U.S. Indicts Chinese Hacker-Spies in Conspiracy to Steal Aerospace Secrets

By Dell Cameron

Published: 2018-10-30 · Archived: 2026-04-05 14:47:38 UTC

The U.S. Justice Department has charged two Chinese intelligence officers, six hackers, and two aerospace company insiders in a sweeping conspiracy to steal confidential aerospace technology from U.S. and French companies.

For more than five years, two Chinese Ministry of State Security (MSS) spies are said to have run a team of hackers focusing on the theft of designs for a turbofan engine used in U.S. and European commercial airliners, according to an unsealed indictment (below) dated October 25. In a statement, the DOJ said a Chinese state-owned aerospace company was simultaneously working to develop a comparable engine.

“The threat posed by Chinese government-sponsored hacking activity is real and relentless,” FBI Special Agent in Charge John Brown of San Diego said in a statement. “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.”

The MSS officers involved were identified as Zha Rong, a division director in the Jiangsu Province regional department (JSSD), and Chai Meng, a JSSD section chief.

At the direction of the MSS officers, the hackers allegedly infiltrated a number of U.S. aerospace companies, including California-based Capstone Turbine, among others in Arizona, Massachusetts, and Oregon, the DOJ said. The officers are also said to have recruited at least two Chinese employees of a French aerospace manufacturer—insiders who allegedly aided the conspiracy by, among other criminal acts, installing the remote access trojan Sakula onto company computers.

Sakula was previously deployed by Deep Panda, a Chinese nation-state threat group, according to cybersecurity firm Crowdstrike. Deep Panda is a leading suspect in the cyberattack on the U.S. government’s Office of Personnel Management (OPM), revealed in June 2015, which compromised the data of 4 million current and former federal employees. Sakula was also used in the 2015 Anthem data breach, which involved the potential theft of roughly 80 million individuals’ personal medical records.

The indictment includes intercepted communications between MSS spies and one of the insiders, including repeated mentions of “the horse,” an alleged reference to the Sakula malware. The hackers are also said to have used IsSpace, a trojan previously used in attacks attributed to DragonOK, a hacking group behind attacks on tech companies in Japan and Taiwan, according to cybersecurity firm FireEye.

The charges against the MSS officers follow the arrest in Belgium earlier this month of Yanjun Xu, an alleged Chinese spy accused of likewise targeting multiple U.S. aerospace companies. Xu was extradited to the United

States on September 9 and will stand trial for allegedly conducting economic espionage and attempting to steal trade secrets.
