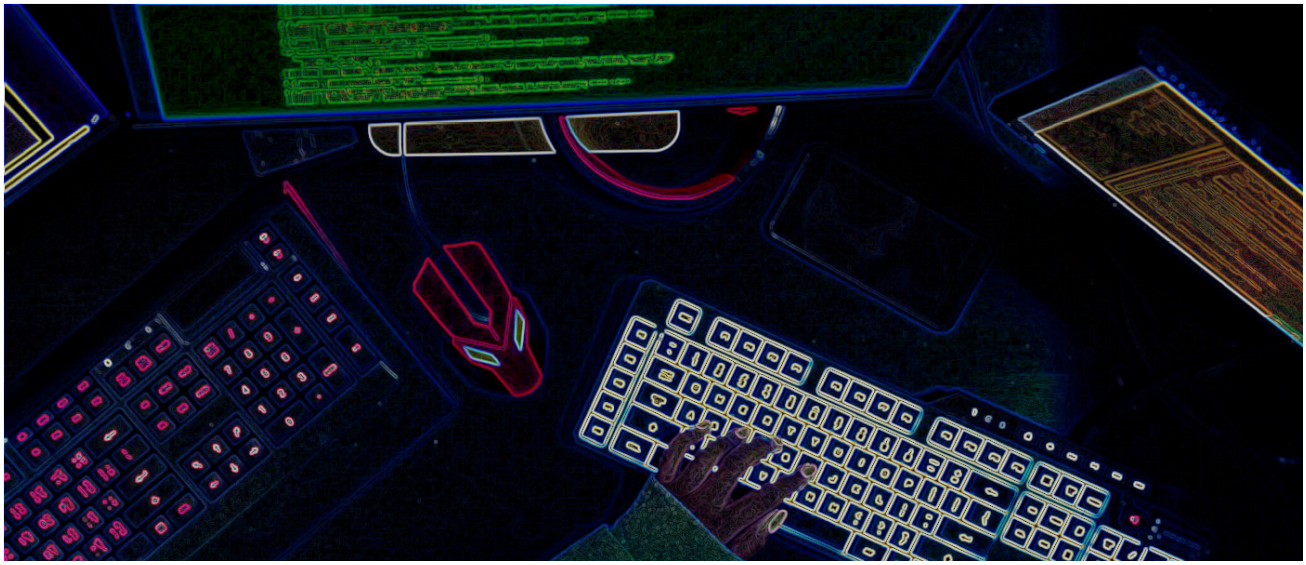
China's APT hackers move to ransomware attacks

bleepingcomputer.com/news/security/chinas-apt-hackers-move-to-ransomware-attacks/

Ionut Ilascu

By
Ionut Ilascu

- January 4, 2021
- 09:36 AM
- 1



Security researchers investigating a set of ransomware incidents at multiple companies discovered malware indicating that the attacks may be the work of a hacker group believed to operate on behalf of China.

Although the attacks lack the sophistication normally seen with advanced threat actors, there is strong evidence linking them to APT27, a group normally involved in cyber espionage campaigns, also known as TG-3390, Emissary Panda, BRONZE UNION, Iron Tiger, and LuckyMouse.

Abusing Windows BitLocker

The attacks happened in 2020 and directly targeted at least five companies in the online gambling sector that operate globally and successfully encrypted several core servers.

While these were ransomware incidents in earnest, the threat actor relied on BitLocker, the drive encryption tool in Windows, to lock the servers.

The researchers from cybersecurity firms Profero and Security Joes responded to these incidents and found that the hackers reached their targets through a third-party service provider, which had been infected through another third-party provider.

Analyzing the attacks revealed malware samples linked to DRBControl, a campaign described earlier this year in a report from Trend Micro and attributed to APT27 and Winnti, both groups active since at least 2010 and associate with Chinese hackers. If APT27 focuses on cyberespionage, Winnti is known for its financial motivation.

In a joint report shared with BleepingComputer, Profero and Security Joes share evidence pointing to these two groups saying that they found a sample of the Clambling backdoor similar to the one used in the DRBControl campaign.

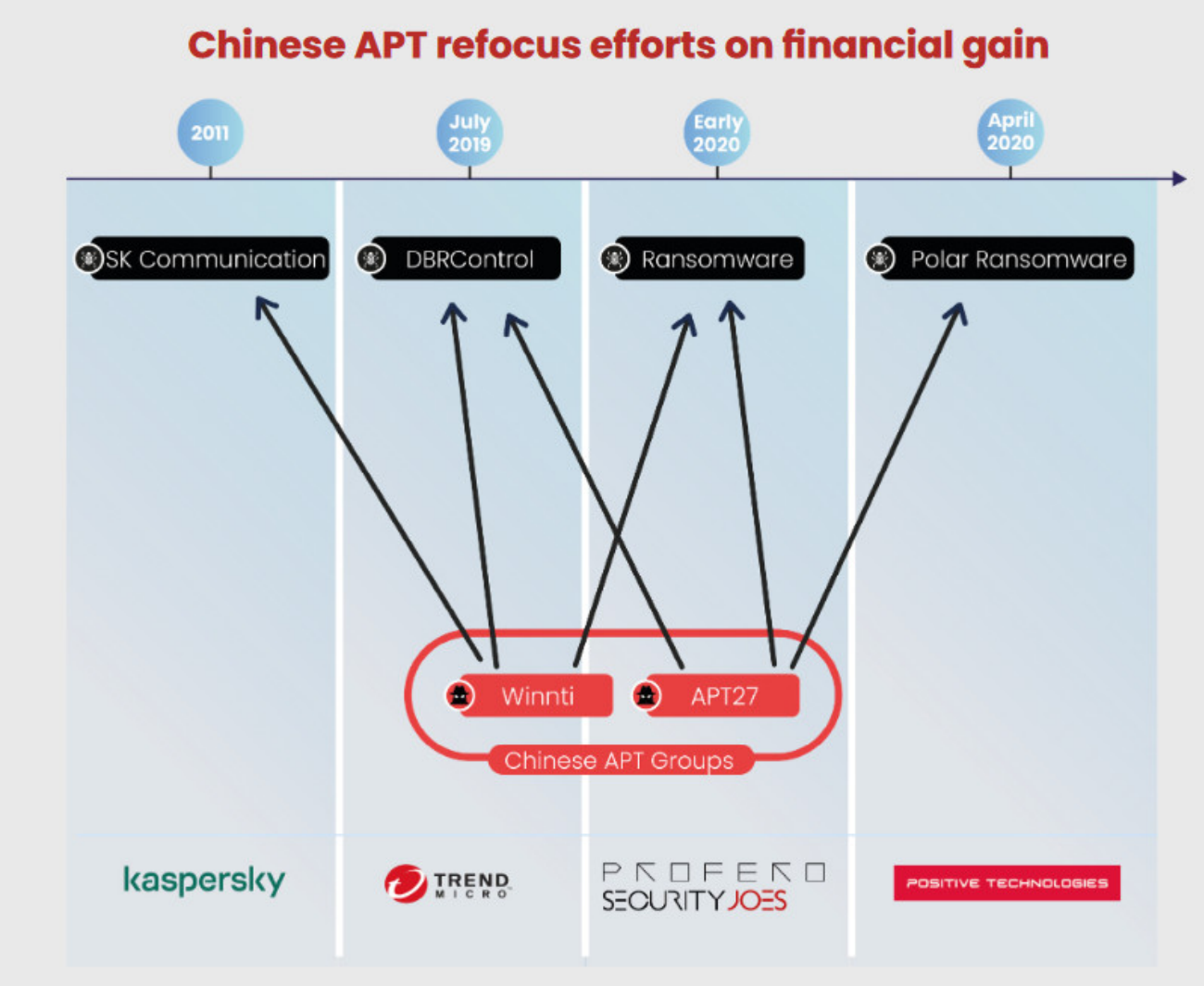
They also uncovered the ASPXSpy webshell. A modified version of this malware has been seen previously in attacks attributed to APT27.

Other malware found on infected computers includes the PlugX remote access trojan, regularly mentioned in cybersecurity reports about campaigns linked to China.

"With regards to who is behind this specific infection chain, there are extremely strong links to APT27/Emissary Panda, in terms of code similarities, and TTPs [tactics, techniques, and procedures]," the report reads.

Although a cyberespionage group engaging in a financially-motivated campaign is unusual, this attack would not be the first time APT27 deploys ransomware on victim systems.

Researchers at Positive Technologies attributed a Polar ransomware attack from April 2020 to APT27, based on the use of malware normally used by this group.



The attacks against the five companies in the gambling sector were not particularly sophisticated and relied on known methods to evade detection and move laterally.

The report from Profero and Security Joes says that the actor deployed PlugX and Clambling malware in the system memory using an older Google Updater executable that was vulnerable to DLL side-loading.

"For each of the two samples, there was a legitimate executable, a malicious DLL, and a binary file consisting of shellcode responsible for extracting the payload from itself and running it in memory. Both samples used the signed Google Updater, and both DLLs were labeled goopdate.dll, however the PlugX binary file was named license.rtf, and the Clambling binary file was named English.rtf."

Additionally, the attacker leveraged a vulnerability from 2017 (CVE-2017-0213) to escalate privileges on the machine. Exploit code for this bug is publicly available.

Daniel Bunce, Principal Security Analyst at Security Joes, told BleepingComputer that the key takeaway from these attacks is the involvement of a cyberespionage group in a financially-driven campaign.

Omri Segev Moyal, CEO at Profero, says that the audacity of such a malicious group is another signal that governments should have a unified approach in the fight against these threats.

Recently, another hacker group believed to work for a government has been linked to ransomware attacks. According to ClearSky, the Iranian-backed hacking group Fox Kitten has been involved in Pay2Key ransomware operations against organizations in Israel and Brazil.

Related Articles:

Hackers target Russian govt with fake Windows updates pushing RATs

Chinese ‘Space Pirates’ are hacking Russian aerospace firms

Hackers stole data undetected from US, European orgs since 2019

Google: Chinese state hackers keep targeting Russian govt agencies

Chinese hacking group uses new 'Fire Chili' Windows rootkit

- APT
- China
- Winnti

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- Previous Article
- Next Article

Comments

edmoncu - 11 months ago

-
-

please list the IOCs here

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: