CYBER SECURITY BRIEFING

A Monthly Recap of Technology & Information Risk

PINKERTON®

FEBRUARY 2018

New Trojan Targets Financial Data

Per Russian media reports on January 25, 2018, cyber-security firm Kaspersky Labs has identified a new trojan called Mezzo.

Reportedly, the trojan enables malicious actors to obtain victims' financial data, and could potentially be used to steal virtual and conventional currency by falsifying information in files exchanged between accounting and banking systems when using accounting software. It is believed that the trojan has the capacity to change account details just before a money exchange is about to take place. Thus the money will be sent to the malicious actor rather than the rightful owner. Experts say that the spread of Mezzo has solely been limited to Russia so far.

Pinkerton assesses it likely that malicious actors will increase the use of Mezzo in the near to medium-term. It is further likely that the trojan mainly will be utilized to hunt virtual currency. Even so, Pinkerton notes that when a computer has been infected, Mezzo has the capability of stealing multiple files from the victim's computer and may be employed to target other systems beyond accounting software. If proven successful, hackers are likely to target victims outside of Russia in the medium to long-term.

Rapid Ransomware Encrypts New Files Created

Per reports on January 23, 2018, ransomware is spreading that encrypts new files created after the system is infected; the "Rapid Ransomware" has been infecting systems since early January.

At least 300 cases of users infected by this ransomware have been confirmed; the actual number is likely to be higher. Once the ransomware starts running, it disables automatic repair, terminates database processes, and clears Windows shadow volume copies. After encrypting the files of a system, the ransomware creates ransom notes with the name How Recovery Files.txt. The victim is then asked to contact the email mentioned in the note to receive payment instructions.

Pinkerton assesses that Rapid Ransomware is likely to affected businesses in the immediate term, especially those who did not install the latest Windows updates when they were released. The older programs contain security vulnerabilities which can be easily exploited by the attackers. Users affected by the ransomware are recommended to immediately open the Windows task manager in their systems and terminate the ransomware process. After terminating the ransomware process, the users are advised to start msconfig.exe and subsequently disable the autoruns. In case the Windows task manager is not accessible, execute the termination after rebooting into Safe Mode with Networking. Pinkerton recommends the installation of anti-malware software that contains behavioral detection as it is likely to mitigate most ransomware infections. Further, clients are recommended to take data backups to ensure safety of data.

Software Licensing Tool Exposes Systems To Attack

On January 22, 2018, security researchers at Kaspersky Lab discovered over a dozen vulnerabilities in a software licensing solution from Gemalto.

The Gemalto Sentinel LDK, a USB dongle which installs licensing solution tokens on a system adds port 1947 to the exception list in the Windows Firewall and leaves the port open following use. Thirteen additional vulnerabilities were discovered, including some which allow for denial-of-service

(DoS) attacks, arbitrary code execution, and capture of NTLM hashes. Due to port 1947 being open, the flaws can be exploited remotely. Kaspersky researchers additionally discovered, that if the dongle was inserted into a locked machine, it would still open the port. The vulnerabilities were discovered between 2016 and June 2017. The delay in public disclosure of the flaws was due to Gemalto working with Kaspersky labs to create and implement fixes.

Pinkerton assesses that any client utilizing the Gemalto Sentinel LDK is at risk. Due to the now public knowledge of the port 1947 vulnerability, it is almost assured that malicious actors will gear attacks against industrial control systems and corporate networks towards exploiting the port vulnerability. In addition to the specific attack types mentioned above, cyber-attackers can likely tailor a variety of malware, including ransomware and trojans to be dropped into systems that are exposed. Pinkerton advises clients to monitor activity through port 1947, and ensure that the port is closed when not in direct use.

GhostTeam Malware Targets Facebook Credentials In Android Devices

Per media sources on January 18, 2018, Google has removed 53 applications from its Play Store after researchers at cyber-security firms Avast and Trend Micro discovered a new Android malware named GhostTeam, which targets Facebook credentials and pushes advertisements to infected devices.

According to sources, an infection could occur when a user installs legitimate application software, called a "dropper." The application then contacts a remote command-and-control server, which downloads secondary applications containing the GhostTeam malware. A second-stage application is downloaded using "fake security alerts" displayed via the legitimate application, thereby gaining access to administrator credentials and capabilities. Per reports, the source in infected devices has been traced to a Vietnamese IP address. The countries most affected are India, Indonesia, Brazil, Vietnam, Australia, and the Philippines.

Pinkerton assesses that such malicious cyber-attacks pose a more dangerous threat than anticipated in the near term. Since GhostTeam is reportedly capable of accessing administrator rights to a device, cyber-criminals can compromise sensitive data for professional purposes; the threat is even more severe if the device is connected to a company network. Further, its capability to gain access to Facebook log-in details, as well as a user's Facebook data, is a potential breach that poses physical risk to the user with regards to location and address. While Google has reportedly removed several applications that pose risks of GhostTeam infections, there is an even chance that the malicious entity may still be active on already-infected devices. Pinkerton notes that commonly used Android applications, such as QR code scanners, device cleaning applications, flashlight applications, and compass applications, are likely to be infected by the malicious entity. Per sources, it is advisable that users with such applications change their Facebook credentials immediately, and enable two-factor authentication.

Malware-Infected Messaging Apps Used For Espionage

According to a research report released by Lookout and the Electronic Frontier Foundation (EFF) on January 17, 2018, researchers have identified a malware-based spying campaign dubbed Dark Caracal, which the report terms "a prolific actor with nation-state level advanced persistent threat (APT) capabilities[...]"

While the campaign has targeted some personal computers, it primarily exploits mobile phones and tablets, with the infection vector using messaging apps and particularly secure messaging apps such as Signal and WhatsApp. By granting permissions in what appears to be legitimate messaging apps, individuals in business, government and politics, the military, law enforcement, journalism, and activism have provided Dark Caracal with access to data, cameras, and microphones on mobile devices. According to the report, researchers found indications that Dark Caracal may have been hosting numerous and far-reaching cyber-espionage campaigns that, in some cases, date back years. The researchers found that attackers have been able to capture audio, take photographs, pinpoint the devices' locations via internal GPS, and mine very large quantities of personal/private data.

As of the report's release, Dark Caracal has compromised smartphones and desktop computers used by individuals in the following countries: China, France, Germany, India, Italy, Jordan, Lebanon, Nepal, the Netherlands, Pakistan, the Philippines, Qatar, Russia, Saudi Arabia, South Korea, Switzerland, Syria, Thailand, the United States, Venezuela, and Vietnam.

Given the data-rich nature of mobile phones, Pinkerton finds it likely that Dark Caracal has mined email assumed to be secure, the full depth of contacts' entries, stored passwords and access codes, and corporations' proprietary information. The impact to companies likely extends to compromised trade secrets, which threatens brand and reputation protection. Pinkerton recommends that IT directors and managers read the full report (https://www.lookout.com/info/ds-dark-caracal-ty) to determine the full implications of this threat. Finally, companies that allow employees to use their mobile phones for personal use as well may need to reconsider their policies regarding what may be installed on company-issued devices.

New Vulnerabilities In Microsoft Office Allow For Zyklon Malware Distribution

On January 17, 2018, security researchers at FireEye released information on a new campaign to distribute Zyklon malware.

Zyklon has been known since 2016 and allows cyber-attackers to conduct multiple types of attacks including keystroke logging, password theft, cryptocurrency mining, and launching distributed-denial-of-service (DDoS) attacks. The new campaign targets insurance, financial services, and telecommunications sectors. The delivery mechanism for Zyklon in this campaign is to attach a zip archive to a spam email. A word document within the zip file contains a Microsoft Word document which exploits CVE-2017-8759 to execute a PowerShell script which downloads the final portion of Zyklon from a remote server. Additionally, Zyklon is delivered by exploiting a vulnerability that dates back to 2000, CVE-2017-11882. The first flaw has been exploited by cyber-actors linked to China and used to target U.S. targets, while the second flaw has been exploited by Iranian-linked state actors and the Cobalt hacking group among others. A final flaw which has been exploited is the Dynamic Data Exchange (DDE) feature in Office. The two CVE flaws both have patches, and the final flaw has resulted in Microsoft disabling the DDE feature.

The far-reaching capabilities of Zyklon make it an extraordinary threat to users. The capability to log keystrokes and steal passwords can allow cyber-attackers to gain access to systems, while the capability to launch DDoS attacks and mine cryptocurrency can slow down systems and reduce productivity throughout networks. Pinkerton advises clients to ensure that systems all have the most recent patches installed, as well as ensuring that updates are run to anti-spam/anti-virus/anti-malware software systems. Pinkerton recommends that clients also ensure that server policies are in place to mitigate spam email reaching users on the network, as well as reinforcing training for users on identifying phishing emails.

Cryptocurrency Miners Intensify Attacks

Per reports on January 17, 2018, hackers are attacking computer systems by using a malware called "RubyMiner."

Through this malware, hackers infect computer systems with the cryptocurrency miner, XMrig. Per reports, hackers send a base64 encoded payload inside a POST request; the system is affected once the administrator accepts and executes this request. So far, the attacks have primarily been targeted at Linux and Windows servers. Per reports, the attacks utilizing the RubyMiner malware have been ongoing since January 10; the frequency and rate of the attacks are reportedly increasing. The attackers were able to scan 30% of networks worldwide within a 24-hour period last week. Reportedly, the top-targeted countries are Germany, Norway, Sweden, the UK, and the U.S.

Given the increasing number of transactions performed using cryptocurrency, Pinkerton assesses that clients are likely to be under an increased threat from cryptocurrency miners in the medium to long term. Pinkerton finds that Internet-based transactions are at risk through these attacks. Businesses with operations using cryptocurrency are likely to experience operational disruptions due to this threat. Pinkerton notes that over 700 servers have been reportedly infected due to the RubyMiner malware so far. However, this malware attacks systems that have an outdated software as compared to other cyber-attacks that are concentrated on more recent software. Thus, updating the device software is crucial in order to avoid this malware.

Lenovo And IBM Switches Vulnerability Found

Per reports on January 15, 2018, a flaw that could be used as a backdoor has been identified in switches manufactured by Lenovo and IBM that runs the Enterprise Network Operating System (ENOS).

The affected switches are Flex System, RackSwitch, and BladeCenter. The vulnerability, also known as an "HP Backdoor," was identified during a Lenovo security audit, which could allow access to the admin interface of the switch. An attacker would, however, need to perform a local authentication and use credentials that are unique to each switch.

Pinkerton advises clients who are implementing Lenovo and IBM Switches in their IT infrastructure to install the latest security patch provided by the manufacturer to eliminate the backdoor. Per the official report by Lenovo, the vulnerability can be exploited only under limited circumstances. However, Pinkerton assesses that since the issue allows admin-level access, it should be interpreted as severe. Clients who are unable to install the recommended firmware are advised to restrict access to switches.

MaMi Malware Threatens Mac Users By Hijacking DNS Servers

On January 12, 2018, more information was released on security researcher Patrick Wardle's finding the first found Mac malware of the year.

The malware called "MaMi" persistently hijacks the Domain Name System (DNS) server, changes the settings to 82.163.143.135 or 82.163.142.137, and sends the Mac user to possibly malicious websites. Currently, MaMi appears to be a work in progress, and all of the possible malicious features have not been activated, though Wardle does not believe he found every feature yet. Wardle found indication MaMi could install local certificates, take screenshots, download and upload files, steal passwords, and more if activated. Wardle's best guess for how it gets on a Mac is through malicious email, fake popups, or social engineering.

MaMi threatens the cyber-security of businesses who use Mac computers, especially if the additional and likely malicious features activate. Taking screenshots of sensitive business information, stealing passwords, and downloading files threaten the safety of sensitive information and trade secrets. Pinkerton advises business Mac computer users to check if they have been infected. Check the DNS server settings and verify if 82.163.143.135 or 82.163.142.137 appear. If it does, Pinkerton advises changing the settings and frequently checking them in case MaMi persistently appears. Pinkerton recommends businesses immediately refresh employees on standard safety practices while on work computers such as not opening attachments or clicking links from unknown sources, not clicking on fake popups, and not giving away log in usernames or passwords.

Malware Campaign Targeting 2018 Winter Olympic Games

According to McAfee Labs, a fileless malware campaign backtracked to Singapore is targeting entities associated with South Korea's 2018 Winter Olympic and Paralympic Games in Pyeongchang.

As of January 8, 2018, identified targets all are based in South Korea and provide support and infrastructure for the upcoming games. The hackers behind the campaign deliver the malware with Korean-language phishing emails presented as an official warning from the South Korean National Counter-Terrorism Center (SKNCTC). The email has an attached .docx file named 'Organised by Ministry of Agriculture and Forestry and Pyeongchang Winter Olympics' (English translation), and advises the recipient to click on Enable Content to view the document with their version of Microsoft Word. Doing so runs a Visual Basic macro that triggers a PowerShell script to download an image file containing another PowerShell script embedded there with the new steganography tool, Invoke-PSImage. The second PowerShell script creates a backdoor, from the computer's RAM. The email vector is not a new delivery method, but according to a McAfee analyst, "This particular malware has not been seen before and it is something custom that was created by the attacker." The attack campaign began just two days after Invoke-PSImage was released, on December 20, 2017.

While the phishing email delivery method has been addressed by tech-security researchers and consultants for over a decade with continual reminders not to open documents or click links in email from unknown or suspicious senders, Pinkerton assesses that the urgency of the rapidly approaching Olympic Games will lead many to open an incoming email from the SKNCTC without question or scrutiny. As such, Pinkerton assesses the threat to all government agencies, national Olympic teams, and corporate sponsors as high. Further, as fileless malware contain no identifiable code or "signatures" that anti-malware tools detect, anti-malware filters on corporate and organizational email servers do not yet provide any protection from this new threat vector. Pinkerton recommends that all corporations and organizations associated with the 2018 Olympics reinforce the high necessity for all personnel involved to take the time to scrutinize all incoming email pertaining to the Games. Finally, Pinkerton finds it highly likely that skilled state and non-state cyber-attack organizations will adopt this new method moving forward.

Survey Finds Industrial Firms Increasingly Targeted In Cyber-Attacks

On January 5, 2018, the Kaspersky IT Security Risks Survey was released. Of the 962 industrial firms who participated in the survey, 28% said they had been the victim of a targeted cyber-attack during 2017, an increase of 8% over 2016.

Additionally, 50% of the industrial firms surveyed said they had been the victim of a malware attack in 2017. Speaking on the findings, Kaspersky said, "The fact that the most dangerous incident type has grown by more than a third strongly suggests that cyber-criminal groups are paying much closer attention to the industrial sector." Approximately 30% of the targeted firms took several days, and 20% took several weeks, to detect a cyber-attack.

Pinkerton assesses that industrial firms are increasingly being targeted in cyber-attacks because they typically cannot easily shut down network operations to prevent the malware from spreading, making cyber-attacks potentially more effective. The severe delay in detection noted in the study suggests that many industrial firms lack the necessary cyber-security infrastructure to detect and deter cyber-attacks. Pinkerton recommends that clients in the industrial sector ensure their employees' strict compliance to company cyber-security procedures and employ a managed security service provider (MSSP) to monitor their network and ensure that proper firewalls are in place to combat cyber-attacks.

Flaw In Messaging Apps Permits Unauthorized Group Members To Be Added

Per reports on January 11, 2018, a flaw in the end-to-end encryption services of instant messaging apps such as WhatsApp and Signal could be utilized to read group conversations covertly.

Reportedly, new group members can secretly be added by anyone controlling or manipulating the companies' servers without the knowledge or permission of the group administrator, thus allowing an outsider to read group conversations.

Through this vulnerability, Pinkerton assesses the risk to clients as moderate. Pinkerton notes that even though WhatsApp argues that a multi-user group will receive a notification when a new member is added, the aforementioned research study states that group management messages can be blocked to avoid sending a notification of the new member. Pinkerton also assesses that even if sent, the notification can easily be missed, posing a threat to clients using these services for official purposes. Businesses are recommended to exercise caution until both WhatsApp and Signal establish a mechanism to ensure that unauthorized persons cannot covertly add members.

Important Vulnerability Discovered In Adobe Flash Player

On January 9, 2018, Adobe published a security advisory in which it announced the discovery of a vulnerability deemed "important."

The vulnerability, CVE-2018-4871, is due to a computation that reads data past the end of a target buffer. This means that there is an out-of-range reading of internal data structure fields, which could open the door for attacks in which hackers could steal sensitive information that is leaked by the system. This vulnerability is present in Adobe Flash Player on Windows, Linux, and Mac machines, Google Chrome and Microsoft Edge, and Internet Explorer 11 versions 28.0.0.126 and earlier. Adobe announced, on January 10, that it has already rolled out a security patch that fixes this problem.

Pinkerton finds that the security advisory underscores the ongoing threat of out-of-range read vulnerabilities that affect the internal memory of technology devices. Similar vulnerabilities have been found in Microsoft and Huawei products in the recent past. Pinkerton advises clients to immediately update their Adobe Flash Player versions on all their platforms to rid themselves of this threat. They are also encouraged to agree to automatic updates as critical security updates are rolled out regularly through system updates. This is the first security patch for Flash Player rolled out by Adobe in 2018, but the second one regarding a flaw affecting all their platforms in the last two months. In December 2017, a security patch was rolled out to correct CVE-2017-11305, which was a "Business Logic" error bug of moderately dangerous vulnerability.

Hewlett Packard Recalls 50,000 Laptop And Mobile Workstation Batteries

Hewlett Packard (HP) is voluntarily recalling 50,000 batteries from laptops and mobile workstations sold in December 2015-2017.

The recall is taking place after HP received eight complaints of lithium-ion batteries overheating, melting, or catching fire. The batteries were both sold as replacements and included in the following laptop models: HP ProBook, HP x360 310 G2, HP Envy m6, HP Pavilion x360, HP 11, HP ZBook 17, and HP ZBook Studio G3. In response to the development, HP has launched downloadable software that automatically detects if the device's battery must be changed to prevent an accident.

Pinkerton finds that in the race to create new, more durable and efficient batteries, the number of malfunctions have increased substantially, resulting in the need for companies to recall their products regularly; this is HP's second recall in less than a year. Pinkerton advises all clients using the HP models listed above to download the software and verify that their batteries are working correctly. In case the battery must be changed, clients should contact HP instead of attempting to replace the battery themselves; a specialized technician will reportedly be sent to resolve the issue.

Microsoft Temporarily Halts Security Updates For Certains

Per reports on January 9, 2018, Microsoft has halted certain security patches for the Windows operating system after complaints from AMD customers that the software updates resulted in their systems presenting an "unbootable state."

Per reports on January 3, the chipset vulnerabilities "Meltdown" and "Spectre," for which the security patches were released, affect the processors developed by several companies. In a statement, Microsoft said that "some AMD chipsets do not conform to the documentation previously provided" to the company. AMD and Microsoft assured users that the issue will be resolved as soon as possible. The list of the temporarily suspended updates can be accessed here: https://support.microsoft.com/en-ca/help/4073707/windows-os-security-update-block-for-some-amd-based-devices; the list of affected devices from AMD is not yet available.

Pinkerton assesses that the chipset flaws are likely to make AMD systems vulnerable in the immediate to near term until the issue is resolved; clients are recommended to regularly monitor system updates and download them as soon as they are made available. As highlighted in the Pinkerton Insights Intelligence Brief on January 5, remote attacks using the Spectre flaw are possible using JavaScript; hence, clients are recommended to be cautious of JavaScript advertisements and popups in their browser, and not click suspicious links. Further, since the flaws allow processors to steal sensitive data that could target business secrets, clients are recommended to follow and disseminate cyber-security best practices in their organization.

Multiple Vulnerabilities Found In Online GPS Devices

In a report published on January 2, 2017, named "Trackmageddon," researchers claimed that they had found several vulnerabilities in online services of Global Positioning System (GPS) location tracking devices.

Per the report, unauthorized third parties have access to location data of such devices that are managed by "vulnerable online services." Access to data by potential cyber-criminals can be executed via weak passwords, exposed and unsecured folders, unsecured Application Programming Interface (API) endpoints, and insecure direct object reference (IDOR) flaws. Per the source, data such as location coordinates, contact numbers, International Mobile Equipment Identity (IMEI) numbers, serial numbers, media access control (MAC) addresses, and personal data, can be easily stolen, depending on the tracking service used, and device configuration. Experts involved in the report have been researching for several months and have concluded that over 100 tracking services have failed to acknowledge and patch the existing flaws in their services.

Pinkerton assesses that such a medium of technology, while having provided an array of conveniences, also continues to pose major threats that impinge on user-privacy. The vulnerability posed toward personal, and professional data that exists in an online database will continue to exist in the near-term, despite continuing efforts to patch the flaws. Further, considering that potential hackers can also access location coordinates, it could also pose physical security risks for a user's safety and security of physical assets. A security advisory was released for services that function on gpsui.net and vmui.net which can be accessed via https://0x0.li/trackmageddon/0x0-20171222-gpsui.net.html. The report also provides another security advisory that lists other services which may be insecure for use as listed in the following link: https://0x0.li/trackmageddon/0x0-20180102-gpsgate.html.

Cyber-Agency Launched To "Control Cyberspace"

On January 3, 2018, Indonesia launched a new cyber-security agency, the National Cyber and Encryption Agency (BSSN), to tackle online religious extremism and fake news on social media.

Indonesian President Joko Widodo appointed Major General Djoko Setiadi to head the agency. The decision comes amidst increasing cases of fake news being circulated on the Internet; in a high-profile hoax in December 2017, it was alleged that China was seeking to wage biological warfare against Indonesia. In a statement, Major General Setiadi said "we will control cyberspace … (and) not only be able to detect but also to penetrate (terrorist) networks."

Pinkerton assesses that the formation of the agency is in response to the persisting threats originating from cyber-space at a time of rapid increase in Internet usage in Indonesia. Per reports, Indonesia's Internet user growth rate is almost three times the global average, with a 51% growth year-on-year. The government has recognized the Internet as a medium for spreading terrorism and religious intolerance, and a means for hampering the democratic process through fake news. As highlighted in previous Pinkerton Insight Intelligence Briefs, the threat of terrorism in Indonesia and other Southeast Asian countries persists. According to a report by The Soufan Center (TSC), at least 1,568 individuals from the region have joined the Islamic State (IS).

Since the country is slated to conduct presidential and legislative elections in 2019, the agency aims to limit the impact of false information and curb the spread of religious intolerance. As a Muslim-majority country and democracy, Indonesia is concerned about the spread of religious intolerance; especially since Jakarta's Christian Governor Basuki Tjahaja Purnama, better known as Ahok, was charged with blasphemy against Islam in 2017 after repeated civil unrest. Pinkerton assesses that increasing restrictions on Internet activity raises privacy and security concerns for business entities and personnel. Clients are recommended to maintain official communication with the relevant agencies to ensure business continuity and secure proprietary data.

Google Apps Script Vulnerability Allows Automated Malware Downloads

Per reports on January 4, 2018, researchers at cyber-security firm Proofpoint discovered a vulnerability in Google Apps Script that would permit hackers to automatically download malware to files hosted on Google Drive.

Google Apps Script is a scripting language, which is used by developers to build web applications and automate tasks. Researchers found that hackers could have used triggers such as "onOpen" or "onEdit" to deliver the malware. Per reports, once the user receives the infected file and opens it, the triggers would cause the malware to be automatically downloaded to the device. Following the discovery, Google blocked "installable triggers" that enable developers to automatically start the installation of a program without user interaction.

Pinkerton finds that the Google Apps Script vulnerability underscores the threat of automated cyber-attacks, which do not require any input by the user, and the ongoing risks associated with cloud computing models. Even though, per reports, this vulnerability has not yet been exploited by hackers, Pinkerton finds that businesses that store information on cloud platforms are likely to be at risk. Further, as attacks on cloud computing models such as Software as a Service (SaaS) are increasing, firms are recommended to revisit their application and endpoint security protocols to protect their assets.

Hackers Expected To Remotely Exploit CPU Vulnerabilities

On January 4, 2018, multiple security researchers confirmed reports from The Register on January 2 regarding vulnerabilities in most Intel, AMD, and ARM processors.

The initial reports centered on Intel processors and their vulnerability to the flaw now known as Meltdown. The second flaw, known as Spectre, affects most processors currently in use. Meltdown was independently discovered by Jann Horn of Google Project Zero, researchers from Cyberus Technology, and a research team at the Graz University of Technology. Spectre was also found independently by multiple researchers including Horn, Rambus, Graz University of Technology, and the University of Adelaide. The flaws allow for side-channel attacks, which can insert malicious applications or code on a device to access data as it is processed. The data that can be accessed includes passwords, images, documents, emails, and instant messaging.

Both flaws cannot be fixed via firmware updates from manufacturers, and instead must be mitigated by updates and patches from operating systems and application producers. A patch known as Kaiser is being used to mitigate the Meltdown flaw. The Spectre flaw has far-reaching implications for cloud computing, leading to providers of cloud services such as Microsoft and Amazon developing their own patches to mitigate it. While patches can mitigate Spectre, they are expected to decrease processing speed by up to 30%. There is currently no evidence of malicious actors exploiting the flaws.

Pinkerton assesses that as the information regarding the flaws has become public, it is highly likely that malicious actors including nation-states will attempt to use the flaw to exploit computer systems. Clients utilizing cloud computing such as Amazon AWS3 or Microsoft Azure will be particularly vulnerable to the flaws and exploitation of data. With the primary attack vector being through local access, Pinkerton advises clients to ensure that measures are in place to prevent or mitigate insider attacks to computer systems. Remote attacks using the Spectre flaw are possible using JavaScript and WebAssembly. Pinkerton advises clients to ensure that any security updates or patches are installed as soon as available to mitigate both Meltdown and Spectre. Additionally, clients should adjust business plans to account for slower processing speeds that are likely to result from the patches.

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