APT41: Indictments Put Chinese Espionage Group in the Spotlight

By About the Author

Archived: 2026-04-05 19:25:59 UTC

The U.S. government has charged seven men in relation to hundreds of cyber attacks against organizations in the U.S. and multiple other countries in Asia and Europe. Two of the men, who were based in Malaysia, were arrested and their extradition to the U.S. has been requested. The other five are based in China and remain at large.

The attacks were attributed to a China-linked organization dubbed APT41 and involved a combination of intellectual property theft and financially motivated cyber crime. While some of our peers monitor APT41 as a single operation, Symantec regards it as two distinct actors: Grayfly and Blackfly.

Grayfly

Grayfly has been particularly active in recent years, mounting high volume espionage attacks against organizations spread across Asia, Europe, and North America. They are interested in a wide range of sectors, including food, financial, healthcare, hospitality, manufacturing, telecoms, and government. It is known for using the Barlaiy/POISONPLUG and Crosswalk/ProxIP (Backdoor.Motnug) malware families in its attacks. Victims are frequently compromised by exploiting public facing web servers.

In recent attacks, Symantec has seen Grayfly deploy Backdoor.Motnug against targeted organizations in conjunction with publicly available Cobalt Strike malware. Backdoor.Motnug provides the attackers with comprehensive remote access to the network and creates proxy connections allowing access to hard-to-reach segments of a target network. In one attack against a telecoms provider, Grayfly was seen using an internal tool capable of interacting with an SMS database, demonstrating that intelligence gathering was the motive of the attack.

Prosecutors in the U.S. have charged three Chinese men – Jiang Lizhi, Qian Chuan, and Fu Qiang – with involvement in attacks that involve Grayfly tools and tactics. The trio are based in the Chinese city of Chengdu and all hold senior positions in a company called Chengdu 404. The company describes itself as a network security specialist and claims to employ a team of white hat hackers who can perform penetration testing along with “offensive” and “defensive” security operations.

The indictment alleges that the three men were also involved in attacks against over 100 different organizations in the U.S., South Korea, Japan, India, Taiwan, Hong Kong, Malaysia, Vietnam, India, Pakistan, Australia, the United Kingdom, Chile, Indonesia, Singapore, and Thailand. Jiang was said to have a “working relationship” with the Chinese Ministry of State Security which would provide him and his associates with a degree of state protection.

Blackfly

Blackfly has been active since at least 2010 and is known for attacks involving the PlugX/Fast (Backdoor.Korplug), Winnti/Pasteboy (Backdoor.Winnti), and Shadowpad (Backdoor.Shadowpad) malware families. The group is best known for its attacks on the computer gaming industry. However, Symantec has also observed attacks on the semiconductor, telecoms, materials manufacturing, pharmaceutical, media and advertising, hospitality, natural resources, fintech, and food sectors.

Recent Blackfly activity observed by Symantec saw the group deploy a slightly modified version of the Winnti malware against a telecoms organization in Taiwan. A feature of the attack was their use of the names of security vendors in naming files in an attempt to avoid raising suspicions. A dropper was signed with an invalid certificate with the subject "McAfee, Inc." The dropper then delivered several DLLs with file names that referenced Symantec software. The attackers had not compromised Symantec software, and were not leveraging it in the attack.

In a separate indictment, prosecutors allege that two Malaysian nationals – Wong Ong Hua and Ling Yang Ching – were involved in attacks that involved Blackfly tools and tactics. Wong is the founder and CEO of a company called Sea Gamer Mall, while Ling is its chief product officer and a shareholder. The duo are alleged to have collaborated with other attackers to mount a string of attacks against computer game companies in order to obtain in-game digital items, such as currencies, and then selling them for profit.

The link between Grayfly and Blackfly

While Grayfly and Blackfly appear to be distinct operations, the indictments allege that there is a link between the two groups. Two Chinese men – Zhang Haoran and Tan Dailin – are charged in a third indictment with collaborating with both groups. The two men are reported to have worked for a time at Chengdu 404, the company that prosecutors identify as linked to Grayfly attacks. However, they are also alleged to have collaborated with the charged Blackfly actors in order to make additional money by mounting attacks on computer gaming companies. The indictment alleges that in several instances, they used their unauthorized access to gaming company networks to kick other attackers off the network, effectively eliminating their competition.

Unwelcome attention

Grayfly and Blackfly have been prolific attackers in recent years and, while it remains to be seen what impact the charges will have on their operations, the publicity surrounding the indictments will certainly be unwelcome among attackers who wish to maintain a low profile. Symantec remains committed to tracking the activity of these groups in order to protect our customers from their attacks.

Protection/Mitigation

Symantec products protect against threats discussed in this blog with the following detections:

- Backdoor.Motnug
- Backdoor.Korplug
- Backdoor.Winnti
- Backdoor.Shadowpad

Indicators of Compromise

Source: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/apt41-indictments-china-espionage