CYBER SECURITY BRIEFING

A Monthly Recap of Technology & Information Risk

PINKERTON®

SEPTEMBER 2019

Cyber-security Enterprise, Imperva, Revealed Data Breach

Breach exposed WAF customer data, including SSL certificates and API keys.

It has been reported that Imperva, a cyber-security startup that protects business apps and critical data from cyberattacks, suffered a data breach. The security breach exposed email addresses, encrypted passwords, API keys, and SSL certificates of an unspecified subset of users of Incapsula –Imperva's Cloud Web Application Firewall (WAF)–. On August 20, 2019, an anonymous third party alerted Imperva about the data breach of its customers registered since September 15, 2017. Imperva is still investigating how and when the leak happened, also if other third parties had accessed to the exposed information. It is unclear from the company's statement whether its servers were compromised or misconfigured. For the moment, the cybersecurity enterprise has reinforced its security measures, such as 90-days password expiration policy by forced password resets; and issued several recommendations to its clients, like, implementing Single Sign-On (SSO), enabling two-factor authentication (2FA), resetting their API keys, and generating and uploading a new SSL certificate.

Since Incapsula detects malicious activity in the web traffic and blocks them, it is highly likely that actors in possession of the exposed data, could intercept the web traffic of a client and divert them to a site owned by the attacker. This practice could be used to insert a bug and hack or affect users' devices. Pinkerton assesses cyber-attackers are likely to increasingly seek to exploit the data exposure now that it has been publicized. Pinkerton recommends all Cloud WAF clients to follow the security measures that Imperva has issued, such as changing their account password, reset their API keys, implement Single Sign-On, enable 2FA and to generate a new SSL certificate. Pinkerton advises all clients to exercise precaution while using the internet and avoiding opening unknown websites. Pinkerton recommends all clients to block the popup windows, and only allow those of official pages.

New Hacking Group Targets Energy Sector Companies

A new hacking group has been targeting the local energy sector in the Middle East.

Security researchers discovered there is a new Advanced Persistent Threat (APT) group called New Lyceum or Hexane, which tends to target the companies related with the energy sector. The hacking group has been active since April 2018, and its attacks have focused on oil and gas companies as well as telecoms in the Middles East, Africa, and Asia, with Kuwait being recognized as its main target. The cyber-security firm Secureworks released a report in which it remarks that there was a spike in Lyceum's attacks during May 2019. Secureworks also explained how the group carries out its attacks. First, Lyceum members use techniques to breach a target organization individual's email account. Once they own the individuals' compromised email accounts, they send spear-phishing emails to their colleagues which contain malicious Excel files that aim to infect other members of the organization, including executives, HR staff, and IT personnel, with a malware. The malicious Excel file contains a payload named DanDrop, a programming language called Visual Basic for Applications (VBA) macro script used in Office programs. The VBA infects the user with the remote access trojan (RAT) DanBot, and then hackers download and execute additional malware on the victim's system. Security researches consider this modus operandi is similar to the one used by Iranian hacking groups but have refrained from linking Lyceum with a specific country's cyber-espionage apparatus.

Pinkerton assesses that Lyceum APT attacks are likely to continue while the group's origin or location remains unknown, and security researchers and international IT teams are not able to prevent the execution of its campaigns. Moreover, security researchers believe that the hacking group could

seek to access operational technology (OT) environments and infrastructure companies, thus expanding its scope of targets. Pinkerton finds it likely that energy-related companies in the regions mentioned above are likely to become increasingly vulnerable to hacking attacks in the medium term. Pinkerton advises clients not to open emails from unknown senders and avoid clicking on suspicious Excel attachments as their email account, as computer system could become compromised. Additionally, Pinkerton recommends clients report suspected phishing attempts to their employer's IT department.

North Korean Hacking Group Targets Retired South Korean Officials

State-sponsored group goes after South Korean diplomats, government, and military officials.

Allegedly a North Korean state-sponsored cyber-espionage group called Kimsuky or Velvet Chollima targeted retired diplomats and military officials from South Korea for the first time. According to IssueMakersLab, a Seoul based cyber-security firm, the attacks targeting officials' Gmail and Naver email accounts took place between mid-July and mid-August. The hackers used spear-phishing attempts where once the victim accessed the email it redirected the user to fake login pages and attackers could log the victim's account credentials. Security researchers consider that retired officials are more vulnerable to attacks as, unlike officials who are still in office, they are not provided with improved cyber-security protections and security alerts about attacks. Additionally, as they continue to maintain ties with incumbent government officials and are engaged in government advisory activities, they have become attractive targets to hackers to gather information and launch attacks against officials who remain in office. Kimsuky was first discovered by Kaspersky and has been active since 2011. The group's primary targets have been various South Korean government activities, nuclear power plants, and military operations. In recent years, the group has expanded its operations to foreign targets including academic institutions, foreign affair ministries, and U.S. think tanks.

Pinkerton assesses that the Kimsuky attacks are likely to continue as security issues remain of great importance to North Korea. Moreover, security researchers and international IT teams are not able to prevent the execution of its campaigns as it has been expanding its operations to other parts of the world outside the Korean Peninsula and it uses new malware in its attacks. In February 2019, Palo Alto Networks Unit 42 researchers detected spear-phishing emails sent in November 2018 which contained a malicious Excel macro document which, when executed, led to a new Microsoft Visual Basic (VB) script-based malware called "BabyShark." The emails appeared to be sent by a nuclear security expert who apparently worked as a consultant for the United States. Pinkerton find it likely that the hacking group could seek to access new foreign targets' systems, especially from the U.S., which are involved in security issues related to North Korea, thus expanding its scope of targets. Pinkerton advises clients not to open emails from unknown senders and avoid clicking on suspicious Excel attachments as their email account and computer system could become compromised. Additionally, Pinkerton recommends clients report suspected phishing attempts to their employer's IT department.

Latest iPhone Update Reintroduces Jailbreak Flaw

iOS 12.4 Apple update has accidentally reopened a security flaw making iPhones vulnerable to hackers.

Cyber-security researchers have found that iOS 12.4, the latest version of the iPhone operating system, reintroduced a bug that facilitates jailbreaking updated iPhones and hacking iPhone users. Jailbreaking allows overriding the security restrictions of Apple, making it possible to install apps and other software not authorized by Apple, making it easier to hack. Due to the error, the security barriers are much lower; therefore, a bug in a malicious webpage or app could escape the iOS sandbox —a mechanism that prevents apps from reaching data of other apps or the system— and steal data from the user. The iOS 12.4 was released in June, and it is the only currently available version of the iOS. According to Jonathan Levin, a security researcher, and iOS specialist, not only the iOS 12.4 iPhones are vulnerable, but also the 11.x and 12.x operation systems. Only iOS 12.3 does not have this error. It is expected that Apple, will issue a new version, the 12.4.1, in the near term to patch the flaw.

Pinkerton assesses that it is highly likely that many iPhones will are currently affected by the jailbreak flaw and therefore vulnerable to hacking attempts. The bug implies a severe security risk for iPhone users, Pinkerton recommends all clients with the 11.x, 12.x, and 12.4 iOS not to voluntary jailbreak their iPhone. Otherwise their iPhone will no longer be protected by the iOS safeguards. Pinkerton advises all clients to exercise caution while browsing the internet or downloading apps. Since the jailbreak is public and free, it is likely that many apps in the could have a copy of the jailbreak in it to hack the users. If it is required to download an app, Pinkerton recommends checking the date, developer, ratings and privacy policies; especially if it is a free app and to not download apps from the web. Usually when the year is very recent, and the developer has no more applications or more information, it is likely a malicious app. Pinkerton advises all clients to verify the links they receive by email, text messages, or social media because from a link the iPhone could be jailbroken and likely hacked. Therefore, it is recommended to open the accounts from official pages or official apps. For the clients that have not yet updated their iPhone, Pinkerton advises not update it, until Apple releases a patch to the flaw. Pinkerton recommends disabling the automatic software update and installing it manually after it has been verified.

Ransomware Attack Affects 23 Texas Government Agencies

Texas cyberattack was able to take a number of government agencies offline.

The Texas Department of Information Resources (DIR) declared it is the victim of a cyber-attack that has been ongoing since August 16. At the time of writing, around 23 government agencies had been affected and taken offline, as email accounts were disabled, and online payments to city departments were prevented. However, the State of Texas networks and systems have not been impacted. Different Texas' institutions, the Department of Homeland Security and the FBI, suspect only one threat actor is responsible for the detected ransomware attack, which primarily disabled local government computers and systems. Further, the ransomware was identified as Nemucod, which "encrypts files and then adds the .JSE" file virus. Nemucod, unlike most ransomware, does not leave a ransom note behind, thus confusing victims. Authorities in Texas have reached out to cyber-security experts, and military and counter-terrorism units, to recover their systems and put them back online. Experts are concerned that these kinds of attacks can cause the disruption of services over localized areas. Moreover, experts state that ransom payments leave cities and organizations vulnerable to more attacks as they are likely to be added to a list "on the dark web" of organizations which pay ransoms.

Pinkerton assesses that ransomware attacks on government departments and organizations are likely to increase as hackers find them easy targets. As governments usually deal with several individuals and businesses, some of them being one-time contacts, attackers are likely to camouflage or remain unknown and out of the government's registration systems. Moreover, as government agencies maintain information on a large number of people, many clients' data could likely be at risk. Since 2017, U.S. government and state actors have become primary targets for ransomware attacks. Experts reveal that the U.S. is the country that suffers from more ransomware attacks, accounting for almost 53% of the global cases. In May 2019, hackers used ransomware to take control of thousands of government computers in Baltimore. Further, in July 2019, Louisiana Governor declared a state of emergency after schools' computer systems from multiple districts suffered a ransomware attack. As it has been shown that several of these government organizations deal with a wide variety of individuals, security controls to monitor and detect cyber-attacks on their network are likely to increase in the medium term.

Portal Of The European Central Bank Hacked

BIRD portal shut down by European Central Bank after malware attack.

The European Central Bank (ECB) has reported that a cyber-attack affected their system. A statement published by the ECB disclosed that unauthorized parties introduced malware into the Bank's Integrated Reporting Dictionary (BIRD) website which was held by a third-party provider. The ECB considers that the contact information of around 481 newsletter subscribers was stolen, including phone numbers, and emails addresses. The bank was forced to close the website and indicated that they had informed the European Data Protection Supervisor about the attack to advise the people whose data was likely compromised. BIRD is an initiative launched by the European Union aimed to provide banks with information and data for analysis and reporting purposes. The ECB has suffered several cyber-attacks in the past. Moreover, the BIRD' site was recently impacted by a cyber-attack in December 2018.

Pinkerton assesses that attacks against financial, governmental, and private agencies will likely continue in the medium to long term as the attacks conducted by hackers have been sophisticated. Pinkerton finds it likely that the technology developed by hackers is evolving faster than the protection hardware and programs implemented by entities since the attacks against banks have increased considerably in the recent time. Pinkerton finds it likely the investment in stronger security information technology systems will likely increase among financial entities in the medium term. Pinkerton recommends all newsletters subscribers of the BIRD site, or other ECB related portals to verify their exposure to determine if any of their data has been compromised. Pinkerton advises its clients to deploy security protocols that avoid the indiscriminate use of their data.

Cloud Atlas Hacking Group Continues Its Cyber-Espionage Activities

Cyberspies use polymorphic malware to target government, diplomatic, and research organizations.

Cloud Atlas, a suspected Russian advanced persistent threat (APT) group, also known as Inception, continues to execute cyber-espionage operations on governments and organizations. Additionally, the hacking group now uses new polymorphic malware, meaning their code continually changes to avoid detection. It was initially discovered by Kaspersky in 2014, targeting users from Russia, Kazakhstan, Belarus, India, and the Czech Republic. In 2018 and 2019, Symantec reported there were also victims from Ukraine, Moldova, Belgium, Iran, France, the U.S., Turkey, Georgia, Bulgaria, Kyrgyzstan, Turkmenistan, Romania, and Portugal. Still, the main target seems to be Russia, where hackers not only attack government organizations, but also international and religious organizations, and the aerospace industry.

Cloud Atlas' first step is to send a phishing email to a high-value target. The email includes a Microsoft Office document that executes a malicious payload if downloaded. In 2018, it was revealed the APT group used a new piece of malware called PowerShower, a document stealer, which works on PowerShell and VBS modules executed on a compromised computer, allowing the group to steal documents and passwords, and spy on active processes. Kaspersky announced Cloud Atlas has been using a new piece of malware called VBShower, which erases evidence of the infection and reaches the command and control server, since April 2019. In the recent attacks, once the device has been infected, a malicious HTML app is downloaded and executed, and after collecting some information, the VBShower starts working. The attacker can then instruct VBShower to download PowerShower, LaZagne, or other tools used by the APT group. Kaspersky remarked that both VBShower and the HTML app are polymorphic. Thus, it is more difficult to track the attacks as security solutions typically rely on indicators of compromise (IoC).

Pinkerton assesses that Cloud Atlas cyber-attacks are likely to continue in the medium to long term as preemptive measures have not been developed due the way attacks are executed, sometimes victimizing unsuspecting users while injecting the malicious HTML app into devices.
As Cloud Atlas malware reportedly supports espionage activities, it is highly likely that both government and business employees' computers and mobile devices likely are at risk. Moreover, as government and economic entities usually maintain information on a large number of people, many clients' data could likely be at risk. Due to the characteristics of the malware, Pinkerton recommends high profile clients located in Russia and the countries listed above to monitor and ensure the security of their network as well as to change their passwords regularly.

Former Amazon Employee Steals Massive Data From Capital

Woman accused of Capital One hack, had stolen data from an additional 30 companies.

Recently, the Seattle's Justice Department declared a 33-year-old woman called Paige Thompson was guilty of stealing massive data from Capital One Financial Corporation and around 30 companies and other entities which have not been named. She is a former Amazon software engineer. At the time of writing, authorities believe the suspect did not sell or share any of the data or profited from it, as they have found she only created one copy of the stolen data. However, the data compromised of names, phone numbers, addresses, Social Security numbers, and bank account numbers. Reportedly, Thompson had a long history of threatening behavior, including threats to kill people and to kill herself, and "appears to have significant mental-health issues." Thompson was discovered as she started to post some of the stolen data on GitHub, an online community used by web developers to share programming code, and information on her Twitter account and in a group chat on Slack, a messaging platform. In a Twitter post, she threatened to kill the police officers as well as the person who called them. Authorities say the suspect will have an additional charge based upon each theft of data.

Pinkerton assesses that hacking cyber-attacks targeting banks and agencies that collect data of millions of people, especially financial information, are likely to continue in the long term as they own relevant confidential information which is highly attractive to hackers. In 2017, Equifax, a consumer credit reporting agency, reported it suffered a data breach which affected approximately 147 million people as their personal information was compromised. Moreover, as it has been shown that several of these financial agencies do not own security controls to monitor and detect cyber-attacks on its network, many clients' data could likely be at risk as it is highly likely that hackers take advantage of remaining security breaches.

Hackers Targeting North American Hotel Employees With Malspam

Malspam targeted the financial staff of multiple entities from the North American hotel industry.

Security researchers from Qihoo 360 Security Center discovered there was a malware spam (malspam) campaign targeting the financial staff of various entities from the North American hotel industry. The malspam, a type of spam email used to deliver malware payloads via malicious URLs or infected attachments, was mainly sent to hotel employees. The attackers sent spam emails which contained an attachment disguised as an invoice detailing unpaid sums of considerable amounts in the form of bills with more information on the services and goods that had not been paid. Once the victims clicked on the attachment, it dropped the NetWiredRC Remote Access Trojan (RAT), which enabled the attacker to gain unauthorized access and remotely control their victims' devices without them noticing. The RAT was dropped with the help of PowerShell script, and then it added itself to the computer's startup folder. Once there, the attackers could execute extra malware payloads, upload files, start new processes, take screenshots, steal credentials, and collect and exfiltrate system and user information, among other actions. Additionally, login credentials could be stolen if they were saved within mail clients, like Outlook, and web browsers, such as Comodo Dragon, Mozilla Firefox, Google Chrome, Chromium, and Opera browsers.

Pinkerton finds it likely that security breaches and cyber-attacks continue to affect the hotel industry in the medium to long term as most of the hotels do not work on preemptive measures and employees do not notice their computers have been infected. Moreover, as hotels usually maintain information on a large number of people, and cyber-attacks typically aim to steal information of hotel customers, many clients' data could likely be at risk. In 2018, several hotel related cyber-attacks were reported in different parts of the world. In June, a hacker was able to breach the systems of FastBooking, a Paris-based company that provides hotel booking software to thousands of hotels worldwide. The attacker stole payment card and personal information of people who booked their hotel reservations at the site. Additionally, in August, almost 130 million guests of Huazhu Hotel Group Ltd, one of the leading hotel chains in China, had their personal information sold on a Chinese Dark Web Forum. Therefore, Pinkerton recommends clients verify there is no unrecognized payment activity and change their passwords when booking through hotel websites as their information is likely to be compromised.

Iranian Hackers Accused Of Cyber-Attacks Against Critical Infrastructure

Suspected Iranian cyber offensives and intrusions may mean Tehran is stepping up its cyber attacks.

It is believed that Iranian hackers accessed Bahrain's government computers within the last month. The latest intrusion reportedly took place on August 5, when hackers infiltrated in the systems of Bahrain's National Security Agency, the Ministry of Interior, and the first deputy prime minister's office. On July 25, the Electricity and Water Authority's systems were shut down due to a cyber-intrusion. Around the same time, Aluminum Bahrain, a major smelter, was targeted in a cyber-attack attributed to Iranian cyber-attackers. The Persian Gulf country hosts the U.S. Navy's Fifth Fleet and U.S. Navy Central Command, and it is an ally of Saudi Arabia. Moreover, Bahrain has accused Iran of meddling in its affairs. Neighbor countries believe Tehran has increased the number and severity of cyber-attacks against regional Gulf adversaries since June when tensions started to rise in the region and toward the U.S. Iran maintains it is not responsible for the cyber-attacks against neighboring countries.

Pinkerton assesses that cyber-attacks against U.S. allies in the Gulf region are likely to continue to target critical infrastructure and government entities throughout the long term as Iran attempts to demonstrate dominance in the cyber-security sector. In 2012, a cyber-attack affected Qatar's natural gas firm RasGas, leaving it without service, and another cyber intrusion deleted data from Saudi Arabia's national oil company's system. In these two events, Iranian hackers were also accused of using a virus called Shamoon. As major companies provide services to a large number of people, supply chains and clients could likely be affected by service disruptions caused by attacks against these enterprises. Pinkerton recommends clients to monitor the news, and statements of companies and national agencies related to their interests for up to date information on cyber-attacks that could affect them. Further, Pinkerton advises clients to monitor and ensure the security of their network.

North Korean Cyber-attacks Generated USD 2 Billion To Date

To fund a weapons program in North Korea, Pyongyang generated $2 billion using cyberattacks.

Reuters disclosed the findings of a report prepared for the United Nations Security Council Sanctions Committee on the history of large-scale cyber-attacks conducted by North Korea. According to experts, North Korea facilitated the illegal transfer of funds from financial institutions, made cryptocurrency exchanges, created income to avoid international sanctions, and laundered stolen proceeds. Investigators estimate that the total amount that North Korea has generated is USD 2 billion (KPW 1.8 trillion). Experts noted that these attacks were likely aimed to generate income to enhance the country's weapons programs. The experts said that at least 35 North Korean actors are under investigation for cyber-attacks in 17 countries. Experts believe that several hackers operate under the direction of the Reconnaissance General Bureau, which is a top military intelligence agency of North Korea.

Pinkerton finds it likely that North Korea will continue conducting cyber-attacks to generate income in the long term as numerous hackers linked with the government have developed sophisticated cyber capabilities which are hard to trace. Moreover, North Korea has been banned from trading commodities such as iron, coal, lead, and seafood since 2017, so it is likely that the country is looking for other ways to obtain funds to enhance its national interests. Pinkerton considers that the U.S. talks with Pyongyang are likely to tense in the short term as this report was released shortly after North Korea carried out its fourth short-range missiles test in the last two weeks. Pinkerton assesses that numerous financial institutions, banks, and cryptocurrency users around the world are at risk of being victims of cyber-attacks generated by North Korean state actors. Pinkerton advises all clients to strengthen their banking security systems and to be attentive to identify any suspicious activity and unidentified movements in their bank accounts.

Over 960 E-Commerce Stores Compromised In Magecart Cyber-Attack

Malware strains are attacking enterprise companies in both Europe and US.

Accenture iDefense cyber-security experts warned that malicious actors are using a new version of the MegaCortex ransomware with more damaging capabilities to target corporations in Europe and the United States. Like any other ransomware, MegaCortex finds lists of drives with corporate data in the infected network and encrypts them. Malicious actors using MegaCortex are asking BTC 2-600 (USD 23,576.07 million) to send the key and restore the affected files. The first version of MegaCortex required manual procedures to execute the malware and used a custom password to install the malware. The new version has an automated execution and a hard-coded password, which allows attackers to render global campaigns. Moreover, the ransomware is capable of automatically scanning the network and terminate anti-malware software to avoid detection.

Pinkerton finds it highly likely that the MegaCortex ransomware will spread to other countries due to its new features. Moreover, the ransom message states that malicious actors "are working for profit" and disregard if the infected network belongs to a small or mid-size enterprise. Thus, the MegaCortex developers likely will share the malware to third parties or initiate a phishing campaign to infect computers worldwide and maximize their gains. Pinkerton recommends training the clients' personnel to avoid suspicious websites or clicking phishing e-mails as this ransomware likely distributes through Trojan downloaders. Clients are advised to ensure that anti-malware software is fully operational and updated to detect and terminate potential threats promptly. Cyber-security experts recommend using the YARA rules to monitor and detect MegaCortex; more information about the specific artifacts linked to the malware is available at https://www.accenture.com/_acnmedia/pdf-106/accenture-technical-analysis-megacortex.pdf#zoom=50. If any network is compromised, Pinkerton always recommends not to pay the ransom as it encourages malicious actors to continue the cyber-attacks.

Security-Related Apps Top Download Charts

Hong Kong protesters are downloading apps to secure their smartphones.

A significant number of protesters in Hong Kong are using security-related applications to disquise their identity, data, and location. Protesters and citizens look for ways to secure their personal data as authorities not only spy on forums and throughout messaging apps, but there have also been cases where police tried to access detainees' phones. iOS App Stores' top download charts include apps that give fake GPS location, password-locked document storage, and a panic button. One of these apps is called Parachute, which automatically records video, audio, and location data when a user is an emergency. The app also sends texts, calls, and emails to emergency contacts. Other measures to protect data are burning SIM cards, using cash instead of other payment methods and turning off their GPS. Hong Kong citizens tend to rely on encrypted messaging apps like Telegram and forums such as LIHKG to share strategies to protect their personal devices' data while avoiding the use of public platforms like Facebook, WeChat, and Twitter. Protesters believe Hong Kong's police is adopting high-tech surveillance methods used in China. Moreover, on August 7, 2019, a U.S. cyber security group identified a new Chinese hacking group which carries out political espionage for Beijing. The group gathered intelligence information on pro-democracy dissidents in Hong Kong in 2016 and 2017, specifically on the pro-democracy Umbrella Movement candidates.

Pinkerton assesses that attempts to intercept messages and access personal data on citizens' devices are likely to continue over the medium term. Pinkerton finds it likely that further cyber-attacks and cyber-intrusions in Telegram and other apps popularly used by protestors are likely to occur in the short term as rallies continue in Hong Kong. Governments or possible attackers likely consider that these apps have valuable information regarding upcoming protests in Hong Kong and around the world. On June 12, 2019, a state actor conducted a distributed denial-of-service (DDoS) attack against Telegram taking the service offline and affecting Hong Kong protesters. Pinkerton recommends clients in the region avoid making comments related to the political situation in Hong Kong on public platforms. Further, if clients are located in Hong Kong verify there is no unrecognized activity in their devices and apps and avoid using public Wi-Fi.

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