CYBER SECURITY BRIEFING

A Monthly Recap of Technology & Information Risk

PINKERTON®

JUNE 2018

Bank of Chile Affected By Cyber-Attack

On May 28, 2018, the Bank of Chile, the largest bank operating in the country, declared in a public statement that a virus presumably sent from outside of the country affected the bank's operations.

According to the announcement, the virus was discovered by internal IT experts on May 24. It impacted workstations, executives' terminals, and cashier personnel, causing difficulties in office services and telephone banking. After the emergency, the Bank of Chile activated its contingency protocol by disconnecting some workstations and suspending normal operations to avoid the propagation of the virus. Although the virus severely affected the quality of banking services, the institution assured that the security of transactions, as well as client information and money remained safe at all times.

Pinkerton assesses that cyber-attacks targeting financial institutions and international banks form part of a trend that is likely to continue increasing in 2018. So far, Pinkerton Vigilance Network sources had identified Mexico and Chile as the two most impacted by cyber-crimes in Latin America; however, Pinkerton finds that no nation is exempt from becoming a target. Clients are encouraged to review the standard regulations on cyber-security for their banks and its contingency protocols in the event of cyber-attacks. Any unrecognized banking operation or phishing scam should be reported as soon as possible to the Bank of Chile emergency phone line (600) 637 3737. For further information concerning security advise from the Bank of Chile, the following website can be consulted: https://ww3.bancochile.cl/wps/wcm/connect/personas/portal/seguridad/inicio-seguridad#Tab_Acorden_Respon3.

Malware Found Pre-Installed On Thousands of Devices

Per Avast researchers, thousands of Android devices were found to be delivered with pre-installed adware known as "Cosiloon;" it was first found in 2016.

Infected devices have been identified in over 100 countries all over the world and include devices from manufacturers such as ZTE, myPhone, and Archos, most of which are not certified by Google. The adware's main function appears to be to create ad overlays; it is difficult to uninstall as it is part of the firmware. Antivirus applications may be able to remove some of the payloads, but the adware is free to install new ones because of its location on the phone. For the time being, it is unknown how Cosiloon got installed on the devices and who is controlling it. The control server of the adware has not been active since April 2018.

Pinkerton finds that the adware's ability to install payloads on an affected device is a threat to the data integrity of affected devices. Clients are advised to allow personnel to access company data, such as emails and remote access to files, only on devices provided by them. The Cosiloon adware highlights the need for proper evaluation of devices before they are introduced into an operational infrastructure. Clients are advised to refrain from utilizing unknown brands of Android devices even if they offer lower costs of acquisition. A common misconception is that all Android devices utilize the same operating system (OS) and that Google provides the same version to all phone manufacturers. However, low-end devices can use uncertified versions of Android that may also be provided by a third party. This is made possible as the source code of the OS is open source.

New Botnet Raises Concerns of Imminent Cyber-Attack

Per reports on May 23, 2018, technology company Cisco has warned of an imminent cyber-attack through the VPNFilter malware.

Over 500,000 routers across 54 countries, a majority of them in Ukraine, have reportedly been hacked; so far, the malware has affected devices made by Linksys, MikroTik, Netgear, TP-Link, and QNAP. Upon infecting a device, the malware can reportedly intercept data including user and website credentials passing through it; monitor the network for communications over the Modbus SCADA protocol; and, destroy the device software to make it unusable. Per cyber-security experts, the malware is highly likely sanctioned by state-sponsored or state-affiliated threat actors; per report updates on May 24, Russia has been named in the investigation.

In the immediate to near term, Pinkerton finds that the VPNFilter malware poses a threat to businesses and personnel worldwide, especially in Ukraine. Apart from affecting business and personal technology devices, Pinkerton finds that the malware poses a credible threat to the continuity of critical infrastructure systems given its capability to completely disable them. Further, given the precedent of Russia-linked cyber-attacks targeting Ukraine, Pinkerton assesses an even chance that hackers will launch the cyber-attack in the run-up to a public event or public holiday. In this regard, Pinkerton notes that the UEFA Champions League Final will be held in Kiev on May 26 and Ukraine's Constitution Day will be celebrated on June 28. The NotPetya ransomware that caused large-scale disruptions worldwide, especially in Ukraine, by erasing data from the computers of banks, energy firms, and senior government officials was launched on the eve of the Ukraine Constitution Day in 2017. In the immediate term, businesses are recommended to make backups of confidential information, install the latest security patches, and use up-to-date anti-virus software to mitigate the risk of an attack.

New Processor Vulnerability Threatens User Data

On May 21, 2018, researchers from Microsoft and Google's Project Zero discovered a new vulnerability in Intel, ARM, and AMD processors.

The vulnerability named Speculative Store Bypass Variant 4 is similar to Meltdown and Spectre processor bugs; if exploited, it grants the attacker access to local memory and web-separated programs such as JavaScript. Intel Processor Developer stated that they have not found evidence of hackers already exploiting this vulnerability and that the patches will likely reduce the processor's performance by 2-8%.

Pinkerton assesses that the flaw will have a lesser impact than the previous processor bugs since browsers and new processors have been protected against vulnerability types such as Meltdown and Spectre. Both Microsoft and Google are working on the necessary updates alongside the processor developers, but replacing old devices will be a better solution due to difficulties in the updates distribution channels. Pinkerton recommends all clients to download the updates and patches needed to avoid the three vulnerabilities mentioned above and to monitor any new announcements on the matter.

Misconfigured Server Allows For Vehicle Takeover

On May 18, 2018, security researchers Vangelis Stykas and George Lavandis discovered a CalAmp server misconfiguration while conducting research on the Viper SmartStart system.

The misconfiguration allowed the use of an old password to reset the current password and take control of both user accounts and remote vehicle systems provided by CalAmp. In addition to the user-facing issues, the misconfiguration also allowed the ability to tamper with all Internet of things (IoT) devices connected to the CalAmp database and obtaining a list of users and location reports from the database. The researchers notified CalAmp in early May, and CalAmp has reported resolving the issue within ten days of notification.

While CalAmp has already addressed and corrected the server misconfiguration, users of CalAmp products are still at risk due to the unauthorized access to user and location data. Pinkerton assesses that while the ability to change passwords is at most a nuisance requiring an additional password reset, the information on users and locations, if made available for sale, is likely to lead to an increase in vehicle thefts among vehicles equipped with CalAmp devices, as it allows thieves to establish patterns of life and best determine when and where a vehicle will be left unattended for a long period of time. Pinkerton advises clients utilizing CalAmp products to ensure passwords are changed out of an abundance of caution, as well as increased monitoring of vehicles in the near term to aid in loss prevention.

Phone Tracking Company Securus Hacked, User Information Compromised

On May 16, 2018, cyber-security researchers at Motherboard revealed that Securus, a company known for allowing law enforcement customers to live track any phone in the U.S., has been hacked.

As evidence of the hack, Motherboard was given several internal company files including a spreadsheet marked “police” that includes 2,800 usernames, hashed passwords, email addresses, and security questions. The hashed passwords used the MD5 algorithm which is easily cracked. The Securus website claims to allow customers to track mobile devices with GPS disabled and determine call origin and termination geo-location data. Securus was previously hacked in 2015.

As Securus gets increased media attention, wireless carriers that sell customer phone data to Securus and the Securus customers exposed by the hack are likely to be impacted by negative brand reputation. Additionally, wireless carriers working with Securus to supply location data without a warrant may be acting unlawfully, and Senator Ron Wyden has asked the Federal Communications Commission to investigate the carriers involved. Aside from the impact to wireless carriers, malicious actors could potentially access phone locations tracked by Securus using the exposed data. Pinkerton recommends customers that store sensitive, personally identifiable information ensure that the information is properly secured and regular penetration testing is performed to ensure the security of company data.

Critical Flaws Affect Cisco’s Products

Per media reports on May 17, 2018, three critical flaws have been detected in the Cisco Digital Network Architecture (DNA) Center, an open, software-driven platform that integrates innovations in networking software.

Each of the vulnerabilities allows hackers to compromise the entirety of the DNA Center. CVE-2018-0222 relates to undocumented static credentials for the default admin account; CVE-2018-0271 enables a remote attack and allows hackers to bypass authentication and obtain privileged access to critical services on the platform; and, exploiting CVE-2018-0268 also permits attackers to bypass authentication. Cisco has issued patches for all three bugs.

Pinkerton finds that continuing to use the outdated version of the DNA Center will expose users to cyber-attacks over the immediate to near term. Clients who use the affected platform are recommended to update it to the latest version. Exploitation of the reported flaws is likely to cause severe disruptions on the operating system, leading to financial losses and data breaches.

Critical Vulnerabilities Reported In Popular Email Encryption Tools

Per media reports on May 14, 2018, users of the Pretty Good Privacy (PGP) and Secure/Multipurpose Internet Mail Extensions (S/MIME) have been warned of critical vulnerabilities.

The detected flaws reportedly allow hackers to decrypt sent or received messages that later can be read as plain text. PGP and S/MIME are widely used technology tools to encrypt emails and other data communication.

Pinkerton assesses that the threat from the PGP and S/MIME vulnerabilities is likely to increase in the immediate to near term. Following the public release about the flaws, there is an even chance that hackers will intensify cyber-attacks over the immediate term. While the extent of disruptions caused by exposure of the information is subjective, Pinkerton finds that the information can broadly be used for financial extortions and private data theft. Pinkerton recommends clients who use the affected tools to uninstall PGP and S/MIME applications until the programs receive official patches.

Amazon Builds Digital Health Team Within Alexa

On May 10, 2018, CNBC reported that, according to an internal document the news organization had obtained, Amazon was building a digital health and wellness team that would function within the company’s Alexa platform.

Although Amazon has been making other strides in recent years to establish a presence in the healthcare industry, the purported Alexa-centered team would signify the company’s fledgling attempt at becoming a digital health provider. Planned services rumored to be offered by the Alexa health group include diabetes management, new mother and infant care, and assistance with age-related issues. Following CNBC’s announcement, spokespersons for Amazon were not willing to comment on the validity of the report.

If the content of CNBC's report is accurate, Amazon is joining companies like Google and Apple in a race to become the foremost digital healthcare provider as the field becomes more pervasive. Digital healthcare, which is expected by industry experts to explode in the next few years, promises to provide consumers with an experience that is more convenient, less expensive, and more comprehensive than services rendered in traditional brick-and-mortar medical offices. While all of those factors appear to create the impression that digital health services are a nearly-utopian panacea for the difficulties currently plaguing the healthcare industry, other factors create a significant barrier to the widespread implementation of such services. Without discussing the numerous practical issues that would preclude the virtual administration of many medical tests and treatments, the single biggest obstacle is privacy since Alexa's "patients" would be sharing sensitive health data. In addition to the privacy concerns presented by any web-connected device, there are myriad regulations and compliance issues concerning protected healthcare information (PHI), as defined by the Health Insurance Portability and Accountability Act (HIPAA), which must be addressed scrupulously by Amazon before the services believed to eventually be offered by Alexa can become viable.

Google Bans Advertisements Ahead of Abortion Referendum

On May 9, 2018, Google announced that from May 10 it would ban all advertisements related to the May 25 Irish abortion referendum amid concerns about "election integrity."

The ban would apply to advertisements on Google and YouTube and follows a similar ban by Facebook that prohibits posts from outside Ireland that could likely influence the referendum. Pinkerton notes that the referendum is targeted at repealing the constitutional amendment outlawing abortion, a matter that has lead to large-scale civil unrest in the country in the recent past. Following Google's announcement, several anti-abortion activist groups have accused the company of attempting to "rig" the election in favor of the pro-abortion side.

Pinkerton finds that the unprecedented move to limit online activity portends stringent regulations on Internet-based advertising in the medium to long term; similar bans and advertisement transparency initiatives on social media platforms, especially regarding political and sensitive social issues, are highly likely. In this regard, clients who use online platforms as a primary means of business activity are recommended to seek counsel as disruptions to their operations such as digital marketing are likely.

Pinkerton finds that the limitation of online activity related to the anti-abortion referendum underscores the threat of targeted fake advertisements and bots aimed at influencing individuals' perceptions. Further, Pinkerton finds that the ban is a strategic move by the companies to secure their brand reputation given the ongoing scandals on data privacy and security. In the event that the referendum is passed, Pinkerton finds that large-scale protests by anti-abortion activist groups, specifically targeted toward Google and Facebook, are highly likely.

Spam Calls Target Politicians On Voting Day

On May 9, 2018, as voting began in Malaysia's general elections, there were reports that members of both the opposition coalition, Pakatan Harapan, and the ruling party, Barisan Nasional, were receiving incessant spam calls on their mobile phones.

The Malaysian Communications and Multimedia Commission said that as per preliminary investigations, the cause of the spam calls seems to be an anonymous bot (automated account) attack originating from various sources and targeting several people and organizations. The agency received "numerous complaints today of phones ringing and then the call drops," which could pose a threat to the telecommunications network and result in a "security risk."

Pinkerton finds that politically motivated cyber-attacks to influence and, at times, disrupt elections have characterized the ongoing elections in Malaysia. In April, there were reports that bots were flooding Twitter with pro-government and anti-opposition messages; however, in the latest incident, the targeting is indiscriminate and affected both the opposition and the ruling party. Pinkerton recommends clients refrain from answering calls from unknown international numbers, especially from the U.S., to ensure device safety, and use reliable applications for caller identification in the immediate to near term. Further, given the systemic technology threat to telecommunications systems, clients are recommended to review contingency protocols for communications in the event of disruptions.

ZooPark Malware Steals Data From Android Devices

On May 5, 2018, Kaspersky Lab discovered a cyber-spying campaign that targets Android users.

Cyber-security researchers stated there are four versions of the malware, known as ZooPark. The malware uses Telegram, a chat app, as well as infecting websites using "watering holes" as the preferred attack vector. The most recent version of ZooPark exfiltrates data including contact information, keylogs, call audio, GPS location, text messages, and other data from an Android device. The malware can also capture images, screenshots, and record audio or video conversations. Many news websites have been identified as infected with ZooPark and the malware redirects visitors to download a link that infects a device. ZooPark does not just scan a system's memory, but also data stored on the SD card, obtaining information on installed applications, browser data, and clipboard data.

Pinkerton assesses that clients with Android devices using the Telegram app are likely more vulnerable to infection of ZooPark. It is likely that malicious actors are using Telegram to continue the spread of the malware and will likely to continue doing so. As each version of ZooPark has become more advanced than the previous version, it is likely to be further developed in the long-term. As mobile devices continue to be used more as a primary tool, malicious actors will highly likely continue to target mobile users to obtain information. Pinkerton recommends clients review procedures for downloading apps on work phones as well as ensuring apps are from a safe and secure source. Pinkerton also advises clients against using Telegram.

Trojan Malware Spread Through False Official Immigration E-Mail

The Colombian National Police and the Center for Cyber Security reported the propagation of malware through an allegedly official e-mail from the Department of Immigration of the Ministry of Foreign Affairs.

According to the authorities, Colombian citizens received the message that they have a pending process and they will not be allowed to leave the country until further notice. The message comes from the following address notifications@migracioncolombia.gov.co, and it includes an attachment with a compressed file in which supposedly more details are included. The cyber-security firm Eset confirmed that the attachment is a variation of the VBA/TrojanDownloader needed to spread the malware and obtain access to the computer equipment.

Pinkerton assesses that malware spreading through apocryphal official virtual messages represent a high threat to cyber-security as users are more likely to fall victim of this kind of scam due to the apparent official character of the message. Clients are advised to verify any electronic correspondence with the institutions or authorities, as soon as they received a suspicious message. Businesses are urged to inform their employees and IT departments to make them aware of the virtual scam. Colombian enterprises are encouraged to register in the Police Cyber Center portal (https://caivirtual.policia.gov.co/user/register) to report any anomalies or cyber threats and prevent further attacks.

Money Transfer Delays Expected After Banking Cyber-Attack

In recent days, cyber-attackers have tried to penetrate Mexico's electronic payment system.

The situation has forced at least three banks to execute contingency plans after suffering several incidents. It has been reported that those attacks were experienced after operating the SPEI, the country's inter-bank electronic transfer system. According to the country's central bank, Banco de Mexico, neither the SPEI infrastructure nor clients money have been affected. This attack comes less than four months after cyber criminals tried to steal money from Bancomext, Mexico's government-run export bank; which caused the bank to suspend its operations in the international payment platform. So far, it is believed that no government banks were targeted in the latest incident.

Pinkerton assesses that cyber-attacks targeting banks will highly likely continue to happen with more frequency locally and internationally. Pinkerton recommends clients to expect money transfer delays in the immediate future given that as part of the banks' contingency plans, operations with SPEI will be connected to the central bank's network. Experts claim that regulators should be aware of these cyber-attacks and the increasing possibility that the crimes could include systemic assaults on financial systems. It is recommended to immediately contact the authorities if becoming a victim of a cyber-attack. Additionally, Pinkerton advises all clients, and especially those in the banking industry, to tighten their security systems and increase their surveillance on these types of assaults.

Changes In Tactics Of Chinese Cyber-Spies

In a report issued by 401TRG at the cyber-security firm ProtectWise on May 3, 2018, the researchers warn about major changes in the tactics of Chinese cyber-spies.

They have observed a growing tendency of hackers focusing on IT staffers, and relying more on spear-phishing method instead of malware. Moreover, they intensify their attempts of gathering code signing certificates from hacked software companies that can be used for future supply-chain attacks. Reportedly, several separate cyber-espionage groups adopted the same methods of advanced persistent threat (ATP). Previously known threats such as BARIUM, Wicked Panda, GREF, and PassCV have been updated and now appear to have similar techniques and infrastructure as the Winnti gang.

Pinkerton assesses that the risk of hacking code signing certificates, source code, and internal technology documentation stored at cloud servers is likely to increase in the medium to long term. Potential target companies operate in Asian countries where the risk of Chinese cyber-espionage is the highest; however, the geographical distances do not limit their interests. The Winnti gang is known for targeting gaming companies in Southeast Asia and most of their activity is financially-motivated. Pinkerton recommends vigilance for all cloud servers providers and users to mitigate the potential fraud risk.

GravityRAT Malware Evades Detection, Launches Targeted Attacks

Per reports on May 1, 2018, a new updated version of the GravityRAT malware evades detection by checking the current central processing unit (CPU) temperature.

Cyber-security researchers at Cisco Talos have been monitoring the GravityRAT malware for nearly eight months and believe that it likely originates from Pakistan. The Trojan lures the target and subsequently launches a targeted attack on users in India. According to cyber-security researchers, the Trojan is equipped with anti-virtual machines (VM) techniques, remote command execution, and file exfiltration. The infection spreads once the user is lured into downloading a Word.docx email attachment that enables macros and asks the target to prove that the user is not a robot.

Pinkerton assesses that the GravityRAT malware is likely to target businesses and government organizations in India in the near to medium term. Businesses are likely to be adversely affected as the Trojan can extract temperatures apart from identifying clock speed, processor name, ID, and manufacturer information. Client personnel are advised to refrain from opening files bearing the extension.ppt, .docx, .pptx, .xlsx, .xlx, .PDF, and .RTF as the user data of the targeted system may be stolen. Businesses are advised to use a secure internet gateway (SIG) such as “Umbrella” to block users from connecting to malicious IPs, URLs, and domains.

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.

Hazard & Event Risk
Operational & Physical Risk
Technology & Informational Risk
Market & Economic Risk

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

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.

Hazard & Event Risk
Operational & Physical Risk
Technology & Informational Risk
Market & Economic Risk

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