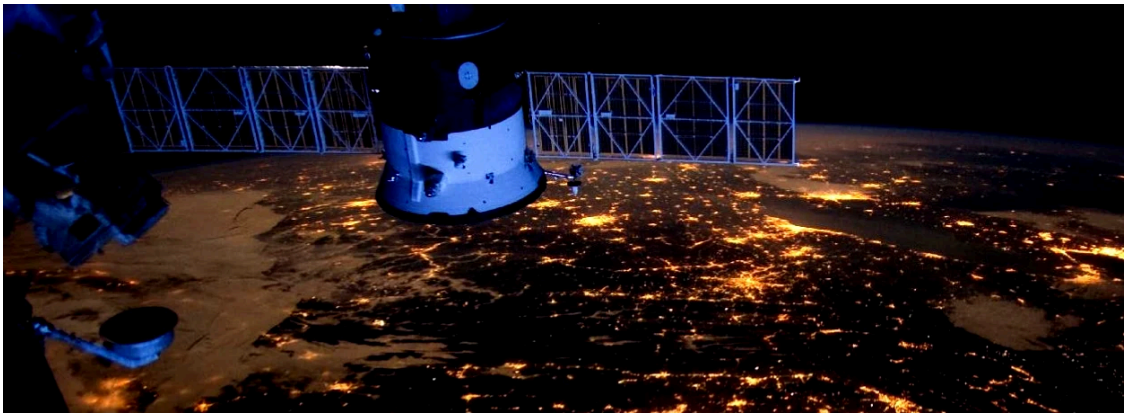
Chinese Hackers Target Satellite, Geospatial Imaging, Defense Companies

By Catalin Cimpanu

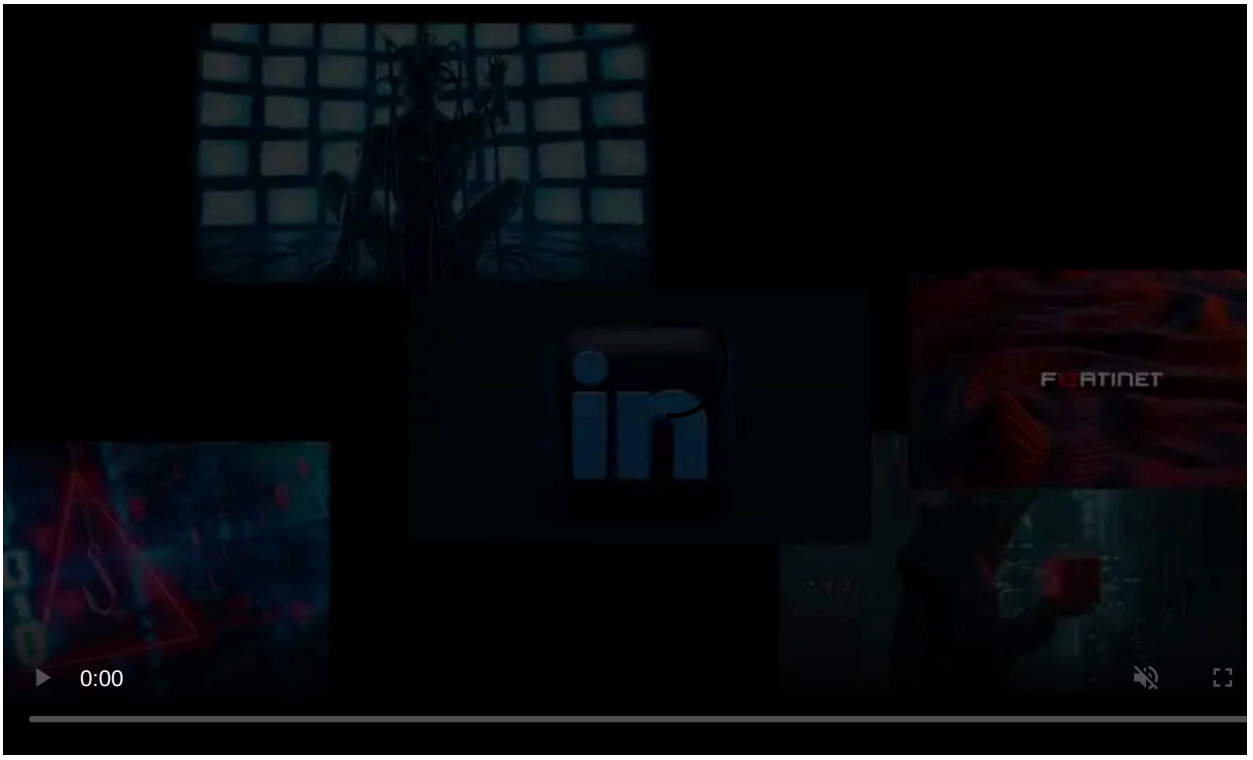
Published: 2018-06-19 · Archived: 2026-04-05 19:51:46 UTC

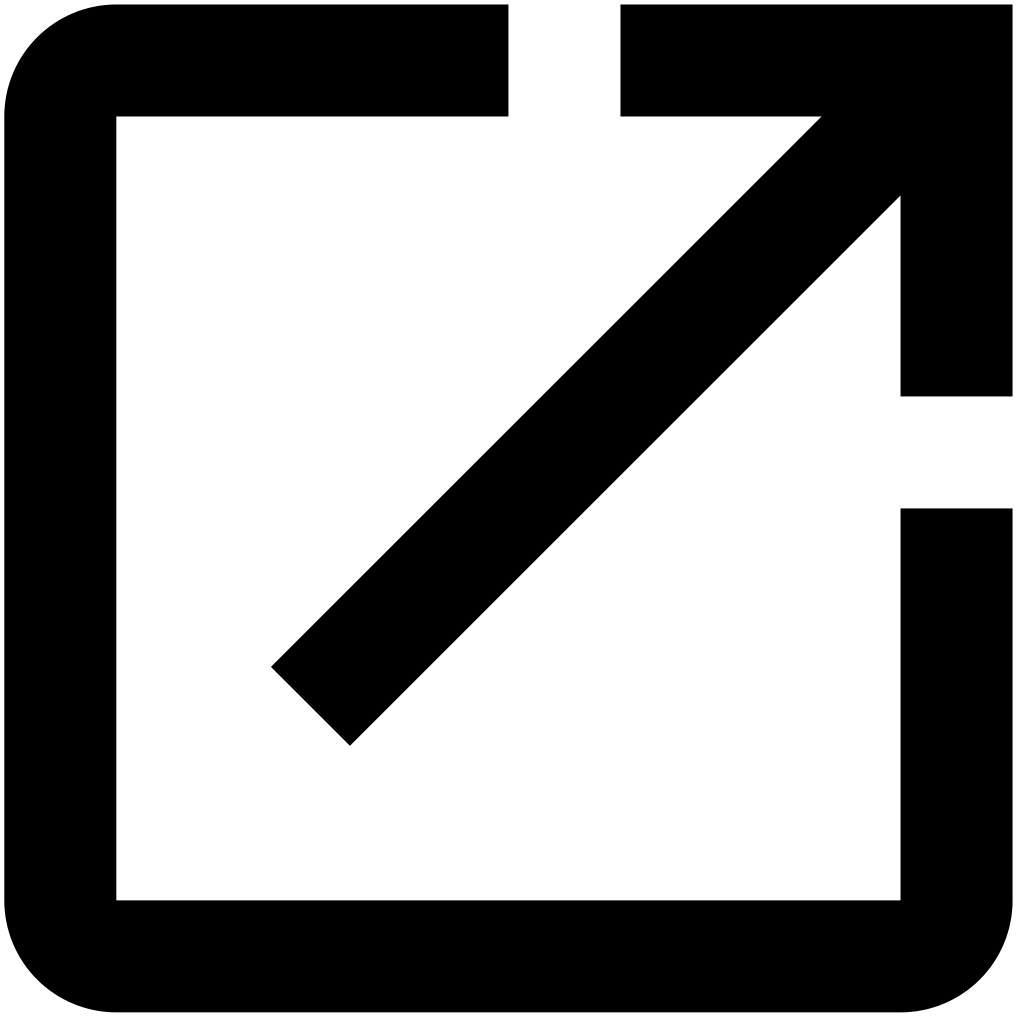


A cyber-espionage group believed to be operating out of China hacked companies who develop satellite communications, geospatial imaging, and defense contractors from both United States and Southeast Asia.

The hacks were detected by US cyber-security firm Symantec, who said today in a report that intruders showed particular interest in the operational side of the breached companies.

Hackers tried to reach and paid close attention to infecting computer systems used for controlling communications satellites or those working with geospatial data collected by world-mapping satellites.


0:00



"This suggests to us that [the group]'s motives go beyond spying and may also include disruption," Symantec said. There are fears that hackers might be able or even attempt to sabotage satellites or poison geospatial data.

Thrip APT behind the hacks

The company said that responsible for the attacks was an advanced persistent threat (APT, a term used to describe cyber-espionage groups) known under the codename of Thrip.

Symantec says it's been tracking this group since 2013, and it has historically believed the group to be operating out of China.

The recent attacks were difficult to detect, the company said. Hackers used a technique known as "living off the land," which consists of using local tools already available on the operating system to carry out malicious operations.

"The purpose of living off the land is twofold," Symantec explained. "By using such features and tools, attackers are hoping to blend in on the victim's network and hide their activity in a sea of legitimate processes. Secondly, even if malicious activity involving these tools is detected, it can make it harder to attribute attacks."

According to Symantec, hackers used the following locally-installed and completely legitimate tools...

PsExec: Microsoft Sysinternals tool for executing processes on other systems. The tool was primarily used by the attackers to move laterally on the victim's network.
PowerShell: Microsoft scripting tool that was used to run commands to download payloads, traverse compromised networks, and carry out reconnaissance.
Mimikatz: Freely available tool capable of changing privileges, exporting security certificates, and recovering Windows passwords in plaintext.
WinSCP: Open source FTP client used to exfiltrate data from targeted organizations.
LogMeIn: Cloud-based remote access software. It's unclear whether the attackers gained unauthorized access to the victim's LogMeIn accounts or whether they created their own.

...to install custom-made malware such as:

Trojan.Rikamanu: A custom Trojan designed to steal information from an infected computer, including credentials and system information.
Infostealer.Catchamas: Based on Rikamanu, this malware contains additional features designed to avoid detection. It also includes a number of new capabilities, such as the ability to capture information from newer applications (such as new or updated web browsers) that have emerged since the original Trojan.Rikamanu malware was created.
Trojan.Mycicil: A keylogger known to be created by underground Chinese hackers. Although publicly available, it is not frequently seen.
Backdoor.Spedear: Although not seen in this recent wave of attacks, Spedear is a backdoor Trojan that has been used by Thrip in other campaigns.
Trojan.Syndicasec: Another Trojan used by Thrip in previous campaigns.

Hacks detected as back as January 2018

Symantec says it detected these attacks only after one of its artificial intelligence and machine learning-based triggered an alert for a suspicious use of a legitimate tool.

Experts say they've used this initial alert to uncover initial signs of compromise and then pulled on a thread to uncover a broader operation targeting multiple companies across multiple countries and industry sectors. The purpose of this hacking campaign was obvious cyber-espionage.

The company says it uncovered this operation in January, but the Thrip hacking campaign could be broader than the company has currently reported.

Source: https://www.bleepingcomputer.com/news/security/chinese-hackers-target-satellite-geospatial-imaging-defense-companies/