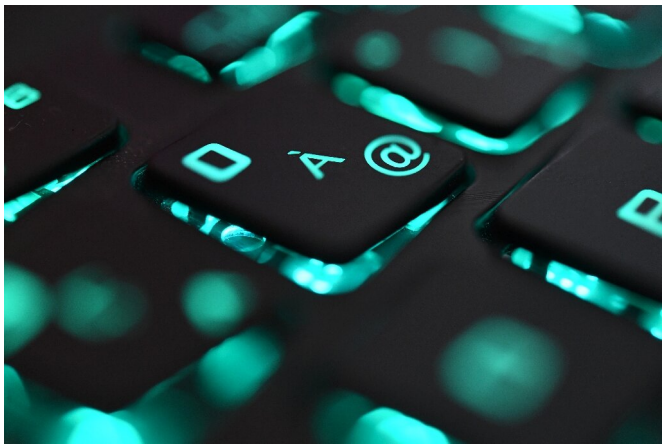
APT41, the China-based hacking operation spanning the world

18 September 2020, by Jing Xuan Teng



Some experts say hacking collective APT41 is tied to the Chinese state

A global hacking collective known as APT41 has been accused by US authorities of targeting company servers for ransom, compromising government networks and spying on Hong Kong activists.

Seven members of the group—including five Chinese nationals—were charged by the US Justice Department on Wednesday.

Some experts say they are tied to the Chinese state, while others speculate money was their only motive. What do we really know about APT41?

Who are they?

Five members of the group were expert hackers and current or former employees of Chengdu 404 Network Technology, a company that claimed to provide legitimate "white hat" hacking services to detect vulnerabilities in clients' computer networks.

But the firm's work also included malicious attacks on non-client organisations, according to Justice Department documents.

Chengdu 404 says its partners include a government tech security assessor and Chinese universities.

The other two hackers charged are Malaysian executives at SEA Gamer Mall, a Malaysia-based firm that sells video game currency, power-ups and other in-game items.

What are they accused of?

The team allegedly hacked the computers of hundreds of companies and organisations around the world, including healthcare firms, software developers and telecoms and pharmaceutical providers.

The breaches were used to collect identities, hijack systems for ransom, and remotely use thousands of computers to mine for cryptocurrency such as bitcoin.

One target was an anti-poverty non-profit, with the hackers taking over one of its computers and holding the contents hostage using encryption software and demanding payment to unlock it.

The group is also suspected of compromising government networks in India and Vietnam.

In addition it is accused of breaching video game companies to steal in-game items to sell back to gamers, the Justice Department court filings said.

How did they operate?

Their arsenal ran the gamut from old-fashioned phishing emails to more sophisticated attacks on software development companies to modify their code, which then allowed them access to clients' computers.

In one case documented by security company FireEye, APT41 sent emails containing malicious software to human resources employees of a target company just three days after the firm recovered from a previous attack by the group.

Wong Ong Hua and Ling Yang Ching, the two Malaysian businessmen, ordered their employees to create thousands of fake video game accounts in order to receive the virtual objects stolen by APT41 before selling them on, the court documents allege.

Is the Chinese government behind them?

FireEye says the group's targeting of industries including healthcare, telecoms and news media is "consistent with Chinese national policy priorities".

APT41 collected information on pro-democracy figures in Hong Kong and a Buddhist monk from Tibet—two places where Beijing has faced political unrest.

One of the hackers, Jiang Lizhi, who worked under the alias "Blackfox", had previously worked for a hacking group that served government agencies and boasted of close connections with China's Ministry of State Security.

But many of the group's activities appear to be motivated by financial gain and personal interest—with one hacker laughing in chat messages about mass-blackmailing wealthy victims—and the US indictments did not identify a strong official connection.

Where are they now?

The five Chinese hackers remain at large but the two businessmen were arrested in Malaysia on Monday after a sweeping operation by the FBI and private companies including Microsoft to block the hackers from using their online accounts.

The United States is seeking their extradition.

None of the men charged are known to have lived in the US, where some of their targets were located.

They picked targets outside Malaysia and China because they believed law enforcement would not be able to track them down across borders, the court documents said.