Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax

Press Release

Monday, February 10, 2020

For Immediate Release
Office of Public Affairs

Indictment Alleges Four Members of China's People's Liberation Army Engaged in a Three-Month Long Campaign to Steal Sensitive Personal Information of Nearly 150 Million Americans

A federal grand jury in Atlanta returned an indictment last week charging four members of the Chinese People's Liberation Army (PLA) with hacking into the computer systems of the credit reporting agency Equifax and stealing Americans' personal data and Equifax's valuable trade secrets.

The nine-count indictment alleges that Wu Zhiyong (吴志勇), Wang Qian (王乾), Xu Ke (许可) and Liu Lei (刘磊) were members of the PLA's 54th Research Institute, a component of the Chinese military. They allegedly conspired with each other to hack into Equifax's computer networks, maintain unauthorized access to those computers, and steal sensitive, personally identifiable information of approximately 145 million American victims.

"This was a deliberate and sweeping intrusion into the private information of the American people," said Attorney General William P. Barr, who made the announcement. "Today, we hold PLA hackers accountable for their criminal actions, and we remind the Chinese government that we have the capability to remove the Internet's cloak of anonymity and find the hackers that nation repeatedly deploys against us. Unfortunately,

the Equifax hack fits a disturbing and unacceptable pattern of state-sponsored computer intrusions and thefts by China and its citizens that have targeted personally identifiable information, trade secrets, and other confidential information."

According to the indictment, the defendants exploited a vulnerability in the Apache Struts Web Framework software used by Equifax's online dispute portal. They used this access to conduct reconnaissance of Equifax's online dispute portal and to obtain login credentials that could be used to further navigate Equifax's network. The defendants spent several weeks running queries to identify Equifax's database structure and searching for sensitive, personally identifiable information within Equifax's system. Once they accessed files of interest, the conspirators then stored the stolen information in temporary output files, compressed and divided the files, and ultimately were able to download and exfiltrate the data from Equifax's network to computers outside the United States. In total, the attackers ran approximately 9,000 queries on Equifax's system, obtaining names, birth dates and social security numbers for nearly half of all American citizens.

The indictment also charges the defendants with stealing trade secret information, namely Equifax's data compilations and database designs. "In short, this was an organized and remarkably brazen criminal heist of sensitive information of nearly half of all Americans, as well as the hard work and intellectual property of an American company, by a unit of the Chinese military," said Barr.

The defendants took steps to evade detection throughout the intrusion, as alleged in the indictment. They routed traffic through approximately 34 servers located in nearly 20 countries to obfuscate their true location, used encrypted communication channels within Equifax's network to blend in with normal network activity, and deleted compressed files and wiped log files on a daily basis in an effort to eliminate records of their activity.

"Today's announcement of these indictments further highlights our commitment to imposing consequences on cybercriminals no matter who they are, where they are, or what country's uniform they wear," said FBI Deputy Director David Bowdich. "The size and scope of this investigation — affecting nearly half of the U.S. population, demonstrates the importance of the FBI's mission and our enduring partnerships with the Justice Department and the U.S. Attorney's Office. This is not the end of our investigation; to all who seek to disrupt the safety, security and confidence of the global citizenry in this digitally connected world, this is a day of reckoning."

The defendants are charged with three counts of conspiracy to commit computer fraud, conspiracy to commit economic espionage, and conspiracy to commit wire fraud. The defendants are also charged with two counts of unauthorized access and intentional damage to a protected computer, one count of economic espionage, and three counts of wire fraud.

The investigation was conducted jointly by the U.S. Attorney's Office for the Northern District of Georgia, the Criminal and National Security Divisions of the Department of Justice, and the FBI's Atlanta Field Office. The FBI's Cyber Division also provided support. Equifax cooperated fully and provided valuable assistance in the investigation.

Assistant U.S. Attorneys Nathan Kitchens, Samir Kaushal, and Thomas Krepp of the Northern District of Georgia; Senior Counsel Benjamin Fitzpatrick of the Criminal Division's Computer Crime and Intellectual Property Section; and Trial Attorney Scott McCulloch of the National Security Division's Counterintelligence and Export Control Section are prosecuting this case. Attorneys with the Office of International Affairs provided critical assistance in obtaining evidence from overseas.

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.

The year 2020 marks the 150th anniversary of the Department of Justice. Learn more about the history of our agency at www.Justice.gov/Celebrating150Years.

Updated July 13, 2022

Topics

Countering Nation-State Threats

Counterintelligence

Cybercrime

Financial Fraud

Press Release Number: 20-157