Seven International Cyber Defendants, Including “Apt41” Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally

justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer

September 16, 2020

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Wednesday, September 16, 2020

Two Defendants Arrested in Malaysia; Remaining Five Defendants, One of Whom Allegedly Boasted of Connections to the Chinese Ministry of State Security, are Fugitives in China

In August 2019 and August 2020, a federal grand jury in Washington, D.C., returned two separate indictments charging five computer hackers, all of whom were residents and nationals of the People’s Republic of China (PRC), with computer intrusions affecting over 100 victim companies in the United States and abroad, including software development companies, computer hardware manufacturers, telecommunications providers, social media companies, video game companies, non-profit organizations, universities, think tanks, and foreign governments, as well as pro-democracy politicians and activists in Hong Kong.

The intrusions, which security researchers have tracked using the threat labels “APT41,” “Barium,” “Winnti,” “Wicked Panda,” and “Wicked Spider,” facilitated the theft of source code, software code signing certificates, customer account data, and valuable business

information. These intrusions also facilitated the defendants' other criminal schemes, including ransomware and "crypto-jacking" schemes, the latter of which refers to the group's unauthorized use of victim computers to "mine" cryptocurrency.

Also in August 2020, the same federal grand jury returned a third indictment charging two Malaysian businessmen who conspired with two of the Chinese hackers to profit from computer intrusions targeting the video game industry in the United States and abroad. Shortly thereafter, the U.S. District Court for the District of Columbia issued arrest warrants for the two businessmen. On Sept. 14, 2020, pursuant to a provisional arrest request from the United States with a view to their extradition, Malaysian authorities arrested them in Sitiawan. The department appreciates the significant cooperation and assistance provided by the Government of Malaysia, including the Attorney General's Chambers of Malaysia and the Royal Malaysia Police.

In addition to arrest warrants for all of the charged defendants, in September 2020, the U.S. District Court for the District of Columbia issued seizure warrants that resulted in the recent seizure of hundreds of accounts, servers, domain names, and command-and-control (C2") "dead drop" web pages used by the defendants to conduct their computer intrusion offenses. The FBI executed the warrants in coordination with other actions by several private-sector companies, which included disabling numerous accounts for violations of the companies' terms of service. In addition, in partnership with the department, Microsoft developed and implemented technical measures to block this threat actor from accessing victims' computer systems. The actions by Microsoft were a significant part of the overall effort to deny the defendants continued access to hacking infrastructure, tools, accounts, and command and control domain names. In coordination with today's announcement, the FBI has also released a Liaison Alert System (FLASH) report that contains critical, relevant technical information collected by the FBI for use by specific private-sector partners.

"The department of Justice has used every tool available to disrupt the illegal computer intrusions and cyberattacks by these Chinese citizens," said Deputy Attorney General Jeffrey A. Rosen. "Regrettably, the Chinese communist party has chosen a different path of making China safe for cybercriminals so long as they attack computers outside China and steal intellectual property helpful to China."

"Today's charges, the related arrests, seizures of malware and other infrastructure used to conduct intrusions, and coordinated private sector protective actions reveal yet again the department's determination to use all of the tools at its disposal and to collaborate with the private sector and nations who support the rule of law in cyberspace," said Assistant Attorney General John C. Demers. "This is the only way to neutralize malicious nation state cyber activity."

"Today's announcement demonstrates the ramifications faced by the hackers in China but it is also a reminder to those who continue to deploy malicious cyber tactics that we will utilize every tool we have to administer justice," said FBI Deputy Director David Bowdich. "The

arrests in Malaysia are a direct result of partnership, cooperation and collaboration. As the cyber threat continues to evolve larger than any one agency can address, the FBI remains committed to being an indispensable partner to our federal, international and private sector partners to stop rampant cyber crime and hold those carrying out these kind of actions accountable."

"The scope and sophistication of the crimes in these unsealed indictments is unprecedented. The alleged criminal scheme used actors in China and Malaysia to illegally hack, intrude and steal information from victims worldwide," said Michael R. Sherwin, Acting U.S. Attorney for the District of Columbia. "As set forth in the charging documents, some of these criminal actors believed their association with the PRC provided them free license to hack and steal across the globe. This scheme also contained a new and troubling cyber-criminal component – the targeting and utilization of gaming platforms to both defraud video game companies and launder illicit proceeds."

"The actions announced today reflect a years-long commitment by the FBI Washington Field Office to pursue the perpetrators of the computer intrusion campaigns described in the indictments, and to bring those perpetrators to justice," said Acting Assistant Director in Charge James A. Dawson, FBI Washington Field Office. "This case demonstrates the FBI's dedication to pursuing these criminals no matter where they are, and to whom they may be connected."

The August 2019 indictment charged Zhang Haoran (张浩然), 35, and Tan Dailin (谭戴林), 35, with 25 counts of conspiracy, wire fraud, aggravated identity theft, money laundering, and violations of the Computer Fraud and Abuse Act ("CFAA"). The indictment charged Zhang and Tan with participating in a "Computer Hacking Conspiracy," which targeted high-technology and similar organizations. The indictment also charged that, as an additional way to make money, Zhang and Tan participated in a "Video Game Conspiracy," through which Zhang and Tan, together with others, sought to make money by hacking video game companies, obtaining and otherwise generating digital items of value (e.g., video game currency), and then selling such items for profit. In several instances, they used their unauthorized access to gaming company networks take action against other unrelated groups engaged in the same fraudulent generation of gaming artifacts, thereby attempting to eliminate the criminal competition.

One of the August 2020, indictments charged Jiang Lizhi (蒋立志), 35, Qian Chuan (钱川), 39, and Fu Qiang (付强), 37, with nine counts of racketeering conspiracy, conspiracy to violate the CFAA, substantive violations of the CFAA, access device fraud, identity theft, aggravated identity theft, and money laundering. The racketeering conspiracy pertained to the three defendants' conducting the affairs of Chengdu 404 Network Technology ("Chengdu 404"), a PRC company, through a pattern of racketeering activity involving computer intrusion offenses affecting over 100 victim companies, organizations, and individuals in the United States and around the world, including in Australia, Brazil, Chile, Hong Kong, India, Indonesia, Japan, Malaysia, Pakistan, Singapore, South Korea, Taiwan, Thailand, and

Vietnam. The defendants also compromised foreign government computer networks in India and Vietnam, and targeted, but did not compromise, government computer networks in the United Kingdom. In one notable instance, the defendants conducted a ransomware attack on the network of a non-profit organization dedicated to combating global poverty.

The defendants associated with Chengdu 404 employed sophisticated hacking techniques to gain and maintain access to victim computer networks. One example was the defendants' use of "supply chain attacks," in which the hackers compromised software providers and then modified the providers' code to facilitate further intrusions against the software providers' customers. Another example was the hackers' use of C2 "dead drops," which are seemingly legitimate web pages that the hackers created, but which were surreptitiously encoded instructions to their malware. However, they also employed publicly available exploits and tools, including the following common vulnerabilities and exposures ("CVE"): CVE-2019-19781, CVE-2019-11510, CVE-2019-16920, CVE-2019-16278, CVE-2019-1652/CVE-2019-1653, and CVE-2020-10189.

The second August 2020 indictment charged Wong Ong Hua, 46, and Ling Yang Ching, 32, both Malaysian nationals and residents, with 23 counts of racketeering, conspiracy, identity theft, aggravated identity theft, access device fraud, money laundering, violations of the CFAA, and falsely registering domain names. The indictment alleged that Wong and Ling conducted the affairs of Sea Gamer Mall, a Malaysian company founded by Wong, through a pattern of racketeering activity involving computer intrusion offenses targeting the video game industry in the United States, France, Japan, Singapore, and South Korea. The indictment alleged that Wong and Ling worked with various hackers, including Zhang and Tan, to profit from the hackers' criminal computer intrusions at video game companies.

The indictment against Zhang and Tan charges the defendants with two counts of conspiracy to commit computer fraud, which carries a maximum sentence of five years in prison; two counts of conspiracy to commit wire fraud, which carries a maximum sentence of 20 years in prison; five counts of wire fraud, which carries a maximum sentence of 20 years in prison; nine counts of intentional damage to a protected computer, which carries a maximum sentence of 10 years in prison; four counts of unauthorized access to a protected computer, which carries a maximum sentence of five years in prison; two counts of aggravated identity theft, which carries a mandatory sentence of two years in prison; and one count of money laundering, which carries a maximum sentence of 20 years in prison.

The indictment against Jiang, Qian, and Fu charges the defendants with one count of racketeering conspiracy, which carries a maximum sentence of 20 years in prison; one count of conspiracy to commit computer fraud, which carries a maximum sentence of five years in prison; one count of intentional damage to a protected computer, which carries a maximum sentence of 10 years in prison; one count of unauthorized access to a protected computer, which carries a maximum sentence of five years in prison; one count of threatening to damage a protected computer, which carries a maximum sentence of five years in prison; one count of access device fraud, which carries a maximum sentence of 10 years in prison;

one count of identity theft, which carries a maximum sentence of five years in prison; one count of aggravated identity theft, which carries a mandatory sentence of two years in prison; and one count of money laundering, which carries a maximum sentence of 20 years in prison.

The indictment against Wong and Ling charges the defendants with one count of racketeering conspiracy, which carries a maximum sentence of 20 years in prison; one count of racketeering, which carries a maximum sentence of 20 years in prison; three counts of intentional damage to a protected computer, which carries a maximum sentence of 10 years in prison; five counts of unauthorized access to a protected computer, which carries a maximum sentence of five years in prison; five counts of furthering fraud by unauthorized access to a protected computer, which carries a maximum sentence of five years in prison; two counts of access device fraud, which carries a maximum sentence of 10 years in prison; two counts of identity theft, which carries a maximum sentence of five years in prison; one count of aggravated identity theft, which carries a mandatory sentence of two years in prison; and three counts of money laundering, which carries a maximum sentence of 20 years in prison. The indictment also alleges false registration of domain names, which would increase the maximum sentence of imprisonment for money laundering to 27 years; the maximum sentence of imprisonment for unlawful access to a protected computer to 10 years instead of five years; the maximum sentence of imprisonment for intentional damage to a protected computer to 17 years instead of 10 years; and the mandatory sentence of imprisonment for aggravated identity theft to four years instead of two years.

The maximum potential sentences in this case are prescribed by Congress and are provided here for informational purposes only; any sentencing's of the defendants will be determined by the assigned judge.

The investigation was conducted jointly by the U.S. Attorney's Office for the District of Columbia, the National Security Division of the Department of Justice, and the FBI's Washington Field Office. 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.

The department is also grateful to Microsoft, including Microsoft's Threat Intelligence Center (MSTIC) and Digital Crimes Unit (DCU), to Google, including its Threat Analysis Group (TAG), to Facebook, and to Verizon Media, including its Paranoids Advanced Cyber Threats Team, for the assistance they provided in this investigation.

Assistant U.S. Attorney Demian Ahn of the District of Columbia, Assistant U.S. Attorney Tejpal Chawla of the District of Columbia, and Trial Attorney Evan Turgeon of the National Security Division's Counterintelligence and Export Control Section are prosecuting this case.

The Justice Department's Office of International Affairs provided critical assistance.

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.