Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research

justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion

July 21, 2020

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Tuesday, July 21, 2020

Indictment Alleges Two Hackers Worked With the Guangdong State Security Department (GSSD) of the Ministry of State Security (MSS), While Also Targeting Victims Worldwide for Personal Profit

A federal grand jury in Spokane, Washington, returned an indictment earlier this month charging two hackers, both nationals and residents of the People's Republic of China (China), with hacking into the computer systems of hundreds of victim companies, governments, non-governmental organizations, and individual dissidents, clergy, and democratic and human rights activists in the United States and abroad, including Hong Kong and China. The defendants in some instances acted for their own personal financial gain, and in others for the benefit of the MSS or other Chinese government agencies. The hackers stole terabytes of data which comprised a sophisticated and prolific threat to U.S. networks.

The 11-count indictment alleges LI Xiaoyu (李啸宇), 34, and DONG Jiazhi (董家志), 33, who were trained in computer applications technologies at the same Chinese university, conducted a hacking campaign lasting more than ten years to the present, targeting companies in countries with high technology industries, including the United States, Australia, Belgium, Germany, Japan, Lithuania, the Netherlands, Spain, South Korea, Sweden, and the United Kingdom. Targeted industries included, among others, high tech manufacturing; medical device, civil, and industrial engineering; business, educational, and gaming software; solar energy; pharmaceuticals; defense. In at least one instance, the hackers sought to extort cryptocurrency from a victim entity, by threatening to release the victim's stolen source code on the Internet. More recently, the defendants probed for vulnerabilities in computer networks of companies developing COVID-19 vaccines, testing technology, and treatments.

The charges were announced by Assistant Attorney General for National Security John C. Demers; FBI Deputy Director David Bowdich; U.S. Attorney for the Eastern District of Washington William D. Hyslop; and Special Agent in Charge of the FBI's Seattle Field Division Raymond Duda.

"China has now taken its place, alongside Russia, Iran and North Korea, in that shameful club of nations that provide a safe haven for cyber criminals in exchange for those criminals being 'on call' to work for the benefit of the state, here to feed the Chinese Communist party's insatiable hunger for American and other non-Chinese companies' hard-earned intellectual property, including COVID-19 research," said Assistant Attorney General for National Security John C. Demers.

"Today's indictment demonstrates the serious consequences the Chinese MSS and its proxies will face if they continue to deploy malicious cyber tactics to either steal what they cannot create or silence what they do not want to hear," said FBI Deputy Director David Bowdich. "Cybercrimes directed by the Chinese government's intelligence services not only threaten the United States but also every other country that supports fair play, international norms, and the rule of law, and it also seriously undermines China's desire to become a respected leader in world affairs. The FBI and our international partners will not stand idly by to this threat, and we are committed to holding the Chinese government accountable."

"The cybercrime hacking occurring here was first discovered on computers of the Department of Energy's Hanford Site in Eastern Washington. As the grand jury charged, the computer systems of many businesses, individuals and agencies throughout the United States and worldwide have been hacked and compromised with a huge array of sensitive and valuable trade secrets, technologies, data, and personal information being stolen. The hackers operated from China both for their own gain and with the assistance and for the benefit of the Chinese government's Ministry of State Security. This prosecution is occurring as a result of the combined unwavering efforts of the National Security Division of the Department of Justice, the United States Attorney's Office for the Eastern District of

Washington, and the Federal Bureau of Investigation. We seek justice for these victims and others affected and we intend to prosecute these defendants for their alleged crimes," said U.S. Attorney William D. Hyslop for the District Eastern District of Washington.

"The complicated nature of cyber investigations is only exacerbated when the criminal is backed by the resources of a foreign government. The nature and value of the material stolen by these hackers cannot just be measured in dollars and was indicative of being state driven. This case demonstrates the FBI's dedication to pursuing these criminals no matter who is sanctioning their activities," said Special Agent in Charge Raymond Duda of the FBI's Seattle Division.

According to the indictment, to gain initial access to victim networks, the defendants primarily exploited publicly known software vulnerabilities in popular web server software, web application development suites, and software collaboration programs. In some cases, those vulnerabilities were newly announced, meaning that many users would not have installed patches to correct the vulnerability. The defendants also targeted insecure default configurations in common applications. The defendants used their initial unauthorized access to place malicious web shell programs (*e.g.*, the "China Chopper" web shell) and credential-stealing software on victim networks, which allowed them to remotely execute commands on victim computers.

To conceal the theft of information from victim networks and otherwise evade detection, the defendants typically packaged victim data in encrypted Roshal Archive Compressed files (RAR files), changed RAR file and victim documents' names and extensions (*e.g.*, from ".rar" to ".jpg") and system timestamps, and concealed programs and documents at innocuous-seeming locations on victim networks and in victim networks' "recycle bins." The defendants frequently returned to re-victimize companies, government entities, and organizations from which they had previously stolen data, in some cases years after the initial successful data theft. In several instances, however, the defendants were unsuccessful in this regard, due to the efforts of the FBI and network defenders.

The indictment charges the defendants with conspiring to steal trade secrets from at least eight known victims, which consisted of technology designs, manufacturing processes, test mechanisms and results, source code, and pharmaceutical chemical structures. Such information would give competitors with a market edge by providing insight into proprietary business plans and savings on research and development costs in creating competing products.

The defendants are each charged with one count of conspiracy to commit computer fraud, which carries a maximum sentence of five years in prison; one count of conspiracy to commit theft of trade secrets, which carries a maximum sentence of ten years in prison; one count of conspiracy to commit wire fraud, which carries a maximum sentence of 20 years in prison; one count of unauthorized access of a computer, which carries a maximum sentence of five

years in prison; and seven counts of aggravated identity theft, which each carries a mandatory sentence of two non-consecutive 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 Eastern District of Washington, the National Security Division of the Department of Justice, and the FBI's Spokane Resident Agency and San Antonio and Norfolk Field Offices. The FBI's Cyber Division assisted in the investigation and, along with FBI's 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. Attorney James Goeke of the Eastern District of Washington and Trial Attorney Scott McCulloch 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.