Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research

Published: 2021-07-19 · Archived: 2026-04-02 12:18:24 UTC

A federal grand jury in San Diego, California, returned an indictment in May charging four nationals and residents of the People's Republic of China with a campaign to hack into the computer systems of dozens of victim companies, universities and government entities in the United States and abroad between 2011 and 2018. The indictment, which was unsealed on Friday, alleges that much of the conspiracy's theft was focused on information that was of significant economic benefit to China's companies and commercial sectors, including information that would allow the circumvention of lengthy and resource-intensive research and development processes. The defendants and their Hainan State Security Department (HSSD) conspirators sought to obfuscate the Chinese government's role in such theft by establishing a front company, Hainan Xiandun Technology Development Co., Ltd. (海南仙盾) (Hainan Xiandun), since disbanded, to operate out of Haikou, Hainan Province.

The two-count indictment alleges that Ding Xiaoyang (丁晓阳), Cheng Qingmin (程庆民) and Zhu Yunmin (朱允敏), were HSSD officers responsible for coordinating, facilitating and managing computer hackers and linguists at Hainan Xiandun and other MSS front companies to conduct hacking for the benefit of China and its state-owned and sponsored instrumentalities. The indictment alleges that Wu Shurong (吴淑荣) was a computer hacker who, as part of his job duties at Hainan Xiandun, created malware, hacked into computer systems operated by foreign governments, companies and universities, and supervised other Hainan Xiandun hackers.

The conspiracy's hacking campaign targeted victims in the United States, Austria, Cambodia, Canada, Germany, Indonesia, Malaysia, Norway, Saudi Arabia, South Africa, Switzerland and the United Kingdom. Targeted industries included, among others, aviation, defense, education, government, health care, biopharmaceutical and maritime. Stolen trade secrets and confidential business information included, among other things, sensitive technologies used for submersibles and autonomous vehicles, specialty chemical formulas, commercial aircraft servicing, proprietary genetic-sequencing technology and data, and foreign information to support China's efforts to secure contracts for state-owned enterprises within the targeted country (*e.g.*, large-scale high-speed railway development projects). At research institutes and universities, the conspiracy targeted infectious-disease research related to Ebola, MERS, HIV/AIDS, Marburg and tularemia.

As alleged, the charged MSS officers coordinated with staff and professors at various universities in Hainan and elsewhere in China to further the conspiracy's goals. Not only did such universities assist the MSS in identifying and recruiting hackers and linguists to penetrate and steal from the computer networks of targeted entities, including peers at many foreign universities, but personnel at one identified Hainan-based university also helped support and manage Hainan Xiandun as a front company, including through payroll, benefits and a mailing address.

“These criminal charges once again highlight that China continues to use cyber-enabled attacks to steal what other countries make, in flagrant disregard of its bilateral and multilateral commitments,” said Deputy Attorney General Lisa O. Monaco. “The breadth and duration of China’s hacking campaigns, including these efforts targeting a dozen countries across sectors ranging from healthcare and biomedical research to aviation and defense, remind us that no country or industry is safe. Today’s international condemnation shows that the world wants fair rules, where countries invest in innovation, not theft.”

“The FBI, alongside our federal and international partners, remains committed to imposing risk and consequences on these malicious cyber actors here in the U.S. and abroad,” said Deputy Director Paul M. Abbate of the FBI. “We will not allow the Chinese government to continue to use these tactics to obtain unfair economic advantage for its companies and commercial sectors through criminal intrusion and theft. With these types of actions, the Chinese government continues to undercut its own claims of being a trusted and effective partner in the international community.”

“This indictment alleges a worldwide hacking and economic espionage campaign led by the government of China,” said Acting U.S. Attorney Randy Grossman for the Southern District of California. “The defendants include foreign intelligence officials who orchestrated the alleged offenses, and the indictment demonstrates how China’s government made a deliberate choice to cheat and steal instead of innovate. These offenses threaten our economy and national security, and this prosecution reflects the Department of Justice’s commitment and ability to hold individuals and nations accountable for stealing the ideas and intellectual achievements of our nation’s best and brightest people.”

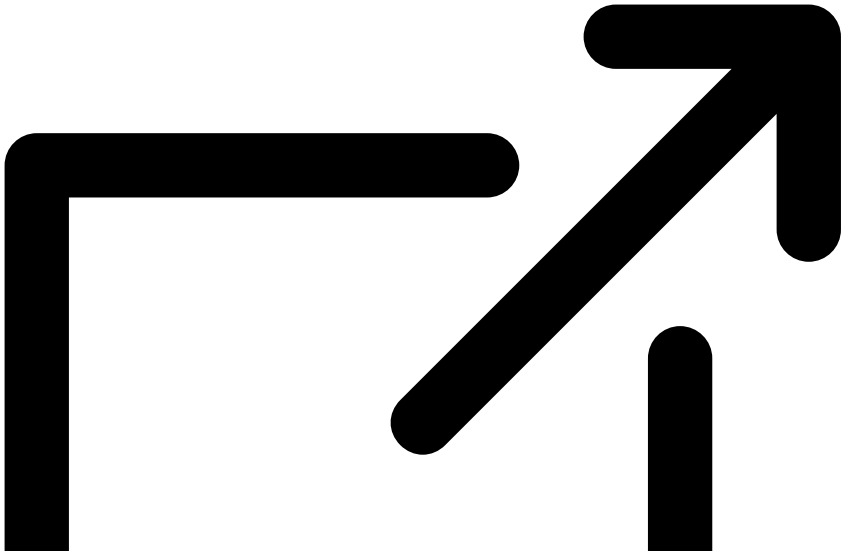
“The FBI’s San Diego Field Office is committed to protecting the people of the United States and the community of San Diego, to include our universities, health care systems, research institutes, and defense contractors,” said Special Agent in Charge Suzanne Turner of the FBI’s San Diego Field Office. “The charges outlined today demonstrate China’s continued, persistent computer intrusion efforts, which will not be tolerated here or abroad. We stand steadfast with our law enforcement partners in the United States and around the world and will continue to hold accountable those who commit economic espionage and theft of intellectual property.”

The defendants’ activity had been previously identified by private sector security researchers, who have referred to the group as Advanced Persistent Threat (APT) 40, BRONZE, MOHAWK, FEVERDREAM, G0065, Gadolinium, GreenCrash, Hellsing, Kryptonite Panda, Leviathan, Mudcarp, Periscope, Temp.Periscope and Temp.Jumper.

According to the indictment, to gain initial access to victim networks, the conspiracy sent fraudulent spearphishing emails, that were buttressed by fictitious online profiles and contained links to doppelgänger domain names, which were created to mimic or resemble the domains of legitimate companies. In some instances, the conspiracy used hijacked credentials, and the access they provided, to launch spearphishing campaigns against other users within the same victim entity or at other targeted entities. The conspiracy also used multiple and evolving sets of sophisticated malware, including both publicly available and customized malware, to obtain, expand and maintain unauthorized access to victim computers and networks. The conspiracy’s malware included those identified by security researchers as BADFLICK, aka GreenCrash; PHOTO, aka Derusbi; MURKYTOP, aka mt.exe; and HOMEFRY, aka dp.dll. Such malware allowed for initial and continued intrusions into victim systems, lateral movement within a system, and theft of credentials, including administrator passwords.

The conspiracy often used anonymizer services, such as The Onion Router (TOR), to access malware on victim networks and manage their hacking infrastructure, including servers, domains and email accounts. The conspiracy further attempted to obscure its hacking activities through other third-party services. For example, the conspiracy used GitHub to both store malware and stolen data, which was concealed using steganography. The conspiracy also used Dropbox Application Programming Interface (API) keys in commands to upload stolen data directly to conspiracy-controlled Dropbox accounts to make it appear to network defenders that such data exfiltration was an employee's legitimate use of the Dropbox service.

Coinciding with today's announcement, to enhance private sector network defense efforts against the conspirators, the FBI and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) released a Joint Cybersecurity Advisory



containing these and further technical details, indicators of compromise and mitigation measures.

The defendants are each charged with one count of conspiracy to commit computer fraud, which carries a maximum sentence of five years in prison, and one count of conspiracy to commit economic espionage, which carries a maximum sentence of 15 years in prison. The maximum potential sentences in this case are prescribed by Congress and are provided here for informational purposes only, as any sentencings of the defendants will be determined by the assigned judge.

The investigation was conducted jointly by the U.S. Attorney's Office for the Southern District of California, the National Security Division's Counterintelligence and Export Controls Section, and the FBI's San Diego Field Office. The FBI's Cyber Division, Cyber Assistant Legal Attachés and Legal Attachés in countries around the world provided essential support. Numerous victims cooperated and provided valuable assistance in the investigation.

Assistant U.S. Attorneys Fred Sheppard and Sabrina Feve of the Southern District of California and Trial Attorney Matthew McKenzie of the National Security Division's Counterintelligence and Export Control Section are prosecuting this case.

The details contained in the charging document are allegations. The defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.
