Deputy Attorney General Rod J. Rosenstein Announces Charges Against Chinese Hackers

Published: 2018-12-20 · Archived: 2026-04-06 15:32:07 UTC

I am honored to be joined by FBI Director Chris Wray, National Security Division Assistant Attorney General John Demers, and Southern District of New York U.S. Attorney Geoffrey Berman.

Today, the Department of Justice is announcing a criminal indictment of two computer hackers associated with the Chinese government. The charges include conspiracy to commit computer intrusions against dozens of companies in the United States and around the world. As with all American criminal charges, individual defendants are presumed innocent unless proven guilty in a court of law.

This case is significant because the defendants are accused of targeting and compromising Managed Service Providers, or MSPs. MSPs are firms that other companies trust to store, process, and protect commercial data, including intellectual property and other confidential business information. When hackers gain access to MSPs, they can steal sensitive business information that gives competitors an unfair advantage.

The indictment alleges that defendants worked for a group known to cyber security experts as APT-10. These groups are designated as APTs, or Advanced Persistent Threats, because they use malware to gain access to computer networks and exfiltrate data over an extended period of time.

These defendants allegedly compromised MSP clients in at least a dozen countries. The victims included companies in banking and finance, telecommunications and consumer electronics, medical equipment, packaging, manufacturing, consulting, healthcare, biotechnology, automotive, oil and gas exploration, and mining.

The defendants allegedly committed these crimes in association with a Chinese intelligence service known as the Ministry of State Security.

This is not the first time the Department of Justice has accused Chinese state actors and associates of stealing commercial information. Since the indictment of five uniformed members of the People's Liberation Army in 2014, our Department has repeatedly cast a spotlight on Chinese state-sponsored criminal activity targeting U.S. companies.

More than 90 percent of the Department's cases alleging economic espionage over the past seven years involve China. More than two-thirds of the Department's cases involving thefts of trade secrets are connected to China. In the last few months of this year, our Department has announced charges in three cases alleging crimes committed at the behest of a branch of the Chinese Ministry of State Security.

It is unacceptable that we continue to uncover cybercrime committed by China against other nations. In 2015, China promised to stop stealing trade secrets and other confidential business information through computer hacking "with the intent of providing competitive advantages to companies or commercial sectors." The activity alleged in this indictment violates the commitment that China made to members of the international community.

We want China to cease illegal cyber activities and honor its commitment to the international community, but the evidence suggests that China may not intend to live up to its promises.

For example, the Chinese industrial policy, known as “Made in China 2025,” lists ten strategic advanced manufacturing industries that the nation has targeted for promotion and development. Many of the companies allegedly targeted recently by Chinese defendants operate in sectors identified by that official policy. Whether through computer hackers operating from China, or Chinese nationals recruited to steal trade secrets from companies in other countries, the goal is the same: to dominate production in strategically important industries by stealing ideas from other nations.

Today’s charges mark an important step in revealing to the world China’s continued practice of stealing commercial data. Responding to that conduct requires a strategic approach to the threats that China poses. That is why the Department of Justice recently announced an initiative to address the full range of threats. One tactic is to increase our enforcement efforts. Another is to conduct foreign investment reviews to protect against China improperly acquiring sensitive information. A third is to find ways to better protect our telecommunications networks.

China stands accused of engaging in criminal activity that victimizes individuals and companies in the United States, violates our laws, and departs from international norms of responsible state behavior. Exposing these actions through the criminal justice system is a valuable tool. Faced with the detailed factual allegations released today, and the corroborating statements of other victimized nations, China will find it difficult to feign ignorance.

America and many allies know what China is doing. We know why they are doing it. And in some cases, we even know which individual people are doing it in association with the Chinese government.

The alleged criminals in this case are named Zhu Hua and Zhang Shilong. We hope the day will come when the defendants face justice under the rule of law in a federal courtroom.

Until then, they and other hackers who steal from our companies for the apparent benefit of Chinese industries should remember: there is no free pass to violate American laws merely because they do so under the protection of a foreign state. The Department of Justice and the FBI will continue to use all available tools to respond to China’s economic aggression and the threat that these actions pose to the prosperity and security of the United States and other nations that respect the rule of law.
