Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians

⋮ 3/25/2024

For Immediate Release

U.S. Attorney's Office, Eastern District of New York

Defendants Operated as Part of the APT31 Hacking Group in Support of China's Ministry of State Security's Transnational Repression, Economic Espionage and Foreign Intelligence Objectives

BROOKLYN, NY – An indictment was unsealed today charging seven nationals of the People's Republic of China (PRC) with conspiracy to commit computer intrusions and conspiracy to commit wire fraud for their involvement in a PRC-based hacking group that spent approximately 14 years targeting U.S. and foreign critics, businesses and political officials in furtherance of the PRC's economic espionage and foreign intelligence objectives.

The defendants are Ni Gaobin (倪高彬), Weng Ming (翁明), Cheng Feng (程锋), Peng Yaowen (彭耀文), Sun Xiaohui (孙小辉), Xiong Wang (熊旺), and Zhao Guangzong (赵光宗).

Merrick B. Garland, United States Attorney General; Breon Peace, United States Attorney for the Eastern District of New York; Lisa O. Monaco, United States Deputy Attorney General; Matthew G. Olsen, Assistant Attorney General of the Justice Department's National Security Division; James Smith, Assistant Director-in-Charge, Federal Bureau of Investigation, New York Field Office (FBI), and Robert W. "Wes" Wheeler, Jr., Special Agent-in-Charge, FBI, Chicago Field Office (FBI), announced the indictment.

"The Justice Department will not tolerate efforts by the Chinese government to intimidate Americans who serve the public, silence the dissidents who are protected by American laws, or steal from American businesses," said Attorney General Merrick B. Garland. "This case serves as a reminder of the ends to which the Chinese government is willing to go to target and intimidate its critics, including launching malicious cyber operations aimed at threatening the national security of the United States and our allies."

"These allegations pull back the curtain on China's vast illegal hacking operation that targeted sensitive data from U.S. elected and government officials, journalists and academics; valuable information from American companies; and political dissidents in America and abroad. Their sinister scheme victimized thousands of people and entities across the world, and lasted for well over a decade," stated U.S. Attorney Peace. "America's sovereignty extends to its cyberspace. Today's charges demonstrate my Office's commitment to upholding and protecting that jurisdiction, and to putting an end to malicious nation state cyber activity."

“Over 10,000 malicious emails, impacting thousands of victims, across multiple continents. As alleged in today’s indictment, this prolific global hacking operation – backed by the PRC government – targeted journalists, political officials, and companies to repress critics of the Chinese regime, compromise government institutions, and steal trade secrets,” said Deputy Attorney General Lisa Monaco. “The Department of Justice will relentlessly pursue, expose, and hold accountable cyber criminals who would undermine democracies and threaten our national security.”

“The indictment unsealed today, together with statements from our foreign partners regarding related activity, shed further light on the PRC Ministry of State Security’s aggressive cyber espionage and transnational repression activities worldwide,” said Assistant Attorney General Matthew G. Olsen of the Justice Department’s National Security Division. “Today’s announcements underscore the need to remain vigilant to cybersecurity threats and the potential for cyber-enabled foreign malign influence efforts, especially as we approach the 2024 election cycle. The Department of Justice will continue to leverage all tools to disrupt malicious cyber actors who threaten our national security and aim to repress fundamental freedoms worldwide.”

“These defendants were part of a Chinese government sponsored hacking group, targeting U.S. businesses and U.S. political officials for intrusion for over a decade as part of a larger, malicious global campaign. These charges are yet another example of hostile actions taken by the PRC to attack not only American businesses and infrastructure, but the security of our nation. FBI New York is united with our partners - internationally, federally, and the private sector – to protect our common goals and ideals from antagonistic nation state actors,” stated FBI Assistant Director-in-Charge Smith.

“APT31 Group’s practices further demonstrate the size and scope of the PRC’s state-sponsored hacking apparatus,” said Robert W. “Wes” Wheeler, Jr., Special Agent-in-Charge of the Chicago Field Office of the FBI. “FBI Chicago worked tirelessly to uncover this complex web of alleged foreign intelligence and economic espionage crimes. Thanks to these efforts, as well as our partnerships with the U.S. Attorney’s Offices and fellow Field Offices, the FBI continues to be successful in holding groups accountable and protecting national security.”

Overview

As alleged in the indictment and court filings, the defendants, along with dozens of identified PRC Ministry of State Security (MSS) intelligence officers, contractor hackers, and support personnel, were members of a hacking group operating in the PRC and known within the cyber security community as Advanced Persistent Threat 31 (the APT31 Group). The APT31 Group was part of a cyberespionage program run by the MSS’s Hubei State Security Department, located in the city of Wuhan. Through their involvement with the APT31 Group, since at least 2010, the defendants conducted global campaigns of computer hacking targeting political dissidents and perceived supporters located inside and outside of China, government and political officials, candidates and campaign personnel in the United States and elsewhere and American companies.

The defendants and others in the APT31 Group targeted thousands of U.S. and foreign individuals and companies. Some of this activity resulted in successful compromises of the targets’ networks, email accounts, cloud storage accounts, and telephone call records, with some surveillance of compromised email accounts lasting many years.

Hacking Scheme

The more than 10,000 malicious emails that the defendants and others in the APT31 Group sent to these targets often appeared to be from prominent news outlets or journalists and appeared to contain legitimate news articles. The malicious emails contained hidden tracking links, such that if the recipient simply opened the email, information about the recipient, including the recipient's location, internet protocol (IP) addresses, network schematics and specific devices used to access the pertinent email accounts, was transmitted to a server controlled by the defendants and those working with them. The defendants and others in the APT31 Group then used this information to enable more direct and sophisticated targeted hacking, such as compromising the recipients' home routers and other electronic devices.

The defendants and others in the APT31 Group also sent malicious tracking-link emails to government officials across the world who expressed criticism of the PRC government. For example, in or about 2021, the Conspirators targeted the email accounts of various foreign government individuals world who were part of the Inter-Parliamentary Alliance on China (IPAC), a group founded in 2020 on the anniversary of the 1989 Tiananmen Square protests whose stated purpose was to counter the threats posed by the Chinese Communist Party to the international order and democratic principles. The targets included every European Union member of IPAC, and 43 United Kingdom parliamentary accounts, most of whom were members of IPAC or had been outspoken on topics relating to the PRC government.

To gain and maintain access to the victim computer networks, the defendants and others in the APT31 Group employed sophisticated hacking techniques including zero-day exploits, which are exploits that the hackers became aware of before the manufacturer or the victim were able to patch or fix the vulnerability. These activities resulted in the confirmed and potential compromise of economic plans, intellectual property, and trade secrets belonging to American businesses, and contributed to the estimated billions of dollars lost every year as a result of the PRC's state-sponsored apparatus to transfer U.S. technology to the PRC.

Targeting of U.S. Government Officials and U.S. and Foreign Politicians and Campaigns

The targeted U.S. government officials included individuals working in the White House, at the Departments of Justice, Commerce, Treasury and State, and U.S. Senators and Representatives of both political parties. The defendants and others in the APT31 Group targeted these individuals at both professional and personal email addresses. Additionally in some cases, the defendants also targeted victims' spouses, including the spouses of a high-ranking Department of Justice official, high-ranking White House officials and multiple United States Senators. Targets also included election campaign staff from both major U.S. political parties in advance of the 2020 election.

The allegations in the indictment regarding the malicious cyber activity targeting political officials, candidates, and campaign personnel are consistent with the March 2021 Joint Report of the Department of Justice and the Department of Homeland Security on Foreign Interference Targeting Election Infrastructure or Political Organization, Campaign, or Candidate Infrastructure Related to the 2020 US Federal Elections. That report cited incidents when Chinese government-affiliated actors "materially impacted the security of networks associated with or pertaining to US political organizations, candidates, and campaigns during the 2020 federal elections." That report also concluded that "such actors gathered

at least some information they could have released in influence operations," but which the Chinese actors did not ultimately deploy in such a manner. Consistent with that conclusion, the indictment does not allege that the hacking furthered any Chinese government influence operations against the U.S. The indictment's allegations nonetheless serve to underscore the need for U.S. and allied political organizations, candidates, and campaigns to remain vigilant in their cybersecurity posture and in otherwise protecting their sensitive information from foreign intelligence services, particularly in light of the U.S. Intelligence Community's recent assessment that "[t]he PRC may attempt to influence the U.S. elections in 2024 at some level because of its desire to sideline critics of China and magnify U.S. societal divisions."

Targeting of U.S. Companies

The defendants and others in the APT31 Group also targeted individuals and dozens of companies operating in areas of national economic importance, including the defense, information technology, telecommunications, manufacturing and trade, finance, consulting, legal and research industries. The defendants and others in the APT31 Group hacked and attempted to hack dozens of companies or entities operating in these industries, including multiple cleared defense contractors who provide products and services to the U.S. military, multiple managed service providers who managed the computer networks and security for other companies, a leading provider of 5G network equipment, and a leading global provider of wireless technology, among many others.

Targeting for Transnational Repression of Dissidents

The defendants and the APT31 Group also targeted individual dissidents around the world and other individuals who were perceived as supporting such dissidents. For example, in 2018, after several activists who spearheaded Hong Kong's Umbrella Movement were nominated for the Nobel Peace Prize, the defendants and the APT31 Group targeted Norwegian government officials and a Norwegian managed service provider. The conspirators also successfully compromised Hong Kong pro-democracy activists and their associates located in Hong Kong, the United States, and other foreign locations with identical malware.

The charged defendants' roles in the conspiracy consisted of testing and exploiting the malware used to conduct these intrusions, managing infrastructure associated with these intrusions, and conducting surveillance and intrusions against specific U.S. entities. For example, defendants Cheng Feng, Sun Xiaohui, Weng Ming, Xiong Wang and Zhao Guangzong were involved in testing and exploiting malware, including malware used in some of these intrusions. Cheng and Ni Gaobin managed infrastructure associated with some of these intrusions, including the domain name for a command-and-control server that accessed at least 59 unique victim computers, including a telecommunications company that was a leading provider of 5G network equipment in the United States, an Alabama-based research corporation in the aerospace and defense industries and a Maryland-based professional support services company. Sun and Weng operated the infrastructure used in an intrusion into a U.S. company known for its public opinion polls. Sun and Peng Yaowen conducted research and reconnaissance on several additional U.S. entities that were later the victims of the APT31 Group's intrusion campaigns. Ni and Zhao sent emails with links to files containing malware to PRC dissidents, specifically Hong Kong legislators and democracy advocates, as well as targeting U.S. entities focusing on PRC-related issues.

The government's case is being prosecuted by the Office's National Security and Cybercrime Section. Assistant United States Attorneys Douglas M. Pravda, Saritha Komatireddy and Jessica Weigel are in charge of the prosecution, with assistance from Matthew Anzaldi and Matthew Chang of the National Security Division's National Security Cyber Section and from the Office's Litigation Analyst Mary Clare McMahon.

The Defendants:

Ni Gaobin (倪高彬)
Age: 38
People's Republic of China

Weng Ming (翁明)
Age: 37
People's Republic of China

Cheng Feng (程锋)
Age: 34
People's Republic of China

Peng Yaowen (彭耀文)
Age: 38
People's Republic of China

Sun Xiaohui (孙小辉)
Age: 38
People's Republic of China

Xiong Wang (熊旺)
Age: 35
People's Republic of China

Zhao Guangzong (赵光宗)
Age: 38
People's Republic of China

E.D.N.Y. Docket No. 24-CR-42 (RER)

Contact

John Marzulli
Danielle Blustein Hass
U.S. Attorney's Office
(718) 254-6323

Updated March 25, 2024

Attachment

Indictment [PDF, 790 KB]