Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information

Published: 2018-12-20 · Archived: 2026-04-06 01:54:21 UTC

Defendants Were Members of the APT 10 Hacking Group Who Acted in Association with the Tianjin State Security Bureau and Engaged in Global Computer Intrusions for More Than a Decade, Continuing into 2018, Including Thefts from Managed Service Providers and More Than 45 Technology Companies

The unsealing of an indictment charging Zhu Hua (朱华), aka Afwar, aka CVNX, aka Alayos, aka Godkiller; and Zhang Shilong (张士龙), aka Baobeilong, aka Zhang Jianguo, aka Atreexp, both nationals of the People's Republic of China (China), with conspiracy to commit computer intrusions, conspiracy to commit wire fraud, and aggravated identity theft was announced today.

The announcement was made by Deputy Attorney General Rod J. Rosenstein, U.S. Attorney Geoffrey S. Berman for the Southern District of New York, Director Christopher A. Wray of the FBI, Director Dermot F. O'Reilly of the Defense Criminal Investigative Service (DCIS) of the U.S. Department of Defense, and Assistant Attorney General for National Security John C. Demers.

Zhu and Zhang were members of a hacking group operating in China known within the cyber security community as Advanced Persistent Threat 10 (the APT10 Group). The defendants worked for a company in China called Huaying Haitai Science and Technology Development Company (Huaying Haitai) and acted in association with the Chinese Ministry of State Security's Tianjin State Security Bureau.

Through their involvement with the APT10 Group, from at least in or about 2006 up to and including in or about 2018, Zhu and Zhang conducted global campaigns of computer intrusions targeting, among other data, intellectual property and confidential business and technological information at managed service providers (MSPs), which are companies that remotely manage the information technology infrastructure of businesses and governments around the world, more than 45 technology companies in at least a dozen U.S. states, and U.S. government agencies. The APT10 Group targeted a diverse array of commercial activity, industries and technologies, including aviation, satellite and maritime technology, industrial factory automation, automotive supplies, laboratory instruments, banking and finance, telecommunications and consumer electronics, computer processor technology, information technology services, packaging, consulting, medical equipment, healthcare, biotechnology, pharmaceutical manufacturing, mining, and oil and gas exploration and production. Among other things, Zhu and Zhang registered IT infrastructure that the APT10 Group used for its intrusions and engaged in illegal hacking operations.

"The indictment alleges that the defendants were part of a group that hacked computers in at least a dozen countries and gave China's intelligence service access to sensitive business information," said Deputy Attorney General Rosenstein. "This is outright cheating and theft, and it gives China an unfair advantage at the expense of

law-abiding businesses and countries that follow the international rules in return for the privilege of participating in the global economic system."

"It is galling that American companies and government agencies spent years of research and countless dollars to develop their intellectual property, while the defendants simply stole it and got it for free" said U.S. Attorney Berman. "As a nation, we cannot, and will not, allow such brazen thievery to go unchecked."

"Healthy competition is good for the global economy, but criminal conduct is not. This is conduct that hurts American businesses, American jobs, and American consumers," said FBI Director Wray. "No country should be able to flout the rule of law – so we're going to keep calling out this behavior for what it is: illegal, unethical, and unfair. It's going to take all of us working together to protect our economic security and our way of life, because the American people deserve no less."

"The theft of sensitive defense technology and cyber intrusions are major national security concerns and top investigative priorities for the DCIS," said DCIS Director O'Reilly. "The indictments unsealed today are the direct result of a joint investigative effort between DCIS and its law enforcement partners to vigorously investigate individuals and groups who illegally access information technology systems of the U.S. Department of Defense and the Defense Industrial Base. DCIS remains vigilant in our efforts to safeguard the integrity of the Department of Defense and its enterprise of information technology systems."

According to the allegations in the Indictment unsealed today in Manhattan federal court:

Overview

Zhu Hua (朱华), aka Afwar, aka CVNX, aka Alayos, aka Godkiller, and Zhang Shilong (张士龙), aka Baobeilong, aka Zhang Jianguo, aka Atreexp, the defendants, both nationals of China, were members of a hacking group operating in China known within the cyber security community as the APT10 Group, or alternatively as "Red Apollo," "CVNX," "Stone Panda," "MenuPass," and "POTASSIUM." The defendants worked for Huaying Haitai in Tianjin, China, and acted in association with the Chinese Ministry of State Security's Tianjin State Security Bureau. From at least in or about 2006 up to and including in or about 2018, members of the APT10 Group, including Zhu and Zhang, conducted extensive campaigns of intrusions into computer systems around the world. The APT10 Group used some of the same online facilities to initiate, facilitate and execute its campaigns during the conspiracy.

Most recently, beginning at least in or about 2014, members of the APT10 Group, including Zhu and Zhang, engaged in an intrusion campaign to obtain unauthorized access to the computers and computer networks of MSPs for businesses and governments around the world (the MSP Theft Campaign). The APT10 Group targeted MSPs in order to leverage the MSPs' networks to gain unauthorized access to the computers and computer networks of the MSPs' clients and to steal, among other data, intellectual property and confidential business data on a global scale. For example, through the MSP Theft Campaign, the APT10 Group obtained unauthorized access to the computers of an MSP that had offices in the Southern District of New York and compromised the data of that MSP and certain of its clients involved in banking and finance, telecommunications and consumer electronics, medical equipment, packaging, manufacturing, consulting, healthcare, biotechnology, automotive, oil and gas exploration, and mining.

Earlier, beginning in or about 2006, members of the APT10 Group, including Zhu and Zhang, engaged in an intrusion campaign to obtain unauthorized access to the computers and computer networks of more than 45 technology companies and U.S. government agencies, in order to steal information and data concerning a number of technologies (the Technology Theft Campaign). Through the Technology Theft Campaign, the APT10 Group stole hundreds of gigabytes of sensitive data and targeted the computers of victim companies involved in aviation, space and satellite technology, manufacturing technology, pharmaceutical technology, oil and gas exploration and production technology, communications technology, computer processor technology, and maritime technology.

In furtherance of the APT10 Group's intrusion campaigns, Zhu and Zhang, among other things, worked for Huaying Haitai and registered malicious domains and infrastructure. In addition, Zhu, a penetration tester, engaged in hacking operations on behalf of the APT10 Group and recruited other individuals to the APT10 Group, and Zhang developed and tested malware for the APT10 Group.

The MSP Theft Campaign

In furtherance of the MSP Theft Campaign, Zhu, Zhang, and their co-conspirators in the APT10 Group engaged in the following criminal conduct:

- First, after the APT10 Group gained unauthorized access into the computers of an MSP, the APT10 Group installed multiple variants of malware on MSP computers around the world. To avoid antivirus detection, the malware was installed using malicious files that masqueraded as legitimate files associated with the victim computer's operating system. Such malware enabled members of the APT10 Group to monitor victims' computers remotely and steal user credentials.
- Second, after stealing administrative credentials from computers of an MSP, the APT10 Group used those stolen credentials to connect to other systems within an MSP and its clients' networks. This enabled the APT10 Group to move laterally through an MSP's network and its clients' networks and to compromise victim computers that were not yet infected with malware.
- Third, after identifying data of interest on a compromised computer and packaging it for exfiltration using encrypted archives, the APT10 Group used stolen credentials to move the data of an MSP client to one or more other compromised computers of the MSP or its other clients' networks before exfiltrating the data to other computers controlled by the APT10 Group.

Over the course of the MSP Theft Campaign, Zhu, Zhang, and their co-conspirators in the APT10 Group successfully obtained unauthorized access to computers providing services to or belonging to victim companies 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 victim companies included at least the following: a global financial institution, three telecommunications and/or consumer electronics companies; three companies involved in commercial or industrial manufacturing; two consulting companies; a healthcare company; a biotechnology company; a mining company; an automotive supplier company; and a drilling company.

The Technology Theft Campaign

Over the course of the Technology Theft Campaign, which began in or about 2006, Zhu, Zhang, and their coconspirators in the APT10 Group successfully obtained unauthorized access to the computers of more than 45

technology companies and U.S. Government agencies based in at least 12 states, including Arizona, California, Connecticut, Florida, Maryland, New York, Ohio, Pennsylvania, Texas, Utah, Virginia and Wisconsin. The APT10 Group stole hundreds of gigabytes of sensitive data and information from the victims' computer systems, including from at least the following victims: seven companies involved in aviation, space and/or satellite technology; three companies involved in communications technology; three companies involved in manufacturing advanced electronic systems and/or laboratory analytical instruments; a company involved in maritime technology; a company involved in oil and gas drilling, production, and processing; and the NASA Goddard Space Center and Jet Propulsion Laboratory. In addition to those victims who had information stolen, Zhu, Zhang, and their co-conspirators successfully obtained unauthorized access to computers belonging to more than 25 other technology-related companies involved in, among other things, industrial factory automation, radar technology, oil exploration, information technology services, pharmaceutical manufacturing, and computer processor technology, as well as the U.S. Department of Energy's Lawrence Berkeley National Laboratory.

Finally, the APT10 Group compromised more than 40 computers in order to steal sensitive data belonging to the Navy, including the names, Social Security numbers, dates of birth, salary information, personal phone numbers, and email addresses of more than 100,000 Navy personnel.

* * *

Zhu and Zhang are each charged with one count of conspiracy to commit computer intrusions, which carries a maximum sentence of five years in prison; one count of conspiracy to commit wire fraud, which carries a maximum sentence of 20 years in prison; and one count of aggravated identity theft, which carries a mandatory sentence of two years in prison.

The maximum potential sentences in this case are prescribed by Congress and are provided here for informational purposes only, as any sentencing of the defendants will be determined by the assigned judge. The charges contained in the Indictment are merely accusations and the defendants are presumed innocent unless and until proven guilty.

The case was investigated by the FBI, including the New Orleans, New Haven, Houston, New York, Sacramento, and San Antonio Field Offices; DCIS; and the U.S. Naval Criminal Investigative Service (NCIS). Mr. Rosenstein, Mr. Berman and Mr. Demers praised the outstanding investigative work of, and collaboration among, the FBI, DCIS, and NCIS. They also thanked the U.S. Attorney's Office for the District of Connecticut, and the Department of Defense's Computer Forensic Laboratory for their assistance in the investigation.

Assistant U.S. Attorney Sagar K. Ravi of the Southern District of New York's Complex Frauds and Cybercrime Unit is in charge of the prosecution, with assistance provided by Trial Attorney Matthew Chang of the National Security Division's Counterintelligence and Export Control Section.
