US indicts Chinese military hackers

Threat Memo - Date: 12/02/2020 - Version: 1.0

TLP:WHITE

FOR INFORMATION	Category	Type	Domain(s)	Sector(s)	Confidence
	Cyberespionage	Targeted intrusions, Indictment	World	Consulting, Finance	A1

Key Points

- The US Department of Justice charged four Chinese members of the People's Liberation Army for conspiracy and hacking.
- Indictments have been a component of the US cyber diplomatic and juridical toolbox since at least 2014.
- In 2019 US technology firms started to enforce the US government's sanctions against selected "foreign adversaries".

Summary

On January 28, the US Department of Justice (DOJ) charged[1] four Chinese members of the People's Liberation Army for conspiracy and hacking into the Equifax consumer credit reporting agency. This targeted intrusion began about May 13, 2017 and continued until at least July 30, 2017. The hackers stole personal data (including names, addresses, social security numbers, birth dates) of 145 million (nearly half of all) US citizens. Personal data of 400 000 citizens of the UK and Canada were also stolen.

The hackers, Wu Zhiyong (吴志勇), Wang Qian (王乾), Xu Ke (许可) and Liu Lei (刘磊) are reportedly members of the PLA's 54th Research Institute, a component of the Chinese military. According to the FBI, the hackers attempted to conceal their operations by routing attack traffic through 34 servers located in nearly 20 countries. They established encrypted communications channels within Equifax's network to blend in with normal network activity. They removed evidence by deleting log files in the compromised networks on a daily basis.

In a press conference, the US Attorney General explained[2] that the US DOJ doesn't normally charge members of another country's military with crimes. It did so in this case because the accused "indiscriminately" targeted American civilians on a massive scale.

The Chinese ministry of foreign affairs immediately replied, saying[3] "For a long time, the US has clearly conducted large-scale, organized theft, network monitoring and control activities against foreign dignitaries, corporations, and individuals. Once again, we strongly urge the US to offer a clear explanation and immediately stop such activities."

Comments

Indictments have been a component of the US cyber diplomatic and judicial toolbox since at least 2014, used to fight advanced state-sponsored threats. This toolbox also includes naming and shaming, interdiction bills, seizure, strategic requests or pressure.

Indictments are typically aimed to create some sort of deterrence, by showing capacity to identify and, to some extent, neutralise assets (humans or toolsets). Human operators would then have to keep a low profile and are certainly prevented from travelling to countries in extradition agreements with the accusing states.

Following the May 2014's indictment of five People Liberation Army's (PLA) officers on economic espionage charges, the origin of targeted intrusions shifted from PLA-associated threat actors to Ministry of State Security (MSS)-sponsored groups. Indeed, MSS hacking teams are reputed to be more skilled that the PLA and better able to hide tell-tale digital trails. In TM-20-006, CERT-EU reported how Chinese hacking groups APT10, APT3, APT17 and APT40 are most likely operating behind "information technology" front companies tied to the MSS.

This US diplomatic and juridical toolbox has also been used against state-sponsored hackers allegedly tied to other countries such as Russia, Iran, and North Korea. The table in Annex indicates the most notable US accusations since 2014.

Finally, recent events indicate that US technology firms are implementing on their side US government's juridical sanctions against named "foreign adversaries" (e.g. Google, Intel and Qualcomm vs Huawei, Instagram vs Iran's Islamic Revolutionary Guard Corps). In some cases, US technologies firms even took the initiative to name and sanction foreign "state-backed" entities (Twitter, Facebook and Google suspended thousands of accounts for "coordinated inauthentic behaviour" during the protests in Hong Kong).

[1] https://www.justice.gov/opa/press-release/file/1246891/download
[2] https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military
[3] https://www.wired.com/2014/05/us-indictments-of-chinese-military-hackers-could-be-awkward-for-nsa/

ANNEX - Noteworthy US judicial actions against foreign state-sponsored hackers

Date	Description	Country	Entity
May 2014	Indictments of five People Liberation Army's (PLA) officers on economic espionage charges. These individuals were reportedly working for PLA Unit 61398.	China	Military
September 2015	United States and China agreed that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property	China	
November 2015	US officials stated that the US could consider criminal charges or sanctions if they determine that Chinese hackers are violating the September 2015 agreement between by the two countries.	China	
March 2016	indictment of seven Iranians, suspected of orchestrating DDoS campaigns against US financial institutions (in 2011, 2012, 2013), on behalf of Iran's government and the Islamic Revolutionary Guard.	Iran	Paramilitary
March 2017	Indictments of four Russian nationals allegedly responsible for the 2014 breach into Yahoo! networks that compromised data of 500 million accounts. Two of the named individuals were reportedly employees of Russia's Federal Security Service (FSB).	Russia	Security services
July 2017	Indictment of two Iranian nationals, Mohammad Reza Rezakhah and Mohammad Saeed Ajily, for their activities associated with cyber intrusions into a US-based software company. One of the group's alleged targets was the proprietary PRODAS - Projectile Rocket Ordnance Design and Analysis System – software.	Iran	
November 2017	Indictment of three Chinese nationals for hacking three companies - Moody's Analytics, Trimble, and Siemens with the intent of obtaining sensitive data and trade secrets. According to the DOJ, the three men, Wu Yingzhuo, Dong Hao, and Xia Lei were owners, employees and associates in the cyber security company Guangzhou Bo Yu Information Technology Company Limited (Boyusec). Public sources associate Boyusec with the APT3 threat actor.	China	Front technology company Security services
November 2017	Charges against six members of the Russian government in the hacking of the Democratic National Committee computers before the 2016 US presidential election.	Russia	Security services
February 2018	Indictment and sanctions of 19 Russian individuals and 5 Russian entities for influence operations targeting political processes of the US.	Russia	Security services
March 2018	Indictment of nine Iran-based hackers-for-hire who operated for an Iranian entity called the Mabna Institute. The indictment specified that the group stole almost 31.5 terabytes (TB) of information from at least 320 universities around the world, with 144 of them located in the US.	Iran	Front research institute
April 2018	Sentencing of Karim Baratov, a Canadian hacker allegedly working in support of Russia's FSB, to five years in prison for participation to a massive data breach in which 500 million Yahoo accounts were compromised.	Russia	Security services
June 2018	Seizure of the command and control servers of a massive botnet, known as VPNFilter. The FBI confirmed that the botnet has been created by Russia-based threat actor APT28 designed backdoors.	Russia	Security services
September 2018	Indictment of a North Korean agent – a member of the Lazarus Group – for theft of data and a "wiper" attack on Sony Pictures in 2014 plus the worldwide "WannaCry" malware attack of May, 2017.	North Korea	
October 2018	Indictment of 10 Chinese individuals for conducting a multi-year campaign targeting the aerospace sector. These operations resulted in the theft of technical information associated with turbofan engines developed for US and European manufacturers, including technology developed by a French aerospace company with an office in Suzhou, Jiangsu province, China. Two of the conspirators were identified as officers of the Jiangsu Province Ministry of State Security (JSSD), a provincial foreign intelligence arm of the MSS.	China	Security services
October 2018	Criminal complaint against Elena Alekseevna Khusyaynova, for her purported involvement in the financial operations within Project Lakhta. Project Lakhta is the term used to describe a Russian disinformation operation that was active since at least 2014 against the US, EU, Ukraine, and other states. This complaint represented the first legal action against a foreign national for interfering in the 2018 US midterm election process.	Russia	Front financial project
December 2018	Indictment of two Chinese citizens – members of the APT10 group - for espionage. The campaign aimed to steal data from military service members, government agencies, private companies, NASA, Jet Propulsion Laboratory and companies involved in aviation.	China	Security services
February 2019	Indictment of four Iranian nationals for conducting a cyber-espionage campaign targeting US government officials. The attackers leveraged multiple social engineering methods, in particular the Facebook platform.	Iran	
May 2019	Indictment of two Chinese hackers for their roles in conducting intrusions into major health insurance provider Anthem as well as several other firms during 2014 and 2015. These two individuals were named as part of a China-based hacking collective.	China	Security services
April 20219	One day after the US designation of the Islamic Revolutionary Guard Corps (IRGC) as a terrorist organisation formally went into effect, the social media network Instagram suspended accounts affiliated with the IRGC organisation and its top commanders.	Iran	Paramilitary
May 2019	Following a US President Executive Order on banning 'foreign adversaries', Google suspended business with Huawei. A number of semiconductor companies such as Intel and Qualcomm also made similar announcements.	China	Technology firm
August 2019	Twitter, Facebook, and Google suspended thousands of accounts for "coordinated inauthentic behaviour" and "attempting to sow political discord" in Hong Kong. The platforms' operators claimed that accounts were associated with state-backed entities.	China	
January 2020	Indictment of four Chinese hackers members of the People's Liberation Army for conspiracy and hacking into the Equifax consumer credit reporting agency.	China	Military