CYBER SECURITY BRIEFING

A Monthly Recap of Technology & Information Risk

PINKERTON®

MARCH 2019

Thunderbolt Ports Expose Computers To Attacks On Motherboard

A flaw discovered in the Thunderbolt connectivity specification could expose PCs to attack the motherboard via USB-C and DisplayPort.

Sources have reported that computer inputs USB-C and DisplayPort with Thunderbolt capabilities are vulnerable to attacks that could severely compromise the device. This type of ports grants Direct Memory Access (DMA) to connected peripherals. This means that such detachable devices (4k monitors, External Graphic Cards (GPU), USB hubs, network cards) interact directly with the computer's motherboard, thus bypassing the microprocessor and enhancing the overall performance. However, it also means that cyber-attackers can secure unfettered access to the main hardware. This vulnerability was detected in 2016 and developers have been encouraged to deploy stronger guards to avoid its exploitation; however, most currently available operative systems remain vulnerable to varying degrees.

As it has been reported in previous instances, peripherals constitute one major vulnerability for systems in general. In this case, Pinkerton assesses that the use of Thunderbolt-enabled devices is likely to expose computers to potentially fatal attacks. DMA-enabled ports rely on an Input-Output Memory Management Unit (IOMMU) defense system; with this, peripherals are given permission to access only the assets required to perform the device's function. However, detachable devices can be coded to present fake credentials to gain access to key assets in the motherboard; in this way, malicious third parties could create backdoors to the computer's main system. This risk is higher for devices using Windows 7, 8, 10 Home, and 10 Pro, which do not support IOMMU. Windows 10 Enterprise, MacOS, FreeBSD, and Linux are vulnerable to a lesser degree, but they still show some weaknesses. Pinkerton advises its clients deploying security protocols that avoid the indiscriminate use of peripherals: avoid integrating devices without previous clearing, audit third-party suppliers, and limit the use of secondhand devices.

Vulnerabilities Detected In 4G And 5G Mobile Networks

Newly discovered cellular network vulnerabilities were discovered that impact both 4G and 5G mobile networks.

As disclosed during 2019's NDSS Symposium, a group of researchers found three different types of cyber-attacks that could be perpetrated against 4G and 5G LTE mobile networks. In their paper "Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information," the researchers state that specialized devices are being used to intercept the mobile signals making them vulnerable to ToRPEDO, Piercer, and IMSI attacks. The ToRPEDO attack allows the aggressor to send fabricated paging messages (messages sent by the network to the device aimed at preparing it for an SMS message or phone call) to the device, to make Denial-of-service (DoS) attacks, and to know the device's location. Once the ToRPEDO attack has been committed, the attacker can retrieve the device's IMSI (the device's ID in the network) to spy on the victim's phone calls and SMS via Piercer and IMSI attacks.

Pinkerton expects the vulnerability in the mobile networks to be solved in the short-term; however, the impact of the vulnerability is yet to be discovered as almost all cellphones run on 4G and 5G LTE networks. On March 5, 2018, a group of researchers managed to modify 4G LTE core protocols to spy on users, to generate fake user location data, as well as to create and send spoof messages to network users. Pinkerton advises all

clients to remain aware of the development of the matter as there is nothing they can do to stop the attack and must relay in the technicians resolving the issue as soon as possible.

Half A Million Personal Profiles Leaked

4.1 GB-sized sensitive database named "GNCTD" was discovered to be unsecured and leaking data of nearly half a million Indian citizens.

Last month, a researcher found that a server that contained sensitive information of 458,388 Delhi citizens had not been appropriately configured, leaving the information accessible to cyber-attackers. The database was named GNCTD, which may stand for Government of National Capital Territory of Delhi, and it was managed by Transerve Technologies, a company dedicated to data collection technology and smart cities development. However, it is not clear yet if the local government was involved in the creation of the database. The administrator who configured the Mongo DB server did not follow the instructions to restrain the access to the server by demanding the use of passwords. The leaked information includes educational records, health conditions, voter ID numbers, and Aadhar numbers from Indian's IDs.

Pinkerton finds that the announcement is worrying as it is not clear yet how long the database has been exposed or how many attackers have taken advantage of the situation. MongoDB is one of the most popular NoSQL databases and is used by companies such as eBay and LinkedIn to store open-source information. Even though MongoDB constantly reminds the administrators of the correct way to configure the servers, they usually leave the servers unprotected. This is not the first time there have been situations like this, as, on February 11, 2019, 5 million personal databases were leaked from a MongoDB server storing the information of 41 Mexican companies. Pinkerton advises all clients using MongoDB or other NoSQL database to make sure that the server is configured correctly and that all security options are enabled.

Russian Hackers Could Exfiltrate Information In Less Than 19 Minutes

A new report states that Russian hackers are able to move laterally through an organization's network in under 20 minutes after the initial breach.

Last month, the cybersecurity firm CrowdStrike issued its 2019 Global Threat Report: Adversary Tradecraft and The Importance of Speed. The company (which gained notoriety after it was hired by the Democratic National Committee over hacking concerns during the 2016 elections) found that state-sponsored hacking groups are substantially faster than even the best gang-operated attacks. The report analyzed over 30,000 intrusion attempts and categorized them by the group suspected of carrying out the attack. The study measured the time between the initial breach and the actual exfiltration of data or attack. On average, cybercriminal gangs take 09:42:23, Iran 05:09:04, China 04:00:26, North Korea 02:20:14, and Russia 00:18:49.

As the threat of state-sponsored hacking becomes more common and effective, Pinkerton assesses that politically motivated cyber attacks pose credible threats to national institutions, infrastructure, and companies alike. In recent months, state-sponsored attacks have been reported against government institutions all over the world; most recently the February 2019 attack against the Australian Parliament. Similarly, companies have been targeted by groups suspected of being funded by foreign governments, with the latest major attack taking place in December 2018 against major California-based newspapers. As foreign actors develop further capacities, it is expected that cyber attacks will be used more often to further national agendas. To limit the effectiveness of sophisticated attacks against key assets, Pinkerton advises its clients to devise cybersecurity strategies that comply with the 1-10-60 rule; that is, intrusions must be detected within one minute, investigated within 10 minutes, and eradicated in no more than 60 minutes.

Cyber-Security Researchers Discover New Mac Malware Variant

Carbon Black has discovered a new variant of Shlayer macOS malware.

Carbon Black, a cyber-security research firm, announced the discovery of a new macOS malware variant of "Shlayer" targeting operating system version 10.10.5-10.14.3. Unknown malicious actors cloak the malware as an Adobe Flash update on large numbers of websites, including some that appear to be legitimate domains. The malware escalates privileges after infection. Distributed through DMG, PKG, ISO, and ZIP files, many of which possess legitimate Apple developer credentials, the malware collects system information, creates a custom URL with the collected information, and then downloads the second stage. Following this second stage, the malware attempts to harvest the password-protected payload and stores it in an archive. The malware then attempts to escalate privileges to gain root access to the device to download additional software and disable the system's Gatekeeper.

As the malware possesses legitimate domains and developer credentials, Pinkerton assesses that the malware poses an increased threat to clients who utilize macOS devices. Further, as the malware affects recent versions of macOS, Pinkerton finds it unlikely that installing the latest versions of macOS will best mitigate the threat of this malware variant. Pinkerton recommends clients closely scrutinize any website-based prompts to update or

install Adobe Flash. Any clients who must use Adobe Flash are recommended to ensure that the program is updated to the most recent version through the program itself.

Malicious Actors Attack Business And Government Agencies

Cyber-attacks from Iran and Chinese hackers, have increased due to President Trump's withdrawal from the Iran nuclear deal and trade conflicts with China.

American government agencies and business have been the target of many malicious attacks by nation-state actors. Analysts at the National Security Agency (NSA) claimed that most of the cyber-attacks are from Iranian and Chinese hackers. Since U.S. President Donald Trump's decision to conclude the nuclear deal with Iran, as well as constant trade tension between China and the U.S., the attacks have increased. According to media reports, Iranian hackers have attacked government agencies, banks, corporations, and other entities. However, the Chinese cyber-attacks have focused on companies related to the U.S. military, such as technology companies, to gather classified information about trade, military intelligence, and plans.

Pinkerton assesses that the consistent cyber-attacks on government agencies and corporations in the U.S. will likely continue as intelligence agencies have not identified the responsible parties yet due to the complexity of the attacks. According to media reports, there are many enterprises have been targeted by malicious actors such as Boeing, T-Mobile, General Electric Aviation, among others; however, there is not enough information to conclude how damaging the attacks were. In 2015, China and the U.S reached a cyber-agreement to monitor malicious cyber-activities to decrease the number of attacks and to cooperate in high-level summits to develop mechanisms against cyber-crimes. Pinkerton recommends clients, especially those with operations in the U.S., ensure their systems have the latest security patches and anti-virus/anti-malware software. Furthermore, Pinkerton advises clients to monitor incoming requests to the internal network, principally from Iranian and Chinese based IP addresses.

Phishing Attack With Google Translate Steals Credentials

A new phishing attack is using Google Translate as a camouflage on mobile browsers to steal credentials.

Open sources have reported that malicious actors initiated a phishing campaign that uses Google Translate as a facade to steal Google and Facebook credentials. According to experts, the process starts with phishing emails pretending to come from Google with the subject "Security Alert." The content warns about an unverified log-in from a Windows device, and it recommends pressing a button to consult the activity. After the user clicks the link, it will redirect to a Google Translate page that simulates a Google Account log-in. Researchers stated that the phishing page is harder to detect through a mobile browser as it hides better the Google Translate interface and resembles a more legitimate Google Account log-in. If the user enters the information requested, the attackers receive the information via email. Afterward, it redirects to a Facebook log-in page to start the same phishing process. Malicious actors can steal accounts, passwords, and other data related to the person's verification settings such as phone number and alternate email address.

Pinkerton expects that more phishing campaigns will appear in short to medium term as malicious actors are rendering more sophisticated methods to steal data from individuals and large firms. Cisco systems estimated that 28.5 billion devices would be connected to IP networks by 2022 which means that approximately every person will own an average of 3.6. Therefore, Pinkerton finds it highly likely that cyber-attackers will remain a relevant threat in the long term. Pinkerton recommends clients to avoid opening Google security alerts or ensure that the source of the email is legitimate. If the link directs the user to a Google Translate page, do not write any data and immediately close the window browser. Pinkerton further advises clients to be vigilant about the information provided in digital sites as well as the reliability of its source.

Senators Ask For Probe On Vulnerabilities Of Foreign-Made Applications

Senators in the U.S. are urging the U.S. Department of Homeland Security to investigate VPNs that are not private.

It has been reported that U.S. Senators Ron Wyden and Marco Rubio asked the Department of Homeland Security (DHS) to carry out a threat assessment of a number of apps owned by or linked to foreign governments. Senators indicated that there are credible concerns that public and free apps can be used by foreign agencies to extract information from users. Of particular concern would be any exposures to data exfiltration from federal employees using these services in their daily life. In a letter addressed to the Director of Cybersecurity and Infrastructure Security Agency, senators specifically mentioned Dolphin, Yandex, and Opera. Of particular concern are the services of VPN and data-saving compression offered by these apps.

As recent reports have pointed to the use of free software as means to introduce malware or carry out cyber attacks, Pinkerton assesses that publicly available free applications pose a higher risk of being designed or exploited for dishonest purposes. Pinkerton has identified numerous threats from malicious apps in the past. It must be noted that most apps offering free VPNs have been traced to China-based or Chinese-owned companies. While VPNs are illegal in the Asian country, the administrators of such systems can use these to extract information from users.

The findings from the DHS assessment may provoke renewed calls to ban products associated with Chinese companies across the North American market. Pinkerton advises to avoid using any free application for the management of sensitive information, as these are more likely to contain malware or exploit vulnerabilities; it is recommended to favor verified vendors that are properly identified and accountable for the misuse of their products or services.

Bank Of Valletta's Operations Have Been Compromised

It's still too early to establish who was behind the cyberattack at the Bank of Valletta, but they insist personal data was not touched.

Recently, the chief business development officer in Bank of Valletta (BOV) announced that there is not enough information to declare who was responsible for the cyber attack on January 13. The cyber attack resulted in the transfer of EUR 13 million (USD 14.5 million) of BOV's accounts to other banks, especially overseas accounts; forcing the bank to suspend all the banking operations. According to the announcement, the attack involved millionaire transactions, but the personal data of the clients were not exposed. The bank is cooperating with national and international authorities to investigate the attack. The BOV resumed operation on January 14.

According to media reports, the investigation to find the actors behind the attack will take several weeks or months, as it is likely that the authorities will not be able to identify the responsible party. The attack was significant breach within the country given that the BOV has almost half of the Maltese market and it is the largest shareholder in the country. Pinkerton finds that authorities have discovered that the unidentified malicious actors transferred money to accounts in the UK, the U.S., Czech Republic, and Hong Kong. Pinkerton recommends resetting passwords of any potentially affected accounts of the BOV and associate banks and regularly changing passwords of accounts with personal information. Furthermore, Pinkerton advises clients to activate two-factor authentication on the website is likely to provide extra security for sensitive information.

Remote Desktop Protocols Have Major Vulnerabilities

Flaws have been detected in popular remote desktop protocols that are allowing malicious severs to potentially reverse hack PCs.

Last month, open sources reported that widely used Remote Desktop Protocol (RDP) has 25 security vulnerabilities that allow malicious servers to attack the client's computer. In a normal situation, an RDP client connects to a remote RDP server. After the connection has been established, the RDP client can access and control the remote computer. However, researchers found that security vulnerabilities allow malicious RDP servers to attack and control the client's device. Experts tested these vulnerabilities on FreeRPD and rdesktop, two of the most common open-source RPDs, and found that significant vulnerabilities allow malicious actors to execute malicious code in the client's device. Cyber-security researchers further warned that Microsoft's RDP is vulnerable to attacks via the client's clipboard. Malicious actors can eavesdrop and copy executable malware into the client's computer.

As technical users and IT administrators commonly use RDP clients to connect remote computers into a specific network, Pinkerton assesses that RDP vulnerabilities will be a relevant risk in the immediate to medium term. Pinkerton recommends clients to inform its IT department about the significant vulnerabilities in the identified RDP clients and to update future versions as it is highly likely that developers will address these issues. As malicious actors are currently rendering complex methods to attack electronic devices, Pinkerton recommends clients to run routine analyses focused on RDP vulnerabilities to ascertain data breaches or malware. If clients use Microsoft built-in RDP, Pinkerton advises disabling the clipboard-sharing function until the issue has been patched.

Airbus Announces Data Breach

Airbus has admitted to a data breach of its "Commercial Aircraft business", which allowed access to some of its employees' personal information.

Airbus recently announced that a data breach was detected in the first days of the year in the "Commercial Aircraft Business" systems, specifically those containing Airbus employees' personal information. After a thorough investigation, the company concluded that no systems related to aircraft production and development were compromised. However, the breach caused the attackers to be able to retrieve IT and professional information of the European Division. The company announced the enhancement of their corporative and personnel cybersecurity protocol and assured that the production lines will continue to work as usual and that no delays are expected to occur as a result of the attack.

Pinkerton assesses this will be a relevant matter for all clients operating in the aircraft industry as the mentioned incident is the second data breach suffered by a major aircraft construction company in less than a year. In March 2018, the American aircraft assembler Boeing suffered a ransomware attack in low importance systems.

Pinkerton recommends all clients to increase their cybersecurity protocols to have better defenses in case of a cyber-attack and to instruct their employees on how the company's security could be compromised if they click on unverified websites, emails, links or if they download unknown documents. vulnerabilities to ascertain data breaches or malware. If clients use Microsoft built-in RDP, Pinkerton advises disabling the clipboard-sharing function until the issue has been patched.

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