CYBER SECURITY BRIEFING

A Monthly Recap of Technology & Information Risk

PINKERTON®

JULY 2018

Google Discovers Critical Bug In Modern Web Browsers

Recently, a Google developer discovered a significant vulnerability in modern web browsers, which allows websites to steal sensitive content such as online accounts in recently visited sites in the same browser.

This malfunction resides in the browsers' handling of cross-origin requests to audio and video files, which puts users at risk of data robbery since it leaves a loophole for remote access to these browsers. The vulnerability could allow an attacker to access and read the content of sites like Gmail and Facebook Messenger. Usually, websites can only request for information from the same origin where it was loaded. However, browsers do not have this restriction leaving the possibility open for visiting other sites without restrictions, to upload videos, and for attackers to log into the user account.

Pinkerton finds that the impact of this malfunction will highly likely become an increasing concern in the near to medium term. This is because the vulnerability can only be partially fixed for now in Edge and FireFox if the latest version of the browser is downloaded. So far, it is preferable that clients use Safari and Google Chrome browsers since those are the only ones that already have a policy which restricts such kinds of cross-origin requests. For other browsers, it is necessary to wait until the temporary fix is written into a standard and tests are made to verify its reliability. Further, clients are encouraged never to play videos or audios while they are using a personal account.

Apps Vulnerable Through Firebase Endpoint

Researchers from cyber-security company Appthority discovered that multiple app developers did not configure their apps' back-end Firebase endpoints correctly, granting attackers access to sensitive data.

The problem affects Firebase, which is an app development tool that allows developers to secure the endpoints with firewalls and authentication measures while creating the app. The researchers took into consideration 2.7 million apps in their study and found that 2,446 Android apps and 600 iOS apps were compromised, and provided the attackers with information such as GPS location records, IDs and passwords, financial records, and health information.

Pinkerton finds that the impact of the flaw is significant because the study revealed that apps belonging to multiple categories such as finance, telecommunications, health, and cryptocurrency had been affected; the compromised Android apps alone had registered 620 million downloads. Pinkerton advises clients to be careful when deciding which web and mobile apps they download and grant permissions to on their devices, especially with apps developed using the Firebase platform. Appthority has already contacted various app developers and Google Inc., Firebase's owner, to notify them of the flaw.

Hackers Target Insecure Cameras

On June 22, 2018, reports released stated that there have been recent cyber-attacks on several brands of security cameras, webcams, and baby and pet monitors.

Many of the devices can be used with a mobile app, which requires the user to enter a device ID and password that is found on the device's box or the device itself. This then connects the user to the vendor's backend cloud server. The IDs are not randomly generated, so malicious actors can create a script that connects to the vendor's backend cloud server and use the default passwords to hijack cameras. Over 810,000 devices were exposed using the sequential IDs with default passwords. At least one of the device brands has been tracked to a Chinese company, Shenzhen Gwelltimes Technology. The company sells devices to vendors across the world. Reseller companies will order cameras from the company with their own brand and then resell these devices on Amazon. According to cyber-security firm SEC Consult, Shenzhen Gwelltimes knows about the security issues but does not appear to have fixed them.

Pinkerton assesses that other companies selling these devices are likely affected by the same security concerns. As the vendor of these devices may not actually be the product's manufacturer, it is likely the public is unaware of the issues. Malicious actors are likely to exploit the vulnerability, especially since Gwelltimes Technology appears to have done nothing to address the vulnerabilities. Clients who have to install an app to access a security camera, webcam, or home camera monitor are likely at the most risk of exploitation by malicious actors. Pinkerton recommends clients who use such devices ensure the default password is changed to best prevent malicious actors from hijacking the camera. As all the brands have yet to be identified, Pinkerton also recommends clients monitor for any unusual activity on their camera devices.

Proof-Of-Concept Attack Underscores Risk Of Naval Remote Hacking

Per a blog post by the Pen Test Partners, threat actors can hack into the navigational system of ships and manipulate their course.

Researchers showed in a proof-of-concept attack that it is possible to access the network of systems that control a ship. The hack was possible as most systems are built around a dual network solution; one for ship controls and the other for standard Internet services such as email and traditional browsing. Some systems act as bridges between the two networks, and a hacker can gain access to control systems through the standard less secure network.

Pinkerton finds that the vulnerability underscores the risk of threat actors gaining remote control of ships, which could have severe economic and operational consequences. IT-security experts have been warning about the possibility of hackers gaining access to control systems for several years, but the shipping industry has not shown adequate interest in the issue. This is likely due to the lack of precedent of attacks, or the industry's unwillingness to make any recorded incidents public. According to a report in 2017, a freight ship lost control of its navigational systems for ten hours outside the East African Coast. Allegedly, the ship's systems had been compromised, but there was no evidence to prove it.

Vulnerability Targeting Android Devices Found

Per reports on June 28, 2018, cyber-security researchers found that the newly discovered RAMpage vulnerability could impact almost all Android devices manufactured after 2012.

The vulnerability, termed CVE-2018-9442, is a variant of the Rowhammer bug; Rowhammer is reportedly a hardware bug present in modern memory cards. When users of the infected devices send repeated write/read requests to the same row of memory cells, the write/read operations create an electrical field that would then alter data stored on the memory cards. In the past, Rowhammer-based cyber-attacks have been executed via JavaScript code, GPU cards, and network packets, and have reportedly been targeted at Android devices and personal computers. Per the researchers, RAMPage can be exploited to gain confidential data from various applications on the user's phone.

In the immediate term, Pinkerton assesses the threat from the RAMpage vulnerability as low given that the researchers are still exploring the scope of the possible exploit. In the immediate term, personnel are recommended to only install apps from reliable sources such as Google Play Store to avoid the risk of installing apps with hidden malicious code. Further, until comprehensive details regarding the vulnerability are disclosed, it is recommended to avoid saving confidential information such as bank details, passwords, and personal data on smartphones, especially Android devices.

Restaurant Chain PDQ's Computer Systems Hacked

Per reports on June 24, 2018, the U.S.-based restaurant chain PDQ's customers' credit card details were subject to theft in a breach of the company's computer systems lasting May 19, 2017-April 20, 2018.

PDQ stated that "an unauthorized person (hacker) exploited part of computer related system and accessed and or acquired personal information from some of our customers." Per reports, the cyber-attack targeted the systems of ten of PDQ's restaurants in the Triangle, North Carolina including in North Raleigh, Wake Forest, Cary, Durham, and Fayetteville. PDQ stated that its branches at the PNC Arena, Raleigh and Tampa, Florida were not targeted in the hack. PDQ has reported the breach to law enforcement agencies and has hired a cyber-security firm to examine the vulnerability of systems exploited in the cyber-attack. No reports of losses incurred by PDQ's customers due to the theft of their credit card information have yet emerged.

Pinkerton assesses that the credit card information used by PDQ's customers from May 2017 to date will highly likely be vulnerable to theft and misuse in the medium to long term. Further, credit cards or other banking tools used to make online payments to companies employing computer systems like that of PDQ's will likely be vulnerable to theft and misuse. Pinkerton recommends PDQ's customers to examine their credit card statements from May 2017 to date and report any suspicious transaction to PDQ at +1-844-328-1737 or info@eatPDQ.com. Pinkerton recommends PDQ's customers to monitor credit cards that were used to make payments to PDQ during the period of the breach. Pinkerton recommends personnel and businesses engaging in online transactions to follow updates on PDQ's internal cyber-security investigations to identify and internally review the systems vulnerability exploited in the hack. Pinkerton recommends businesses that could be exposed to similar systems vulnerability to issue an advisory to customers to secure brand reputation.

Satellite And Defense Organizations Targeted In Cyber-Espionage Campaign

Per media reports on June 19, 2018, a new hacking campaign launched through China-based computers attempts to interfere with companies developing satellite communications, geospatial imaging, and defense contractors from the U.S. and Southeast Asia.

According to the cyber-security firm Symantec, which reported the threat, the intruders showed particular interest in the operational side of the breached companies. The cyber-espionage group responsible for the attack has been known since 2013 by the codename Thrip; the recent attacks were detected following an alert on the suspicious use of a legitimate tool at one of the affected systems, which later led to the discovery of the advanced multilayer hack on several organizations. China has officially denied any involvement in state-sponsored hacking, while Symantec did not indicate actors responsible for the attack command.

Pinkerton assesses that the threat of cyber-attacks on companies and organizations considered significant for national safety and development remains high and is likely to continue in the medium term. Further, Pinkerton notes that the recent breach underscores the capability of hackers to disrupt the operations of the affected companies. The report about cyber-espionage breaching satellite communications operators follows another major data leak, reported in the Pinkerton Insights Intelligence Brief on June 11, 2018, when hackers accessed the computers of a Navy contractor and stole hundreds of gigabytes of data including confidential information.

Advanced Battery Saver App Gains Access To Vulnerable Data

Per media reports on June 21, 2018, the Advanced Battery Saver application available on Google Play Store is a malware campaign targeting Android users.

The app was reportedly giving hackers access to sensitive log data, text messages (SMS), data received from the Internet, and full network access; further, by displaying false advertisements and engaging users' interaction, it was generating revenue for the app's authors. The ad-clicker also obtained the infected devices' details such as phone numbers, International Mobile Equipment Identity (IMEI) number, model, brand, and location. Reportedly, before taking the malware down from the Google Play Store, approximately 60,000 users were affected.

Pinkerton finds it likely that the malware will continue being distributed on different platforms in the near to medium term. Further, Pinkerton assesses a high risk of data exploits for the users of already infected devices. Clients are recommended to revise installed apps, delete suspicious programs, and pay close attention to access requirements listed before installing any new software. Pinkerton notes that elementary functions such as torch, calculator, battery saver, and weather forecast are included as the originally authorized software; however, there are multiple versions created by various unlicensed authors that are available to download from Google Play Store and third-party websites. These are likely to contain malicious codes and ad-clickers that are aimed at obtaining data stored on the device.

PyRoMineIoT Malware Mines For Cryptocurrency, Infects Vulnerable IoT Devices

Per reports on June 12, 2018, the recently discovered cryptocurrency miner malware, "PyRoMineIoT" is misusing a National Security Agency-linked remote code execution exploit to spread as well as to use infected machines to scan for vulnerable Internet of Things (IoT) devices.

Similar to the PyRoMine cryptocurrency miner discovered in April, the malware is Python-based, uses the EternalRomance exploit for propagation purposes, and mines for Monero. The malware is hosted on the IP address 212[.]83.190[.]122 and, once a system is infected, downloads VBScript. The VBScript sets up a Default account with the password "P@ssw0rdf0rme" and adds the account to the local groups "Administrators," "Remote Desktop Users," and "Users." It then enables Remote Desktop Protocol (RDP) and adds a firewall rule that allows traffic on port 3389. Further, it also downloads a Monero miner, XMRig. The malware has not generated revenue yet.

Given that the malware has been active since June 6, Pinkerton finds that it has likely affected systems across the world; further, since the older variant had impacted certain countries the most - Singapore, India, Taiwan, Cote d'Ivoire, and Australia - the threat to these countries remains high. Since the infection is spread via "an obviously malicious-looking website" disguised as security updates for web browsers, clients are recommended to be cautious of such webpages and refrain from clicking any link without establishing the credibility of the source. Further, per experts, clients in Saudi Arabia and Iran using IoT devices with the admin - admin username and password pair - are at risk of infecting vulnerable devices with the malware. Pinkerton recommends clients to update the security patch for the EternalRomance exploit released in April to minimize the threat.

Cyber-Security Law Passed Despite Privacy Concerns

On June 12, 2018, 91% of Vietnamese lawmakers voted in favor of a cyber-security law amid violent nationwide protests against its approval.

Per the law that will take effect from January 1, 2019, technology companies such as Google and Facebook will have to store data in Vietnam, open local offices, and remove content termed "offensive" by the government within 24 hours of being ordered to. Further, the law will provide the authorities with more liberty in detaining and prosecuting people for online activities that they deem "illegal." The U.S. and Canada have vehemently opposed its passage, stating that the legislation poses "serious obstacles to Vietnam's cyber-security and digital innovation future, and may not be consistent with Vietnam's international trade commitments." Further, per the Vietnam Digital Communications Association, the law is likely to reduce the country's gross domestic product (GDP) by 1.7% and reduce foreign investment by 3.1%.

Further, Pinkerton notes that the cyber-security law underscores the increased crackdown on online activity by Vietnamese authorities in the recent past. In 2017, the authorities requested Facebook to take down 159 accounts and YouTube to take down 4,500 videos that were allegedly "illegal." In June 2017, a Vietnamese blogger was sentenced to ten years in prison for defaming the regime on social media. Further, authorities have deployed 10,000 members of a military cyber-warfare unit to monitor "wrongful views" on the Internet.

Pinkerton assesses that there is an even chance that the approval of the authoritarian cyber-security law portends more stringent regulation on foreign business operations in Vietnam, which is likely to adversely impact investor perception and the ease of doing business in the country. In addition to restrictions on freedom of expression, Pinkerton finds that given Vietnam is an export-driven economy, the law is likely to adversely impact multinational firms' business expansion plans in the region and increase operational costs. Further, Pinkerton finds that the demand for companies to hand over private data will be a deterrent for technology companies keen to invest or start operations in Vietnam. Clients with business operations linked to Vietnam are recommended to review these trends as the law would require changes in companies' IT infrastructure and policies in the near to medium term.

New KillDisk Malware Variant Found In Targeted Attacks

Recently, cyber-security company Trend Micro found a new version of the KillDisk malware targeting organizations in Latin America.

This destructive virus operates by deleting files and wiping the computer's disk, making systems inoperable. One of the most recent KillDisk attacks in May was related to a foiled heist against a bank, leaving its SWIFT network unavailable and internal systems inoperable for several days. The malware was detected in 2015 in attacks against Ukraine's energy sector, and in late 2016 when a Linux-targeting variant that had file-encrypting capabilities was discovered.

Pinkerton assesses that such cyber-attacks will likely be an increasing security concern among organizations operating in the region in the near to medium term. This is because it is not yet clear if the attack was an opportunistic cyber-criminal campaign or was a coordinated attack that will

have further repercussions; however, it appears that attackers are likely more interested in complete systems rather than individuals. Pinkerton recommends clients with operations in Latin America to avoid any unknown web downloads and to stay aware of uncommon messages from computer systems in the workplace. Additionally, it is advised to install intrusion detection software on the utility's network.

Advanced Malware Strain Suspected Of Cyber-Espionage Attack

On June 8, 2018, ESET security researchers confirmed that they discovered a new and rarely used malware strain, InvisiMole.

The complex piece of spyware has only been found on a few dozen computers in Russia and Ukraine. The overall assessment of the advanced cyber-espionage technology is that the malware was likely developed over the course of several months, if not years, with the intent to hack nation-state or financially-motivated targets. ESET researcher Zuzana Hromcova said that all infection vectors, including installation through physical access to the machine, are possible. The malware's coding is comprised of two modules. The less sophisticated module, RC2FM, can manipulate the local system, search and steal data, and activate a user's microphone and webcam. The unique features of the more advanced module, RC2CL, include the ability to safe-delete its own files as well as convert into its own proxy to facilitate communication between the first module and the attacker's server.

Pinkerton assesses that due to the highly-targeted campaign, the probability of cyber-espionage attacks affecting clients who work with, or within, Russia and Ukraine is low. However, the nature of the attacks is focused on highly sensitive sources, and the importance of the acquired data is highly likely to be confidential. The malicious actors behind InvisiMole and how it spreads remain unknown and except for a single file that was dated in October 2013, nothing else is traceable. ESET products used on compromised computers have been the only source of detection thus far. Pinkerton finds that the level of knowledge available to security experts is currently inefficient to protect clients properly from this specific cyber-threat. However, adhering to basic cyber-security practices such as properly configuring servers, properly managing credentials, and promptly installing software updates will aid in mitigating most cyber-threats. Pinkerton advises clients who work with the targeted countries to take precautionary measures to detect infected computers and prevent sensitive information from being exposed.

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