Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years

Published: 2018-10-30 · Archived: 2026-04-06 03:14:24 UTC

Chinese intelligence officers and those working under their direction, which included hackers and co-opted company insiders, conducted or otherwise enabled repeated intrusions into private companies' computer systems in the United States and abroad for over five years. The conspirators' ultimate goal was to steal, among other data, intellectual property and confidential business information, including information related to a turbofan engine used in commercial airliners.

The charged intelligence officers, Zha Rong and Chai Meng, and other co-conspirators, worked for the Jiangsu Province Ministry of State Security ("JSSD"), headquartered in Nanjing, which is a provincial foreign intelligence arm of the People's Republic of China's Ministry of State Security ("MSS"). The MSS, and by extension the JSSD, is primarily responsible for domestic counter-intelligence, non-military foreign intelligence, and aspects of political and domestic security.

From at least January 2010 to May 2015, JSSD intelligence officers and their team of hackers, including Zhang Zhang-Gui, Liu Chunliang, Gao Hong Kun, Zhuang Xiaowei, and Ma Zhiqi, focused on the theft of technology underlying a turbofan engine used in U.S. and European commercial airliners. This engine was being developed through a partnership between a French aerospace manufacturer with an office in Suzhou, Jiangsu province, China, and a company based in the United States. Members of the conspiracy, assisted and enabled by JSSD-recruited insiders Gu Gen and Tian Xi, hacked the French aerospace manufacturer. The hackers also conducted intrusions into other companies that manufactured parts for the turbofan jet engine, including aerospace companies based in Arizona, Massachusetts and Oregon. At the time of the intrusions, a Chinese state-owned aerospace company was working to develop a comparable engine for use in commercial aircraft manufactured in China and elsewhere.

Defendant Zhang Zhang-Gui is also charged, along with Chinese national Li Xiao, in a separate hacking conspiracy, which asserts that Zhang Zhang-Gui and Li Xiao leveraged the JSSD-directed conspiracy's intrusions, including the hack of a San Diego-based technology company, for their own criminal ends.

"For the third time since only September, the National Security Division, with its US Attorney partners, has brought charges against Chinese intelligence officers from the JSSD and those working at their direction and control for stealing American intellectual property," said John C. Demers, Assistant Attorney General for National Security. "This is just the beginning. Together with our federal partners, we will redouble our efforts to safeguard America's ingenuity and investment."

"State-sponsored hacking is a direct threat to our national security. This action is yet another example of criminal efforts by the MSS to facilitate the theft of private data for China's commercial gain," said U.S. Attorney Adam

Braverman. "The concerted effort to steal, rather than simply purchase, commercially available products should offend every company that invests talent, energy, and shareholder money into the development of products."

"The threat posed by Chinese government-sponsored hacking activity is real and relentless," said John Brown, FBI Special Agent in Charge of the San Diego Field Office. "Today, the Federal Bureau of Investigation, with the assistance of our private sector, international and U.S. government partners, is sending a strong message to the Chinese government and other foreign governments involved in hacking activities. We are working together to vigorously investigate and hold hackers accountable regardless of their attempts to hide their illicit activities and identities."

On October 10, the Department of Justice announced that a JSSD intelligence officer was extradited to the Southern District of Ohio, on charges that he attempted to steal trade secrets related to jet aircraft engines, and in September, in the Northern District of Illinois, a U.S. Army recruit was charged with working as an agent of a JSSD intelligence officer, without notification to the Attorney General.

As the indictment in the Southern District of California describes in detail, China's JSSD intelligence officers and hackers working at their direction masterminded a series of intrusions in order to facilitate intrusions and steal non-public commercial and other data. The hackers used a range of techniques, including spear phishing, sowing multiple different strains of malware into company computer systems, using the victim companies' own websites as "watering holes" to compromise website visitors' computers, and domain hijacking through the compromise of domain registrars.

The first alleged hack began no later January 8, 2010, when members of the conspiracy infiltrated Capstone Turbine, a Los-Angeles-based gas turbine manufacturer, in order to steal data and use the Capstone Turbine website as a "watering hole."

China's intelligence service also sought, repeatedly, to hack into a San Diego-based technology company from at least August 7, 2012 through January 15, 2014, in order to similarly steal commercial information and use its website as a "watering hole."

Chinese actors used not only hacking methods to conduct computer intrusions and steal commercial information, they also coopted victim company employees. From at least November 2013 through February 2014, two Chinese nationals working at the direction of the JSSD, Tian Xi and Gu Gen, were employed in the French aerospace company's Suzhou office. On January 25, 2014, after receiving malware from an identified JSSD officer acting as his handler, Tian infected one of the French company's computers with malware at the JSSD officer's direction. One month later, on February 26, 2014, Gu, the French company's head of Information Technology and Security in Suzhou, warned the conspirators when foreign law enforcement notified the company of the existence of malware on company systems. That same day, leveraging that tip-off, conspirators Chai Meng and Liu Chunliang tried to minimize JSSD's exposure by causing the deletion of the domain linking the malware to an account controlled by members of the conspiracy.

The group's hacking attempts continued through at least May of 2015, when an Oregon-based company, which, like many of the other targeted companies, built parts for the turbofan jet engine used in commercial airliners, identified and removed the conspiracy's malware from its computer systems.

Count Two of the indictment charges a separate conspiracy to hack computers in which Zhang Zhang-Gui, a defendant charged in Count One, supplied his co-defendant and friend, Li Xiao, with variants of the malware that had been developed and deployed by hackers working at the direction of the JSSD on the hack into Capstone Turbine. Using malware supplied by Zhang, as well as other malware, Li launched repeated intrusions that targeted a San Diego-based computer technology company for more than a year and a half. These intrusions caused thousands of dollars of damage to protected computers.

Count Three of the indictment charges Zhang Zhang-Gui with the substantive offense of computer hacking a San Diego technology company, which was one of the targets of the conspiracies alleged in Counts One and Two.

The charges contained in the indictment are merely accusations, and the defendants are presumed innocent unless and until proven guilty.

The FBI, led by the San Diego Field Office, conducted the investigation that resulted in charges announced today. This case is being prosecuted by Alexandra Foster and Sabrina Fève of the United States Attorney's Office for the Southern District of California and Jason McCullough of the National Security Division's Counterintelligence and Export Control Section. The Criminal Division's Office of International Affairs also provided assistance in this matter, and the Department appreciates the cooperation and assistance provided by France's General Directorate for Internal Security (DGSI) and the Cybercrime Section of the Paris Prosecutor's Office during the investigation of this matter.

Case Number: 13CR3132-H
