Chinese hackers linked to months-long attack on Taiwanese financial sector

therecord.media/chinese-hackers-linked-to-months-long-attack-on-taiwanese-financial-sector/

February 21, 2022

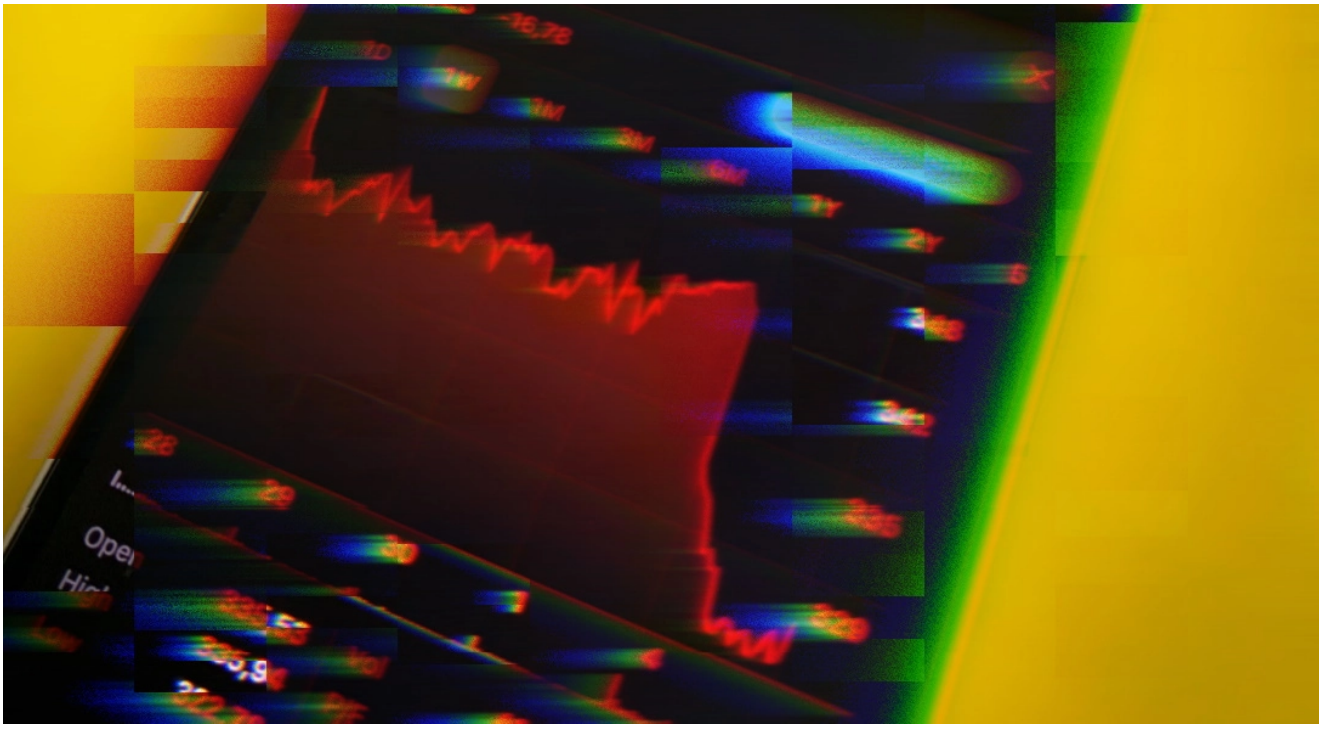

Image: Hakan Nural, The Record

Catalin Cimpanu

February 21, 2022

- China
- Malware
- Nation-state
- News

- Taiwanese security firm links APT10 Chinese espionage group to attacks on local financial sector.
- Attacks targeted a vulnerability in a security product used by roughly 80% of the Taiwanese financial sector.
- Initially, the espionage campaign went undetected because it was misidentified as a credential stuffing attack.

A hacking group affiliated with the Chinese government is believed to have carried out a months-long attack against Taiwan's financial sector by leveraging a vulnerability in a security software solution used by roughly 80% of all local financial organizations.

The attacks are believed to have started at the end of November 2021 and were still taking place this month, according to a report shared with The Record today by Taiwanese security firm CyCraft.

The company attributed the intrusions—which it tracked under the codename of **Operation Cache Panda**—to a well-known Chinese cyber-espionage group known in the cybersecurity industry as APT10.

The security firm told The Record in an interview earlier today that it couldn't share the name of the product exploited in the current attacks because of the ongoing law enforcement investigation and because of the efforts to have a patch released and installed across the local financial sector.

APT10 disguised intrusions behind credential stuffing attack

Instead, the company said that the attacks initially went undetected because they were misclassified.

Investigations into the November 2021 attacks missed the part where hackers exploited the software vulnerability and only saw a credential stuffing attack that APT10 used as a cover and a way to get access to some trading accounts, which they used to execute large transactions on the Hong Kong stock market.

But CyCraft researchers said that the credential stuffing attacks were only used as a cover. In reality, APT10 exploited a vulnerability in the web interface of a security tool, planted a version of the ASPXCSharp web shell, and then used a tool called Impacket to scan a target company's internal network.

The attackers then used a technique called reflective code loading to run malicious code on local systems and install a version of the Quasar RAT that allowed the attackers persistent remote access to the infected system using reverse RDP tunnels.

CyCraft said it was able to uncover the truth behind the November 2021 attacks after one of its customers was hit in February 2022.

"Further investigation showed that what was initially presumed to be two separate waves of cyberattacks was actually one prolonged attack campaign in which the attackers leveraged advanced obfuscation techniques not previously observed," the company told The Record today.

"The objective of the attacks does not appear to have been financial gain but rather the exfiltration of brokerage information, PII data, and the disruption of investment during a period of economic growth for Taiwan," it added.

The attacks are not surprising, as Chinese cyberespionage groups have had Taiwan in their sights for years, having repeatedly and relentlessly attacked almost all sectors of its local government and economy.

Tags

- APT
- APT10
- China
- CyCraft
- malware
- nation-state
- supply chain attack
- Taiwan
- vulnerability

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.