ALSTON & BIRD

WWW.ALSTON.COM

CYBER ALERT ■

JANUARY 29, 2019

Ten Lessons from Six 2018 DOJ Indictments of State-Sponsored Hackers

By Kim Peretti , Emily Poole, and Nameir Abbas

2018 was a banner year for criminal indictments of state-sponsored actors, with double the number of indictments for cybercriminal activity compared to the historical total. The Department of Justice announced charges against 41 criminal actors connected to the Chinese, Russian, Iranian, and North Korean governments over the course of 2018, in the process offering a glimpse into the operations of some of the most sophisticated cybercriminal actors in the world. And while we tend to view these indictments as a reflection of ongoing geopolitical maneuvering, focusing on the extent to which they may deter future state-sponsored cybercriminal activity, we should not overlook the insight we can gain from the details contained within the four corners of the charges about how such state-sponsored groups target and exploit companies, time and time again.

The Indictments

China

October 2018

In October 2018, the DOJ unsealed charges filed by the U.S. Attorney's Office for the Southern District of California and the National Security Division's Counterintelligence and Export Control Section against two Chinese intelligence officers and their co-conspirators for their efforts to steal IP and sensitive business information from companies involved in the development of a new commercial airliner engine. This was the second-ever indictment against Chinese state-sponsored hackers, the first being the May 2014 indictment of five hackers who were members of an elite cyber-espionage unit within China's People's Liberation Army.

The hacking efforts alleged in the indictment began in 2010 and continued until at least 2015, while a Chinese state-owned company was developing a comparable commercial airliner engine. The attacks extended not only to the companies directly involved in development of the engine but also to companies manufacturing parts for the engine.

Significantly, the indictment was one of several filed by the DOJ last fall against Chinese intelligence officers and those working at their direction for allegedly stealing American intellectual property, including a November 2018 indictment of a state-owned company for conspiring to steal trade secrets of an American semiconductor company.

December 2018

Just two months later, in a groundbreaking indictment, the U.S. Attorney's Office of the Southern District of New York's Complex Frauds and Cybercrime Unit outlined the alleged hacking activities of two Chinese citizens associated with Advanced Persistent Threat 10 (APT10), a hacking group with connections to the Chinese government. These hackers are suspected of conducting a years-long global hacking campaign to steal sensitive IP and business information from companies and government agencies around the world.

The campaign in question began as far back as 2006 with unauthorized access to the systems of dozens of technology and technology-related companies in the U.S. along with U.S. government entities. In some cases, the hackers managed to steal "hundreds of gigabytes of sensitive data and information" from the victims. Beginning at least in or about 2014, the campaign extended to managed service providers (MSPs) with access to IT infrastructure of companies around the world.

Notably, the DOJ acted in concert with partner agencies in other countries to publicize the indictment, taking the unusual step of alleging that China was acting in violation of a 2015 agreement with the U.S. on commercial espionage.

Russia

July 2018

Russia's alleged hacking activities in the lead-up to the 2016 U.S. election are well-known but worthy of emphasis. As outlined in the charges brought by the DOJ's Special Counsel's office, throughout 2016, Russian intelligence officers engaged in a campaign to gain unauthorized access to and exploit the systems of various arms of the Democratic Party and the Clinton campaign, including associated individuals. These officers proceeded to leak and publicize the stolen information.

This was the second indictment against Russian state-sponsored actors for hacking activities. The first indictment was only a year prior in March 2017, when the DOJ brought charges against four defendants, including two officers of the Russian Federal Security Service (FSB), for hacking activity that resulted in unauthorized access to the contents of millions of email accounts.

October 2018

In October 2018, the U.S. Attorney's Office for the Western District of Pennsylvania and the National Security Division's Counterintelligence and Export Control Section released an indictment against Russian intelligence officers for intrusions into the systems of anti-doping agencies around the world and associated officials, organizations investigating Russia's use of chemical weapons, and others. These activities were allegedly provoked by anti-doping measures taken against Russian athletes following the 2014 Sochi Winter Olympics

and before the 2016 Rio de Janeiro Summer Olympics. The hackers publicly released stolen data, including medical information on athletes and sensitive records and emails from anti-doping agencies, in some cases doctoring the records.

Iran

In March 2018, the U.S. Attorney's Office for the Southern District of New York charged nine Iranians with conducting a cyber-theft campaign on behalf of the Islamic Revolutionary Guard Corps and other Iranian government clients, during which the hackers allegedly entered systems belonging to hundreds of universities, as well as various companies and government offices, in an attempt to steal academic and proprietary data. From 2013 through 2017, the hackers purportedly targeted more than 100,000 accounts of professors around the world, broadly targeting intellectual property of all types from the compromised systems.

Just as for China and Russia, this is not the first time that Iranian state-sponsored hackers were the subject of a federal indictment. In March 2016, the DOJ released an indictment of Iranian state-sponsored actors in connection with their alleged involvement in an extensive campaign of distributed denial-of-service (DDoS) attacks against the U.S. financial sector. And while not associated with activity tied to the Iranian government, the U.S. Attorney's Office for the District of New Jersey indicted two individuals in November 2018 for authoring, from inside Iran, the SamSam ransomware attack that affected more than 200 victims, including hospitals, public institutions, and municipalities such as the city of Atlanta.

North Korea

In September 2018, the U.S. Attorney's Office for the Central District of California and the National Security Division's Counterintelligence and Export Control Section unsealed a criminal complaint charging a North Korean citizen, Park Jin Hyok, for his part in a years-long conspiracy to conduct several destructive cyberattacks as a member of the government-sponsored hacking team known as the Lazarus Group. This is the first indictment against the government of the Democratic People's Republic of Korea. The hacking campaign has made global headlines several times in the past few years, starting in 2014, when Park allegedly took part in the cyberattack against Sony Pictures Entertainment. Park is also charged for his suspected part in the theft of $81 million from Bangladesh Bank in 2016, as well as the 2017 WannaCry 2.0 ransomware attack that caused extensive damage to computer systems around the world.

Common Threads: Motives, Techniques, Activities, and Lessons to Learn

While the indictments reveal activity that is both far-reaching and varied, the groups' motives, techniques, and activities share much in common. These commonalities serve to emphasize the breadth and complexity of information systems in the digital age, and also the difficulty in protecting those systems from determined, competent, and well-resourced threat actors.

More importantly, the indictments highlight common patterns for a cyber intrusion: a successful spear-phishing attempt, followed by attempts at privilege escalation via credential theft, installation of malware, and exfiltration of targeted data (or disruption of operations). The threat actors often remain undetected

for an extended period and may effectively cover their tracks upon departure, a common feature of state-sponsored cyber intrusions dating back to the infancy of such activity.

For example, in the complaint against North Korean hacker Park Jin Hyok, the government outlines how the attackers sent spear-phishing emails that mimicked legitimate emails from large technology companies, prompting victims to click on malicious links. Once a spear-phishing email was successful and access was gained, the attackers were able to move laterally through both Sony's and Bangladesh Bank's networks. In both cases, the attackers allegedly used highly customized malware, the result of extended covert reconnaissance, to disrupt company operations.

The Iranian hackers also relied heavily on spear phishing as a means of effectuating their hacking campaign. These spear-phishing emails were highly tailored and based on reconnaissance activity by the hackers. Once successful in stealing the victims' credentials, the hackers would then gain access to the victims' accounts and steal an array of proprietary and sensitive data. The Iranian hackers also attempted "password spray" attacks, in which hackers attempt to gain unauthorized access to a large number of online accounts by using a set of common passwords.

While the alleged attacks by Russian hackers were more targeted in nature than the attacks by Iranian hackers on universities, both sets of attacks follow a similar pattern. In each case, the hackers began their attacks by sending spear-phishing emails, often conducting research on their targets in order to send highly customized messages. Once they gained access using stolen credentials, they installed different types of malware, then proceeded to monitor victim activity and exfiltrate data. An interesting wrinkle mentioned in the indictment regarding Russian activity against anti-doping agencies is the partial reliance on "close-access" attempts to compromise systems through Wi-Fi connections such as hotel Wi-Fi networks. This involved the hackers flying to locations around the world, gaining physical proximity to their targets to facilitate hacking when more remote hacking proved unsuccessful.

On top of more conventional spear-phishing emails, the Chinese hackers used "watering hole" attacks—in which malware is installed on legitimate websites to infect the systems of website visitors. Both Chinese hacker indictments also show that once the hackers gained initial access to the systems of a target company or one of its vendors, such as a managed service provider (MSP), the hackers were able to steal credentials, escalate their privileges, and move from system to system.

While each attack is certainly unique, similarities between them show that there are key lessons to be learned about how a company can take steps to protect itself from and respond to similar attacks.

Lesson 1: Anyone Can Be a Target

The 2018 indictments in some cases allege highly targeted and specific cyberattacks, but taken together cover a startling amount of ground. Between ostensibly political and retaliatory operations in the case of Russia, economic espionage across a variety of sectors in the case of China, IP theft from largely universities and companies in the case of Iran, and sometimes indiscriminate activity in the case of North Korea, it would be difficult to clearly delineate the targets of nation-state activity. Bear in mind also that the 2018

indictments reveal only a glimpse of the full picture, given the virtual certainty of persistent, unindicted (and in some cases undetected) state-sponsored hacking activity.

Lesson 2: Keep Your Guard Up If Political or Economic Winds Are Shifting

Cyberattacks can be politically or economically motivated. They can be part of a years-long and general campaign, or of a more discrete and focused effort. The key point is that nearly all companies, given the right circumstances, could become an attractive target for government-sponsored hackers. The recent FBI alert regarding possible malicious activity by Iranian hackers following the U.S. government's withdrawal from the Joint Comprehensive Plan of Action (JCPOA) highlights this possibility, with the perceived risk of Iranian hacking activity increasing as tensions between Iran and the United States increase. More generally, companies should assess their cyber risk in light of the sensitivity of their operations, absorbing industry intelligence and law enforcement alerts in the process.

Lesson 3: Phishing Is Still King

If you learn anything from the 2018 hacker indictments, it should be that phishing—and particularly, spear phishing—is so often the first domino in a sophisticated and damaging intrusion. Every nation-state actor mentioned in these indictments used well-executed spear phishes to gain an initial foothold in a victim's systems. For example, in addition to sending messages that closely mimicked Facebook and Google security alerts, North Korean hackers also sent emails that seemed to come from senior personnel and recruiters at top companies. Likewise, the Iranian hackers conducted research on targets and tailored their emails to include details on articles that the victim had published.

Lesson 4: Vendor Networks Remain a Prime Target

The 2018 indictments show that hackers know that a target's greatest vulnerability is often its vendors. Whether hacking a vendor to gain information related to a target (such as Chinese hackers attacking an aerospace company's parts manufacturers), or using the vendor's access to the target to enter the target's systems (such as Chinese hackers attacking MSPs to gain access to systems around the world), a determined hacker will explore all possible avenues of entries into a company's systems.

Lesson 5: Prioritize Email Account Security

Email accounts are frequent targets of hackers because of the wealth of information they contain. However, hackers don't always need to steal email credentials to hack into an account—especially when they can guess the password. As recent attacks have demonstrated, any email account that is not protected by multifactor authentication may be at risk, and state-sponsored actors as well as criminal actors are exploiting this, recognizing their value as a target.

Lesson 6: Internal Defenses Are Key

In nearly all the attacks described in the indictments, once the hackers were able to gain initial access to a victim's systems, they didn't just stop there. By moving laterally within a company's systems, hackers can

find additional credentials, escalate privileges, steal more proprietary information, or just cause as much damage to a company's systems as possible.

Lateral movement can be planned and purposeful, as in the case of Chinese hackers targeting MSPs to gain access to tech companies or North Korean hackers attempting to cause maximum damage to Sony's systems (Sony ended up having to remove nearly 8,000 work stations to contain the spread of the attack). However, as the world saw following the 2017 WannaCry 2.0 ransomware attack, hackers are also increasingly using self-propagating malware that can spread indiscriminately from system to system. Such attacks demonstrate the importance of not just protecting against intrusions coming from the outside, but having controls in place that prevent attackers from having free rein once access has been gained. Companies should consider, for example, enforcing the principle of "least privilege" for their users, requiring multifactor authentication for access to sensitive internal systems, and segmenting networks. Companies should also consider engaging in regular compromise assessments and cyber-threat hunting to detect and isolate threats before they spread.

Lesson 7: Prepare for Ransomware

The success of a ransomware attack often depends on two things: a victim using unpatched software and failing to maintain adequate backups of their systems. For example, the 2017 WannaCry ransomware attack caused widespread damage by exploiting an unpatched vulnerability in Windows systems, as outlined in the DOJ indictment of the North Korean hacker. To prevent ransomware from seriously disrupting a company's operations, companies should consider, for example, not only regularly patching software, but also taking steps to regularly back up data and ensuring that the backups themselves are well protected.

Lesson 8: Attackers Play the Long Game

The indictments underline the fact that effective cyberattacks are often the result of persistent efforts by hackers, over months or even years, to gather information on their targets. Before gaining access, hackers often conduct extensive research to craft customized spear-phishing emails, and once access is gained, and the more information a hacker has on the structure of their target's systems, the more damage they can cause. For example, North Korean hackers allegedly spent up to a year in the Bangladesh Bank network before attempting to transfer funds. As part of the attack by Russian hackers on anti-doping agencies, the attackers conducted total reconnaissance of victim networks, noting related IP addresses, network ports, and associated domains, and researching password requirements for the victim's databases. Companies should therefore remain vigilant for suspicious activity, recognizing that isolated or periodic instances of unexplained network activity may actually be signs of a larger attack.

Lesson 9: Beware the Insider Threat

When it comes to state-sponsored hacking activity, companies should also assess the risk of an insider threat and the possibility of employees working on behalf of a nation-state actor. As described in the October 2018 indictment against Chinese hackers, this unfortunately became a reality for a French aerospace company with offices in China, when several employees were suspected of working in coordination with Chinese intelligence officers and recruited hackers to steal company information.

Lesson 10: "An Ounce of Prevention Is Worth a Pound of Cure."

The indictments unfortunately show that when it comes to state-sponsored hacking activity, criminal actors are tenacious, and it may be difficult for companies that find themselves in the crosshairs to protect their systems. Recognizing this risk, companies should be sure that they have a plan in place for *when* an attack happens, including procedures for accessing data backups, involving law enforcement including knowing which law enforcement agency or section of the DOJ may be most appropriate to investigate the particular activity, and bringing in outside resources.

Cybersecurity Preparedness & Response Team Co-Chairs

Kimberly Kiefer Peretti | 202.239.3720 | kimberly.peretti@alston.com
Jim Harvey | 404.881.7328 | jim.harvey@alston.com

Follow us: @AlstonPrivacy | www.AlstonPrivacy.com

www.alstonsecurity.com

ALSTON & BIRD

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86 10 8592 7500
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, TX 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 1950 University Avenue ■ 5th Floor ■ East Palo Alto, CA 94303-2282 ■ 650-838-2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333

Cybersecurity Preparedness & Response Team Co-Chairs

Kimberly Kiefer Peretti | 202.239.3720 | kimberly.peretti@alston.com
Jim Harvey | 404.881.7328 | jim.harvey@alston.com

Follow us: @AlstonPrivacy | www.AlstonPrivacy.com

www.alstonsecurity.com

ALSTON & BIRD

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86 10 8592 7500
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, TX 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 1950 University Avenue ■ 5th Floor ■ East Palo Alto, CA 94303-2282 ■ 650-838-2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333