CYBER SECURITY BRIEFING

A Monthly Recap of Technology & Information Risk

PINKERTON®

JUNE 2019

First American Financial Admits Data Breach

First American Financial may have given unauthorized access to financial information of its customers.

It has been reported reported that First American Financial (FAF), a real estate title insurance company, admitted that a breach of its consumer's data has been ongoing for years, due to a design defect in one of its applications. FAF exposed millions of documents, dating as far back as 2003, including bank account numbers, mortgage and tax records, wire transaction receipts, driver's licenses, social security numbers, and other sensitive information. The documents did not require any authentication to be accessed, as anyone who knew the URL for a valid document could view the documents. FAF did not comment on the exact number of breached documents, but KrebsOnSecurity, a cyber-security research firm, estimates that they were around 885 million potentially exposed files. The title insurance company stated that it has already addressed the issue, and ordered external access capabilities to the identified application shut down.

Pinkerton assesses that the compromised documents in First American Financial's application likely will be used by phishers in Business E-mail Compromise (BEC) scams. In a BEC scam, attackers impersonate a real estate escrow firm agent, show personal documents or sensitive information to the victims to build trust, and finally induce them to wire money in a bid for buying a property. According to the U.S. Federal Bureau of Investigation (FBI), BEC scams are the costliest form of cyber-crime reported to the present, as it is estimated that around USD 12 billion (EUR 10.7 billion) were netted by cyber-criminals between 2013 and 2018 through this scheme. Further, given the length of years this breach existed, this likely explains current or past customers of the institution whose identities or home titles were stolen. Pinkerton recommends, in the event sensitive information was shared with First American Financial as far back as 2003, to suspect from e-mails that meet the stated characteristics of a BEC scam and do not come from a minimal personal acquaintance.

Major Digital Companies Against Government Eavesdropping On Chats

GCHQ is proposing plans to eavesdrop on encrypted chats, and businesses don't agree.

Recently, it was reported that the UK Government Communication Headquarters (GCHQ) proposed enabling eavesdropping on encrypted chat services, such as that of Apple or Whatsapp. Those two companies, along with 50 other providers, signed an open letter that condemns the proposal as a "security threat." The proposal requires chat service companies to include a third blind recipient in the conversations to avoid encryption breaking, undermining users' security and trust, according to the providers. The government would be included as "cc" recipient in each two-way conversation, turning it into a group chat, and a secret government participant would be added to existing group chats. According to the UK National Cyber Security Centre's (NCSC) Technical Director, the proposal is mainly intended as a counter-terrorism strategy. During 2015-2016, Apple engaged in a dispute with the U.S. Federal Bureau of Investigation (FBI) over encryption and alleged the same reasons. As the GHCQ requires chat service companies to include a third recipient in the conversations, it skips the process of breaking a code, for which it likely would need the providers' aid, and directly accesses sensitive data. It remains unknown how the GCHQ would handle sensitive data.

Pinkerton assesses that the eavesdropping on encrypted chat services proposal, if instituted, would compromise users' privacy and security, and likely without most users' knowledge. Pinkerton assesses that this proposal would constitute an exposure threat to sensitive company communications. If the proposal is instituted, Pinkerton further finds it likely that privacy advocates would engage in protest activity, causing localized traffic and travel disruptions. Pinkerton assesses that the proposal would also likely face regulatory scrutiny from the UK Parliament over data privacy and storage, as well as EU regulatory bodies while the UK is still part of that body.

TeamViewer Hack By Chinese ATP Group In 2016 Reported

Chinese hackers breached TeamViewer in 2016.

Der Spiegel reported that TeamViewer, a popular remote-support software, was attacked in 2016 by Chinese hackers. TeamViewer "allows users to access and share their desktops remotely," taking full control of someone else's PC via the Internet. The Chinese hacker group called Winnti, an Advanced Persistent Threat (ATP) group discovered in 2010, typically attacks the online video game industry using a trojan malware. The companies affected are located mainly in the U.S., Russia, Japan, and South Korea. Winnti usually infects users' systems through its software and malicious updates, which install malware and then download a backdoor payload to control the users' computers remotely. The backdoor lets the attacker bypass the security system and access to the victims' network and data undetectably. TeamViewer was criticized for not reporting this cyber-security incident as many businesses make use of this software.

Pinkerton assesses that this group's attacks present an ongoing threat to business interests – particularly involving thefts of both personal and company confidential data – for companies that allow employees to use company-issued computers for personal use, and generally in the computer game industry. Even though TeamViewer stated that it had an immediate response when the hack occurred and that no user was reportedly affected, it is highly likely that the long-term TeamViewer breach caused potentially large numbers of security breaches that have gone unreported or undetected. Moreover, it is vulnerable to constant attacks from other ATP groups, as it is an attractive program to hacking ends. In May 2016, there was another cyber-security intrusion in which TeamViewer users informed that their bank accounts had been manipulated by hackers who exploited another flaw in the software. Nonetheless, the company said it was the users' fault for using the software carelessly. As TeamViewer is a popularly used software, it is highly likely that both government and business employees' computers and mobile devices are at risk. Due to the characteristics of the software, Pinkerton recommends clients, together with their IT teams, reevaluate their cyber security systems, verify each account uses a different and strong password, and run the program only when needed instead of letting it auto-start.

North Korean Hacking Group Can Access Bluetooth Connected Devices

Korean threat actor creates malware that identifies connected Bluetooth devices.

Last month, Kaspersky Lap reported that a North Korean Advanced Persistent Threat (APT) group called ScarCruft has created code able to access users' personal information via devices connected to Bluetooth. ScarCruft is a state-sponsored group that conducts cyber-espionage operations, which first was identified and tracked in 2016. This APT group uses spear phishing and "watering-hole" tactics, which compromise specific targets by infecting websites they usually visit. The group has now extended the amount of data it can collect; according to Kaspersky researchers, ScarCruft also focuses on stealing data from mobile and Bluetooth devices through Windows Bluetooth API, and use exploits for Adobe Flash and Microsoft Internet Explorer as well. So far, the main targets of this group are trade companies and diplomatic entities from Vietnam, Russia, Nepal, China, Hong Kong, India, Romania, and Kuwait, which have trade agreements with North Korea. ScarCruft maintains a low profile, and is considered a highly-skilled and evolving group. Kaspersky experts recommend Bluetooth users to implement endpoint detection and response, and security measures that allow the recognition of threats in the corporate network.

Pinkerton assesses that this group's exploitation of Bluetooth connected devices, Adobe, and Microsoft Internet Explorer, presents an ongoing threat to business interests – particularly involving thefts of trade secrets and intellectual property. As the ScarCruft code's spyware functionality reportedly supports espionage activities, it is highly likely that both government and business employees' computers and mobile devices likely are at risk. Due to the characteristics of the malware, Pinkerton recommends high profile clients, together with their IT teams, reevaluate their cyber security systems – at all levels from networks to close-proximity Bluetooth connectivity.

Spyware Vulnerability Threatens Corporate Interests On Work Phones

Select WhatsApp users were the target of an advanced cyber-actor.

WhatsApp has identified a vulnerability by which malicious actors were able to install malicious surveillance software in devices that count with the application. The software was linked to the NSO Groups, an Israeli cyber intelligence firm; but it was created for government use only, and how the software ended up in the hands of non-government cyber-attack groups is not yet known. The software threatens the app's security system because it allows hackers to view messages in the infected telephones or computers, as the app's system encrypts texts and images and this information is only available for the sender and recipients. According to media reports, malicious actors have been calling devices and infecting them; how many WhatsApp users' devices have been infected remains unclear.

Pinkerton assesses that this WhatsApp-related attack vector likely poses a direct threat to companies' sensitive communications and intellectual property security, due to a high likelihood that many employees and executives (particularly those with teenage children) have WhatsApp installed on their company-issued smartphones. Pinkerton finds it likely that the exploited vulnerability and installed malicious surveillance software has affected a very large number of WhatsApp users, as the application has 1.5 billion users worldwide. WhatsApp has not yet disclosed whether the combination of the app's vulnerability and the surveillance software enables access other data in these devices, such as stored business documents, company email communications, photos, or other applications and intellectual property.

Malware Targets E-Commerce Websites To Steal Private Financial Information

Researchers found attackers injecting malicious JS Scripts into online shopping websites.

Recently, researchers from Chinese cyber-security company Qihoo 360's NetLab found that more than 150 e-commerce websites contained malicious scripts that allowed cyber thieves to steal private financial information. Researchers monitored the magento-analytics domain for seven months and found that attackers entered the malicious scripts hosted in the domain to several e-commerce websites that ran over Magneto CMS software. The malicious code triggered card skimming procedures to automatically steal payment information including card number, name of the customer, expiration date, and CVV. Further, the malware sent the stolen information to another file located at one of the magneto-analytics servers that malicious actors controlled. Experts are still investigating the method the attackers used to infect the websites or the vulnerabilities they exploited to initiate the attack. They added that malicious actors used the magento domain to mask their activities as it is unrelated to the Magneto CMS platform. Although researchers traced the malware to Panama, it has moved to servers in the U.S., Russia, and China. On May 9, seven e-commerce retailers in Japan reported data breaches of their servers that affected 15,000 customers. Cyber-security personnel noticed the breach six months after the attack began.

Pinkerton assesses that card-skimming malware will remain a significant cyber-security threat in the medium to long term as the e-commerce market expands and malicious actors render more efficient techniques to mask their activities. Pinkerton finds it highly likely that the number of websites infected by similar malware will continue increasing. Pinkerton recommends that clients with online retailing activities include common cyber-security standards like the Content Security Policy (CSP), and ensure that the web host continuously monitors suspicious logs. Clients using online payment methods are advised to look for suspicious details to identify fake settlement screens, and constantly review card-purchase statements.

Malicious Actors Target Confluence Software

Miners and rootkits were installed during a hack of Confluence servers.

Cyber-security analysts reported that malicious actors had exploited a Confluence Server vulnerability to install a Monero cryptocurrency miner. First, attackers sent a Kerberods malware that downloaded a shell script located at the Paste bin address. After it executed and installed two more shell scripts, the malware installed a trojan dropper. Finally, Kerberods ran the Monero miner with a rootkit component which used a self-propagation method. The rootkit element helped the malicious actors mask the additional traffic generated in the CPU during to the crypto-mining process. Since March 2019, malicious actors have used the same vulnerability in Confluence Server and Data Center to infect computers with ransomware and malware that deploys distributed denial-of-service (DDoS), which had the potential of shutting down infected networks.

Pinkerton assesses that Confluence servers will remain vulnerable in the near to medium term as malicious actors have been able to develop new exploits for Confluence's vulnerabilities and continue damaging devices with unpatched versions of the software. According to cyber-security experts, crypto-mining can reduce the performance of an infected device significantly, and increase its power consumption. Moreover, approximately 20% of these activities trigger security breaches that allow other malicious actors to initiate network-based attacks. Wherever possible, Pinkerton recommends that clients avoid using the Confluence software until Atlassian, the software company, releases a patch that guarantees a high level of security. However, if the use of Confluence is essential for the clients' operations, Pinkerton advises that clients update the software to patch any identified vulnerability and monitor the developers' reports about security breaches or future attacks. Finally, Pinkerton recommends that clients ensure that standard cyber-security measures are enabled, including anti-virus and virtual private networks, to mitigate further damage.

Ransomware Attack Prompts Servers Shutdown

Baltimore City's servers shut down after ransomware attack.

Malicious actors targeted the Baltimore City Hall server network with a ransomware virus that forced the government to shut down most of its servers. As of May 8, authorities have not identified the ransomware which spread through the city government's computer networks. The ransomware virus first encrypts a device's data, then malicious actors demand a ransom which is usually paid with cryptocurrency in exchange for the decryption key to restore the inaccessible files. According to the Baltimore mayor, emergency response services remained operational during the attack. However, cyber-security experts are still investigating the origin of the attack and the method used to infect the Baltimore network. Although the mayor stated that there is "no evidence that any personal data has left the system," officials are still investigating the extent of the damage. According to media outlets, the ransomware attack affected Baltimore's departments of Public Works, Finance, and Transportation.

As the government was required to shut down its servers, and a similar attack deeply affected Baltimore's phone services last year, Pinkerton assesses that the city's networks are highly vulnerable to cyber-attacks. Moreover, Pinkerton finds it likely that the local government has not updated its cyber-security services and protocols to prevent, detect, and react more efficiently to ransomware attacks. If further attacks occur, Pinkerton finds that sensitive information of companies or individuals that government offices store in their servers likely will be compromised.

Pinkerton recommends clients with businesses in Baltimore and the surrounding region monitor official statements about the extent of the attack, and ensure that their systems cannot be affected by the city government's predicament. As malicious actors continue developing more sophisticated malware and ransomware, and cyber-attacks remain an international concern, Pinkerton recommends that clients regularly back up all important data to local air-gapped servers to mitigate damage in the event of a ransomware attack, and maintain all updates on early detection systems and anti-malware software.

Amazon Sellers Victims Of Fraud

Amazon hit with extensive fraud when hackers siphoned merchant funds.

It has been reported that 100 seller accounts on Amazon were compromised during May–October 2018, as hackers managed to siphon funds from the identified merchant accounts. Amazon said that these accounts were likely accessed through phishing techniques, inducing users to provide their confidential login information. Hackers likely added details to the merchant Amazon accounts, making it possible to transfer victims' money to their bank accounts. The stolen money derived from sales or loans by Amazon. The money was traced to criminals' bank accounts with Barclays Plc and Prepay Technologies. Neither bank made a statement on the matter. However, Amazon lawyers requested a London judge to approve searches of account statements at Barclays Plc and Prepay to investigate the fraud, and identify and pursue the criminals responsible for the thefts.

Pinkerton assesses that phishing scams, not relying on technological issues but cybersecurity savviness, are increasingly popular and likely more effective for accessing users' private information and log-in credentials. Phishing occurs when an attacker, pretending to be a trusted entity, dupes a victim into opening a URL link in an email or direct message (DM), and to deliver sensitive information. Amazon, covering phishing fraud, states on its website that it will never send an unsolicited email asking to provide sensitive personal information like social security number, tax ID, bank account number, credit card information, or ID questions; and when receiving a suspicious email, Amazon recommends reporting it immediately.

President Approves Internet Legislation

Russia adopts law that gives government more control over domestic internet.

The Russian government officially implemented a controversial law which gives government regulators greater control over the internet. President Vladimir Putin approved and signed the legislation on May 1. The new legislation will centralize the network and introduce traffic monitoring to control communication within the country and based on national security the government regulators would decide what can be posted, seen or discussed about online. The law will limit domestic online traffic to develop an independent national network. The companies operating in Russia have until November 1 to adopt the new regulations. Since the law was proposed, it has caused many protests and opposition across the country.

Pinkerton assesses that this new regulation is a part of the government plans to create more independent networks to avoid being targets of foreign cyber attacks. Additionally, it is expected that the authorities will likely continue creating a legal framework to gain more power over the IT systems and network. Nonetheless, there are concerns that this law could limit the freedom of speech as the government would have the ability to control content based on national security arguments. Pinkerton finds that protesters and the opposition will likely continue demonstrating against the regulations. Pinkerton recommends clients with operations in the country study the new law carefully to check if the company follows the legal framework or to work on it before the deadline in November. Furthermore, Pinkerton advises clients to verify the safety of the system and corroborate that sensitive information is stored and transferred securely with backups in other locations if possible.

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