CYBER SECURITY BRIEFING

A Monthly Recap of Technology & Information Risk

PINKERTON®

JULY 2019

Eight Major Technology Firms Hacked

Eight networks of the world's biggest technology service providers were hacked by workers from the China Ministry of State Security.

Hackers allegedly working for China's Ministry of State Security broke into the networks of at least eight major technology services providers and retrieved sensitive information from their clients in a years-long attack. According to a U.S. indictment, the global hacking campaign, known as Cloud Hopper, aimed to steal western intellectual property (IP) to advance Chinese economic interests. However, the Chinese Foreign Ministry denied all accusations, claiming to oppose acts of cyber-espionage. Reuters identified the following affected providers: Hewlett Packard, IBM, Fujitsu, Tata Consultancy Services, NTT Data, Dimension Data, Computer Sciences Corporation, and DXC Technology. Hackers reportedly infiltrated the company's networks, by tricking employees into downloading malware or giving away their credentials. Once they infiltrated, hackers managed to access server administrator's controls, and passed through the "jump server," identifying commercially sensitive information and then encrypted and exfiltrated data. The number of companies whose information was breached is currently unknown, but Sabre Corp, a hotel reservations provider, and Huntington Ingalls, a nuclear-powered submarines builder, are among the affected companies.

Pinkerton assesses that large companies relying on the stated providers' services, particularly those involved in the defense or technology development industries, were highly likely affected by Cloud Hopper attackers, compromising a substantial part of their IP. Due to alleged IP laws laxity and judicial protectionism, piracy and counterfeiting remain concerning issues in China, costing the U.S. around USD 600 billion (CNY 4.1 trillion) per year, according to President Donald Trump's accusations. Pinkerton further assesses that sensitive commercial secrets retrieved through the identified attacks will likely lead to IP infringement, potentially benefiting several Chinese competitors that, thanks to a cheaper workforce, can offer cheaper versions of foreign goods.

Vulnerability Found In Microsoft Outlook For Android

A spoofing bug in Microsoft Outlook for Android Open can open the door to an email attack chain.

Security researchers detected a spoofing vulnerability in Microsoft Outlook for Android, which opens the door to cross-site scripting (XSS) attacks. In this kind of attack, the hacker uses a trusted website or software application to send malicious code to a user in the form of a browser side script. Hence, the attacker could exploit the flaw by sending a crafted email message to a victim with a link containing malicious JavaScript. Once the user clicks on the link, the malicious scripts run without validation, which then reflects to the victim's browser and executes in the context of the user's session. Microsoft already patched the vulnerability and released the updated version (3.0.8), in which Outlook for Android now is able to parse the specially crafted email messages.

Pinkerton assesses that cyber-attacks that exploit this flaw in Microsoft Outlook will be resolved in the short term as the patched update has already been released. However, as it is a popular email app which is currently being used by over 100 million users, it is highly likely that many clients are currently exposed if they still have Outlook versions before 3.0.8. Outlook has presented other bugs. In 2018, the app had a flaw in which allowed attackers to steal users' Windows passwords if they previewed an email that had a Rich Text Format (RTF) attachment containing a remotely hosted Object Linking and Embedding (OLE) compound document. Pinkerton recommends clients install the updated version from Google Play Store as soon as possible and verify their devices do not present any unrecognized actions.

Hacker Accessed Restricted NASA Documents Using Raspberry Pi

Raspberry PI was the cause of an early 2018 cyberattack at NASA.

A hacker was able to access restricted documents held by the National Aeronautics and Space Administration (NASA) in April 2018 using a Raspberry Pi, which is a tiny single-board computer generally used as a tool for learning computer programming, robotics, and "Do it yourself" (DIY) projects. The attacker created a portal using the Raspberry Pi to connect to the Jet Propulsion Laboratory (JPL) system and stole 23 files while remaining undetected for 10 months. Some of the stolen files are related to robotic space and earth science missions, including information regarding the International Traffic in Arms Regulation and Mars Science Laboratory mission. Additionally, as the hacker connected to two of three JPL networks, NASA had to temporarily disconnect various space-flight-related systems from the JPL network. Consequently, JPL installed more monitoring agents on its firewalls and NASA's Office of Inspector General is leading an ongoing investigation into the incident, as the culprit has not been found.

Pinkerton assesses that cyber-attacks targeting the networks of NASA and other government institutions are likely to occur in the long term as they own relevant confidential information which is highly attractive to foreign governments and hackers. In 2018, the Department of Justice charged two Chinese hackers who worked for Huaying Haitai Science and Technology Company. The hackers tried to steal intellectual property from technology companies and accessed NASA and the U.S. Navy's cloud services. Moreover, as it has been shown that several of the federal agencies do not own either a complete inventory of their systems' components nor security controls to monitor and detect cyberattacks on its network, it is highly likely that hackers take advantage of remaining security breaches. Therefore, clients who own companies linked to governmental agencies are likely to be vulnerable to hacking attacks. Pinkerton recommends clients to monitor the news, and statements of companies and national agencies related to their interests for up to date information on cyberattacks that could affect them. Further, Pinkerton advises clients to employ a managed security service provider (MSSP) to monitor and ensure the security of their network.

A Ransomware Attack Hit Florida, Hackers Demanded Payment

Florida city decides to pay $600,000 to hackers who seized its computer system.

Recently, it was disclosed that the Riviera Beach City Council in Florida agreed to pay XBT65 (USD 613,015) in ransom after a ransomware attack paralyzed the computer system of Palm Beach. Local authorities reported that hackers encrypted the information stored on the city's system, which put at risk the email, the water utility pump stations, and 911 records of the town. Moreover, the online utility payments' system and email server were disabled. The attack began on May 29 when an employee of a police department downloaded an infected email attachment which unleashed malware on the city's network. The authorities have spent at least USD 900,000 (EUR 796,738.50) to rebuild its computer network. Further, the Riviera Beach's website was restored, and new email accounts were created for all the staff members. This is not an isolated event, other city's governments across the country, including Atlanta, New Jersey Newark, and Sarasota have been forced to pay considerable sums of money due to cyber-attacks.

Pinkerton assesses that ransomware attacks against individuals, as well as public and private agencies, including governmental entities, will likely continue in the medium to long term as hackers have sophisticated its attacks. Pinkerton considers that the technology developed by hackers is evolving faster than the protection hardware and programs implemented by entities as it occurred on 2017 when the U.S. National Security Agency (NSA) lost control of the Eternal Blue hacking tool which became a cyber weapon used by hackers. Pinkerton recommends all clients to reinforce their database systems, secure their backups, and to isolate detected infected systems to protect them against cyber-attacks, primarily if it contains confidential and sensitive information. Pinkerton recommends all clients to encourage their employees to avoid downloading files or opening links coming from unverified sources.

U.S. Cyber Command Intensifies Probes Of Foreign Electrical Grid

US Cyber Command is targeting Russia's electrical grid more aggressively.

The New York Times has reported that the United States Cyber Command (USCYBERCOM) is responsible for infiltrations in Russia's electrical infrastructure. Allegedly, the increased frequency and sophistication of the probes are intended to warn Russia that the U.S. will aggressively prevent attempted cyber-attacks and to maintain the ability to quickly launch a large-scale cyber-attack against the country's electrical grid. The U.S. reportedly started penetrating Russia's electrical grid in 2012, but intrusions increased significantly in the past few months by sending malware from inside its system. The USCYBERCOM will be able to undertake operations with the Department of Defense's authorization instead of the President's.

Pinkerton assesses that the practice of cyber-intrusions into government networks is likely a practice of several sophisticated state-sponsored cyber entities. The capability has been previously demonstrated in cyber-attacks, widely attributed to Russian hackers, against U.S. and Ukrainian critical infrastructure over the last three years. Future attacks initiated by nation-state actors are likely to increase during times of significant political turmoil or major national events such as election cycles. As the capability to infiltrate and disrupt critical infrastructure increases globally, countries are likely to face increased critical infrastructure outages, which is highly likely to increasingly affect network reliability and business continuity over the long term.

Russian Hackers Likely Responsible For Major Cryptocurrency Theft

The largest crypto exchange theft may have been carried out by Russian hackers.

The Japanese newspaper, Asahi Shimbu, reported that it is believed that a Russian or Eastern European hacker group gained remote access to the computers of the Japanese crypto exchange Coincheck exchange employees using a malware sent via email. In January 2018, Coincheck lost 500 NEM tokens, a platform, and blockchain-based peer-to-peer cryptocurrency, worth USD 534 million, due to a breach in their system. This event is the largest theft of cryptocurrency. The viruses were recognized as "Mokes" and "Netwire," which had been used by Russian hackers in 2011 and 2007 respectively. Before Asahi Shimbun's disclosure of the Russian group, authorities thought a North Korean state-sponsored hacking team were responsible for the Coincheck hack.

Pinkerton assesses that cyber-attacks targeting cryptocurrency exchanges are likely to continue in the long term as they have not developed preemptive measures against hackers and security breaches. In May 2019, unidentified hackers stole 7,000 bitcoin (BTC) (USD 65.3 million) from Binance, a cryptocurrency exchange founded in China and currently located in Japan, using phishing and viruses. Also, in March and May 2019, a North Korean hacking group used phishing methods to attack UpBit and, allegedly, insiders helped outside attackers to hack Bithumb, both important South Korean cryptocurrencies. Even though some cryptocurrency companies have been able to work with other major cryptocurrency exchanges and foundations to recover the equivalent of the lost funds, Pinkerton finds it likely that the frequency of these attacks is likely to affect investors' confidence in cryptocurrency platforms.

Nationwide Internet Shutdown During National ExamsInformation

Ethiopia remains offline in a bid to curb cheating during secondary school final exams.

Ethiopia has been without internet access since June 11. Text messaging services have also been shut down nationwide since June 13. According to the media, it is allegedly due to a government measure to stop students from cheating during 10 and 12th grade national exams to enter university or to enroll into national vocational courses, which last from the late May to June 18. NetBlocks, a civil society group which focuses on digital rights, cyber-security, and internet governance, said only 12% of connectivity remains working, mainly in diplomatic and international institutions, and banks. Neither Ethio Telecom, the state-owned telecoms monopoly, nor the government has not made any declarations about the situation. The United Nations Human Rights Council declared in 2016 that government internet access restriction is a human rights violation.

Pinkerton assesses that internet and text messaging service disruptions are likely to continue until June 19, when exams have concluded. In 2017, a government official declared that the shutdown which took place that year was a measure to prevent another leakage of exam papers as it happened years back. Moreover, other countries like Somalia, Zambia, and Algeria have also reportedly employed blackouts as a measure to prevent widespread leakages during national exams. Pinkerton finds it likely that governments' control over internet access can lead to a total shutdown during other future events such as elections and protests. Moreover, the shutdowns are likely to affect investor confidence in the region as the shutdown has cost businesses operating in Ethiopia and estimated USD 4.5 million (GBP 3.6 million) a day.

Massive Power Outrage Affects Millions Of Users

Massive power outage in Argentina and Uruguay caused by failure in an electrical grid results in blackouts.

Media reports have reported that most of the power had been restored in Argentina, Uruguay, and Paraguay after the electrical blackout on June 16. This power cut affected millions of people in these countries, causing several issues including train delays, out of order traffic lights, stopped public transportation, disrupted communication systems, and interrupted regional elections. Argentine President, Mauricio Macri, claimed that it is unclear what caused the electrical failure, but authorities will start an investigation. The Argentine Energy Secretary declared that the Argentine Interconnection System (SADI) failed.

Pinkerton assesses that more blackouts will likely occur in the short to medium term until the authorities conclude the investigation about what caused the outage and effectively address the issue. The outage is widely assessed to be the result of a cyber-attack or a weather problem. The governments will be required to fix or upgrade the system once they examine the blackout root cause. This situation demonstrates the instability of the power grid in the region. Pinkerton finds that clients with operations in these countries will highly likely experience delays in the supply chains and logistics as the transportation system was disrupted and several businesses were forced to shut down on June 16. The power blackout also affected the most vulnerable sectors, including the health system, where clients will also face delays in medical services such as doctors' appointments or emergency assistance in the short term. Pinkerton recommends clients monitor the investigation's result to determine how vulnerable the regional grid is and to consider this information as part of the operations' risks. Furthermore, Pinkerton advises evaluating the economic cost of these risks in regional business plans.

Malware Affects Philadelphia's Court System

Philadelphia courts thrown into chaos because of a computer virus.

Malware has shut down Philadelphia's court system, blocking anyone from filing documents or foreclosures postponements, signing up for jury duty, navigating the court's website, and using its e-mail system. Philadelphia's court system stated that, as they discovered malware on a limited number of computers and they have shut down the system as a precaution since May 21. No details as to what kind of malware is affecting their system were provided because of ongoing investigations. The court remains open in person, sending people to physical courts and pushing lawyers to make paper filings. Housing law processes, due to the lack of electronic system, are reportedly showing disruptions, as requirements or foreclosures postponements are not being delivered on time. Philadelphia Unemployment Project asked a judge to halt foreclosures, arguing "basic due process protections," but the judge did not grant the delay. It is currently unknown when the court systems will be functional again. On May 7, Baltimore's city government system was also shut down because a ransomware attack with an EternalBlue virus, which Microsoft already had a patch but was not installed at the time. This ransomware virus encrypted Baltimore's governmental data, and then malicious actors demanded a ransom in exchange for the decryption key.

As shutdowns in local government systems in the United States are showing an increasing trend, Pinkerton assesses that malicious actors are profiting from the cities' networks vulnerabilities, deeply affecting public services continuity and people's privacy. Pinkerton finds it likely that many local governments have not updated their cybersecurity services and protocols, as to prevent, detect, and react to this kind of attacks. For clients involved in foreclosure in Philadelphia, Pinkerton recommends seeking legal advice as to monitor the development of their processes since a human error likely would lead to losing property, in case a foreclosure postponement is not filed promptly.

Triada Adware Found To Affect Up To 20,000 Android Devices

Hackers scam Android phone makers as software vendors to install Triada adware.

A German information security agency recently noted firmware-based malicious software present on several Android devices, including the Doogee BL7000, the M Horse Pure 1, and the Keecoo P11 models. At the time of writing, there are approximately 20,000 affected Android smartphones detected in Germany. It is not known if there are additional cases in other countries and if Triada adware is responsible for all affected devices or if additional malware is involved. In March, Google reported that hackers loaded up adware as pre-installed software in Android devices in 2018. The software was believed to help phone original equipment manufacturers (OEMs) add features to Android OS besides the ones that are already part of the Android Open Source Project. However, the features included a side of adware known as "Triada." So far, Google has shared that the Android malware authors went by the vendor name of "Yehuo" or "Blazefire" and that they appear to speak Chinese. Google sent out software updates to remove the adware from affected products, but it did not inform which product models were affected.

Pinkerton assesses that these cyber-attacks on Android devices will continue in the long term as it has been shown that Android malware authors are becoming more sophisticated, and that protection from Google has not sufficiently addressed the issue. Kaspersky Lab detected Triada in 2016 in China. At that time, once Triada was installed, it gained access to the phone and modified SMS messages. Google took security measures, but in 2017, another security firm reported more cases of affected Android smartphone models. Further, as Android smartphones are highly used, and it is not known in which other countries Triada cases have occurred, many clients could likely be exposed to future malware intrusions. Pinkerton recommends clients verify their Android phones do not have suspicious add features or present unrecognized actions. Moreover, Pinkerton advises clients to confirm if there is information regarding the add features information to verify if they are part of the Android Open Source Project.

Chinese IP Address Used For DDoS attack Against Telegram

Telegram briefly went offline after a powerful DDOS attack hit its servers.

Allegedly a state actor conducted a distributed denial-of-service (DDoS) attack against Telegram, a popular encrypted messaging app, on June 12, taking the service offline. Telegram's founder later announced the attack came from a Chinese IP address and that the company received a massive number of garbage requests which caused the server to stop processing authentic requests. This event affected Hong Kong protesters as they are currently using Telegram's service to communicate, organize strikes, and alert each other since protests began on April 28.

Pinkerton assesses that DDoS interruptions are likely to continue over the long term. Pinkerton finds it likely that further DDoS attacks against Telegram are likely in the short term as rallies continue in Hong Kong. Even though a DDoS attack does not affect users' data saved in the app, cyber-intrusions in the app are likely to occur in the future if governments or possible attackers believe that this app has valuable information regarding upcoming protests in Hong Kong and around the world. Pinkerton finds it highly likely that future service interruptions on Telegram will coincide with announced protest dates in Hong Kong.

Quest Diagnostics Hack Exposes Millions Of Patients

12 million patients may have had their personal information exposed.

Allegedly a state actor conducted a distributed denial-of-service (DDoS) attack against Telegram, a popular encrypted messaging app, on June 12, taking the service offline. Telegram's founder later announced the attack came from a Chinese IP address and that the company received a massive number of garbage requests which caused the server to stop processing authentic requests. This event affected Hong Kong protesters as they are currently using Telegram's service to communicate, organize strikes, and alert each other since protests began on April 28.

Pinkerton assesses that DDoS interruptions are likely to continue over the long term. Pinkerton finds it likely that further DDoS attacks against Telegram are likely in the short term as rallies continue in Hong Kong. Even though a DDoS attack does not affect users' data saved in the app, cyber-intrusions in the app are likely to occur in the future if governments or possible attackers believe that this app has valuable information regarding upcoming protests in Hong Kong and around the world. Pinkerton finds it highly likely that future service interruptions on Telegram will coincide with announced protest dates in Hong Kong.

TECHNOLOGY & INFORMATION RISK

Are the proper controls in place to fully protect your bottom line?

"High tech" is synonymous with "rapid change." Systems you put in place two years ago might be ineffective today. You can improve corporate controls a variety of ways, including enhanced IT monitoring and better business intelligence.

About Pinkerton

Pinkerton traces its roots to 1850 when Allan Pinkerton founded the Pinkerton National Detective Agency. Today, Pinkerton offers organizations a range of corporate risk management services from security consulting and investigations to executive protection, employment screening and security intelligence. With employees and offices worldwide, Pinkerton maintains an unmatched reputation for protecting clients and their assets around the globe.

PINKERTON
101 North Main Street, Suite 300
Ann Arbor, MI 48104
+1 800-724-1616
www.pinkerton.com