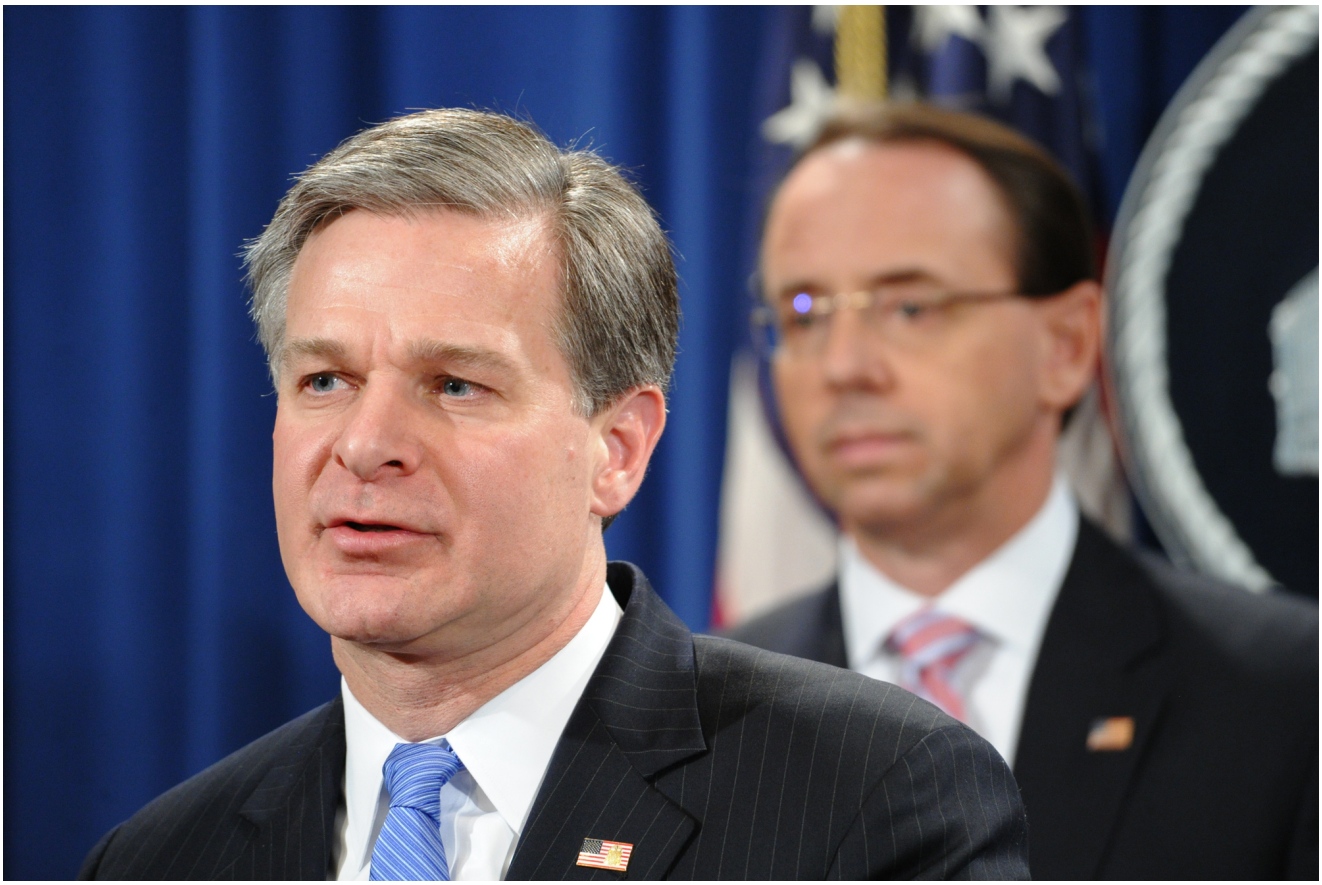
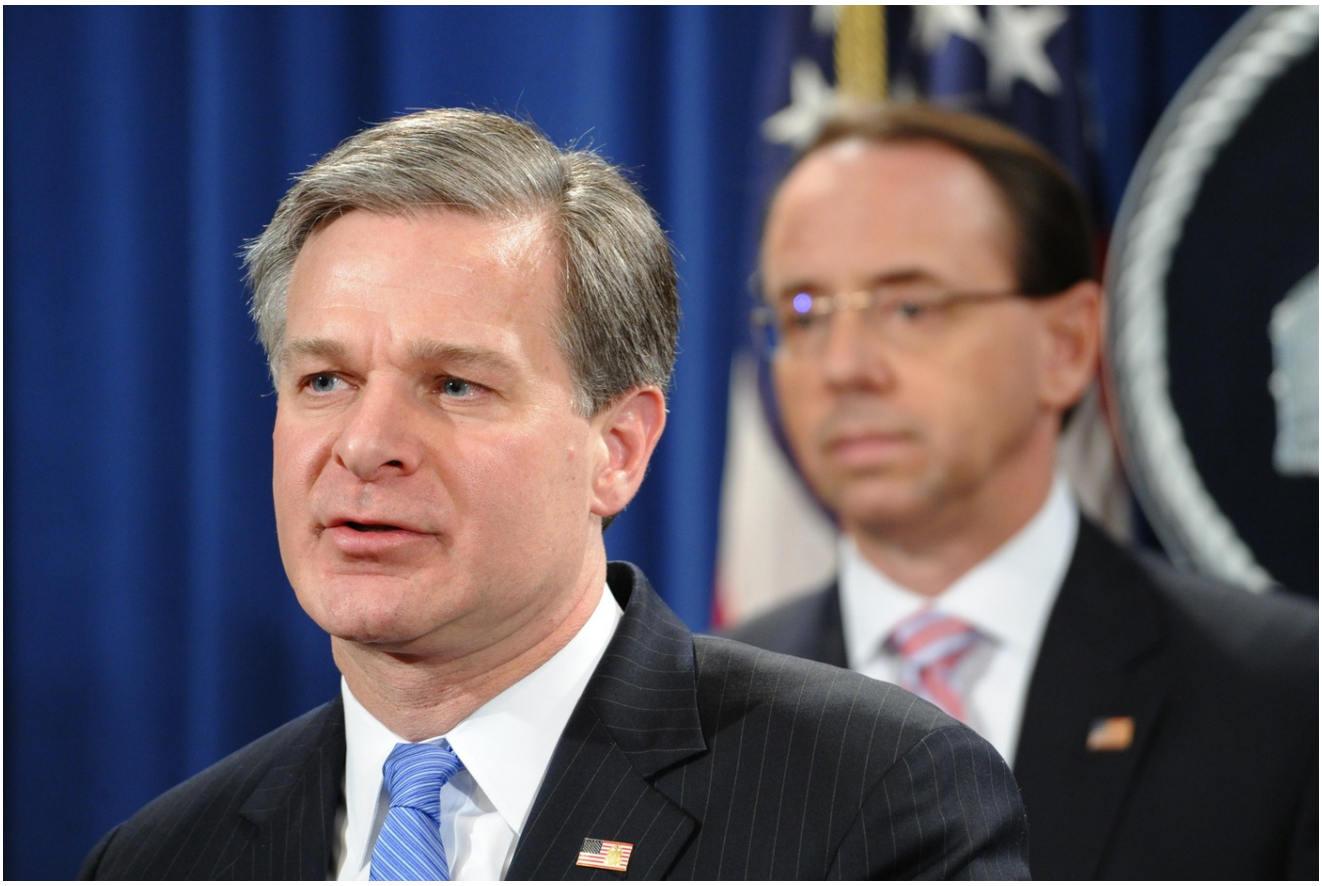
Chinese Hackers Indicted

fbi.gov/news/stories/chinese-hackers-indicted-122018



Members of APT 10 Group Targeted Intellectual Property and Confidential Business Information



FBI Director Christopher Wray speaks at a December 20, 2018 press conference at the Department of Justice announcing charges against Zhu Hua and Zhang Shilong, both Chinese nationals and members of the APT 10 hacking group, as Deputy Attorney General Rod J. Rosenstein looks on.

Two Chinese men have been charged in a massive, years-long hacking campaign that stole personal and proprietary information from companies around the world, the FBI and the Justice Department announced at a press conference today in Washington, D.C.

The men, Zhu Hua and Zhang Shilong, are part of a group known as Advanced Persistent Threat 10, or APT 10, a hacking group associated with the Chinese government. A New York grand jury indicted the pair for conspiracy to commit computer intrusion, conspiracy to commit wire fraud, and aggravated identity theft. The indictment was unsealed today.

According to the indictment, from around 2006 to 2018, APT 10 conducted extensive hacking campaigns, stealing information from more than 45 victim organizations, including American companies. Hundreds of gigabytes of sensitive data were secretly taken from companies in a diverse range of industries, such as health care, biotechnology, finance, manufacturing, and oil and gas.

FBI Director Christopher Wray described the list of companies, not named in the indictment, as a “Who’s Who” of the global economy. Even government agencies like NASA and the Department of Energy were among the victims. The hack is part of China’s ongoing efforts to steal intellectual property from other countries.

“Healthy competition is good for the global economy. Criminal conduct is not. Rampant theft is not. Cheating is not,” Wray said at the press conference.

APT 10 used “spear phishing” techniques to introduce malware onto targeted computers. The hackers sent emails that appeared to be from legitimate addresses but contained attachments that installed a program to secretly record all keystrokes on the machine, including user names and passwords. The group also targeted managed service providers (MSPs), companies that remotely manage their clients’ servers and networks. MSP hacks allowed APT 10 members to indirectly gain access to confidential data of numerous companies who were the clients of the MSPs.

> **“China’s state-sponsored actors are the most active perpetrators of state-sponsored espionage against us.”**
>
> FBI Director Christopher Wray

“When hackers gain access to MSPs, they can steal sensitive business information that gives competitors an unfair advantage,” said Deputy Attorney General Rod J. Rosenstein during today’s announcement.

APT 10 also accessed the personal information of more than 100,000 U.S. Navy personnel.

In remarks announcing the indictments, Wray noted that FBI and Department of Defense investigators worked together to analyze hundreds of malware samples. Investigators found links between victims and APT 10. The FBI’s Cyber Action Team, in collaboration with the Department of Homeland Security, also provided technical assistance and investigated the incidents.

Although the two indicted hackers are believed to be in China, they can be arrested if they travel.

This indictment is the latest in a series of charges against international hackers who target the United States and its allies. In October, seven Russian government operatives were charged with hacking into international anti-doping agencies. Last month, two Iranians were charged with using ransomware to infiltrate critical networks in the United States and Canada.

The cyber espionage threat from China is the most pervasive, Wray stressed.

“China’s goal, simply put, is to replace the U.S. as the world’s leading superpower, and they’re using illegal methods to get there. They’re using an expanding set of non-traditional and illegal methods,” Wray said. “China’s state-sponsored actors are the most active perpetrators of state-sponsored espionage against us.”

WANTED BY THE FBI

APT 10 GROUP

Conspiracy to Commit Computer Intrusions; Conspiracy to Commit Wire Fraud; Aggravated Identity Theft

ZHU HUA

ZHANG SHILONG

DETAILS

On December 17, 2018, a grand jury in the United States District Court for the Southern District of New York indicted ZHU HUA, aka "Afwar," aka "CVNX," aka "Alayos," aka "Godkiller," and ZHANG SHILONG, aka "Baobeilong," aka "Zhang Jianguo," aka "Atreexp," two members of a hacking group operating in China known in the cybersecurity community as Advanced Persistent Threat 10 (the "APT 10 Group"), with conspiracy to commit computer intrusion, conspiracy to commit wire fraud, and aggravated identity theft. The defendants worked for Huaying Haitai Science and Technology Development Company located in Tianjin, China, and they acted in association with the Chinese Ministry of State Security's Tianjin State Security Bureau.

As alleged in the Indictment, from at least 2006 through 2018, the defendants conducted extensive campaigns of global intrusions into computer systems aiming to steal, among other data, intellectual property and confidential business and technological information from more than at least 45 commercial and defense technology companies in at least a dozen states, managed service providers ("MSP"), which are companies that remotely manage the information technology infrastructure of businesses and governments around the world, and U.S. government agencies. The victim companies targeted by ZHU HUA and ZHANG SHILONG were involved in a diverse array of commercial activity, industries, and technologies, including aviation, space and satellite technology, manufacturing technology, oil and gas exploration, production technology, communications technology, computer processor technology, and maritime technology. In addition, for example, the APT 10 Group's campaign compromised the data of an MSP and certain of its clients located in at least 12 countries including Brazil, Canada, Finland, France, Germany, India, Japan, Sweden, Switzerland, the United Arab Emirates, the United Kingdom, and the United States. The APT 10 group also compromised computer systems containing information regarding the United States Department of the Navy and stole the personally identifiable information of more than 100,000 Navy personnel.

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

Select image to view/download poster.