AEC7062DE8E8EB644CE39CA30C4D9B5B117C12A1F486C0C3 FF7(15)	2024-07-17 02:10:28	2024-08-26 03:36:28
<u>43.246.209.139</u>	3389	60286C8A1E495AEC7062DE8E8EB644CE39CA30C4D9B5B117C12A1F486C0C3 FF7(15)	2024-02-24 16:56:12	2024-08-26 13:33:15
103.27.109.206	3389	60286C8A1E495AEC7062DE8E8EB644CE39CA30C4D9B5B117C12A1F486C0C3 FF7(15)	2024-08-27 12:33:38	2024-08-27 12:33:38
103.27.109.52	3389	60286C8A1E495AEC7062DE8E8EB644CE39CA30C4D9B5B117C12A1F486C0C3 FF7(15)	2024-08-27 12:37:01	2024-08-27 12:37:01
103.43.16.65	3389	60286C8A1E495AEC7062DE8E8EB644CE39CA30C4D9B5B117C12A1F486C0C3 FF7(15)	2024-03-16 18:11:13	2024-08-26 03:48:3 8
<u>45.115.236.143</u>	3389	60286C8A1E495AEC7062DE8E8EB644CE39CA30C4D9B5B117C12A1F486C0C3 FF7(15)	2024-07-11 02:05:03	2024-08-17 03:44:37

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	НК
45.115.236.]142	Topway Global Limited	НК
45.115.236.]143	Topway Global Limited	НК
103.27.109.]52	Topway Global Limited	НК
103.27.109.]206	Topway Global Limited	НК
103.43.16.]65	Topway Global Limited	НК
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.

Search

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, <u>request a demo</u> 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