CYBER SECURITY BRIEFING

A Monthly Recap of Technology & Information Risk

PINKERTON®

APRIL 2018

Data Breach Exposes Frost Bank Checks

Frost Bank announced that a third-party lockbox software was compromised, allowing unauthorized actors to access images of checks in its image archive.

Frost Bank further stated that malicious actors could forge checks with information gained through the breach. The bank immediately blocked all access after the discovery of the breach. According to the bank, approximately 470 commercial customers utilized the compromised software program.

While Frost Bank stated that their own systems remained uncompromised, Pinkerton finds it likely that malicious actors could use the check image of Frost Bank customers to gain access to personally identifiable information (PII), including bank accounts, addresses, names, and routing numbers. Pinkerton finds it highly likely that malicious actors will attempt to leverage this information in phishing campaigns and fraudulent activity. Pinkerton further assesses that malicious actors will likely attempt to compromise other lockbox software to gain access to PII.

Hacking Campaign Threatens Maritime And Engineering Industries

Per reports, the Chinese hacker group known as “TEMP.Periscope” and “Leviathan” is suspected of targeting engineering and maritime industries in a campaign that was initiated in the summer of 2017.

Most of the targets up until now have been from the U.S., but reports indicate that operations in Europe and Hong Kong have been targeted as well. Evidence from the attacks suggests that the group has been trying to retrieve information such as development and intellectual property data, as well as research and material that could be used in negotiations. The group is using tools such as file stealers, backdoors, and scripts for remote administration. An analyst at the cyber-security firm FireEye who uncovered the attacks said that the targets are connected to the South China Sea (SCS) dispute.

Pinkerton assesses that clients in the sectors of defense, maritime exploitation and engineering, and sea transports with operations in and around the SCS are at risk of being subjected to attempts of intrusion. Further, due to the nature of the dispute, all types of information about operations in the area may be regarded as intelligence. Intrusions may also be directed towards small-scale fishing operations and leisure cruise lines.

The ongoing dispute in the SCS is driven by a Chinese territorial claim to almost the entirety of the maritime area, which is being disputed by the Philippines, Malaysia, Japan, and Vietnam, but also the U.S. to ensure freedom of navigation.

Government To Create A New Cyber-Security National Agency

Chile's Defense Ministry has published the new Cyber-Defense Policy meant to diminish the number of cyber-attacks suffered by its citizens and institutions.

The Policy will focus on six points: the creation of new military Cyber-Defense Command and a national defense Fast Response Cyber-Security Incident Team (CSIRT) that will coordinate the rest of the CSIRT of the Chilean institutions. The creation of a CSIRT for every armed force branch, the development of a new Cyber-Defense and Technology Security Office in charge of giving counsel on the matter. Additionally, to bolster the overall cyber-security capacities of the Defense Ministry and finally, to increase the budget for the country's cyber-security effort. The defense policy will be revised every four years to respond to the necessities of the current cyber-security environment.

Pinkerton finds it highly likely that this measure corresponds to country's levels of cyber-violence. According to Kaspersky Lab, during the first six months of 2017 34.2% of the Chilean population had suffered cyber-attacks, 19.6% out of which were attacked while connected to the Internet, and the remaining 14.6% were attacked via USB devices while offline. Meanwhile, in Argentina, cyber-attacks reached 3.13 million cases in 2017; in response to this threat, on February 13, 2018, the Argentinian president Mauricio Macri ordered the increase in the budget and the acceleration on the implementation of the new Cyber-Security Command. Pinkerton advises all clients operating in Latin America to revise and increase their cyber-security countermeasures, to keep their antivirus databases updated, and to remain attentive to local authorities' pronunciations on the matter as new cyber-security measures are likely to be implemented in the region.

Security Flaw In Apollo Hospitals' Platform Reveals Details Of One Million Patients

A security flaw has revealed details of one million patients of Apollo Hospitals, a leading corporate hospital chain.

According to French cybersecurity researcher Elliot Alderson who recently revealed security flaws on various platforms including Aadhar and Paytm, said that the personal details of millions of people of Apollo Hospitals were at stake and that a serious security issue was discovered in the system. The hospital's digital platform "Ask Apollo" connects patients and doctors, while providing services like video and voice call consultations with doctors. The platform comprises of details of over one million patients. Per reports, the flaw was fixed on March 17.

Pinkerton assesses that attacks on large-scale corporate hospitals in India are likely to intensify in the near to medium term as the healthcare sector in the country continues to grow. Client personnel who use the services of Apollo Hospitals are recommended to take adequate security measures and avoid responding to emails or phone calls from unknown sources requesting personal details about their health insurance and medical history. While reports claim that the security flaw has been fixed, client personnel are recommended to take additional security measures to protect personal details that include their medical history and contact the hospital authorities for further assistance. Clients in the healthcare sector are recommended to back up data in multiple locations such as removable media and cloud servers and to do so on a daily basis to minimize losses in the event of a cyber-attack.

Medical Records Software Vulnerable

According to a security report published by Rapid7, the Boston-based software company says that an independent researcher has found two security issues in two medical records and billing software packages produced by DocuTrac: QuicDoc and Office Therapy.

According to Rapid7, the researcher found that the two programs each create three admin-level user accounts with hardcoded credentials during installation, of which the administrator installing and configuring them will not be aware, and that have virtually full access to the records database. Further, the researcher found that the two software packages have weak encryption that does not secure all of the stored data. DocuTrac was notified prior to the report's release but has not announced yet whether a patch will be released.

Pinkerton assesses that these security issues make massive quantities of medical patient and billing records vulnerable for all hospitals, clinics, mental health facilities, and private medical practices using Office Therapy and QuicDoc software. Pinkerton recommends that clients utilizing the identified software packages evaluate their potential exposure, and restrict physical access to facility computers to only authorized personnel. Further, given the potential for very large data thefts, government and corporate providers of medical and mental health services will benefit from proactive reviews of their contingency plans for damage control and brand protection in the event of a breach.

Thirteen Critical Vulnerabilities Found In AMD Processors

Security firm CTS Labs claims they discovered 13 critical vulnerabilities in AMD Ryzen and EPYC processors in an announcement on March 13, 2018.

Dan Guido of Trail of Bits confirmed the flaws on social media after CTS Labs sent him the findings to independently investigate. CTS Labs notified AMD as well as companies that use the compromised processors for cloud services. A patch does not currently exist given that CTS Labs only notified AMD 24 hours prior to releasing the information. The EPYC server, Ryzen Pro, Ryzen Mobile, and Ryzen Workstation are open to malicious actors. Malicious attacks could include taking control of Ryzen and EPYC Secure processors and Ryzen Chipset, malware infections, stealing credentials on high-security networks, evading endpoint security solutions, and physically damaging hardware. AMD is currently investigating the report to confirm the findings and evaluate the report's merit.

The confirmation and impact depth of these 13 critical vulnerabilities highly likely represents a security risk to cloud service businesses and businesses that depend on cloud service, especially without a patch to fix them. A rise in phishing scams to obtain usernames and passwords is likely since the attacks require administrator privileges. However, Pinkerton recommends businesses increase alertness for cyber-attacks focusing on gaining administrator privileges if their computers have any of the affected processors. Due to the lack of response time, the threat will likely continue until a patch or workaround is available. Pinkerton advises businesses with affected processors to increase monitoring for security threats.

RottenSys Botnet Can Control Android Devices

Hackers are extensively using RottenSys malware and creating a massive botnet that has already affected almost 5 million Android devices.

The botnet will have extensive capabilities including silently installing additional apps and User Interface (UI) automation. In the last two years, it has been responsible for displaying ads on the affected devices, and its creators likely gain USD 115,000 (EUR 93,357) every ten days. Since February 2018, the botnet has been added with a component that gives attackers ability to control all devices. The RottenSys is currently active in the Chinese market and is related to Chinese apps. Most affected devices are Huawei, Xiaomi, OPPO, Vivo, LeEco, Coolpad, and GIONEE.

Pinkerton assesses that the threat from RottenSys malware is high, and likely to increase in the medium term. Android systems users in China are at a high risk; there is an even chance the malware will spread on an international scale. While previously the impact of the malware was not considered harmful to the users, the new component significantly increases the risk of losing stored data, credentials, personal information, and increases vulnerability to financial frauds. Personnel are advised to review lists of permissions required by apps installed on their devices and make sure the system is updated to ensure safety.

Cyber-Attack Targets Government Data

Per reports, a cyber-espionage group, who accessed sensitive data of UK government departments and military through a third-party contractor, were able to make detection more difficult by utilizing legitimate apps together with new tools and old malware.

The group, which goes under the name APT15, reportedly deployed the three backdoors RoyalCLI, BS2005, and RoyalDNS after gaining access to the contractor's network. Investigators say that the attack allowed the group to, for example, dump local credentials and access password protected systems after a user had changed his or her credentials.

Pinkerton assesses it likely that cyber-espionage groups will continue to target third-party contractors to access sensitive information of primary organizations. As noted in a previous insight on September 9, 2017, the threat of third-party cyber risks is rising, and Pinkerton finds that the security gap between primary organizations and their employed contractors in many cases remains a security concern. Amid the upcoming implementation of the General Data Protection Regulation (GDPR), Pinkerton recommends primary organizations to engage with contractors on this issue.

More Than 550,000 Email Servers At High Risk Of Exploitation

A critical vulnerability has been detected in all versions of Exim, a free software used as a mail transfer agent.

According to statistics from the recent Mail (MX) Server Survey (March 1, 2018), over 56% (556,213) of email servers use Exim. The bug was first reported by Taiwanese security researcher, Meh Chang who tracked it as CVE-2018-6789, proving that it can leverage the vulnerability by sending a crafted malicious request that causes the buffer overflow as well as execute the remote code overflow. Reportedly, Exim has released version 4.90.1, which fixes the vulnerability.

Pinkerton assesses that there is a high threat of cyber-attacks to email servers that utilize Exim in the near to medium term. Even though the company distributor has released an updated version, Pinkerton finds that the flaw affects more than half of the email servers in use and patching the issue is likely to take a few weeks or even a few months. Clients using Exim are recommended to deploy the updated version 4.90.1 or above as soon as possible. Pinkerton notes that the risk of exploitation related to the detected bug in the system is likely to increase in the near term as the information about the vulnerability has spread widely.

More Than 900,000 Users Affected By 2016 Uber Security Breach

On March 6, 2018, the Attorney General's Office announced that more than 900,000 users of the ride-sharing service Uber in Mexico users might be affected by the massive data breach experienced in 2016.

According to the media, hackers stole data from over 57 million users. Uber was required to alert the authorities of the breach; however, the event was not known by this information was not made public until November 2017, as the ride-hailing company paid hackers USD 100,000 (EUR 80,534.75) to erase the stolen data instead. The stolen data includes phone numbers, email addresses, and the names of passengers and drivers. Uber Mexico has informed that the company is following the government's recommendations to increase the safety levels of their information storage infrastructure. On the other hand, the Attorney General's Office continues investigating the scope of the breach and the exact number of users that were affected in Mexico.

While it remains unknown if affected users will be notified regarding the status of their personal information, Pinkerton recommends all Uber users in Mexico to change their password and be on the lookout for any unrecognized activity linked to their payment method that they have registered in the app. Pinkerton also advises clients to be observant of safe password practices, such as having secure passwords (combining alphanumerical values, upper and lower class values, punctuation signs, etc.), using different passwords on every site or app that requires one, and changing their passwords regularly. According to the latest reports, financial phishing scams increased 6% worldwide in 2017.

Hackers Take Advantage Of Cortana's Security Flaws

Israeli hackers discovered that Windows AI, Cortana, could be deceived to browse insecure web pages and download malware to a device running Windows 10 system while it is still locked.

Microsoft has already solved two of the flaws found by the hackers; the first problem was that when an attacker plugged in a USB with a network adapter to the device, he could then voice command Cortana to access dangerous websites or connect to an unsecured Wi-Fi network controlled by the attackers. The second one is to use an infected Cortana to transmit a fake recording of the user's voice to other computers with the same AI and order it to enter the websites desired by the criminals. Hackers will be reporting their new findings on Kaspersky Security Analyst Summit taking place in Cancun in March 2018.

The security flaws in AI software such as Cortana, Alexa or Siri pose a severe threat in the Internet of Things (IoT), as their network connectivity enhances their capabilities and the potential risks. If the AI is compromised, the rest of the network will likely be endangered as well. Pinkerton advises all clients utilizing Cortana to enable "respond only me" option so that the AI will only follow its owner's instructions. Furthermore, clients must update their antivirus databases, avoid entering unsafe web pages, and remain on the lookout for software patches and updates released by Microsoft.

Sensitive Information Stored On Browsers At Increased Risk

Per reports, a researcher at the cyber-security firm Exabeam found that users generate personal data on browsers, being dubbed as the user's "web dossier," which can be misused for targeted attacks.

During the study, the researcher found evidence that 56 websites recorded geolocation information and 56 websites recorded the IP address of the user. The websites studied were commonly used platforms including Google, YouTube, Facebook, Reddit, Amazon, and Twitter. Further, traces of user interaction get left behind on the browsers including browsing history, search queries, email addresses, and files seen or downloaded. Such information can be utilized for the identification and profiling of secure users in targeted phishing attacks. Additionally, information stored for automatic form completion as well as passwords in internal password manager make personally identifiable information (PII) vulnerable. In this regard, the researcher notes that the recent Olympic Destroyer malware used to disrupt the PyeongChang 2018 Olympic Winter Games "took advantage of user credentials saved in the browser."

Pinkerton assesses that there is a high threat of cyber-attacks and leaks of confidential information through browsers. Further, since malware detection systems mostly look for signs of large-scale data exfiltration, small-scale data operations go unnoticed which further increases the threat. As a basic precautionary measure, clients are recommended to use virtual private networks (VPN) to protect geolocation information. Further, by using incognito mode or manually deleting browsing history from the browser, some of the information can be protected from being stored. Researchers also recommend using third-party separate managers for passwords instead of the internal password manager.

Human Rights Groups Report Delays Spyware Claims

In recent days, human and digital activists reported to the media that the investigations regarding smartphones infected with spying software had not been properly addressed by the Mexican Government.

According to local sources, in June 2017, a group of activists filed a complaint with the Attorney General's Office. They claimed the government infected their phones to spy on them with a software known as Pegasus. Although the Mexican president, Enrique Pena Nieto, requested the authorities to investigate the charges, no significant or relevant progress has been made since. Finally, media reported that the group formed by the Miguel Agustin Pro Juarez Human Rights Center (Prodh), human rights advocacy group Article 19, Mexicans Against Corruption and Impunity, and digital rights group R3D, has already asked for an independent investigation.

Pinkerton assesses that even if the allegations of espionage by the Mexican Government have not been proven truthful, businesses operating in the country are encouraged to manage a high level of cybersecurity tools to protect their privacy and sensitive information. Latin American countries might not have a strong cultural awareness regarding cyber threats and espionage through mobile devices such as smartphones; becoming an easy target for hackers and criminals. To avoid becoming the target of a mobile device attack, it is advised not to open unrecognized SMS or emails with suspicious links on them, do not download uncertified mobile applications on the mobile devices, and do not store sensitive data in smartphones. Any suspicious activity must be reported to the IT department or telecom company.

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