U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage

Published: 2017-11-27 · Archived: 2026-04-06 03:21:13 UTC

An indictment was unsealed today against Wu Yingzhuo, Dong Hao and Xia Lei, all of whom are Chinese nationals and residents of China, for computer hacking, theft of trade secrets, conspiracy and identity theft directed at U.S. and foreign employees and computers of three corporate victims in the financial, engineering and technology industries between 2011 and May 2017. The three Chinese hackers work for the purported China-based Internet security firm Guangzhou Bo Yu Information Technology Company Limited (a/k/a "Boyusec").

Acting Assistant Attorney General for National Security Dana J. Boente, Acting U.S. Attorney Soo C. Song for the Western District of Pennsylvania and Special Agent in Charge Robert Johnson of the FBI's Pittsburgh Division announced the charges.

The indictment alleges that the defendants conspired to hack into private corporate entities in order to maintain unauthorized access to, and steal sensitive internal documents and communications from, those entities' computers. For one victim, information that the defendants targeted and stole between December 2015 and March 2016 contained trade secrets.

"Once again, the Justice Department and the FBI have demonstrated that hackers around the world who are seeking to steal our companies' most sensitive and valuable information can and will be exposed and held accountable," said Acting Assistant Attorney General Boente. "The Justice Department is committed to pursuing the arrest and prosecution of these hackers, no matter how long it takes, and we have a long memory."

"Defendants Wu, Dong and Xia launched coordinated and targeted cyber intrusions against businesses operating in the United States, including here in the Western District of Pennsylvania, in order to steal confidential business information," said Acting U.S. Attorney Song. "These conspirators masked their criminal conspiracy by exploiting unwitting computers, called 'hop points,' conducting 'spearphish' email campaigns to gain unauthorized access to corporate computers, and deploying malicious code to infiltrate the victim computer networks."

"In order to effectively address the cyber threat, a threat that respects no boundaries and continues to grow in both its scope and complexity, law enforcement must come together and transcend borders to target criminal actors no matter where they are in the world," said Special Agent in Charge Johnson.

Summary of the Allegations

According to the allegations of the Indictment:

Defendants Wu, Dong, Xia, and others known and unknown to the grand jury (collectively, "the co-conspirators") coordinated computer intrusions against businesses and entities, operating in the United States and elsewhere. To

accomplish their intrusions, the co-conspirators would, for example, send spearphishing e-mails to employees of the targeted entities, which included malicious attachments or links to malware. If a recipient opened the attachment or clicked on the link, such action would facilitate unauthorized, persistent access to the recipient's computer. With such access, the co-conspirators would typically install other tools on victim computers, including malware the co-conspirators referred to as "ups" and "exeproxy." In many instances, the co-conspirators sought to conceal their activities, location and Boyusec affiliation by using aliases in registering online accounts, intermediary computer servers known as "hop points" and valid credentials stolen from victim systems.

The primary goal of the co-conspirators' unauthorized access to victim computers was to search for, identify, copy, package, and steal data from those computers, including confidential business and commercial information, work product, and sensitive victim employee information, such as usernames and passwords that could be used to extend unauthorized access within the victim systems. For the three victim entities listed in the Indictment, such information included hundreds of gigabytes of data regarding the housing finance, energy, technology, transportation, construction, land survey, and agricultural sectors.

Defendants: At all times relevant to the charges, the Indictment alleges as follows

- **Wu Yingzhuo**, aka "mxmtmw," "Christ Wu" and "wyz," was a Chinese national and resident of Guangzhou. Wu was a founding member and equity shareholder of Boyusec.
- **Dong Hao**, aka "Bu Yi," "Dong Shi Ye" and "Tianyu," was a Chinese national and resident of Guangzhou. Dong was a founding member and equity shareholder of Boyusec, who held the title of "Executive Director and Manager."
- **Xia Lei**, aka "Sui Feng Yan Mie," was a Chinese national and resident of Guangzhou. Xia was, at certain times relevant to the charges, an employee of Boyusec.

Victims: Moody's Analytics, Siemens AG ("Siemens") and Trimble, Inc. ("Trimble").

Time period: As alleged in the Indictment, the conspiracy began at least as early as 2011 and continued to May 2017.

Crimes: Eight counts as follows (all defendants are charged in all counts).

Count(s)	Charge	Statute	Maximum Penalty
1	Conspiring to commit computer fraud and abuse	18 U.S.C. § 1030(b)	10 years
2	Conspiring to commit trade secret theft	18 U.S.C. §§ 1832(a)(5)	10 years
3	Wire fraud	18 U.S.C. § 1343	20 years

4-8	Aggravated identity theft	18 U.S.C. §§ 1028A(a)(1), (b), (c)(4), and 2	2 years (mandatory consecutive)

Any sentence will be imposed by the court only after consideration of the U.S. Sentencing Guidelines and the federal statute governing the imposition of a sentence, 18 U.S.C. § 3553.

Summary of Defendants' Conduct Alleged in the Indictment

Defendant	**Victim**	**Criminal Conduct**
Wu	Trimble	In 2015 and 2016, Trimble was developing a Global Navigation Satellite Systems technology designed to improve the accuracy of location data on mobile devices. In January 2016, while this project was in development, Wu accessed Trimble's network and stole files containing commercial business documents and data pertaining to the technology, including Trimble trade secrets. In total, between December 2015 and March 2016, Wu and the other co-conspirators stole at least 275 megabytes of data, including compressed data, which included hundreds of files that would have assisted a Trimble competitor in developing, providing and marketing a similar product without incurring millions of dollars in research and development costs.
Dong	Siemens	In 2014, Dong accessed Siemens's computer networks for the purpose of obtaining and using employees' usernames and passwords in order to access Siemens' network. In 2015, the co-conspirators stole approximately 407 gigabytes of proprietary commercial data pertaining to Siemens's energy, technology and transportation businesses.
Xia	Moody's Analytics	In or around 2011, the co-conspirators accessed the internal email server of Moody's Analytics and placed a forwarding rule in the email account of a prominent employee. The rule directed all emails to and from the employee's account to be forwarded to web-based email accounts controlled by the conspirators. In 2013 and 2014, defendant Xia regularly accessed those web-based email accounts to access the employee's stolen emails, which contained proprietary and confidential economic analyses, findings and opinions.

An indictment is merely an accusation and a defendant is presumed innocent unless proven guilty in a court of law.

The FBI, Naval Criminal Investigative Service and Air Force Office of Special Investigations conducted the investigation that led to the charges in the indictment.

The government’s case is being prosecuted by Assistant U.S. Attorney James T. Kitchen of the Western District of Pennsylvania, and Cyber Counsel Jessica Romero and Trial Attorney Jennifer Kennedy Gellie of the National Security Division’s Counterintelligence and Export Control Section.

Source: https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations