CYBER SECURITY BRIEFING

A Monthly Recap of Technology & Information Risk

PINKERTON®

APRIL 2019

More Than 1 Million Asus Computers Compromised

ASUS software update allows hackers to install back doors to retrieve specific MAC addresses, and target specific users.

Last month, researchers from Kaspersky Lab discovered that during 2018, ASUS suffered a security breach that would have compromised more than 1 million computers worldwide. So far, the state-backed hacking group Barium APT has been designated as the author of the cyber-attack. The attack allowed the hackers to install back doors in ASUS Live Update to retrieve specific MAC addresses, the device's unique network identifier, to target specific users. Then, the cyber-attackers performed a supply chain attack in which they inserted malicious code in a fraudulent update, signed with real ASUS digital certificates to legitimize its download and to make it remain unnoticed. The researchers notified Asus of the attack on January 31.

Pinkerton expects the real impact of the attack to be known in the following days as Kaspersky notified other anti-virus firms of the attack. So far, Symantec announced that 13,000 of its users were affected and Kaspersky has detected 57,000 cases since the investigations began. In September 2017, another massive supply chain attack surprised 2.3 million users of CCleaner cleanup software; and another cyber-attack, allegedly performed by Barium Apt, was reported in July 2017, when the group compromised NetSarang's software, affecting millions of devices. Pinkerton advises all Asus clients to remain aware of the company's announcements on the matter. Furthermore, if clients are users of Kaspersky antivirus software, they are encouraged to download a specially designed tool developed by the cybersecurity firm to determine if their device has been compromised.

FEMA Discloses Data Breach Affecting Over 2.3 Million People

FEMA data breach leads to disaster victims' information exposed.

The United States Federal Emergency Management Agency (FEMA) has informed that due to a mistake, the data of 2.3 million beneficiaries of the Transitional Sheltering Assistance program was exposed. FEMA declared that it shared the database which contained unnecessary data like date of birth, residential address, and in some cases sensitive data linked to bank accounts with an outside; reportedly, the agency revealed the financial data of at least 1.8 million people affected by the hurricanes Maria, Irma, and Harvey. Currently, the Agency has taken corrective steps to delete the information from the contractor's system; furthermore, it has updated the contract with the contractor to guarantee the compliance of its information exchange and cyber-security protocols.

Pinkerton assesses that because of the nature of the exposed data, this breach is likely to pose a significant threat to the impacted persons. Fraud and identity theft are the crimes that likely could happen if a malicious actor got a hold of the database. Pinkerton finds it likely that the FEMA will take further actions to prevent future data breaches. At present, it has announced that its workers will have additional training on security and privacy according to the Department of Homeland Security. Pinkerton assesses an even chance that in future contracts of service providers that receive personal data, the FEMA will include as a requirement specific measures linked to cybersecurity and information safekeeping. Pinkerton advises clients working with the FEMA or similar agencies to assess the probable impacts it could have an obligation to comply with those cyber-security standards. Pinkerton advises potentially impacted clients or workforce to closely monitor financial and credit statement for any abnormal activity in the medium to long term.

Manufacturing Company Discloses Data

A WordPress flaw is allowing unauthenticated remote attackers to hack websites.

WordPress developers have announced the release of the 5.1.1 version after a RIPS Technologies GmbH researcher, a cybersecurity consultant, discovered a flaw in the Content Management Software (CMS). The CMS oversees the creation and manipulation of digital content, including program coding. The vulnerability is executed when the hacker performs a Cross-Site Request Forgery (CSRF) attack - when a trustworthy user inserts malicious code in a website - by commenting in the sites comment section, which is an automatic feature on all WordPress versions before 5.1.1. This is the first time that a vulnerability can be exploited remotely by an untrustworthy user on WordPress.

Bearing in mind that the researcher reported the vulnerability in the comment section – thus affecting all sites – and that malicious attackers can exploit it remotely, Pinkerton assesses that the mentioned flaw poses a significant risk to clients using WordPress. Although WordPress downloads security updates automatically, users have the possibility of turning off this functionality. Therefore, Pinkerton recommends all clients that have developed websites within this platform, to ascertain if it is running under the version 5.1.1 and, in case it is not, to download it at the earliest convenience. Pinkerton further recommends considering making backups of the published information, in the event of probable malicious attacks prompted by potential vulnerabilities.

Citrix Announces Data Breach

Citrix found a data breach in which Iranian hackers stole 6TB of sensitive data.

Recently, Citrix announced that they had found a data breach which compromised 6TB of their clients' sensitive information. As disclosed by the company, the FBI warned them that Resecurity, a cybersecurity firm, had discovered the breach on March 6. The hackers performed a password spraying attack, which consists of finding and exploiting the less secure passwords to spread malware and gain special permissions to gather the desired information. According to Resecurity, the attack was directed by the Iranian-backed hacking group IRIDIUM.

This serious data breach, facilitated through the simple and highly effective method of password spraying, highlights the need for increased password security practices. A research study by the UK's National Cyber Security Centre (NCSC) found that 75% of employees from participating organizations used one of the top 1,000 passwords. IRIDIUM previously conducted a cyber-attack on Citrix in December 2018 and has been linked to more than 200 attacks worldwide. They mainly target technology and energy companies but have also attacked government agencies. Pinkerton advises all clients relying on Citrix to contact the company immediately to ascertain if their information was compromised. Further, organizations are encouraged to reiterate the importance of strong passwords to their employees and consider the use of multi-factor identification to reduce the risk of successful cyber-attacks.

New Campaign Using Ursnif And Bebloh Trojans Reported

New Ursnif tojan is targeting tens of thousands of users across Japan.

The cyber-security company Cybereason issued a report on a new malicious campaign carried out in Japan, which uses Ursnif trojan to steal bank-related information. The cyber-attack begins when the user receives a phishing email that contains an infected Office document, which asks for permission to enable macros; thus, tests to verify if the victim is in Japan begin. Once it is confirmed, a PowerShell payload – fixed in an image – executes Bebloh trojan, which would later download the Ursnif from the malicious actor's server. Attacks using the mentioned trojan are not uncommon in the country; however, in this campaign, the hackers have overhauled and added functionalities that make it more persistent and difficult to detect. Some of the features are modules targeting anti-PhishWall and Rapport; IE, Outlook, and Thunderbird stealers; and software specialized on disk encryption and theft of cryptocurrency.

Pinkerton assesses that attackers will continue to develop malicious campaigns in the long-term; those likely will keep using Ursnif trojan in combination with other malware to target Japanese users of online banking services. The mentioned trojan first appeared in 2013, but its usage has been extended since its code became public in 2015. Furthermore, the expansion of financial services has also made this type of attacks more attractive. Pinkerton finds it that there is an even chance that the module focused on disabling the anti-PhishWall and Rapport functions and poses a risk to the potential victims. Although the researchers were not able to corroborate that said module is running as the attackers intended, its presence denotes an interest in overriding security measures; those features likely will be worked on in future campaigns. Pinkerton recommends clients operating in Japan to consider informing personal that manages bank credentials of this new malicious campaign. Pinkerton further advises clients ascertaining the origin of office documents before enabling macros.

Vulnerability Found In Google Chrome

Google Chrome Zero-Day vulnerability being exploited.

Researchers from Google's Threat Group announced that they found a vulnerability in Google Chrome that is already being exploited by cyber-attackers. The vulnerability was named CVE-2019-5786 and exists in a use-after-free bug (a flaw that lets attackers modify the memory, allowing them to grant themselves special privileges) in File Reader. File Reader is an API, which is a set of protocols, routines, and communications that permit software interaction. Through this vulnerability, the cyber-attackers could have privileges inside Google Chrome that allowed them to run malicious code and evade the browser's sandbox and malicious software detection programs. Google has announced that a patch to solve the issue is now available and will be implemented via the browser's update.

Pinkerton finds likely that the real impact of the vulnerability will be disclosed in the following weeks as Chrome developers will not release the technical details of the flaw until its users are out of peril. This vulnerability affects all Chrome users with devices supported by Windows, Linux, or Mac operating systems and can be exploited by just entering an infected site. Pinkerton advises all clients using Google Chrome to download the update immediately and to remain aware of Google's statement regarding the technical details of the vulnerability as more internet related features may have been affected.

Several Universities Targeted By Cyber Espionage Attack

MIT and other universities have been singled out by a cyber-espionage group for naval secrets.

It has been reported that at least 27 universities in the U.S., Canada, and South East Asia – including The University of Hawaii, the University of Washington, Duke University, South Korea's Sahmyook University, and the Massachusetts Institute of Technology (MIT) –, were victims of a cyber espionage attack. Presumably, the purpose of the attacks was to obtain maritime information regarding warfare and technology strategic information of submarine missiles. iDefence, the cybersecurity intelligence unit of Accenture Security, explained the hackers used spear phishing tactics, which consisted of sending emails presumable sent by trusted organizations and contained a malware that let the attackers access the information of the targets. Most of the affected institutions are part of the Woods Hole Oceanographic Institution hub of oceanographic research at the U.S., which has close relations with the U.S. Navy. The alleged cyber-attacker is a Chinese group named Mudcarp, also known as Temp, Periscop, and Leviathan.

Pinkerton assesses that these attacks are likely to be part of a larger espionage strategy, as Chinese hackers have been accused of previous cyber campaigns focused on obtaining strategic military, corporate, and civilian technology. This is not an isolated case; in past days, FireEye informed that Periscope had launched a phishing campaign that targets engineering, defense, and transport companies in the maritime sector. FireEye, also indicated they found that a great number of the attacks targeted Germany, U.S., and UK; countries that are imperative for the Chinese Beal and Road Initiative. Pinkerton recommends all clients to increase their security measures as well as to alert their IT teams to look for phishing emails and malicious malware in all their servers. Moreover, all clients are advised to encourage their employees to avoid downloading files or opening links coming from unverified sources.

Phishing Campaign Targeting Maritime Sector

Engineering, transport, and defense companies are being targeted by Chinese hackers via phishing emails.

FireEye researches released a report on the activities of a cybercriminal group identified as Advanced Persistent Threat 40 (APT40). FireEye has found that the group, also known as Periscope, has launched a phishing campaign that targets transport, engineering, and defense companies in the maritime sector. The researchers observed that enterprises with active operations in the South China Sea or conducting investigations on maritime topics were also attacked. At present, APT40 is using phishing emails to distribute malware like Gh0st RAT trojan to compromise the companies' network; once the latter is accomplished, the attackers will gather specific credentials to extract the desired information. Based on the areas and the hours APT40 is operating, FireEye has hypothesized that the group is based on Beijing.

Pinkerton finds it likely that the phishing campaign will continue in the mid-term as the criminal attacks are very profitable and in constant evolution, making it difficult for anti-malware software to spot them. Since mid-2018, another hacking group known as DarkHydrus APT started a massive phishing campaign using Google Drive as their control-and-command center (C2) to avoid detection. Moreover, according to FireEye researchers, the hacking group APT40 has links with the Chinese government. Pinkerton recommends all clients with operations in the South China Sea to increase their security procedures as well as to alert their IT teams to search for phishing emails and malicious software in the company servers. Furthermore, all clients are advised to encourage their employees to avoid downloading files or opening links coming from unverified sources.

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