CYBER SECURITY BRIEFING

A Monthly Recap of Technology & Information Risk

PINKERTON®

MARCH 2018

Cyber-Security Researchers Identify New Internet-Of-Things Botnet

As reported on February 15, 2018, cyber-security researchers with NewSky Security identified a new Internet-of-Things (IoT) botnet. The researchers dubbed this botnet "DoubleDoor" and observed attacks between January 18-27, 2018.

The majority of the attacks originated from South Korean Internet Protocol (IP) addresses. The botnet can bypass firewall authentication services on targeted devices and render other security measures "useless." This new botnet is using two exploits, CVE-2014-7755 (an exploit for Juniper Networks SmartScreen OS) and CVE-2016-10401 (an exploit for Zyxel modems). Through the first exploit, malicious actors can gain access to NetScreen firewalls by using a hardcoded password and any username. The other exploit, also using a hardcoded password, attempts a privilege escalation exploit to gain access to superuser permissions. NewSky Security also noticed that the botnet further monitors systems to ensure the success of the attack. This monitoring always uses a randomized string of eight characters that prevents devices from recognizing their malicious nature. The malware appears to mainly be effective if the victim runs an unpatched version of Juniper ScreenOS firewall and unpatched Zyxel modems, limiting the scope of the botnet to expand.

Pinkerton assesses that the number of attacks using this botnet to remain low over the medium-term. However, due to its ability to bypass authentication and security measures, Pinkerton assesses malicious actors will likely evolve its capabilities to expand the scope of attacks. Pinkerton assesses that malicious actors are highly likely to utilize the botnet of IoT devices in distributed denial of service (DDoS) attacks. Pinkerton recommends that clients, particularly those using the identified systems, operating IoT devices review policies and procedures regarding the updating of IoT security profiles. Pinkerton further recommends that clients operating IoT devices review the operations logs for the devices to monitor for suspicious activity, particularly those matching the eight-character strings.

Mac Trojan Virus Can Fully Control A Computer

In recent days, Digita Security cyber consultant reported it had just identified a Trojan virus that has been operating since 2016, Coldroot.

The malware infects a computer when disguised as a document; it is downloaded to the computer from a webpage the virus modifies the operative system privacy configuration to access key functions. Once installed the Trojan grants access to passwords, create files, delete files, views the desktop in real time, downloads and uploads documents, and shuts down the device. Mac addressed the issue with a patch in Sierra operative system.

According to experts, more than 15 million new malware files were identified in 2017. Even though most of the malware target Microsoft users, 250,000 were identified to target iOS operative system in the first semester of 2017. Mac users are advised to install Sierra operating system latest patch and to update their antivirus databases since developers will likely add Coldroot in their upcoming updates. Further, clients must be aware when entering unprotected web pages, downloading suspicious programs or documents, particularly if it is required to enter personal data and passwords.

City Union Bank Target Of Cyber-Attack

Per reports on February 19, 2018, India's City Union Bank was targeted by hackers through the society for worldwide interbank financial telecommunication (SWIFT) system.

It is estimated that the hackers transferred USD 2 million (EUR 1.6 million) using the SWIFT system. The bank's Chief Executive Officer (CEO), N. Kamakodi, said that the cyber-attack was carried out by international cyber-criminals but there was "no evidence of any internal staff involvement." Further, he said that the account holders are part of this "conspiracy." The bank was able to block one of the remittances.

Pinkerton assesses that banks in India are likely to continue to experience similarattacks in the near to medium term due to the increasing vulnerability of the SWIFT system. Client personnel using the services of the bank are advised to check their account for any discrepancies. Businesses using the bank services for high-value transactions are advised to contact the bank as a precautionary measure before carrying out any new transaction, and contact the relevant officials on the customer care number 044-71225000 or the email address customercare@cityunionbank.com. Any suspicious activity associated with the bank should be immediately reported to the requisite authorities.

Newly Discovered Saturn Ransomwares

Per media reports on February 16, 2018, new ransomware called Saturn has been discovered that can encrypt files on an infected server.

Each affected file will have .saturn extension added to its name. It also delivers a note with instruction and a key to login to the TOR ransom site. The payment is set at USD 300 (EUR 242) and doubles after seven days. The malware is spreading rapidly as its authors allow anyone to become a distributor for free via a newly launched affiliate program, Ransomware-as-a-Service (RaaS). By generating infected files from the RaaS portal, a user will receive 70% of the total payment from every victim, while Saturn creators keep 30%.

Pinkerton assesses that Saturn ransomware is likely to continue to spread and infect systems in the medium term. The threat is higher due to the easily accessible distribution method as it can be in possession of anyone. Due to cyberattacks, clients are likely to be exposed to data loss and additional costs of USD 300 (EUR 242) for each infected computer. Pinkerton recommends clients to incorporate reliable systems of data backup that can be used in an emergency situation.

Crypto-jacking Threatens Critical Infrastructure

On February 08, 2018, critical infrastructure security firm Radiflow published that they have discovered a cryptocurrency mining malware which was taking advantage of the monitoring and control operating system of a water utility in Europe.

This finding is especially relevant as it is the first known instance in which mining malware has been used in an industrial control system. This kind of practice in which an operating system (commonly a PC or a mobile device) is co-opted to illicitly mine cryptocurrency when you visit an infected site is called crypto jacking. The researchers that discovered this case are especially concerned as "industrial control systems require high processor availability, and any impact to that can cause serious safety concerns."

Pinkerton considers that this will be an increasing security concern among critical infrastructure operators in the near to mid-future. This is because industrial complexes tend to be ideal environments for crypto jacking as many of them do not use a lot of processing power for baseline operations, but do draw a lot of electricity, making it easy to mask CPU and power consumption. Pinkerton recommends all clients who have industrial control systems to installed intrusion detection products on the utility's network as to detect any possible intrusions.

Vulnerability Affects 25 Lenovo ThinkPad Models

Per a security warning published by Lenovo on February 9, 2018, two critical vulnerabilities connected to the Windows 10 LAN drivers for Broadcom chipsets installed in the computers could be used as exploits by attackers.

The vulnerability affects 25 Lenovo ThinkPad laptops, a model series that is popular among businesses. The first vulnerability, specified as CVE-2017-11120, gives would-be attackers remote control of the Wi-Fi chip by letting them install a backdoor into the firmware. The second, known as CVE-2017-11121, may be used to cause an effect similar to denial-of-service by overflowing the Wi-Fi firmware.

Based on the popularity of the system, Pinkerton finds that the vulnerabilities specified above are likely to affect a large number of business operations around the world. Pinkerton assesses that firewalls and standard anti-virus protection are likely to maintain system integrity in the immediate term. However, clients are still advised to follow the recommendation by Lenovo to update WiFi-drivers accordingly. Information about the vulnerabilities was first made public in September 2017, then affecting Apple IOS and Google Android products. So far there are no reports of the bugs having been used in any attacks. A list of the affected Lenovo models may be found on: https://support.lenovo.com/us/sv/solutions/len-17237.

Government Websites Infected With Monero Miners

On February 11, 2018, an information security consultant discovered that ico.org.uk had been injected with Monero miners.

Upon further investigation, the consultant, Scott Helme, discovered another 4,274 websites which had been infected. The infected websites included government websites in the U.S. and the U.K. such as uscourts.gov, manchester.gov.uk, and gmc-uk.gov. When a user visited the websites, the Coinhive Monero miner would run and would temporarily use up to 40% of the user's central processing unit (CPU) while they were on the site. The cause of the Coinhive miner injection was discovered to be a text-to-speech script, BrowseAloud, which allows visually impaired viewers to have the site read out loud to them. TextHelp, the maker of BrowseAloud, were notified of the issue by Helme and have disabled the script until their engineering team can identify and fix the problem. Helme believes that returning visitors to the site could still be at risk, as the miners can load from a cache even if the script is now disabled on the site. The UK's National Cyber Security Center is also investigating the incident.

Pinkerton assesses it is likely that other miner infections will target accessibility tools in the short- to medium-term. With the increase in cryptocurrency mining attacks in the past few months, it is likely that hackers will continue to look for easy ways to achieve widespread infection. The regulations requiring accessibility on all government sites provide an opportunity for hackers to reach a large number of users on sites where they would not be expecting to need extra protection. Pinkerton recommends clients clear their cache on a regular basis to remove any malicious scripts that may have been stored there.

Search Engine Permits Access To Sensitive Data Stored On Cloud Platform

Per reports on February 14, 2018, hackers have launched a website that permits users to access sensitive information stored on the cloud platform.

The "Buckhacker" search engine combines data from the cloud computing platform Amazon Web Services (AWS). AWS is a popular data storage platform used by a majority of private firms, governments, and universities. Per reports, Buckhacker targets the AWS Simple Storage Servers (S3), commonly referred to as "buckets." The Buckhacker service consists of collecting bucket names, which are usually the names of the companies storing information on the server, copying the data stored in the bucket, and publishing it on the database for public access. Therein, by searching the bucket name, users are privy to sensitive information particular to the company. Following the publication of the findings, Buckhacker's Twitter profile stated that the website was going "offline for maintenance."

Pinkerton finds that the Buckhacker website underscores the continuing threat of data theft from cloud computing platforms. While hacking of data on cloud platforms is common, Pinkerton notes that Buckhacker is unique in the ease of access provided to hackers. Though the Buckhacker website has gone offline, Pinkerton finds that clients with information stored on AWS S3 are still at a heightened risk as their sensitive information has likely already been leaked. In the immediate term, clients are recommended to consider moving highly sensitive information out of the platform until the issue is resolved. Further, along with updating passwords on storage platforms and devices, businesses are recommended to revisit their endpoint security protocol to mitigate the risk of cyber-attacks.

Cloud Services Fail To Detect ShurL0ckr Malware

Per media reports on February 7, 2018, Cloud-Access Security Broker (CASB) Bitglass detected new ransomware, called SherL0ck, which was able to bypass Google Drive's and Microsoft Office 365's cloud antivirus protections.

Only five of the 67 antivirus engines were able to detect ShurL0ckr. Reportedly, 44% of the cloud servers in at least one of their application had some form of malware. Microsoft's OneDrive had the highest rate of infected files (55%), while Google Drive had 43% of infected files. Dropbox and Box-hosted files also remained unsafe with 33% of infected files.

Pinkerton assesses that malware and ransomware targeting cloud-stored files will likely become more popular threats to enterprises and cloud application developers in the medium term. Increasingly, distribution and easy access via dark web encourage cyber-criminals even with low technological experience. They can buy the malicious program and pay a contribution to its distributor. The built-in antivirus programs of servers are

unlikely to give sufficient level of protection. Clients that rely on cloud storage systems are advised to use additional forms of information security to ensure business continuity and to avoid financial or data loss.

Apple iBoot Component Source Code Leaked

On February 8, 2018, the source code of the March 2016 iOS 9.3 iBoot, Apple's iOS secure bootloader, was discovered leaked online on GitHub. Apple has already sent a Digital Millennium Copyright Act (DMCA) takedown request to have the source code removed.

However, the source code has been leaked for four months on Reddit and is now being shared among jailbreaking experts using private file sharing sites. iOS experts who analyzed the leaked copy of iBoot code indicated there were few modifications version to version. Additionally, some security experts expressed surprise at how long it has taken for this version of iBoot to leak considering widespread reverse engineering of the code for scientific research and bug hunting purposes.

Pinkerton assesses that the iBoot source code leaked presents an opportunity for malicious actors to identify any new vulnerabilities in iOS systems. If any vulnerabilities are identified, it would likely lead to jailbreaks and other nefarious activities such as cracking locked iPhones or installing malware. Although the iBoot code effects on the current iOS version are unclear, it likely could be carried through to iOS 11. Pinkerton recommends clients that utilize iPhones or iPads ensure devices are updated with the newest software release to ensure the latest protections from Apple.

Lenovo Issues Recall On 83,000 ThinkPad Laptops

On February 7, 2018, news media published more information regarding the February 6, 2018, Lenovo recall of over 83,000 14-inch ThinkPad X1 Carbon 5th Generation laptops manufactured between December 2016 and October 2017.

About 78,000 laptops were sold in the United States, and about 5,500 sold in Canada. Lenovo identified a loose screw that could damage the lithium-ion battery and overheat it, making it a fire hazard. Three reports of overheating due to a loose screw which damaged the laptops triggered the recall. So far, no one has reported incidences of fire, injury, or damage to anything except the laptop. Lenovo suggests customers with a laptop affected by the recall go to https://support.lenovo.com/X1C_5GEN_RECALL to check if their laptop is included using the manufacturer date and serial number. Lenovo is offering free inspection and repair for all affected computers with a scheduled appointment. They reported they have fixed the issue for future manufacturing.

Pinkerton finds that while the threat of injury and damage is reported to be low, that businesses using these laptops still face a present threat. A laptop overheating to the point of damage could result in loss of data and business continuity depending on the range and application of the device's use. While no fires have been reported, the possibility presents an additional threat of injury and damage. Pinkerton recommends businesses immediately check with the website Lenovo advertised to determine if their laptop is included in the recall. If it is, Pinkerton further recommends saving all data to another device or in the business's secure online cloud, stopping use of the laptop, and scheduling an appointment with Lenovo to fix the issue.

Seattle Accuses Facebook Of Violating Campaign Finance Law

On February 5, 2018, the Seattle Ethics and Elections Commission, a city regulatory body that governs election conduct, accused Facebook of violating a city law requiring disclosure of political and election ad purchases.

The accusation by the Commission marks the first time a regulatory body has attempted to expand regulations to cover U.S. political and election ads on the internet. According to the head of the Commission, Facebook could face penalties of up to USD 5,000 per advertising buy. Facebook has yet to respond directly to the accusation, only affirming that it is committed to transparency in political advertising and that it had provided some data to the Commission. There is no current federal law that requires online ad sellers such as social media companies and Google to disclose the identity of buyers. However, there is federal legislation pending to expand rules currently governing political advertising on television and radio to cover internet ads. The specific 1977 Seattle law at issue requires companies that sell election ads to maintain "public books," displaying the identity of the purchaser, the cost, and the "exact nature and extent of the advertising services rendered." Facebook admits that, during the 2016 presidential election, foreign nationals were able to buy ads using aliases.

Due to the increased scrutiny and federal investigations into election interference, Pinkerton assesses that the pending federal legislation will highly likely go into effect in the medium-term. Pinkerton further assesses that state regulatory bodies are likely to apply existing regulatory practices on

political internet ads. Pinkerton recommends clients in the social media field and those clients involved with advertising and marketing, particularly that of a political nature, monitor any potential regulations.

Monero-Mining ABD.miner Botnet Infects At Least 7,400 Android Devices

On February 5, 2018, a botnet called ABD.miner was reported to have infected at least 7,400 Android devices since February 3, 2018.

It scans and targets port 5555, a debugging port that allows access to critical operating system features, to infect a device with malware that mines for Monero cryptocurrency. The botnet targets devices with port 5555 enabled, which must be done manually since all Android devices are delivered with that specific port disabled. It uses code from a strain of Linux-based malware called Mirai that has been used to target networking and Internet of Things (IoT) devices. About 40% of infected devices are in China, and about 30% are in South Korea. Monero-mining malware attacks increased as the Monero trading price increased. According to security experts, ABD.miner is only using one wallet address.

The ABD.miner botnet uses a device's energy and functions to generate cryptocurrency for an unknown actor or actors. Unauthorized access to an Android device poses a danger to personal information and could lead to further problems such as identity theft, phishing attacks, social engineering attacks, and installation of additional malware. Pinkerton finds that users who do not enable port 5555 on their Android devices do not face a threat of infection by ABD.miner because it only scans for and targets enabled port 5555 devices. However, a botnet is designed not to attract attention, so unless an antivirus program is specifically searching for it, it can be difficult to detect. Pinkerton recommends Android device users use a free botnet check website to confirm their device is not infected. Pinkerton also recommends Android users install third-party anti-virus software and keep it updated to help prevent infection.

Grammarly Vulnerability Discovered, Security Patch Released

Per reports on February 6, 2018, a researcher at Google's Project Zero found a flaw in Grammarly that would allow cyber-criminals access to user data.

The researcher found that the "high severity bug" on Grammarly's popular feature, browser extension, exposed authentication tokens to third-party websites. The authentication tokens can be used to access users' Grammarly accounts by redirecting the user to a specific website. Grammarly informed that the flaw affected only the Grammarly Editor; the Grammarly Keyboard, the Microsoft Office add-in, and text typed in websites while using the extension, have not been affected. Per reports, Grammarly was informed of the vulnerability on February 2, following which an update was released.

Pinkerton assesses that since Chrome and Firefox browser extensions are commonly used features, there is an even chance of cyber-criminals having exploited the vulnerability despite the quick response by Grammarly. Cybercriminals are increasingly using undiscovered flaws and sophisticated techniques to access sensitive data. Since Grammarly is "continuing to monitor actively for any unusual activity," clients using the software are recommended to report any suspicious activity that would allow the company to make a comprehensive assessment of the vulnerability's impact. Further, at this point, clients are not required to take any action to download the security patch as it is downloaded automatically. According to cyber-security experts, to avoid such vulnerabilities, online services should protect authentication tokens by using HTTPS and by enforcing the same-origin policy (SOP).

Critical CISCO Web VPN Service Vulnerability Discovered

On January 31, 2018, TechTimes published an article which announced the discovery of a bug in Cisco's Adaptive Security Software WebVPN.

All devices connected to the VPN network are vulnerable, as attackers are able to reset, send codes, and take complete control of the equipment. The security flaw was discovered by NCC Research Group, and the full details will be published on February 3, 2018. This leaves users a few days to download Cisco's emergency patch and avoid a serious threat to their security and communications chain.

Since the full details of this security flaw will be revealed in the upcoming days, Pinkerton urges all clients using Cisco's WebVPN to review the security advisory in Cisco's webpage, and in case one of the products they are currently using is vulnerable, they are advised to download the software patch immediately. Users presently occupying the software without a maintenance contract with Cisco must contact Cisco's Technical Assistance Center to get the patch. Companies should make sure that they are always using the latest available version of an updated software, as critical security vulnerabilities are regularly discovered by independent software developers and cybersecurity companies, and they are fixed through updates or security patches issued by the developer.

Adobe Flash Player Vulnerable To Zero-Day Flaw

Per reports on February 1, 2018, a zero-day vulnerability in Adobe Flash Player 28.0.0.137 and earlier versions has been exploited by North Korean hackers to target individuals in South Korea who are allegedly researching on the country.

According to the advisory by Adobe, the vulnerability, CVE-2018-4878, allows attackers to "take control of the affected system." Further, the "limited, targeted attacks" against users utilize MS Office documents, spam emails, and web pages. According to experts, the vulnerability has been exploited by North Korean hackers at least since November 2017.

Pinkerton assesses that since Adobe is likely to address the vulnerability through an update by February 5, a credible and active threat exists for clients using the Adobe Flash Player in the immediate term. Further, Pinkerton assesses that the attacks are highly likely given the strained relations between the North and the South; on February 1, 2018, violent protests were reported in Seoul, ahead of the 2018 Winter Olympic Games to be held from February 9. Pinkerton notes that vulnerabilities in the Adobe Flash Player have been highlighted in previous Pinkerton Insights Intelligence Briefs; on January 10, Adobe released an update for an earlier vulnerability, CVE-2018-4871; the latest version, Version 28.0.0.137, was part of the Patch Tuesday updates. As per the advisory, clients are recommended to use Protected View for Office that opens unsafe documents in Read-only mode. Clients can confirm whether their systems are vulnerable by consulting the notice issued by the Korea Internet & Security Agency (KISA): https://www.krcert.or.kr/data/secNoticeView.do?bulletin_writing_sequence=26998.

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