CYBER SECURITY BRIEFING

A Monthly Recap of Technology & Information Risk

PINKERTON®

AUGUST 2019

Capital One's Data Breach Impacts More Than 100 Million People

About 100 million people in the U.S. had their Capital One data breached by a former cloud service employee.

Capital One Financial Corporation reported that a malicious actor gained illegal access to personal information of millions of customers that applied for credit cards from 2005 to early 2019. According to Capital One's disclosure statement, the breach affected 100 million people in the U.S. and 6 million customers in Canada. The malicious actor, arrested on July 29 and identified as a former employee of Amazon Web Services (AWS), stole names, addresses, fragments of payment history, credit limits, and other information provided to the company during the application process. Additionally, 140,000 Social Security numbers, 1 million Social Insurance numbers, and 80,000 bank account numbers of secured credit card users were compromised. A spokesman of AWS confirmed that Capital One used their cloud services to store information and stated that the malicious actor exploited a misconfiguration in the firewall protecting one of its applications. The disclosure statement on Capital One's website adds that after they noticed the breach, the company fixed the vulnerability and contacted the authorities. Moreover, it says that it is unlikely that the malicious actor shared or sold the collected data.

Pinkerton assesses that Capital One customers are still vulnerable to further cyber-attacks as the malicious actor made public the process of the data breach in several open-source websites, including GitHub, Slack, and Twitter. According to FBI investigators of the case, the suspect was easily traced as she used her real information, pictures, and consistent usernames in the different websites. The high level of exposure of the suspect and her activities prompts an increased risk that outside individuals could have accessed the stolen data. The police investigations further revealed that the suspect had intentions of finding data stored in AWS clouds. Media outlets added that the suspect often shared information about being unemployed, having gender identity issues, and suicidal thoughts. Pinkerton finds it likely that the suspect likely targeted AWS due to her background in the company. Pinkerton recommends its clients with personal or business accounts in Capital One monitor their payment history and report any suspicious activity. As other malicious individuals could use the stolen data, Pinkerton finds that phishing campaigns against the affected customers are likely. Thus, Pinkerton advises reporting suspicious e-mails from financial or governmental institutions urging the user to click a link embedded in the text asking for personal information or downloading an attached file. Finally, Pinkerton recommends clients with stored data in cloud services to render or update all cyber-security protocols that comply with global standards established by the Center for Internet Security.

Ransomware Attack On Johannesburg Power Company

A power company in Johannesburg suffered disruptions after systems were infected with malware.

Recently, the system of the power company of Johannesburg, South Africa, called City Power, was infected by a ransomware virus. This kind of virus is usually operated by syndicates who aim to solicit money. The ransomware encrypted all City Power's database and applications, making its website and electricity vending system unavailable. Consequently, many customers who are provided prepaid power meters were not able to acquire electricity units, leaving them without power. Six hours after the attack, the City of Johannesburg made an announcement on Twitter saying almost all impacted applications and networks had been restored and that customers' personal information was not compromised. However, the City Power website and systems remained offline, and the system to dispatch and order material were slowed.

Pinkerton assesses that ransomware attacks to big companies are highly likely to continue in the long term as preemptive measures have not been developed due the way attacks are executed, sometimes victimizing a large number of unsuspecting users while injecting malicious code into applications' components. Experts say cyber criminals now use ransomware as a more focused tactic as they profile and target larger organizations which are likely to pay a meaningful level of ransom. Additionally, there has been an increase in supply chain attacks. In March 2019, a Norwegian aluminum company producer called Norsk Hydro was attacked with ransomware, and the costs of the incident were higher than USD 40 million (NOK 347.97 million). Other major industrial firms have been hit by ransomware in the past months, such as ASCO, an aircraft parts maker, Hexion, a chemical company, and Aebi Schmidt, a special-purpose vehicle maker. As major companies usually give services to a large number of people, it is likely that many clients' data could be at risk. Furthermore, clients could be affected by the disruption of the services of 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 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.

Criminal Group Renders New Malware To Target POS Devices

FIN8 is back, and is using a new method to attack point of sales systems to steal payment card information.

Media outlets have reported that cyber-security experts from Gigamon Applied Threat Research (ATR) detected a new malware from FIN8, a financially-motivated cyber-criminal organization, which targets point-of-sale (POS) devices to steal credit card information. FIN8 was initially known for attacking retail and hospitality businesses, but more recently it has targeted the hotel industry. The new malware, Badhatch, creates a backdoor in the POS systems that allows malicious actors to control the victim's network using command and control (C&C) communications. The attack begins with a phishing campaign that, after the victim clicks on the attached Microsoft Word file, downloads a PowerShell script that installs the backdoor. As malicious actors continue infecting internal corporate systems, they inject POS scraping tools in computer systems that contain payment information. The director of Gigamon ATR stated that the use of Europay, Mastercard, and Visa (EMV) chips does not guarantee being affected by this malware. Although the EMV chip can restrict the access to some cryptographic information of the card, malicious actors are still able to complete 'card-not-present' processes, such as online purchases.

Pinkerton assesses that cyber-attacks targeting POS devices will remain a significant threat for businesses in the long term. Financially-motivated cyber-criminals frequently adapt their products to render successful campaigns as they exploit human and technological vulnerabilities. As the infection begins with phishing campaigns, untrained employees represent an increased risk for clients as they would unknowingly download the malware without reporting suspicious e-mails or attachments. Moreover, malicious actors target the identified business sectors (hotel, retail, and hospitality) as their POS systems often use outdated versions of Microsoft Windows operating systems. Gigamon researchers said that it is uncommon that business use anti-malware software in their POS systems. Pinkerton recommends its clients using POS devices to install anti-virus products and ensure that their operating systems are running the most updated versions as developers frequently patch exploits and vulnerabilities. Further, Pinkerton advises that clients encourage its personnel to report e-mails coming from legal or financial institutions with attached files or links as they likely are part of a phishing campaign.

Cryptocurrency Thefts Reach USD 1.2 Billion

Cyrptocurrency exchanges and regulators are fighting an uphill battle against hackers.

Cryptocurrencies theft and fraud amounted to USD 1.2 billion (EUR 1 billion) during the first quarter of 2019. According to CipherTrace, an American cyber-security company, losses in 2019's first quarter already total 70% of the 2018 figure. This past March, the U.N. Security Council reported that North Korean hackers had stolen USD 571 million (EUR 512 million); perpetrators remain unknown, and the assets have yet to be recovered. In May, Binance, one of the most prominent cryptocurrency exchanges, suffered a cyber-attack, that permitted hackers to steal about USD 41 million (EUR 36 million). In June, USD 4.3 million (EUR 3.8 million) worth of Bitrue was stolen and in July USD 28 million (EUR 25 million worth of Bitpoint. All thefts involved "hot wallets," cryptocurrency accounts connected to the internet that are necessary to make online transactions. Many cases involved phishing techniques that allowed hackers to access to secret keys and passwords. CipherTrace linked the increase of crypto-currency fraud in the first quarter of 2019 to the rise of cross-border payments, from the U.S. to offshore accounts, through Bitcoin transactions. Compared to the first quarter of 2017, Bitcoin transactions increased to 66%. CipherTrace further warned that the sector, besides of stronger security measures, lack enhanced protocols to identify hackers and recover funds. Even though blockchain technology, upon which crypto-currencies are based, allows transactions to be tracked, the number of exchanges and participants make it extremely difficult to uncover the attackers.

Pinkerton assesses that in the short to the medium term, crypto-currency fraud will likely keep increasing until stricter and consistent regulation is implemented globally, as hackers typically profit from these currencies' anonymity. For the same reasons, Pinkerton further assesses that the number of asset losses in the first quarter of 2019 is likely to be much higher, as they are so difficult to trace and commonly are undetected. In addition to not being regulated by any central bank, crypto-currencies are only subject to some regulation or standard-setting bodies in 17 countries plus the European Union (EU) member states. However, this increasing trend in crypto-currency fraud will likely lead to bans on privacy coins or severer scrutiny to banks, to prevent money-laundering or terror financing.

Cyber-Criminals Target Several Institutions With Spam Campaign

A spam campaign was found that targeted financial institutions and governmental organizations in Colombia.

Trend Micro researchers identified that a group of cyber-criminals rendered a spam campaign that spread the Proyecto RAT malware on networks of governmental and financial institutions in South America. The attack affected Colombia the most. Cyber-criminals used a disposable e-mail address service (YOPmail) to create the command and control (C&C) server. Afterward, the malicious actors could send numerous RTF files attached to deceiving e-mails. If victims follow the e-mail's instructions, users will download macros which deliver the remote access tool (RAT), usually Imminent Monitor RAT, although several other types of RAT malware have been detected. The newest RAT malware, Warzone, has web browsing, keylogger, and password-stealing capabilities. Finally, the malware executes a second payload that consists of Proyecto RAT, which has a Uniform Resource Locat (URL) address to continue C&C communications using the YOPmail service in the newly infected device.

Pinkerton assesses that these cyber-attacks likely will continue in Latin American countries as the success rate of these campaigns largely depends on the victims' response, and there is little cyber-security awareness in the region. According to the most recent Global Cyber-security Index report, Uruguay has the best cyber-security practices in Latin America; however, it is the 51st place out of 175 countries. Mexico, Colombia, and Argentina rank the 63rd, 73th, and 94th place, respectively. During a scam campaign, after the deceiving e-mail has been sent, the potential victim's response is crucial to stop the spread of the infection and avoid data breaches. Therefore, Pinkerton recommends its clients update or create simple guidelines or brochures that inform users about downloading files from e-mails with threatening or suspicious messages. To encourage victims to download the malware, malicious actors frequently use the names and appearance of legitimate financial or governmental institutions along with a message that frightens or stimulate the user, such as lawsuit notifications, bank account suspensions, or monetary rewards. Pinkerton advises confirming the information with the corresponding institutions and reporting it within the company to avoid compromising the computer networks.

Unique Phishing Campaign Targets American Express

A base HTML element was used to hide a malicious URL in a phishing scam that targeted American Express customers.

Cyber-security experts using Microsoft's Office 365 Advanced Threat Protection announced a unique phishing campaign that targeted American Express' customers and is able to bypass security scans. Malicious actors sent a deceiving e-mail urging customers to verify their information due to a "system maintenance" otherwise, the account would be suspended temporarily. The e-mail contains a link to a fake American Express webpage where potential victims input their data. The campaign targets business users and consumers. The innovation of the campaign consists of its capability of masking the malicious Uniform Resource Locator (URL) and avoid being detected by URL filters and gateways with scanning services. The developers of the phishing attack divided the malicious URL into two segments that scanners are unable to combine and recognize as a threat.

Pinkerton assesses that phishing campaigns against financial institutions will continue in the long term. Malicious actors continue developing different procedures that make these campaigns more believable for their targets in addition to masking methods that bypass scanning and security systems. As malicious actors can coordinate campaigns that target a significant number of people and include credible warnings that encourage users to follow the fake email's instructions, these cyber-attacks are frequently successful among unknowing people. Pinkerton recommends its clients that use business accounts to inform their personnel about the American Express phishing campaign. If any incident is reported, Pinkerton advises updating corporate passwords, informing the financial institution, and checking for unauthorized or suspicious transactions. Further, Pinkerton recommends its clients render cyber-security protocols for its personnel that encourages them to report e-mails asking for sensitive information and confirming the validity of the e-mails with the financial institution directly.

Ransomware Attack Cost County Public Administration 130,000 USD

La Porte County is just one of multiple municipalities paying to get files back from hackers.

Open sources reported that the public administration of La Porte County, Indiana had to pay approximately USD 130,000 (BTC 12.05) in Bitcoin to malicious actors who successfully infected its networks using the Ryuk ransomware. The IT department detected the cyber-attack on July 6 and isolated the infection to 7% of the public administration's systems. However, the ransomware affected two domain controllers which disabled government e-mails and the county's website. Authorities decided to pay the ransom to recover the encrypted files as the FBI decryption keys failed and the ransomware impacted the government's backup servers.

Pinkerton assesses that this attack sets a relevant precedent for malicious actors to continue rendering ransomware campaigns as it weakens the 87th Annual Conference of Mayors' resolution of not paying ransoms to discourage cyber-criminals. Pinkerton finds that similar cyber-attacks will remain a significant challenge for law enforcement and a credible threat for institutions in the medium to long term. According to Europol's most recent Internet Organized Threat Assessment, ransomware is "the key malware threat" for private and public institutions. The Online Trust Alliance (OTA) issued a report on July 9, which reflects that ransomware attacks in 2018 cost USD 8 billion (EUR 7.11 billion) globally. According to Emsisoft cyber-security experts, there is a 3%-5% chance of decrypting files infected by the Ryuk ransomware. However, Pinkerton recommends clients buying cyber-security insurance policies to mitigate potential financial losses; restoring the affected computer networks are still costly even if the ransom is not paid.

Further, Pinkerton recommends assessing possible system vulnerabilities and ensuring that cyber-security protocols and data management procedures are updated and fully operational to detect and mitigate future cyber-attacks promptly.businesses operating in Ethiopia and estimated USD 4.5 million (GBP 3.6 million) a day.

Financial Records Stolen From Tax Agency

Personal data of 5 million Bulgarians was hacked and then leaked to local media.

A hacker (or hacker group) was able to retrieve personal details from the National Revenue Agency (NRA), a department of the Bulgarian Ministry of Finance, and emailed download links to the stolen data to local news. The hacker claimed having stolen 110 databases from NRA's network, totaling nearly 21 GB; the hacker shared 57 databases, comprising 11 GB. According to officials, the attack happened at the end of June but just was recently disclosed. Shared information of over five million people and companies included names, personal identification numbers, addresses, social security numbers, and financial earnings. Most of the information backed to 2007, but newer information was also released. Officials confirmed that 30% of the data that went public was information kept by the NRA. The government stated it plans to seek help from the European Union (EU) cyber-security agency to audit its most sensitive systems, to prevent further attacks.

Pinkerton assesses that the rest of retrieved data, belonging to nationals, foreigners, and companies financially established in Bulgaria, is most likely to be held for a ransom, as these attacks typically are financially motivated. If this information is put on sale online, as a result of the government refusing to pay for a possible ransom, buyers would likely exploit it to break into other accounts or attempt to steal identities. Identity theft poses further threats, as retrieved information would likely allow them to open credit cards, take out loans, or make online purchases. Financial intercepted data also would likely allow them to impersonate legitimate organizations, through phishing emails or even calls, and demand payment. Pinkerton recommends clients financially established in Bulgaria to create different strong passwords for every account they hold and to check their credit reports, as soon as possible.

Jenkins Servers Exposed Due To Misconfiguration

GE Aviation classifies this server exposure to sensitive files to be a medium risk vulnerability.

Cyber-security researchers reported that servers belonging to GE Aviation became vulnerable to public and malicious access due to faulty DNS configurations. An independent researcher stumbled upon the open server, which contained source codes, private keys, passwords, system configuration details, and other proprietary information. Initially, the research intended to determine the number of Jenkins servers detectable through the Shodan search engine. Jenkins is popular among developers to carry out automated integration and deployment of software or other automated processes. An outdated DNS configuration left the server open to public access. GE Aviation received notification of the breach; and proceeded to secure the information and update credentials. The company classified the breach as a medium-risk event pointing out that there was no indication third parties accessed any sensitive information.

Several events throughout 2019 point to the fact that careless information management is one of the main causes of system vulnerabilities and data breaches. The risk posed by unwitting exposures is maximized due to the fact that such events could provide attackers with tools to quietly infiltrate other systems. In the most recent event, potential attackers could have used configuration details and credentials to later find backdoors into sensitive systems deployed by GE Aviation in the aerospace industry. Researchers have so far detected 5,495 open projects based on Jenkins servers; such availability further highlights the likely exposure of other assets and companies. Pinkerton advises performing regular audits to ensure that systems configurations are up to date and that the use of third-party software or suppliers is done under the established standards.

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

Magecart was targeted again by a malicious skimmer that breached over 960 e-commerce stores.

Open sources reported that Sanguine Security Labs identified an automated Magecart campaign that compromised the financial and personal data stored by 962 e-commerce stores in 24-hours. According to cyber-security experts, the malicious actors rendered an attack that breached the e-commerce's websites worldwide and inserted a card-skimming script. The script added a fake payment section in which customers' uploaded information such as name, address, card data, and phone numbers that malicious actors collected successfully. Researchers did not release information about the method that malicious actors used to infect e-commerce websites. However, cyber-security experts speculate that the automated attack likely consisted of scanning and exploiting security flaws on e-commerce's software infrastructure. The head or threat research at RiskIQ stated that the Magecart Group 7 rendered the magecart campaign. This group does not use servers to support their attacks, but directly insert them on the victim's website.

Pinkerton assesses that the increasing number of magecart attacks highly likely will remain a significant threat for clients with digitally-based businesses and for customers that frequently use e-commerce websites in the medium to long term.

Although Magento is one of the e-commerce platforms that remains the primary targets of cyber-criminals, experts of RiskIQ stated that card skimming techniques have been reported on every web environment and have targeted large-scale companies, including Ticketmaster, OXO, and British Airways. Experts added that for every high-profile attack, thousands of attacks go undisclosed. Cyber-security researchers have warned that although magecart groups mostly focus on financial data, there have been reports of another type of data, including login credentials, using similar methods. Pinkerton recommends clients using e-commerce platforms to ensure that the web infrastructure to the latest versions as these attacks scan for flaws that allow cyber-criminals inject scripts on PHP-based platforms. This measure includes clients using third-party payment platforms as they have also been targeted by malicious actors. Pinkerton further advises updating cyber-security protocols to identify and mitigate the risks of potential attacks, such as Content Security Policies, to avoid sanctions from international cyber-security regulations. Clients who frequently use e-commerce websites are advised to monitor their financial activity and report any suspicious activity. Further, Pinkerton advises continually resetting passwords to personal and financial information or using a password manager.

7-Eleven Payment App Breached

900 Japanese customers lose money due to mobile app flaw.

Recently, 7-Eleven payment app users in Japan were stolen about JPY 55 million (USD 510,000), after a security breach. According to the company, 900 out of 1.5 million registered accounts had been accessed, from China and other locations outside Japan, without authorization. According to ZDNet, the app contained a password reset function that allowed anyone to request a new password for other people's accounts, having the password reset link sent to their email address, instead of the owner's. Cyber-criminals needed only user's email, date of birth, and phone number to request a password reset link. Cyber-criminals could have taken large sums of money from the user's credit card and retrieved sensitive data as well. The company stated that it would compensate users for their losses, and suspended accepting new users or allowing users of the service to add money to the app.

Pinkerton assesses that human errors in the design of software likely constitute an important exploit for hackers to access encrypted channels and retrieve sensitive information, despite an overall increase in security investment. Companies typically secure their software against malware and hacking but neglect the implementation of additional levels of security. As the real impact of the identified breach remains unknown, Pinkerton recommends 7-Eleven app users monitor their credit card status and, as a precautionary measure, change all passwords, since cyber-criminals could profit from retrieved emails, date of birth or phone number data to access other users' accounts.

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