CYBER SECURITY BRIEFING

A Monthly Recap of Technology & Information Risk

PINKERTON®

JANUARY 2019

A New Zero-Day Exploit Found In Microsoft Windows

New unpatched Windows zero-day exploit on Twitter was recently discovered by a hacker..

Media outlets reported that a researcher found a new zero-day exploit in Microsoft Windows that allows malicious actors to read any file in the targeted computer. According to experts, malicious actors can take advantage of the "MsiAdvertiseProduct" function in the Microsoft Windows software to copy data from the targeted computer so that the destination of the files is always readable. Malicious actors can get privileged system access using the exploit. Additionally, the CEO of Acros Security supported the researcher's findings and confirmed that Microsoft Windows users are vulnerable to attackers using the exploit.

Pinkerton assesses that users of the current version of Microsoft Windows software will remain vulnerable to cyber-attacks in the immediate to medium term. As three different zero-day exploits have been found in the past three months and developers need time to create the patches to solve the problem, Pinkerton finds that there is an even chance of further vulnerabilities in the software. Pinkerton recommends clients using Microsoft Windows to always install system updates as the new patches aim to solve zero-days exploits. Pinkerton further advises clients to contact cyber-security companies that offer temporary solutions to unpatched exploits until Microsoft fully addresses the system's vulnerability.

Researchers Discover Security Liabilities In Hola VPN Service

A free VPN service that has been downloaded over a million times is failing to mask the digital footprints of users, say researchers.

Researchers from Researchers at Trend Micro, a Japan-based cyber security and defense company, revealed that the more than 175 million users from the virtual private network (VPN) service Hola VPN are currently at risk of a possible attack. This risk arises from the fact that the service provider does not use an encrypted tunnel when a client using the free software accesses a supernode during an active session, which would allow possible attackers to intercept this traffic and perform Man-in-The-Middle (MiTM) attacks. This lack of encryption could also lead to the possible leak of the user's IP address, which could, in turn, be used to track down the user, thus potentially endangering the person using a VPN service to protect their identity and physical location.

Even after being exposed as an unsafe service, it is unlikely that Hola VPN will change the way it operates since it has a free version of the service, and it depends partially on this way of proceeding to make a profit. In 2015 the founder of the service revealed that the service's Chrome extension sells its users' bandwidth to cover the cost of giving the service for free to a large number of users. Pinkerton recommends clients using Hola VPN to switch to another VPN service provider which does encrypt its communications. They are also advised to explain to all their employees the importance of adhering to the selected service provider instead of using one of their choosing as not all VPN services have the same security standards.

Vulnerability Affects Millions of Apps

A critical SQLite flaw has left millions of app vulnerable to hackers.

A major vulnerability named Magellan was discovered by Tencent's Blade cybersecurity researchers in the popular SQLite database manager. Being the most used disk-based database manager engine, SQLite gives support to millions of apps and programs such as Android apps, Windows apps, IOs Apps, Adobe software, Skype, and Google Home. An attacker can take control over Chromium and Brave type browsers, such as Google Chrome, Firefox, and Opera as they are supported by the database. To do this, the aggressor deceives the user to enter a specially created malicious website. The vulnerability allows the attackers to send malicious codes and initialize processes in the affected software to prevent applications from working and to access the affected program's memory.

Pinkerton assesses that the impact of this flaw will be significant in the medium-term, as developers are not sure how long it will take to patch the vulnerability in all the affected software completely. So far, SQLite has released an emergency update, and Google Chrome released a statement announcing that the company has issued a patch that will contain the flaw's damage potential. Pinkerton recommends all clients to update the affected software as soon as possible, to remain aware of new press releases regarding the impact of the vulnerability, and to contact with their IT team to take the adequate precautionary measures.

NASA Employees At Risk As Agency Reveals Server Breach

NASA reports a serious breach of employees' personally identifiable information, after a server may have been compromised a few months ago.

Sources have reported that the NASA's Chief Human Capital Officer sent an e-mail to employees to confirm a server breach that took place back on October 23. The internal communication mentioned that leaked information included an undisclosed amount of personally identifiable information such as Social Security numbers and other personal employee data. Although there was no statement on the exact number and impact of the exfiltration, it was declared that all personnel hired, separated, or transferred between July 2006 and October 2018 were potentially compromised. There were no indications that missions or critical operations had been affected in any way. It is expected that affected individuals will be contacted and advised on steps necessary to contain the impact from this breach.

Pinkerton assesses that this security breach is part of a global trend in unauthorized retrievals of personal information that affects even highly-secured institutions. This type of violations could endanger individuals as it exposes them to extortion and phishing. Attacks of this type against NASA have been recorded in the past, despite strong cybersecurity measures. Institutions, corporations, and even individuals are at risk of data exfiltration by malicious agents with political or financial motives, but also from privates without an agenda known as "bedroom enthusiasts." Pinkerton advises its clients to perform regular backups of personal information to limit the risk from extortion or ransom caused by malicious data exfiltration. Pinkerton also recommends performing regular updates and assessments of local servers to ensure sound security systems are in place.

Unprotected MongoDB Contains Information Of 66 Million Individuals

Scraped LinkedIn profile data belonging to more than 66 million individuals was detected in an unprotected database that anyone could access.

Cyber-security researchers have discovered an unprotected MongoDB database that appeared to expose the scraped data of 66 million individuals. The data included the full name, personal or professional email, phone number, employment history, location details, skills, and a link to their LinkedIn profile. Based on the last piece of information, cyber-security researchers believe the database contained scraped data from LinkedIn. The information appears to have been obtained from publicly available records.

While the information may have been scraped from publicly available records, Pinkerton assesses that the exposed data will likely be used by malicious actors to conduct phishing attempts in the medium term. Pinkerton finds it likely that the exposed data will enable malicious actors to make phishing attempts appear more legitimate, increasing the threat posed by any such campaign. Pinkerton recommends that clients who maintain LinkedIn profiles watch for suspicious activity and monitor any associated email accounts for phishing attempts.

Banks Attacked From Inside Network

Banks in Europe were being attacked from the inside of their network via electronic devices connected directly to the company's infrastructure.

Last month, multiple banks in Europe have been attacked from inside the network by various electronic devices that are connected directly to the company's infrastructure. Malicious actors hid entry points by planting devices, so they did not attract attention. The attacks, dubbed DarkVishnya, have hit at least eight banks using netbooks or inexpensive laptops, Bach Bunny, or Raspberry Pi mini-computers. Access was gained from various places in the bank's central and regional offices, some even from branches in different countries. The attacks bypassed network defenses, and once inside the local network, the device would appear as an external flash drive, unknown computer, or even a keyboard. Then, the malicious attackers scanned digital premises to find shared folders and web servers with public access to gain information such as login credentials. Estimated losses are up to tens of millions of euros.

The success of the attacks is likely due to the attackers not relying on malware, as the tools they used like PowerShell bypassed most banks technologies and domain policies. Pinkerton finds that since the attack has proven successful, further cyber-attacks using this method will become more popular in the short to medium term. Although the type of information taken is not fully known at the time of writing, it is likely the malicious actors gained access to valuable information to accounts. Pinkerton recommends clients operating in the banking sector block PowerShell if possible to help attempt to minimize this type of attack. Clients who use banks in Europe are recommended to monitor their accounts for any suspicious activity.

Malicious Fitness Applications Steal Money

iOS applications that are posing as fitness-tracking tools have been stealing users' money by taking advantage of the Touch ID feature.

Cyber-security researchers have discovered several fraudulent, malicious applications that masqueraded as fitness apps on the iOS store. The applications abused the iPhone's Touch ID feature to place payments. Both apps, called "Fitness Balance app" and "Calories Tracker app" appeared legitimate and had multiple five-star reviews. However, when a user first downloaded the app, it requested that the user scan their fingerprints. Once scanned, a pop-up briefly requested payments before disappearing. If the user has a credit or debit card connected to their Apple Account, the apps verified the purchase and sent the money to an unknown malicious actor. The apps have since been removed from the iOS store.

Pinkerton assesses that the apps were likely developed by the same unknown malicious actor and display a great degree of sophistication. While the apps have been removed, Pinkerton finds it highly likely that the malicious actor will attempt similar schemes in the medium term. Pinkerton recommends that clients using iOS only install vetted, approved apps on enterprise devices. Pinkerton recommends that clients using fitness apps and other apps that request permission for payments, closely monitor linked accounts for any suspicious activity.

Data Breach Hits 100 Million Quora Users

Quora admits some data was compromised due to unauthorized access by a malicious third party.

Question-and-answer website Quora disclosed through e-mail that the personal information of about 100 million users was compromised due to a data breach orchestrated by "a malicious third party" on November 30. The compromised information included users' names, e-mail addresses, encrypted passwords and data externally linked to Quora from social networking platforms such as Facebook and Twitter. The company stated that some users were impacted more than others and is in the process of notifying affected users and resetting their passwords to protect information in all the accounts.

Pinkerton assesses that malicious actors will likely continue to target vulnerabilities in websites similar to Quora to conduct cyber-attacks and extract users' personal information. Pinkerton recommends that clients using digital social interaction platforms such as Quora provide minimal personal information while signing up and periodically change the passwords of connected social media accounts. Pinkerton further recommends clients who use Quora monitor their information over the short to medium term for any suspicious activity. If clients have further queries regarding the data breach and best practices to safeguard personal information, Pinkerton recommends clients visit the following website: https://help.quora.com/hc/en-us/articles/360020212652.

TECHNOLOGY & INFORMATION RISK

Hazard & Event Risk
Operational & Physical Risk
Technology & Informational Risk
Market & Economic 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