CYBER SECURITY BRIEFING

A Monthly Recap of Technology & Information Risk

PINKERTON®

FEBRUARY 2019

Ad Agency Targeted By New Magecart Group

A new threat actor operating under the "Magecart" umbrella landed a skimmer on hundreds of websites through a supply chain attack.

Security researchers at RiskIQ reported a new group as part of the Magecart collective which recently targeted French advertising agency Adverline. The new group, known as Magecart Group 12, conducted their attack by injecting malicious code into a JavaScript library that controls retargeting advertising. The malicious code, similar to previous Magecart attacks, contains a web-based skimmer which steals credit card information. As a result of the attack, Trend Micro identified over 270 e-commerce sites with the skimmer installed, across a range of commerce lines. Some affected sites included those used for travel, cosmetics, healthcare, and apparel. As noted by security researchers, the skimmer code prevents deobfuscation and analysis by conducting frequent internal integrity checks.

Pinkerton assesses that given the ongoing success of Magecart attacks, they will continue in the immediate to long term. Additionally, with a new threat group joining the Magecart collective, Pinkerton assesses it likely that there will be both an increase in attacks as well as significant developments and innovations to the coding used to conduct them. Pinkerton advises clients who have conducted any e-commerce activities with companies based in France to monitor their credit card bills for abnormal activity. Additionally, given Magecart's willingness to attack high-profile targets such as attacks on Ticketmaster, British Airways, and Newegg last year, any clients involved in e-commerce are advised to ensure all cyber-security measures have the most recent security patches and updates installed, and that cyber-security best practices are being used to secure commerce networks.

Flight Booking Vulnerability Affects Airlines

Flight travelers around the world were exposed to a flight booking system flaw that allowed hackers to access and modify travel details and claim frequent flyer miles.

A cybersecurity researcher discovered a vulnerability in the flight booking systems powered by the Amadeus system, which is used by 141 airlines around the world, including major carriers such as Lufthansa and United Airlines. The researcher found that an attacker only needs to get the victim's Passenger Name Record (PNR) and use it in the link that is sent to users with their booking confirmation, specifically by replacing the value of the "Rule_Source_1_ID" section. The attacker then has access to the victim's ID and last name, and can access their airline account and retrieve the user email and phone to cancel flights, assign meals or seats, and transfer the frequent-miles credit to another account.

Pinkerton assesses that the impact of this flaw will be significant for the airline industry in the medium-term, as the information of millions of users may have been breached, especially because the PNR authentication system did not have a brute force lock, so the cyber-attacker could try infinite combinations without being stopped. Amadeus has stated that the vulnerability has been addressed with the implementation of captchas, anti-bot protocols, and enhanced passwords. Additionally, Amadeus has installed a Recovery PTR to secure users' sensible data. Pinkerton recommends all clients to revise that their flight booking accounts have not been vulnerated, and if they have, to immediately notify the corresponding airline. Furthermore, all clients are encouraged to change their account's username and password as soon as possible to ensure the account's security.

Researchers Find Oklahoma Department Of Securities Data Leak

A misconfigured sever was found to be exposing terabytes of data from the Oklahoma Department of Security.

Cyber-security researchers from UpGuard identified the exposure of approximately three terabytes of data from the Oklahoma Department of Securities on December 7, 2018. The exposure occurred because of an unsecured rsync service on an Oklahoma Office of Management and Enterprise Services owned IP address, which allowed users to download all stored files at that location, including personal information, internal documentation, communications, and system credentials from 1986-2016. The Securities Commission used outdated software, further exacerbating the security risk. Of particular note, the exposed data included email backups, identification card images, tax documents, passwords, and internal strategy communications. The exposed information also included data for 10,000 brokers, including social security numbers, birth dates, genders, and other personally identifying information. Cyber-security researchers also identified credentials for remote access to Department of Securities computers, IT services, and third-party security filing credentials.

Pinkerton assesses that the high-profile incident highlights the threat posed by the use of outdated software and technologies. Due to the sensitivity of the exposed information, Pinkerton finds it highly likely that the exposed credentials and securities information will lead to malicious campaigns and identity theft activities. Of particular note, due to the nature of information exposed, Pinkerton assesses that realistic phishing campaigns are likely to be employed. Pinkerton recommends that clients who operate in Oklahoma or have historically done so monitor accounts for suspicious activity and monitor any associated email accounts for phishing attempts.

Malvertising Campaign Targets P2P Users With Multiple Threats

Users of P2P sites should be aware of a malverting campaign with a twin threat: info-stealing malware and ransomware.

Cyber-security experts have confirmed that a campaign of malicious advertisement (malvertisement) targets users of Peer-To-Peer (P2P) sites to deploy multiple threats. Video streaming and torrent sites are more likely to be affected by these threats because site administrators rarely regulate or verify advertisers. Thus, malicious operators are known to introduce ads with the intention of luring users into domains where exploit kits are deployed. The most recent malvertising campaign was observed to use the Fallout EK and GrandSoft EK. Fallout is the most common exploit kit according to researchers. It works by breaching the system and then deploying two systems that increase the likeliness of payout for the attacker: the Vidar info-stealer and the GrandCrab 5.04 ransomware. In this way, attackers will steal sensitive information first and then encrypt the target files to demand a ransom.

Pinkerton assesses that criminals will continue to favor the use of ransomware attacks; this type of attack is expected to become one of the major cyber threats for 2019. Pinkerton further finds that the use of uncertified sites carries a very high risk of being the victim of cybercrime. The sophistication and availability of malware make attacks easier to carry out and more profitable. For instance, the Vidar system is available online for USD 700 (EUR 606.2), and it is easy to customize and program to deploy massively. Users can program the software to steal specific information such as system data, saved passwords, or digital wallets. To effectively deploy the malware, exploit kits such as Fallout can detect and analyze the user's browser history to deliver malicious content specific to the user. Pinkerton advises clients to avoid visiting uncertified websites; if doing so, avoid clicking on banners and pop-ups. It is also recommended to make regular back-ups in external drives to limit the effectiveness of ransomware attacks.

Manufacturing Company Discloses Data

Hackers were able to compromise the Titan Manufacturing and Distributors, Inc. computer system to steal payment card data for over a year.

Titan Manufacturing and Distributors, Inc. announced that unidentified cyber-attackers were able to hack its systems and installed a malware, which allowed them to extract customers' data even though the company does not keep records of it. The malicious software was set up on November 23, 2017, and remained in function until October 25, 2018. Therefore, all clients that used the company's online services during the mentioned period might have had their data stolen. Investigations suggest that the compromised information is: name, telephone number, billing address, as well as the number, expiration date, and verification code of credit cards used in transactions. At present, the company continues investigating the incident with a third party.

Due to the highly sensitive banking information that was compromised during the cybersecurity incident, Pinkerton assesses that it poses a significant threat to all clients that used Titan Manufacturing and Distributors online services during the stated period. Although on its disclosure statement the company did not give the numbers of affected customers, in another communication it was divulged that at least 1,838 residents in Washington were impacted. Pinkerton advises all potentially affected clients to exercise caution and closely monitor credit statements in the medium to long term for any unusual transactions. It is highly likely that the company will contact and notify the affected clients via e-mail of this incident during the present week and give further instructions on the measures taken to protect its clients' safety. Therefore, Pinkerton recommends potentially affected clients to be aware of the company's message to ascertain if their data was stolen and, if positive, to consider the given recommendations.

Unprotected Database Exposes 200 Million Resumes

Chinese job seekers had resumes accessible to anyone without authentication due to an unprotected MongoDB database.

Cyber-security researchers discovered an unprotected MongoDB database that appeared to expose the scraped data of 200 million individuals in China. The cache contained resume information for job seekers and included such data as personal information, job expectations, and professional experience. Cyber-security researchers initially discovered the database on December 27-28. It is unknown how long the database was unprotected. The data appears to have been scraped by a tool from websites that contained resume details. According to cyber-security researchers, a dozen IP addresses were noted in the database's log.

Pinkerton assesses that the exposed data will highly likely be used by malicious actors to conduct phishing attempts in the medium term. Pinkerton finds it likely that the data will enable malicious actors to make phishing attempts appear more legitimate, increasing the threat posed by any such campaign. Pinkerton further assesses that the resumes will likely increase the insider threat in China as malicious actors are able to use the resume data to appear more legitimate or masquerade as qualified candidates. Further, Pinkerton finds it likely that the data will be used by malicious actors in identity theft activities. Pinkerton recommends that clients who maintain online resume profiles in China watch for suspicious activity and monitor any associated email accounts for phishing attempts.

New Mobile Scamming Attack Targets WhatsApp Users

WhatsApp users are advised to not click on the my-love.com link, which steals personal data from phones.

This past month, the Federal Ministerial Police (PFM) issued a cyber-security alert about the propagation of a link in the instant messaging app, WhatsApp that steals personal information from smartphones. Through a statement, the authorities reported that by clicking on the link, a webpage called my-love.com, which pretends to be a Christmas card, is opened. Once the user enters the website, personal information is stolen. After that, the unaware victim is encouraged to forward the message to one of their contacts. The PFM recommended ignoring the message, whether it comes from unknown or saved contacts or numbers, and under no circumstances click to open the alleged Christmas card.

Pinkerton finds that WhatsApp is among the fastest growing instant messengers and practically a social network in itself. In this tendency, it is essential to follow some measures to ensure the security and privacy of personal information. To reduce the security risk on devices, including cell phones, Pinkerton recommends clients to avoid accessing information whose source is not reliable. A good practice is to eliminate all types of unsolicited messages and emails to prevent being a victim of a scam. Additionally, Pinkerton advises adopting technology that shields financial, personal, and economic information by using defensive software and installing anti-malware protection on all devices. Recently, the Institute for Independent Research in Information Security Issues in Germany (AV-TEST) published an evaluation of the new antivirus available for Android devices; the details can be found at https://www.av-test.org/en/antivirus/mobile-devices/..

Hospitals Exposed To Cybersecurity Threats

According to the Clearwater Cyberintelligence Institute, excessive user permissions and endpoint leaks are two of the most common cyber risks for hospitals.

According to a new report that has been issued by the Clearwater Cyber Intelligence Institute, the three most common cyber risks threats that hospitals currently face are user authentication deficiencies, endpoint leakage, and excessive user permissions, which in total constitute 37% of all critical risk scenarios. These three risks were identified through IRM Analysis, which is a database of millions of risk records which have been gathered over the last six years from NIST-based risk analyses of Clearwater customers. It is important to consider that the results of this analysis take into consideration only the risk profiles of hospitals, Integrated Delivery Networks, and business associates.

Pinkerton considers that these three risk vectors will be an increasing security concern among institutions involved in the healthcare providing industry during the near-future. The most critical of these risks are those related to authentication deficiencies, as they are the most easily preventable and the gateways to making the other types of risks more easily exploitable. To mitigate these risks, Pinkerton recommends clients to set up password strength requirements, put in place single sign-on controls, and setting up locking account mechanisms after too many failed login attempts. Regarding the other two risks, it is recommended to consult an expert in order to establish suitable security measures 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.

Data Of 30,000 Victorian Civil Servants Stolen

The work details of over 30,000 government employees were stolen during a data breach in which part of the Victorian Government party was downloaded by an unknown party.

Recently, an unidentified attacker gained access to a directory of the Victorian Government; stealing the data of 30,000 local civil servants. The document, which is for internal use only, contained the names, positions, official phone numbers, and e-mails. The attacker might have also stolen cellphones numbers if they were included in the directory; however, no bank related information was compromised. The authorities notified the affected parties and remitted the case to the Office of the Victorian Information Commissioner and the Australian Cyber Security Centre for further investigation. A spokesman of the Premier's Department has stated that measures will be taken to avoid future breaches.

Although the stolen data does not appear to be highly sensitive, Pinkerton assesses that the breach has an even chance of impacting both Victorian civil servants and clients in close communications with them. At present, the intentions of the attacker behind the data breach are unknown; consequently, the authorities have warned the civil servants of possible phishing schemes, social engineering, or other malicious activities. If there is an increase in such deeds, Pinkerton assesses there could be three likely objectives, which are gaining further data of civil servants, obtaining information related to internal workings, or gathering information of related third parties. Pinkerton recommends clients residing in Victoria or maintaining contact with local authorities to be aware of possible unsolicited communications in short to medium term. Moreover, Pinkerton advises not volunteering sensitive information without first ascertaining the legitimacy of the communication.

Phishing Reported Against Netflix Users

A new phishing method was discovered in which the scammers pretend to be Netflix are is deceiving users in Mexico to provide personal data.

Last month, the cyber police of Sonora State in Mexico warned about a new phishing method that is being used against Netflix users in Mexico. Per reports, the scam is carried out through a message stating that a payment method update is necessary. By using Netflix's official logo and username, users are deceived into providing personal data to the scammers. Such information includes –but is not limited to– username, password and payment information. Up until the writing of this report, there are no reports of similar scams happening in countries other than Mexico.

Pinkerton assesses that fake messages to Netflix clients constitute a severe risk for user's information as, according to reports, the attacker's account has not been disabled yet. False messages may contain or have applications that download malicious malware directly into the client's device. Considering these risks, Pinkerton suggests clients that have been affected to contact the Netflix Company and to ignore all received messages until the problem is solved. Pinkerton recommends clients to ensure their devices are updated and to change their passwords in case their information has been compromised.

TECHNOLOGY & INFORMATION RISK

Are the proper controls in place to fully protect your bottom line?

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

“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

©2019 Pinkerton Consulting & Investigations, Inc. All Rights Reserved.