DOJ reveals indictment against Chinese cyberspies that stole U.S. business secrets

By Chris Bing

Published: 2017-11-27 · Archived: 2026-04-06 03:15:06 UTC

A group of Chinese hackers recently indicted by the Department of Justice were involved in an international cyber-espionage operation connected to a foreign intelligence agency, security researchers tell CyberScoop.

On Monday, senior Justice Department officials announced eight relevant criminal charges against the Chinese hackers. Although the indictment was originally issued in September, it was sealed until Monday.

The criminal activity allegedly dates as far back as 2011.

Court documents describe that Chinese nationals Wu Yingzhuo, Dong Hao and Xia Lei hacked into and stole data from several American companies, including Siemens AG, Moody's Analytics and GPS technology company Trimble. The trio worked together at a company named Boyusec, also known as the Guangzhou Bo Yu Information Technology Co.

Business registration records show that Wu and Dong are executives at Boyusec.

Conservative news outlet The Washington Free Beacon reported in November 2016 that Boyusec, which it described as a Chinese cybersecurity firm, acts as a front for Beijing's intelligence collection mission. Boyusec is a technology contractor for China's Ministry of State Security (MSS), according to The Free Beacon.

Over the past several years, Wu and Dong have used their own names to register multiple dummy domains which dispensed malware.

Further technical review of Wu, Dong and Xia's apparent intrusion techniques — which were extensively detailed by the FBI and Justice Department — now suggests the three Chinese nationals are likely affiliated with a known hacker group already identified by security researchers and labeled "APT3," according to an analysis conducted by cybersecurity firms FireEye and Recorded Future.

"We believe that the indicted individuals and Boyusec are linked to APT3," said Ben Read, an analyst with FireEye.

FireEye has stated that APT3 is "state-sponsored."

The connection between the three Chinese nationals and APT3 underscores the thin border that divides China's government and private sector institutions, experts say. The indictment does not cite a connection between the suspects and the Chinese government.

Chris Doman, a security analyst with AlienVault, told CyberScoop that APT3 is known for targeting western defense contractors and American aerospace companies as well as domestic dissidents in Hong Kong. More

recently, the hackers have focused on the latter, said Doman.

Recorded Future, another firm which has done significant research on APT3, said they too were confident that the indicted individuals are associated with Boyusec and that the Chinese security company is an extension of APT3 —which in turn represents China's MSS.

"We have a high degree of confidence that APT3 is the MSS," said Priscilla Moriuchi, director of strategic threat development at Recorded Future. "The use of this MSS front company, Boyusec, is emblematic of how the MSS conducts operations in both the human and cyber domains."

Moriuchi continued, "the MSS is composed of national, provincial, and local elements. Many of these elements, especially at the provincial and local levels, include organizations with valid public missions to act as a cover for MSS intelligence operations. Some of these organizations include think tanks such as CICIR, while others include provincial-level governments and local offices."

APT3, which is also known as Gothic Panda, Pirpi or UPS by the cybersecurity community, is responsible for more than 75 breaches that have occurred between mid-2005 and 2016.

Researchers told CyberScoop that APT3 was hacking into victim networks as recently as September 2016, leading some to believe the group may still be active today.

"[The indictments] are important because this is the first set of indictments against Chinese actors since 2014, and the first ever indictments against intelligence officers as opposed to military officers," said Moriuchi.

In 2015, former U.S. President Barack Obama and current Chinese President Xi Jinping came to an agreement that China would discontinue its use of hackers to steal intellectual property and other valuable data from American companies.

Experts generally agree that the 2015 truce has resulted in a substantial decline in such activity.

In a statement sent to CyberScoop, a Justice Department spokesperson said the department had little luck working with the Chinese government to arrest or investigate those indicted.

"As part of the October 2017 Law Enforcement and Cybersecurity Dialogue, the Department used the established mechanism to request China's assistance in investigating and putting a stop to Boyusec's activities," the spokesperson said. "We received no meaningful response. Accordingly, at this stage, we have pursued every available avenue to hold the actors accountable in this case and have determined that there is no longer a law enforcement justification to keep the charges under seal. We will continue to press the Chinese government to take steps to prevent this kind of behavior in the future and to hold the actors accountable under Chinese law."

The spokesperson reiterated that the indictment did not state that the hackers were working on behalf of the Chinese government.
