IBM X-Force Exchange ALL

Tropic Trooper's New Approach

phishing (/search/%23phishing) xftas (/search/%23xftas) email (/search/%23email) cybercrime (/search/%23cybercrime) campaign (/search/%23campaign)

0

Raccolta pubblica | 2 Follower

TLP: (https://www.us-cert.gov/tlp) BIANCO

(https://twitter.com/intent/tweet?text=Tropic%20Trooper%E2%80%99s%20New%20Approach&url=https%3A%2F
Troopers-New-Approach-4235d84efed96f140a83f735c68578d0) (https://www.li
mini=true&url=https%3A%2F%2Fexchange.xforce.ibmcloud.com%2Fcollection%2
4235d84efed96f140a83f735c68578d0&title=Tropic%20Trooper%E2%80%99s%20
(http://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fexchange.xforc
Approach-4235d84efed96f140a83f735c68578d0&t=Tropic%20Trooper%E2%80%9
(https://exchange.xforce.ibmcloud.com/api/doc/#rss_feed)

Advisory Type

- Malware

Overview

Security researchers at Trend Micro have released technical details about Tropic Trooper, also referred to as KeyBoy. It has recently been used in campaigns that target government, transportation, technology and the healthcare industries in Taiwan, Philippines, and Hong Kong. Tropic Trooper uses Microsoft Office documents, containing exploits, to deliver malware to it's victims. The researchers analyzed several additional malicious documents that don't need to download a payload from the Internet (as others observed did), as the backdoor's dropper is embedded within the document itself. The backdoor loads the encrypted configuration file and decrypts it. It will then use the Secure Sockets Layer to connect and communicate with the command and control servers. It was mentioned that the adversaries have been fine tuning their sophisticated malware over a period of time. To better protect organizations, it was recommended by Trend Micro that: organizations keep their systems and applications up to date, implement and enforce a policy of least privilege, turn off or limit access to system administration tools, and to educate users about spear phishing emails as they rely heavily on social engineering to trick users.

Time Frame

- March 14, 2018 -- Trend Micro article published.
- March 21, 2018 -- XFE collection created.
- March 22, 2018 -- Published in XFTAS newsletter.

Technical Details (attack chain)

- Exploits security flaws (VUL CVE-2017-11882 or VUL CVE-2018-0802) in Microsoft Office's Equation Editor.
- Downloads an installer package (.msi) and executes on the victim's system.
- The system configuration file drops a backdoor installer and then deletes itself. The backdoor installer will drop a normal sidebar.exe file, a Windows Gadget tool, a malicious loader, and an encrypted configuration file. UserInstall.exe will abuse the BITSadmin command line to create a job, and launch sidebar.exe.
- The malicious loader utilizes DLL hijacking on sidebar.exe and launches dllhost.exe. The loader will then inject a DLL backdoor into dllhost.exe.

Indicators of Compromise

Related Hashes (SHA-256):

- MAL 1d128fd61c2c121d9f2e1628630833172427e5d486cdd4b6d567b7bdac13935e

BKDR_TCLT.ZDFB:

- MAL 01087051f41df7bb030256c97497f69bc5b5551829da81b8db3f46ba622d8a69

BKDR64_TCLT.ZTFB:

- MAL 6e900e5b6dc4f21a004c5b5908c81f055db0d7026b3c5e105708586f85d3e334

TROJ_SCLT.ZTFB:

- MAL 49df4fec76a0ffaee5e4d933a734126c1a7b32d1c9cb5ab22a868e8bfc653245

TROJ_TCDROP.ZTFB:

- MAL b0f120b11f727f197353bc2c98d606ed08a06f14a1c012d3db6fe0a812df528a
- MAL d65f809f7684b28a6fa2d9397582f350318027999be3acf1241ff44d4df36a3a
- MAL 85d32cb3ae046a38254b953a00b37bb87047ec435edb0ce359a867447ee30f8b

TROJ_TCLT.ZDFB:

- MAL 02281e26e89b61d84e2df66a0eeb729c5babd94607b1422505cd388843dd5456
- MAL fb9c9cbf6925de8c7b6ce8e7a8d5290e628be0b82a58f3e968426c0f734f38f6

URLs related to C&C communication:

- URL qpoe.com (/url/qpoe.com)
- URL wikaba.com (/url/wikaba.com)

DETTAGLI RACCOLTA COMMENTI (0)

Report (16)

URL	wikaba.com Report acquisito il 20 mar 2018 20:10:56 da Chris R
URL	dns-stuff.c... Report acquisito il 20 mar 2018 20:10:56 da Chris R
URL	qpoe.com Report acquisito il 20 mar 2018 20:10:55 da Chris R
URL	tibetnews.t... Report acquisito il 20 mar 2018 20:10:55 da Chris R
URL	2waky.com Report acquisito il 20 mar 2018 20:10:55 da Chris R

Visualizza tutti i report

Allegati (0)

Raccolte collegate (0)

Cronologia versione (1)

Chris R

Ultima modifica: 22 mar 2018 13:46:54

- URL tibetnews.today (/url/tibetnews.today)
- URL dns-stuff.com (/url/dns-stuff.com)
- URL 2waky.com (/url/2waky.com)

CVE's

- VUL CVE-2017-11882
- VUL CVE-2018-0802

References

- https://blog.trendmicro.com/trendlabs-security-intelligence/tropic-trooper-new-strategy/ (https://blog.trendmicro.com/trendlabs-security-intelligence/tropic-trooper-new-strategy/)

#xf-malware-advisory