CYBER SECURITY BRIEFING

A Monthly Recap of Technology & Information Risk

PINKERTON®

MAY 2018

New Crypto Currency Mining Malware Also Disables Security Services

During April 2018, Fortinet Cyber Security Company discovered a new cryptocurrency miner named Monero that not only allows attackers to use the infected computer to mine the cryptocurrency but also disables the cybersecurity services.

Monero or PyroMiner is downloaded as a zip, and once inside, it takes control of the Remote Desktop Protocol, a protocol that allows a computer to connect with another one over a network connection, and modify the firewall to allow the malware to get through. The attackers can now block Windows Update, disable the rest of the cybersecurity defenses, and keep installing malware on the victim's computer. So far, PyroMiner only attacks Windows-powered computers, and it spreads using the EternalRomance exploit, a flaw in Windows coding patched by Microsoft in March 2017.

Pinkerton considers likely that the malware will spread faster in the following months due to the number of users who have not updated their Windows operating system. On February 4, 2018, Tripwire Cyber Security Company published an article stating that EternalRomance, EternalSinergy, and EternalChampion exploits had been updated and now could efficiently spread through Windows 2000 to 2016 operative systems. Pinkerton advises all clients to update their antivirus database and Windows operative system. Additionally, it is recommended to avoid entering untrusted web pages and remain attentive to Windows announcements regarding software patches and updates.

LinkedIn Security Liability May Have Compromised Users' Personal Data

A security researcher from Lightning Security has reported that he discovered a security bug which made it possible for third parties to access users' data, including private information such as email addresses and phone numbers.

The bug was affecting the popular LinkedIn AutoFill plugin which automatically fills in some data from users profiles on approved third-party websites. Due to security reasons, LinkedIn only extends this functionality to websites that it has whitelisted, such as Microsoft, Twitter, and dozens of others. The problem appears when a website has an XSS bug, commonly referred to as cross-site scripting, as this enables an attacker to exploit the flaw and push malicious code on a domain, riding on the whitelisted website. According to the researcher who discovered this flaw, "LinkedIn states that this functionality is restricted to whitelisted websites; however, until my report, any website could abuse this functionality."

Even though LinkedIn has said that they have already fixed the bug and that they have not discovered any evidence of abuse, Pinkerton recommends clients who have used this function to be on the lookout for any suspicious activity related to their email or phone. LinkedIn users are also advised to take advantage of the strict privacy settings offered by the social network service, such as not to display their email address or their full name. Clients using Google accounts to access LinkedIn are advised to do a routine account security checkup and to assure themselves that they are currently using all of the security features made available by Google.

Untraceable Method To Unlock Electronic Locks Identified

On April 25, 2018, security researchers from F-Secure announced the conclusions of a 15-year study of the Assa Abloy's Vision by VingCard electronic locking system.

The study was spurred following the theft of a researcher's laptop during the 2003 ph-neutral hacker conference in Berlin. The theft occurred in a room secured by the aforementioned locking system and showed no signs of forced entry and no key log entries. The researchers discovered that any old or expired keycards from assigned to the system could be converted into master keys. F-Secure provided their findings to Assa Abloy in April 2017, and the two companies have worked together over the last year to create a solution. Assa Abloy has released a system update to correct the issue.

Pinkerton assesses that although there is only one known instance of an attack conducted by the method identified by F-Secure, it is likely that other similar incidents have occurred, especially when considering the Vision by VingCard system is deployed in over 160 countries and on millions of doors. While a system update has been issued, there is an additional likelihood that similar vulnerabilities exist in other electronic lock systems. Pinkerton advises clients who utilize electronic locking systems to ensure any security updates are installed and to report any "ghost" entries to system manufacturers to determine if similar vulnerabilities exist.

Necurs Botnet Uses A New Technique To Attack Victims

Per media reports on April 27, 2018, the world's largest spam botnet, Necurs, is using a new technique to attack victims.

Targeted victims receive an email with an archive folder attached; when opened, it gives access to a file with ".URL" extension. The link serves as a remote script file that downloads and automatically executes a final payload. This method varieties from previous and more advanced methods of cyber-attacks. The simplified infection chain permits the avoiding of email malware scanners.

Pinkerton finds that the threat of wide-scale spreading of the infecting email will continue in the near to medium term until the existing detection rules are updated to address the issue. Pinkerton recommends personnel not to open files received via email attachments if they don't recognize the sender address. Reportedly, in 2017, the world's largest spam botnet had a monthly bot population of 5 -6 million unique bots. With the new undetectable simple technique, Necurs is likely to increase its capabilities in the medium term; new malware distributed by the botnet are likely in the medium to long term.

Energy Ministry Website Encrypted By Ransomware

Per reports on April 24, 2018, hackers locked Ukraine's energy ministry's website by using a ransomware which forcibly shut down and encrypted the files on the website.

A ransom of 0.1 bitcoin worth about USD 927.86 (GBP 664.98) has been demanded in exchange for the encrypted files and restoration of the webpage. According to a government official, the attack is isolated and no other government website has been affected.

Pinkerton finds that the use of ransomware poses a significant threat to infrastructural functions in Ukraine, and notes that the country has been the target of a growing number of cyber-attacks in the recent past. Particularly, the energy sector has been a prime target in previous attacks; however, other important institutions, such as the financial system, have also been disrupted by targeted attacks including during the NotPetya attack in June 2017. Even though per the Ukrainian officials the impact of the recent attack is limited, Pinkerton assesses that the number of significant cyber-attacks in Ukraine showcases structural weaknesses in the cyber defense of companies and government departments with important societal infrastructural functions.

Ride-Sharing App Careem Hit By Cyber-Attack; User Data Stolen

Per reports on April 23, 2018, Dubai-based ride-sharing app Careem was hacked and data of at least 14 million users compromised in the Middle East, North Africa, Turkey, and Pakistan.

This was the first successful cyber-attack of this magnitude on the company's database, with personal information like email addresses, names, phone numbers, and trip data being stolen. The company said that there was no evidence of credit card details or passwords being stolen. The breach was detected on January 14 when the company was alerted to a message left behind by the hackers.

Pinkerton assesses that ride-sharing apps are likely to continue being targeted in the near to medium term. Increasingly, smartphone users in big cities across the world are using app-based cab services along with making digital payments. Client personnel using the services of Careem are advised to verify with the company whether their personal details were compromised. While the company claims that credit card details and passwords were not compromised, it is advisable to check the credit card statements for any discrepancies. Pinkerton recommends Careem users strengthen the security of their devices with strong passwords, and remain vigilant for any suspicious activity related to the payment method registered on the app. Pinkerton finds that the use of ransomware poses a significant threat to infrastructural functions in Ukraine, and notes that the country has been the target of a growing number of cyber-attacks in the recent past. Particularly, the energy sector has been a prime target in previous attacks; however, other important institutions, such as the financial system, have also been disrupted by targeted attacks including during the NotPetya attack in June 2017. Even though per the Ukrainian officials the impact of the recent attack is limited, Pinkerton assesses that the number of significant cyber-attacks in Ukraine showcases structural weaknesses in the cyber defense of companies and government departments with important societal infrastructural functions.

New Android Malware Distributed Through DNS Hijacking Technique Targets Smartphones

Per reports on April 17, 2018, a new Android malware is being distributed through the domain name system (DNS) hijacking technique that targets smartphones in Asia, according to cybersecurity firm Kaspersky Labs.

The malware named "Roaming Mantis" steals user information including the credentials that give the attacker access and control to the Android device. The malware was detected in nearly 150 networks in Japan, Bangladesh, and South Korea. The attackers target those routers that are vulnerable and distribute the malware through the hijacked DNS settings of the infected routers.

Pinkerton assesses that the malware is likely to continue targeting Android devices of those businesses in the near to medium term that have not taken adequate security measures to protect their routers. Client personnel are advised not to click on any link that claims to provide better browsing experience or update to the latest Google Chrome version without verifying the authenticity. Businesses are advised to regularly check their router's user manual to ensure that the DNS settings haven't been compromised. As a precautionary measure, do not install firmware for the router from third parties; update the router's firmware only from the official source.

Trustjacking Vulnerability Affecting iPhones

Researchers at Symantec Cyber-Security Company discovered a vulnerability affecting all iOS-powered devices.

The device is breached when the user connects the device via a USB cable to a computer and then selects the "trust this device" option, as this will enable the iTunes Wi-Fi Sync capability. From now on every time the user´s device connects to the same Wi-Fi network that the trusted computer, an attacker using the same network may access the iOS device. Once the devices are breached, the attacker will have access to the user's files, see what the device is doing in real time, and may also send malware that will eventually let him control the device even if it isn´t in the same Wi-Fi network.

Pinkerton expects the situation to continue since the iOS device user only confirms the trust device option one time and is not constantly notified and may have trusted multiple computers in different networks. Also, the user's personal computer may have been infected without him knowing it, and attackers may send malicious data to the device via its PC. Symantec communicated the flaw to Apple, and the company did a first approach to solving the problem by asking for the IOS device password before trusting any new computer. Pinkerton advises all clients to be careful and selective to which computers they connect their iOS devices, avoid plugging them in high-risk areas like Cyber coffees or public computers and to encrypt sensible data located in the device.

Survey Finds That Organizations Are Struggling To Appoint Cyber-Security Personnel

According to a survey done by the independent nonprofit organization ISACA (Information Systems Audit and Control Association), over 50% of organizations surveyed had vacant cyber-security positions, mainly because of the available applicants lacking the adequate skills.

The survey also found that 30% of employees, who work in the field of information security, believe that only one in four of their colleagues is qualified. The report concluded that organizations need to invest in automation and their hiring processes to improve.

Pinkerton finds that insufficient cyber-security capabilities are a significant operational risk for all sectors, but primarily for clients with a focus on digital information. Clients are advised to consider operational implications of this such as breaches and data theft and plan for contingencies accordingly. Further, for the time being, cyber-security organizations are not only battling threat actors that are quickly evolving, but also new legislative challenges, such as the European Union's General Data Protection Regulation (GDPR) that will be enforced on May 25, 2018. Pinkerton assesses it likely that organizations will continuously find it challenging to find the right competence in candidates for cyber-security positions. Continuous training of existing personnel can mitigate the operational risk; however, this solution may require cyber-security organizations to grow to maintain operational capability.

Cyber-Security Law Introduces Stricter Regulations For Online Content

Per reports on April 12, 2018, the government of Tanzania has voted in favor of new cyber-security regulations under the Electronic and Postal Communications (Online Content) Regulations 2018.

As such, the government is introducing stricter regulations of online content by forcing online media channels and bloggers to pay a registration as well as annual fee to operate their websites. Reportedly, operating a personal blog will cost around USD 900 (EUR 729.5) per year. It will also be illegal to post material that is considered by the government as "indecent, obscene, hate speech, extreme violence or material that will offend or incite others, cause annoyance, threaten, or encourage or incite crime, or lead to public disorder." Unless such material is removed within the timeframe of 12 hours from identification, the publisher will be subject to high fees or even up to a year in prison. Further, social media users will be under scrutiny in an effort to regulate morals and ensure the authenticity of users. For example, the regulation instructs internet cafés to install surveillance cameras and online platforms to record activities of users. All Tanzanians who utilize mobile devices will also have to set a password for their phones or face high fees or even prison charges.

Pinkerton finds that the tighter restrictions on online content are likely introduced as a measure to limit political opposition and mobilization of critics in Tanzania and is likely to have a negative impact on the accessibility and sharing of information online. Even though the government's argument behind the restrictions is to increase cyber-security, Pinkerton finds it likely that the restrictions will have a repressive effect on free speech. Furthermore, Pinkerton assesses that the new regulations likely will have a negative impact on bloggers and small and medium-sized businesses in the immediate to long term. The high registration and annual fees will likely exclude small and new businesses or bloggers from online platforms and thus reduce online diversity.

Microsoft Vulnerability Allows Hackers To Steal Personal Information

On April 12, 2018, a security investigator of the CERT Coordination Center disclosed a vulnerability of Microsoft Outlook.

According to the report, this could allow hackers to steal sensitive information – including Windows user's login credentials, just by convincing the victims to preview an email with Microsoft Outlook without requiring any additional interaction. It was also informed that this vulnerability resides within an incomplete patch that was recently released by the company after receiving a disclosure report about the possible security breaches 18 months ago. Additionally, the CERT announced that when the passwords are not complex enough, the attackers tend to be easily able to crack them in a short amount of time.

Pinkerton recommends all clients with Microsoft Outlook accounts to change their passwords as soon as possible and keep changing them periodically. To create a complex password it is recommended that it has a minimum of 12-14 characters in length; includes a mix of capital letters, lower-case letter, symbols, and numbers; is not an obvious dictionary word, and does not rely on obvious nor common substitutions. Furthermore, it is advised to install the new security patch as soon as Microsoft delivers it in order to prevent Outlook from automatically initiating SMB connections when it previews in emails. Finally, Pinkerton strongly encourages clients never to click on links provided in suspicious emails.

On April 10, 2018, information from researchers with technology threat detection company Bastille became available.

The researchers have identified a new threat vector involving insecure radio frequency (RF) communication protocol controls of public emergency threat (siren) systems, dubbing the threat "SirenJack." The vulnerability involves emergency alert systems that ATI Systems has installed in industrial and military facilities, as well as universities and large cities. Bastille reports that RF communications used to send commands to outdoor warning

systems are not encrypted. After identifying a targeted siren's radio frequency, an attacker can send the system a command patterned on legitimate commands and activate that siren. Bastille notified ATI Systems of the vulnerability prior to releasing the findings to the public; reportedly ATI Systems has assured that its new systems encrypt the RF communications. The Bastille researcher's initial discovery involved the 14-year-old warning system in the city of San Francisco.

While newer ATI warning systems set up in government, university, military, and municipal environments likely cannot be hacked and activated by malicious attackers, Pinkerton finds it likely that the majority of the ATI emergency warning systems in use in the U.S. are older – and likely vulnerable. The point at which ATI Systems changed the radio communications from unencrypted to encrypted is not known, which raises questions regarding SirenJack capabilities for all but the newest installations. Further, it is not yet known whether the emergency warning systems produced by other companies have the same or similar flaws. Second order consequences of SirenJack attacks likely would include public panic, accidents, unavailability of EMS and law enforcement first responders for other emergencies.

Coalition Complains About Children's Data Violation by YouTube

On April 8, 2018, a coalition filed an official complaint with the U.S. Federal Trade Commission (FTC) stating that YouTube violated the Children's Online Privacy Protection Act (COPPA) by collecting data without parental consent on children who use YouTube.

The coalition is composed of 20 groups centered around child advocacy, privacy, and consumer groups. Location and the type of device used to access YouTube are among the personal information collected without authorization. The coalition wants the FTC to investigate YouTube for violating internet privacy laws designed to protect children. Google owns YouTube and would be held responsible for paying the potentially large fees if the FTC conducts an investigation and concludes YouTube violated children's online privacy. The full text of the complaint can be viewed at: http://www.commercialfreechildhood.org/sites/default/files/devel-generate/tiw/youtubecoppa.pdf.

The complaint, even without an established investigation, will likely reinforce the current public sentiment concerning individual data protection. Brand reputation will likely be negatively affected. Public support for more regulation regarding online privacy and personal information will likely increase, which would likely further affect businesses who handle personal information. Pinkerton recommends businesses monitor the FTC response and YouTube response to the complaint.

New Malware Spreads As Fake Browser Update

Per reports on April 11, 2018, a new malware spreads through hacked websites as a fake browser update.

According to cyber-security researcher Malwarebytes, the new malware is spread using new sophisticated techniques through online websites with a modified JavaScript that loads a malicious payload on the system. The JavaScript files on the hacked websites are replaced or modified by the attackers to target the visitors to the site. A fake update notification pops up when the user visits the infected website that spreads the malware. Once infected by the fake update campaign, the system runs the Chtonic banking malware, a variant of ZeusVM.

Pinkerton finds that the malware is likely to target businesses that visit websites that use the Squarespace, Joomla, and WordPress content management systems in the near to medium term. Client personnel are advised to be cautious when they receive a browser update notification. Once the user permits the update, the script analyzes the target system, giving the attacker access to deliver the actual payload. Client personnel are advised to take adequate precautionary measures for their systems as accepting the browser update notification will give the attacker full control including remote access to the system and file transfer.

U.S. Government To Require Social Media History With Visa Applications

On March 30, 2018, the U.S. Department of State issued a formal publication notice, regarding the government plans to require almost all visa applicants to the U.S. to submit their social media history.

The new change to visa applications would require those applying for visas to submit five years of social media handles for specific platforms as well as previous phone numbers, email addresses, prior immigration violations, and family history of involvement in terrorist activities. The move follows U.S. President Donald Trump's administration's emphasis on "extreme vetting" of immigrants to the U.S. The Department of State estimates the new process would affect almost 15 million applications, including those who apply for business trips, students, and vacation. A 60-days for public comment on the new process began on March 30.

Although courts struck down the first two versions of President Trump's travel ban, the new process has a narrower scope and the court will likely consider its legality in the spring. Even if implemented in some form, Pinkerton assesses that the new process will likely face immediate challenges by concerned groups, and be tied up within the U.S. judicial system, likely resulting in delayed implementation over the long-term. The new process will

likely be criticized, especially by privacy and civil liberties advocates. Protests over the new process are likely in the short- to mid-term. If passed, the new process would likely limit legal immigration to the U.S. and slow the visa process down, making it more difficult to be accepted. In return, it would likely affect foreign clients traveling to the U.S. Pinkerton further assesses the implementation of the new process would likely affect clients who rely on foreign employees finding qualified candidates. Pinkerton further assesses this new move would highly likely deter qualified candidates from applying to or desiring to move to the U.S. due to the onerous process.

European Commission Preparing Policy Crackdown On "Online Disinformation"

Per reports on April 1, 2018, the European Commission (EC) is planning to issue a warning to social media companies regarding "online disinformation" or "fake news" by publishing its first policy on the issue later this month.

The development comes in the wake of increasing reports of "fake news" and especially the recent Cambridge Analytica scandal involving Facebook, which per the EC "threaten to subvert democratic systems." Further, various countries including France and Germany have taken cognizance of allegations of Russian interference in European elections over the past year by drawing "anti-fake news laws."

Several European commissioners involved in the development of the proposal have highlighted that the greatest threat to cyber-security is increasingly focused on "deploying cyber-means to manipulate behaviour," social divisions, and subvert and question democratic processes and institutions. In particular, the EC is keen on developing a clear process for social media companies to operate during "sensitive election periods." In this regard, the May 2019 European Parliament polls have been identified as "vulnerable to mass populist and Eurosceptic online disinformation." It is so far unclear what the policy will entail; however, per indications, it is likely to focus on requiring greater transparency on the internal "black box" algorithms used by tech companies to promote information, limits on psychometric targeting of users by "harvesting" their personal information for political ends, and disclosures on the funding channels of "sponsored content" on social media platforms.

Pinkerton finds that the development underscores the trend of heightened regulatory controls on the use of personal information for targeting social media content and corporate branding in Europe; an issue that is likely to remain prominent in the long term especially given the ongoing focus on the General Data Protection Regulation (GDPR). As with other regions that have increased regulatory controls on online disinformation, such as Indonesia (as indicated in the Pinkerton Insights Intelligence Brief on January 4), Pinkerton notes that there are concerns of this curbing free speech and legitimate political criticism. Nonetheless, Pinkerton assesses it highly likely that the "zero accountability" nature of social media platforms is likely to record credible changes in the medium term, requiring strict compliance reviews to ensure business continuity and development, especially to protect brand reputation and competitiveness. Clients with investments tied to the sector are recommended to monitor developments and seek legal counsel in assessing the likely changes in the medium to long term, as these will affect the marketing, technical, and operating security of businesses.

Several Local Government Websites Hacked

Per reports on April 4, 2018, several Israeli websites have been breached by the hacker Darkcoder.

Per reports, the websites of several municipalities, the Israeli Opera, and the Teachers Union were hacked to display images stating "Jerusalem is the capital of Palestine" and "Zionists can't stop me." The cities of Eilat, Acre, Kfar Saba, Netanya, Gan Yavne, Or Yehuda, Nesher, and Givat Shmuel were affected in this cyber-attack. Per cyber-security experts, the attack is a part of the annual "OpsIsrael" campaign that has previously targeted websites and social media accounts of the Israeli government.

Pinkerton finds that the breach of Israeli websites by pro-Palestinian hackers is likely to continue in the near to medium term, especially during the "March of Return" that is scheduled to continue until May 2018. Further, Pinkerton finds that the cyber-attack underscores the threat of fake news spreading through such data breaches which could considerably escalate tensions in conflict zones such as the Gaza Strip.

Pinkerton notes that the "OpsIsrael" campaign is an annual cyber-attack against Israel that takes place on April 7 every year. Though it is likely that the hackers may have attacked early this year due to the ongoing protests in the West Bank as was highlighted in the Pinkerton Insights Intelligence Brief on April 2, there is an even likelihood of another cyber-attack on April 7. Businesses in Israel and pro-Israeli organizations worldwide are recommended to exercise heightened caution in the immediate term; further attacks are also likely on May 15 which is commemorated as the anniversary of Nakba, the founding day of Israel in 1948.

HiddenMiner Malware Can "Potentially Fail" Devices

Per reports on April 1, 2018, the newly discovered malware "HiddenMiner" can destroy Android devices and make it almost impossible to uninstall.

The malware mines for Bitcoin alternative Monero by using Android devices. It is similar to the Loapi malware discovered in 2017 that used a phone's processor and strained it to an extent that it almost caused the device to explode. The new malware strain that was discovered by the cyber-security firm Trend Micro is found in third-party app marketplaces, posing as a legitimate Google Play update app. While the malware has so far targeted China and India, it is likely to spread to other countries.

Pinkerton assesses that the new malware is likely to continue targeting businesses in India and China in the near to medium term. With India and China being the leading contributors to the global app economy, the attackers have been targeting users in these countries due to the boom in the usage of Android devices. Client personnel downloading applications on Android devices are recommended to exercise caution as most of these applications are found in Google Play Store. Businesses using operating systems older than Android 7.0 version are more vulnerable to the malware as it takes advantage of a bug found in the older versions. Client personnel whose devices are infected are advised to be more cautious with the permissions granted to applications as the malware, in this case, may lead to the affected device overheating and potentially exploding.

Apple iOS Camera App Bug Detected

On March 24, 2018, Infosec Security Corporation announced that it discovered a bug in the Apple iOS Camera QR-reader that may be turned into a vulnerability.

The problem is that the QR-reader parser, which is the tool that analyzes the structure of a URL, doesn't recognize the URL when it is set into a specific format (e.g., https://xxx\@facebook.com:443@infosec.rm-it.de/) and it redirects the user to a different webpage. This bug can be exploited in such a way the QR-reader sends a user to a malicious website while making him believe that it is redirecting him to the desired one.

Apple has not made any announcements regarding this matter, but Pinkerton considers it likely that the problem will be fixed in the following software update. On March 2017, the chairman of iFlytek, a cloud service provider, stated that nearly 23% of the Trojans and viruses are currently being transmitted by QR because it is very easy to implant them into such codes. Clients must avoid using the QR-reader for the time being until the bug has been fixed, especially with web pages requiring sensible data such as banking web pages. Clients are also advised to always be on the lookout for software patches and updates which often solve security flaws such as this one.

Crypter Services Used To Avoid Detection

Per reports on March 27, 2018, cyber-security experts from Trustwave found that the jRAT backdoor uses crypter services hosted on the dark web to avoid detection.

The jRAT malware, also known as Adwind, AlienSpy, Frutas, Unrecom, and Sockrat, is a Remote Access Trojan (RAT) that has reportedly affected over 50,000 users between 2013-2016; per reports, the malware has once again started affecting systems worldwide and presents an ongoing threat. By utilizing the jRAT backdoor, cyber-attackers can remotely control the infected system, thereby capturing keystrokes, exfiltrating credentials, taking screenshots, and accessing the computer's webcam. Per Trustwave, the malware is distributed through phishing emails that contain an attachment or a link; the emails are sent as invoices, quotation requests, shipment notifications, remittance notices, and payment notices.

Pinkerton finds that the study by Trustwave underscores the threat of cyber-attacks that use unique malware obfuscation methods. While cyber-security authorities worldwide are undertaking efforts to detain those using crypter services, Pinkerton notes that measures to circumvent these attacks are minimal given the anonymity of the malware. Nevertheless, personnel are recommended to practice heightened caution when accessing emails from unknown sources as they are the most common method of sending malicious links.

Boeing Hit By WannaCry Attack

On March 28, 2018, the Boeing Company was hit with a WannaCry virus attack at their Charleston, South Carolina manufacturing plant.

The first reports coming out of Boeing were calling for "all hands on deck," and said that the 777 program might have gone done due to the attack. However, later in the day, Boeing issued a statement concerning the attack which stated that the vulnerability was limited to only a few machines in their Commercial Airplanes division and that none of their programs, including the 777 program had been interrupted by the attack. The vulnerabilities were solved by deploying software patches. The Boeing Company stated that their military programs were not affected by the virus.

Pinkerton assesses it likely that other companies will fall victim to WannaCry attacks in the near-term. While there have been patches published which can help fix the vulnerabilities that allow for successful WannaCry attacks, the success of the patches is dependent on companies ensuring that they are installed on all of their devices. Pinkerton recommends clients ensure their Windows devices are current on all updates and patches to increase their cyber-crime prevention practices. Pinkerton also recommends clients maintain a running inventory of all software and devices on their networks to make it easier to identify compromised systems.

Critical Vulnerabilities Discovered In Telecontrol Products

On March 28, 2018, automation company Siemens notified customers of critical vulnerabilities found in some telecontrol and building automation products as well as some SIMATIC systems affected by a high severity flaw.

One advisory published by Siemens discusses several critical and high severity flaws that affect Siveillance and Desigo building automation products. The flaw stems from a vulnerable version of Gemalto license management system (LMS). The vulnerability affects Gemalto Sentinel LDK, which can be exploited for remote code execution and denial-of-service (DoS) attacks. The company also warned that building automation products were also impacted, including Siveillance Identity and SiteIQ Analytics, and Desigo XWP, CC, ABT, Annual Shading, and Configuration Manager. In a separate advisory, Siemens indicated there was a critical vulnerability affecting TIM 1531 IRC. This is a communication module that connects remote stations based on SIMATIC controllers. A third advisory published describes a high severity flaw in SIMATIC PCS7, SIMATIC NET PC, SIMATIC WinCC, and SIMATIC WinCC Runtime Professional products. This vulnerability allows attackers to cause a DoS condition on the products by sending a message to the RPC service. However, Siemens has made patches and mitigations available for the affected systems.

Due to the vulnerable Gemalto product, it is likely that millions of industrial and corporate systems were exposed to remote attacks. Clients that use any of the affected telecontrol and building automation products are likely vulnerable to exploitation. Any attacks would likely affect building systems such as heating, ventilation, lighting, and others, which would likely affect overall building security. As building automation products become more popular, malicious actors will likely attempt further attacks on these devices. Pinkerton recommends clients limit access to the ports in the network infrastructure by using firewalls to reduce the risk or protect network access to devices. Pinkerton also advises clients to apply cell protection concept, use a virtual private network (VPN), and ensure recent patches have been installed and are up to date.

FTC Launches Official Investigation Of Facebook Privacy Practices

On March 26, 2018, the U.S. Federal Trade Commission (FTC) confirmed that it had initiated an official investigation into social media giant Facebook's privacy practices following a data breach that affected 50 million users.

News of the breach surfaced publicly on March 17, 2018, when multiple major news media outlets reported that conservative data mining firm Cambridge Analytica had illegally harvested Facebook user data for the purpose of developing "psychographic" profiles and personalizing advertisements for U.S. President Donald Trump's 2016 campaign. Facebook CEO Mark Zuckerburg, who denies culpability and alleges that Cambridge violated information privacy agreements made between both parties, has been asked to testify at a Senate Judiciary Committee hearing on data privacy scheduled for April 10, 2018; the CEOs of Twitter and Google have also been invited to testify. The hearing will examine how consumer data is gathered, distributed, and stored by companies like Facebook, as well as explore proactive measures those companies can take to mitigate the risk of future breaches.

Pinkerton assesses that as data mining technologies become increasingly sophisticated, corresponding consumer data protection regulations are an inevitable emergent. In 2016, the European Union passed the General Data Protection Regulation, which will go into effect on May 25, 2018; future breaches like the one currently being investigated would cost Facebook approximately EUR 1.3 billion (USD 1.6 billion) in fines under the new law. U.S. officials have been more hesitant to impose such regulations, arguing that doing so would create barriers to commerce and stifle much-needed economic growth. However, although the U.S. may value liberty at the expense of security more than some nations, a threshold does exist. While digital marketing tools like Google Analytics have been utilizing similar data sets to calibrate advertising for the last several years, the stakes feel strikingly more ominous when that data could influence political outcomes. As such, the Facebook-Cambridge Analytics scandal is likely to provide the impetus for the public pressure that will urge legislators toward a new frontier in U.S. data privacy.

AVCrypt Ransomware Tries To Uninstall Security Software

Per media reports on March 23, 2018, the newly discovered ransomware called AVCrypt tries to uninstall existing security software before encrypting files on the targeted computer.

Further, the ransomware attempts to delete a variety of Windows services, including Windows Update. However, it displays an alert before it starts executing the encryption and there are numerous debug messages. The malware does not leave contact information or instructions in a message attached to the encrypted file which is renamed by adding "+" before the original file name. Per reports, attacks by ransomware that similarly uninstalls antivirus software have been reported at a Japanese university.

Pinkerton assesses that the threat of AVCrypt ransomware is likely to increase in the medium to long term. According to the researchers, the debug messages and alerts indicate that the tool is still in the development phase. However, its malicious code can already be a threat for operating systems and expose users to irreversible data loss. Pinkerton assesses that the malware can be re-classified as a wiper instead of ransomware, depending on its further development. Wiper malware attacks are spread to wipe the hard drive of the targeted device. In 2017, users in several countries were infected by Petya ransomware which had been modified to act efficiently as a wiper.

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