APT32 RETURNS WITH NEW TECHNIQUES TO ATTACK SOUTH EAST ASIAN COUNTRIES

Delaware, USA – March 22, 2019 – APT32, also known as the OceanLotus group, is notorious for the cyber espionage campaigns targeting Asian countries and large-scale watering hole attacks. Researchers of ESET analyzed recent group campaigns and found changes in the group's actions. The adversaries send carefully crafted emails for each target, disguised as current political news and contained legitimate images. In earlier attacks, they used Word documents containing modified exploits for the CVE-2017-11882 vulnerability as attachments. If the victim enabled macros, the code dropped the legitimate EXE file along with the malicious libraries on the system and created scheduled tasks to execute this file every 10 minutes. The executable was used to install backdoor leveraged by APT32 in earlier attacks, however, it connected to the new set of command and control servers.

Since the beginning of this year, the group started to use self-extracting archives to drop and execute malicious OCX files. To avoid detection by antivirus solutions, attackers continually modify the configuration of their backdoors. Each new version leaves fewer traces on the attacked system performing most of the operations in memory and creating files with random names. As in the past campaigns, attackers use an extensive network for C&C communications. To detect the exploitation of the CVE-2017-11882 vulnerability, you can use free SIEM and Yara rules available at Threat Detection Marketplace:
https://tdm.socprime.com/tdm/info/1132
https://tdm.socprime.com/tdm/info/1786/
You can also study all the known techniques used by the APT32 and find the means to detect them in the MITRE ATT&CK section:
https://tdm.socprime.com/att-ck/

SEARCH:

Search... Search

FOLLOW US ON:

RELATED POSTS

BlackWater Backdoor Finds New Way to Misuse Cloudflare Workers

Turla APT Uses NetFlash Dropper and PyFlash Backdoor in Watering Hole Attacks

Hacker Wars: njRat Hides in "Free" Hacking Tools Published on Underground Forums