CYBER SECURITY BRIEFING

A Monthly Recap of Technology & Information Risk

PINKERTON®

NOVEMBER 2018

Malicious Actors Attack Summit Website

Saudi summit website was attacked and left inoperable for at least 6 hours by hackers potentially due to Khashoggi death.

A high profile Saudi Arabia summit website was attacked by hackers. Pictures started to circulate on Twitter showing the Future Investment Initiative website and a mock photo of journalist Jamal Khashoggi being executed. After six hours, the website was functioning properly again but had been inaccessible during that time. The summit has had several high-profile dropouts after allegations the country was behind the death Khashoggi. Khashoggi died on October 2 when visiting the Saudi Arabian consulate in Istanbul, Turkey, where officials there allege he was murdered.

Pinkerton assesses that the cyber-attack on the Future Investment Initiative website was highly likely to highlight the death of Khashoggi. However, the hack likely will lead to other malicious actors having access to the website. The information spread on social media is likely to be leveraged for further attacks. Pinkerton also assesses that further cyber-attacks to expose the death of Khashoggi are likely in the immediate to medium term. After the website exposure and image released, Pinkerton finds it likely that further politicians and business executives from across the world will pull out of the summit. Saudi Arabia is likely to continue to face backlash as several have argued that the explanations for Khashoggi's disappearance are not credible. Pinkerton recommends clients monitor for any further government breaches in Saudi Arabia until the summit is over as negative views of the country will likely affect doing business there..

Cathay Pacific Data Breach; 9.4 Million Passenger Records Accessed

According to Cathay Pacific Airways, 9.4 million of its passengers and Hong Kong Dragon Airlines Limited had their data accessed without permission.

Cathay Pacific Airways Ltd released a statement saying that approximately 9.4 million passenger records were accessed during a two-week data breach first detected in March 2018. Cathay Pacific's Chief Executive Rupert Hogg offered a sincere apology for data theft that occurred during the security breach, saying that the company immediately notified Hong Kong Police and engaged the help of a leading cybersecurity company to contain the breach when it was detected. According to Cathay Pacific's statement, known (specific) information accessed included passengers' names, dates of birth, nationalities, passport numbers, email and mail addresses, identity card numbers, telephone numbers, and travel histories. The company contacted the affected passengers to provide information and has noted that no evidence of the data being exploited has been found.

That the stolen records do not appear to have been exploited so far, but included passengers' travel histories, leads Pinkerton to find it unlikely that financial exploitation was the goal. Rather, Pinkerton finds it likely that the breach was conducted or directed by a government to track individuals over time and locations of travel. However, while financial gain may not have motivated the attack, there is an even chance that the personally identifiable information (PII) records will be sold. For companies and individuals that routinely or occasionally use Cathay or its Hong Kong Dragon Airlines subsidiary for travel, this situation may correlate with recent scrutiny by China's Ministry of State Security; corporate security departments may need to investigate this situation for any connections with reports from management and executives of government harassment, surveillance, or compromise attempts.

Researchers Identify Trojan That Bypasses Anti-Virus Detection

Cisco Talos security researchers are warning of an infection campaign that leverages malicious RTF files to deliver information-stealing Trojans.

Last month, cyber-security researchers identified a new infection campaign for delivering Trojan malware that bypasses anti-virus detection. The campaign leverages malicious RTF files to deliver Agent Tesla, the Loki information stealer, and Gamarue, among other Trojans. Malicious actors are able to exploit a patched vulnerability in Microsoft infrastructure, the Equation Editor component of Microsoft Office. Through the exploit, malicious actors issue command and control (C&C) traffic. Malicious actors embed infected Microsoft Object Linking and Embedding objects and Macintosh Edition Manager subscriber objects with high levels of obfuscation to avoid detection. Agent Tesla Trojan is designed for information stealing, as well as delivering additional forms of malware. The trojan is able to steal passwords and conduct a number of rootkit functions, including keylogging, screenshot capturing, webcam access, and clipboard stealing. The malware targets internet browsers and a number of other applications to steal passwords.

As the Trojan is able to bypass anti-virus detection, Pinkerton assesses the Trojan constitutes a high threat to clients. Further, as the malware targets a large number of popular Internet browsers and other applications to steal passwords, Pinkerton finds it likely that the malicious actors have an expansive target list. Pinkerton recommends that clients closely scrutinize emails and other communications tools for suspicious attachments. Pinkerton recommends clients ensure the installation of the latest patches for Microsoft products to mitigate the threat of malware.

Cryptomining Malware Installing With Fake Adobe Updates

Palo Alto Networks has discovered a fake Flash updater that has users installing files to sneak a cryptocurrency mining bot, XMRig, into computers.

Just recently, cyber-security researchers at Palo Alto Networks identified a fake Flash updater is installing cryptocurrency mining bot XMRig. There have been 113 fake updates identified installing the crypto mining malware. The attacks have been targeted computers since August and exploiting for mining Monero. Impersonating Flash updates are coming up as pop-up notifications from the official Adobe installer. The fake Flash updates then install unwanted programs like XMRig, but the malware can also update the Flash Player to the latest version. Networks are also a target for the fake Adobe Flash updates. Once XMRig is installed, it looks at all of the computer's resources to mine for Monero and also places a real Flash update on the system in order to prevent the user from suspecting the malware. A fake Flash updater was also found on the internet.

As the crypto mining malware is packaged with Adobe and looks authentic, Pinkerton assesses it is likely more instances of XMRig was installed than what is currently identified. Further XMRig attacks are likely in the medium term. As the malicious actor is using two techniques, it highlights the risk and expansion of cryptojacking. Pinkerton assesses the technique is likely to be used in the long term if it continues to be successful. Pinkerton recommends clients with Adobe ensure they are checking the authenticity of the software and if a warning appears with the update to not install the program.

Cyber-Security Researchers Identify Flaws in WECON Products

A number of vulnerabilities have been found in products from China-based WECON yet the vendor has been slow to release patches.

Cyber-security researchers have identified a "significant number of vulnerabilities" in products manufactured by the Chinese company, WECON. These products include human-machine interfaces, industrial PCs, and programmable logic controllers, used primarily in the energy, water, wastewater, and critical manufacturing industries. According to cyber-security researchers, the vulnerabilities include information disclosure flaws, an out-of-bounds write bug, and a stack-based buffer overflow flaw. The latter two flaws enable malicious actors to conduct code executions. As of the time of writing, WECON is aware of the vulnerabilities but has yet to release patches for any of them.

As the flaws require a malicious actor to get a user to open a file to exploit the vulnerabilities, Pinkerton finds it likely that malicious actors will leverage phishing attacks against clients using WECON devices. Pinkerton assesses that WECON will likely release a patch for the vulnerabilities in the medium term. Pinkerton recommends that clients using WECON devices, particularly those in the identified industries, educate employees about the threat of phishing campaigns. Pinkerton further recommends that clients update the systems with patches as soon as they become available.

Several Organizations Hacked By Russians

The US Department of Justice is reporting seven GRU officers have allegedly hacked into Wi-Fi networks worldwide.

The US Department of Justice (DoJ) reported a cyber-attack by the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU). According to a report published by Info Security Magazine, organizations based on Switzerland, Brazil, and The Netherlands were victims of this hack. According to the DoJ, the perpetrators gained access to the organization's files and credentials of the workers to obtain the information they needed. When they could not get the information, an appointment would be held in the offices of the government or private organization to make the hack via nearby WiFi access. Dutch intelligence officers found this tactic was used during several international investigations involving Russia. Westinghouse Electric Provider, a US Nuclear Power Provider also reported recent attacks to their network facilities.

Pinkerton assesses that this discovery will further incentivize the international community to continue doubting Russia's statements regarding any international matter. Pinkerton recommends clients appoint an expert on the matter to check their whole internal network, to make sure the networks are safe. Pinkerton recommends clients have at least two Wi-Fi networks in the places they receive visitors to avoid providing them access credentials to the main network in the offices.

Cyber-Security Researchers Identify New Android Trojan

Cybercriminals are currently testing a new malware called GPlayed. This trojan provides its operator adaptability to various tasks and shaping up to be a serious threat.

Cyber-security researchers announced the identification of a new, sophisticated Android trojan. Dubbed "GPlayed," the malware, as of the time of writing, appears to target Russian speakers. Malicious actors can extend the functionality of the malware through plugins, bypassing the need to update the package on the device. The malware is further able to migrate code from desktop platforms to mobile devices. Masquerading as the Play Store app, using a similar icon, and calling itself the "Google Play Marketplace," the malware appears similar to a legitimate app. Through permissions, the malware can take control of an infected device; spy on various features including contacts, geolocation, calls, and texts; and steal payment data. The malware also appears capable of functioning as a banking trojan. Once loaded onto an Android device, the malware enables Wi-Fi and registers the device to a command and control server.

Pinkerton finds it likely that malicious actors will expand the scope of targets beyond Russian speakers in the medium term to attack other targets. Pinkerton assesses that the modularity of the malware makes it an attractive tool for malicious actors and renders it difficult to combat. Pinkerton assesses that clients using enterprise Android devices are at the greatest risk from GPlayed, particularly those in Russian speaking areas. Pinkerton recommends that clients using such devices monitor app requests for escalated privileges to mitigate the threat of GPlayed. Pinkerton further recommends that such clients scrutinize apps to ensure the installation of the correct app.

DHS Issues Cyber-Security Warning In Agriculture Industry

The DHS and Threats to Precision Agriculture are warning the agricultural industry of cybersecurity risks by emerging technology that is being adopted in this field.

The U.S. Department of Homeland Security (DHS) issued a report warning of an increased cyber-threat to the agriculture industry. The report cites the increased use of technologies such as Internet-of-Things (IoT) and global position systems (GPS) devices, as well as machine learning in the industry. Without sufficient protections, DHS warns that the industry is at risk of malicious actors and "hacktivism." DHS warned that the industry is at particular risk of spear phishing, malware, and physical access attacks.

Pinkerton assesses that industries closely associated with the agriculture industry, including fertilizer producers, seed companies, trade associations, food processors, and commodity brokers, are also at increased risk of cyber-attacks. Pinkerton finds it likely that hacktivism campaigns and malicious actor attacks against the agriculture industry are likely. Pinkerton finds it likely that any successful attack against the agriculture industry would likely cause significant disruptions to operations, brand reputation, and economic output. Pinkerton recommends that clients involved in the identified industries review policies and procedures and follow industry best practices for securing IoT and other devices.

Regulator Issued Fine To Tesco Bank Over Theft

Britain's Tesco Bank has been fined £16.4 million for failing to act and protect their customers during a 2016 cyber attack.

Recently the UK Financial Conduct Authority (FCA) issued a GBP 16.4 million (USD 21.4 million) fine to Tesco Bank, charging the bank with failing to "exercise [sic] due skill, care and diligence in protecting its personal current account holders against a cyber attack [sic]." The move comes after malicious actors stole GBP 2.26 million (USD 2.94 million) during a 48-hour attack in November 2016. Malicious actors exploited vulnerabilities in Tesco Bank's debit card and deficiencies in its cyber-crime response policies and team. The FCA stated that it has no tolerance for banks that do not provide adequate protection to customers.

Pinkerton finds it likely that the levied fine establishes a precedent for the FCA to levy fines against other financial institutions that suffer major cyber-thefts. Pinkerton finds it likely that the regulator will likely aggressively scrutinize and target other financial institutions in similar circumstances. Pinkerton further finds it likely that such financial institutions will face negative brand reputation. Pinkerton recommends that UK financial institution clients review cyber-crime policies and procedures, as well as conduct regular drills to mitigate the threat of cyber-crime.

Phishing Attach Mimics Microsoft Office 365 - Word

A new phishing attack is using Azure blob storage to impersonate Microsoft by sending out spam emails with PDF attachments that are supposedly from a law firm based in Denver.

Cyber-security researchers have identified that malicious actorsare conducting a new phishing attack involving Office 365. Malicious actors are able to leverage Azure Blob Storage to gain a Microsoft SSL certificate, rendering the phishing attack more believable. Azure Blog Store is a Microsoft storage platform that hosts unstructured data such as texts, images, or video and can be connected to through HTTP and HTTPS. Connecting to it through HTTPS displays an SSL certificate. This method was recently used by unknown malicious actors in a phishing campaign sending out spam emails containing PDF attachments purported to come from a law firm in Denver, Colorado. The attachment contained a malicious link to a form masquerading as an Office 365 utility.

Pinkerton assesses that malicious actors are likely to increase the use of this phishing method as it enables a phishing email to appear more credible. Pinkerton finds it likely that clients utilizing enterprise Office 365 are at the greatest risk of this phishing scheme. Pinkerton recommends that clients who receive suspicious emails report them immediately to the relevant department. Pinkerton further recommends clients conduct education campaigns about suspicious website URLs and other phishing techniques to mitigate the threat.

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