CYBER SECURITY BRIEFING

A Monthly Recap of Technology & Information Risk

PINKERTON®

MAY 2019

Vulnerability In Oracle WebLogic Server Benefiting Hackers

Hackers are found to be exploiting Oracle WebLogic RCE flaw to aid in spreading ransomware.

Cybersecurity specialists from Cisco Talos have detected that hackers are benefiting from the vulnerability found in Oracle WebLogic Service to spread ransomware named Sodinokib. This ransomware was designed to encrypt files in the directory of the users and delete them. The victims have been forced to pay up to 2,500 in Bitcoin (USD 13.26 million) -the amount is duplicated if the user does not pay within the specified days - for recovering their files. The execution of Sodinokib does not need the interaction with users; that means, the victim is not requested to open a malicious link or email to be affected.

Pinkerton assesses that hackers are highly likely to continue to successfully exploit the Oracle WebLogic vulnerability in short to medium term as this ransomware was designed to be installed even when avoiding opening any malicious malware. Pinkerton advises users to be cautious and monitor their network for unusual activity. Owners of bitcoin accounts as they are likely targets of cyber attacks. Pinkerton recommends clients download and update their Oracle WebLogic version as the company made his latest version available after the vulnerability was detected in their system.

Researcher Finds A Critical Unpatched Flaw In Oracle WebLogic

The Oracle WebLogic application was found to contain a critical deserialization remote code execution vulnerability that affects all versions of the software.

Recently, cybersecurity researchers from KnownSec 404 shared a post to warn enterprises of an unpatched flaw in Oracle WebLogic server application. Oracle WebLogic is a Java-based multi-tier enterprise application server that separates the different application operational layers, which allows companies to quickly deploy new products and services on the cloud. The vulnerability is a deserialization remote code execution that affects the versions WebLogic 10.X and WebLogic 12.1.3. The flaw allows attackers to remotely execute arbitrary commands on the affected servers by sending a malicious HTTP request without authorization requirements. Most of the Oracle WebLogic servers are located in the United States, China, Iran, Germany, and India.

Pinkerton finds it likely that these flaws will continue to affect Oracle WebLogic users in the medium term as Oracle only releases security updates every three months and the last one was published this month. Researchers have already shared the details of the vulnerability with Oracle's team. However, the flaw is unlikely to be patched until July. According to ZoomEye cyberspace search engine, there are approximately 36,000 WebLogic servers with public access, and it is not known how many have the vulnerable versions. Pinkerton recommends clients who use Oracle WebLogic application to constantly update it to the latest version to avoid having the past vulnerabilities. Researchers suggest users find and delete "wls9_ async_responde.war" and restart the WebLogic service or prevent access to the "/_async/ and /wls/wsat/ URL via access policy control. Further, Pinkerton advises clients who reside in the mentioned countries to verify any anomalies in the application.

Britain's Government Restricts Huawei's Products

Theresa May has ordered that Huawei be banned from supplying core parts of the upcoming 5G mobile phone network.

After a meeting at the National Security Council, media reports claimed that the British Prime Minister would restrict the commercialization of specific Huawei's products due to security concerns. However, the government has not officially released the statement. According to these reports, the British phone companies will be able to buy "non-core" Huawei's technology, but the core parts of the 5G network are banned. Many countries, led by the U.S., have limited all or certain products of the Chinese company. Nonetheless, the company has denied the espionage and sabotage claims and has stated that Huawei is not controlled by the government several times.

Pinkerton assesses that the restrictions and regulations of Huawei's products will likely continue in the UK and other countries in the medium to long term, as the U.S. government has been promoting these actions. Additionally, the government has been prioritizing the development of a cybersecurity system. Pinkerton finds that the British government is divided due to the different postures about the Huawei's issue, like the home, defense, and foreign ministries are concern about the long-term consequences of these products. Nonetheless, the head of the National Cyber Security Center has claimed that the company's network is "sufficiently safe." Pinkerton assesses as likely that this case could set a precedent of product's restrictions of foreign companies in the sector. Furthermore, Pinkerton advises clients monitoring the CYBERUK event organized by the National Cyber Security Center on April 24-25, where the private and public sector will discuss this matter. During the event is expected that the government will officially confirm the announcement and would propose new strategies regarding cybersecurity.

Hacker Downloads Thousands Of Confidential Documents From Embassy

Hackers stole thousands of documents from Mexico's embassy in Guatemala, and posted them online.

In recent days, the Mexican Ministry of Foreign Affairs confirmed that the Mexican Embassy in Guatemala suffered a cyber-attack. On April 15, 2019, a hacker, found on Twitter as w@)x55Taylor, posted the Embassy's stolen data online. It is estimated that at least 4,800 sensitive documents of the diplomatic staff were downloaded from the database of the Embassy. Among the information illegally obtained were scanned passports and visas, consular activities reports, birth and death certificates, payment cards, letters of diplomatic immunities, rights and privileges to the diplomatic employees, confidential documents, information of imprisoned Mexicans in Guatemala, documentation of the employees' vacations and time off, vehicles, and medical expenses. The Mexican government announced that the failure on the database had been repaired so that the information is no longer available for downloading it; however, the hacker sent a link to the site TechCrunch with the backup of the documents.

Pinkerton finds it highly likely that these types of cyber-attacks are expected to continue in the near and medium term as many Embassies do not have the adequate security measures to protect their databases from hackers. This attack was directed by a hacker who admitted that in the past he has found vulnerabilities in other sites and has asked to be paid for his discoveries in exchange for not publishing the information found. Pinkerton advises all clients, especially those utilizing the Mexican Embassy in Guatemala, to take the proper security measures as sensitive information was shared publicly and could be used for malicious purposes. Pinkerton recommends all clients to reinforce the database system of their companies and the government websites, to protect them against any attack, primarily if it contains confidential information of their employees.

Hackers Steal Passwords Through Instagram's Nasty List

The 'Nasty List' phishing scam is being used by hackers to steal passwords on Instagram.

A phishing scam called 'The Nasty List' operating through Instagram was reported to be harvesting users' login credentials. 'The Nasty List' attempts to obtain sensitive information by disguising as a trustworthy entity. This phishing scam sends a direct message (DM) through an already compromised account followed by the targeted user. "OMG your (sic) actually on here at number 38" or "WOW. Your (sic) on here!!! ranked 100" are the most typical DMs that 'The Nasty List' uses to initiate the cyber-attack. The message includes a link to a fake Instagram log-in, where users are supposed to provide their username and password. As reported by Microsoft, phishing attacks increased by 250% during 2018. This method has demonstrated to be more effective than others, as it does not rely on technical deficiencies, but on users' lack of cybersecurity awareness.

Pinkerton assesses that Instagram users who provided their credentials through 'The Nasty List's fake log-in are likely to have their accounts compromised. Attacked users should check if they can still log-in with their credentials, and in that case, they should change their password as soon as possible through the site settings. A good practice is to create a six character or plus password, using a mix of letters, numbers, and punctuation marks. Users whose passwords were already modified should get in touch with the Instagram Help Center to regain control of their accounts. Pinkerton recommends, as to prevent any further phishing attack, to set up Two-factor Authentication (2FA), which is an extra layer of security used to ascertain that a user is the owner of the presented credential. A 2FA would only permit access after successfully presenting two or more pieces of evidence as an authentication mechanism. The setting process of 2FA is explained in detail on the Instagram Help Center.

Sophisticated Spyware Framework Called TajMahal Detected

JustDial, India's largest local search service, is leaking information of customers who accessed the service via website, mobile app, or calling.

Cyber-security researchers have revealed a highly sophisticated spyware framework called TajMahal which was possibly created five years ago. The Advanced Persistent Threat (APT) is a high-tech, modular-based malware toolkit which contains various malicious espionage plugins. The TajMahal framework consists of two packages: "Tokyo" and "Yokohama," which contain 80 different malicious modules. These modules are encrypted in a Virtual File System (VFS), and they log keystrokes, steal browser data, record and take screenshots, and steal documents sent to the printer queue and a particular file from a USB.

Pinkerton finds it likely that this malware will affect users in the medium term even if Kaspersky has only detected one victim case. Further, researchers still do not know how all the modules in the VFS work. Hence, variabilities in the toolkit are likely undetected. The toolkit was used in 2018 by hackers to spy on diplomatic organization computers from a Central Asian country, but researchers suspect that the hacker group has been active since 2014. As the malware focuses on spyware functions, it is highly likely that both government-related individuals' and businesses employees' computers are at risk.

Hotels Involuntarily Leak Clients' Private Data Everyday

Symantec Corp found that 2 out of 3 hotels inadvertently leak guests' personal data.

Symantec Corp, an American company that provides cyber-security software and services, released a study which compiles information from more than 1,500 websites from hotels in 54 countries. The study reported that two out of three hotel websites unintentionally allow third-party sites to look at personal and booking information from clients. Symantec reported that the exposed information included full names, email addresses, credit card, and passport details. The company also stated that this information is likely to be used by cyber-criminals who are interested in government and business influential personnel. Other actors that could use the private information are advertisers who track user's browsing tendencies and tastes. Further, the researchers explained that the leak of guests' data normally occurs when the hotel site sends confirmation emails that include a direct link to the booking information.

Pinkerton finds it likely that this security breach continues to affect users in the medium term as 25% of the data privacy officers of the studied hotel websites did not respond to Symantec's results and caution notice. Further, some hotels admitted they are still updating their systems to comply with Europe's new privacy law, the General Data Protection Regulation (GDPR), which went into effect last year. As online hotel reservations are more broadly used, the information of millions of clients is likely to be compromised when booking through hotel websites. On December 4, 2018, Marriott International suffered a data breach that exposed personal information of approximately 500 million people. Pinkerton recommends clients that are planning to make a hotel reservation online to take precautionary measures.

Spyware App Misused iOS Certificates To Track User Information

App abuses the iOS enterprise certificate to bypass Apple's App Store rules.

It has been reported that a spyware app, called Assistenza SIM, misused iOS certificates to track user contacts, videos, photos, and real-time location data. There are indications the spyware could also record phone calls remotely. Apple has already revoked the app's enterprise certificate, which enables its installation on iOS devices. An earlier version of this spyware tracked Android user information and got access to Wi-Fi passwords and emails, as well as data from apps like Facebook, Gmail, WhatsApp, Viber, and WeChat. In both cases, Assistenza SIM pretended to be a carrier helpline app that users could install to get in touch with the operators. Spyware such as Assistenza SIM work in the background and cannot be detected by users after installing the app on the phone and entering the license key. This enables the app to monitor, track information, and store it on the cloud. Spywares pretend to offer content which Apple would not normally allow (such as pornography, gambling, and online piracy), inciting the users to install the app, provide some credentials and continuously have internet access.

Pinkerton assesses that the users who installed Assistenza SIM on their iOS devices are highly likely to have had their information and calls stored by the app developers. Even though Apple has prevented users from installing this spyware app, information already leaked is presumably available to purchase online. Assistenza SIM is not the only spyware of its kind; many malicious software developers are likely to evade cyber-security scrutiny through the Apple Developer Enterprise Program, which only requires them to pay USD 300 (EUR 266) annually to distribute their apps. Pinkerton recommends, when installing apps on devices, to verify if the content offered observes Apple's guidelines, and to verify if they are trusted app providers.

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