CYBER SECURITY BRIEFING

A Monthly Recap of Technology & Information Risk

PINKERTON®

DECEMBER 2018

Amazon Email Accounts Exposed Before Black Friday

A web site issue caused some Amazon user's email addresses to be disclosed during a data leak.

Before Black Friday, Amazon user's email addresses were exposed due to a technical error. Amazon notified users that email addresses disclosed had been resolved. However, little information is available regarding the technical error or how long emails were exposed. Amazon notified users via email, stated there is not a need to change passwords or take any further action.

As the incident took place right before one of the largest shopping seasons of the year, Black Friday, Pinkerton finds it likely that malicious actors obtained access to user's email addresses. Pinkerton finds it likely that phishing attacks are to occur in the short to medium term, especially as other shopping holidays occur such as Cyber Monday. With the lack of information released from Amazon, Pinkerton recommends clients with Amazon accounts change their passwords out of an abundance of caution. Pinkerton further recommends clients monitor their accounts for any suspicious activity.

Uber Fined Over Data Breach

Uber has been fined by British and Dutch authorities for failing to protect customer's data during a cyberattack that occurred in 2016.

Recently, Uber was fined by Britain's Information Commissioner's Office GBP 385,000 (USD 491,000) and Dutch officials imposed an EUR 600,000 (USD 679,000) fine for violating data protection laws. These fines are over a data breach in 2016, where British and Dutch authorities state Uber failed to protect customers' data. British officials stated that there were "avoidable data security flaws" and Dutch officials said Uber did not report the breach to authorities in the 72-hour requirement by regulations. Uber has stated improvements had been made to the security systems since the cyber-attack in 2016.

Although Uber has made improvements to their security system, the fines over data protection laws will likely set a precedent going forward for other companies who may be hacked with security flaws. The UK and the Netherlands officials are likely to take into account security flaws and reporting breaches within the required timeline when determining data breach fines in the future. Pinkerton recommends clients review any security gaps to mitigate fines in the event of a data breach. Pinkerton further recommends clients in general review their cyber-security procedures to mitigate the threat of cyber-attacks.

Fancy Bear Using New Trojan In Recent Attacks

A new Trojan has been used by a well-known Russian state-sponsored cyber-espionage group targeting government entities around the globe.

Palo Alto Networks security specialists have reported that a known Russian state-sponsored cyber-espionage group known as Fancy Bear had begun using a new trojan as part of recent global cyber-attacks. The trojan is included to deliver a secondary payload in the attacks and contains an email based command and control channel. The trojan is a variant of the Zebrocy trojan, which reaches back through the command and control channel to trigger the download, this is done in an effort to avoid detection. The overarching purpose of the attacks is to gather system information, obtain access to POP3 email accounts, and obtain desktop screenshots. The primary targets of Fancy Bear are EU, U.S., and former Soviet state governments.

Pinkerton assesses that the latest evolution in attacks by Fancy Bear is highly likely an attempt to both evade detection and increase capability for exploitation. The use of the trojan to reach back to a command and control server to deliver a secondary payload increases the likelihood of successful infection, especially given the use of targeted email attachments using well-crafted documents related to recent incidents. Pinkerton advises clients who conduct business with governments in the affected regions to thoroughly examine any emails with attachments that pertain to recent disasters or security incidents to aid in preventing infection and exploitation.

Malicious Actors Target Dell Customers

Hackers were recently detected trying to steal customer information from Dell.com accounts.

Dell has announced that malicious actors initiated a cyber-attack that allegedly targeted Dell customers' data. According to the company's notification, on November 9, Dell employees detected malicious actors attempting to retrieve customers names, e-mails, addresses, and passwords from Dell.com accounts. As the disclosure states, there is no evidence to support that the unauthorized users retrieved any information or that they targeted credit-related data. However, the company will reset all customers' passwords as a measure to protect the information in all the accounts. As of the time of writing, there is no available information about the origin of the cyber-attack or about the method the malicious actors used to breach Dell's systems.

Pinkerton assesses that experts and regulators will further examine this incident in the near to medium term, and will make an announcement regarding this matter. European regulators will likely look for the enforcement of the General Data Protection Regulation if any investigation reveals data mismanagement or the fact that information has been retrieved from the malicious actors in this incident. Experts declared that more information about this incident is needed to provide a full assessment of the impact of the cyber-attack. Pinkerton recommends clients with Dell accounts reset identical or similar passwords used in other accounts. Pinkerton advises clients to monitor further reports on this incident and be mindful of unauthorized or irregular credit activities in case any sensitive information was retrieved from the company's accounts.

Commerce Websites Using Magento Are At Risk Of Hacking

Up to 80% of European Magento websites may be at risk due to a security oversight.

After the Payment Card Industry Security Standards Council European Community Meeting, an announcement was made stating that 80% of European websites that use Magento – the most used e-commerce platform in the world - are at risk of hacking. The results are part of the research carried out by Foregenix, an e-commerce security firm. The total sample under this study was 170,000 Magento websites. Of these websites, malware was detected in at least 2,548 and out of these; 1,521 are compromised by credit and debit card stealing. In most cases, vulnerabilities would be highly limited by performing routine cyber-security maintenance.

Pinkerton finds that e-commerce websites are at high risk of hacking if administrators do not maintain a cyber-security plan for their systems as these gaps let hackers get into the system. Pinkerton further finds that users of the Magento 1 (90% at risk) platform can substantially reduce the risk of hacking by installing the latest patches and, if possible, migrate to the Magento 2 platform (40% at risk). Although the number of infected websites in the study amounted only to 2.5%, this risk can be further decreased with regular updating, multi-factor password authentication and regular updates of the administrator interface.

Thirteen Critical Sectors Exposed To Hacking

A joint committee on national security in the UK is urging Theresa May to appoint a cybersecurity minister in cabinet to help build national resilience.

A few weeks ago, the Joint Committee on the National Security Strategy published its report on the vulnerabilities to the UK's Critical National Infrastructure (CNI). Thirteen sectors were assessed for vulnerabilities, among them: energy, health services, transport, and water. The committee found that the preventive measures taken so far are not enough to face the level of urgent threats the country faces. Members of Parliament(MP) found that these sectors are exposed to major and possibly catastrophic attacks. They also stated that the National Cybersecurity Centre does not have enough resources to face all threats from state and non-state actors. MPs demanded more involvement at a ministerial level and even the appointment of a cyber-security minister. The country's National Cyber Security Strategy was introduced two years ago; then, on 2017, the WannaCry ransomware attack caused a nearly one-week disruption in its National Health Service. This year, the Joint Committee assessed public and private actors within the CNI. It found that the National Cybersecurity Centre does not have enough resources to fulfill all its duties.

Pinkerton assesses that this will be a relevant matter for all clients operating in the country, especially in the 13 most affected sectors, in the long term. Pinkerton finds that the UK is struggling to create effective public policy and to manage its cyber-security institutions with highly skilled personnel. Pinkerton further finds it likely that British authorities will introduce new regulations in the future to standardize cybersecurity capabilities in private government suppliers. It is recommended that all clients implement a wider set of cyber-security and safety measures in all their devices to avoid exposure. According to specialists, a way to minimize information risks is through a perimeter firewall, whose objective is to protect access to the local network through the Internet. It is recommended to have a physical firewall or a computer that acts as a gateway between the internet and the local network to prevent attacks.

New Cybersecurity Law To Be Implemented

A proposal for an all-powerful cybersecurity law in Thailand has some businesses and activists concerned.

Reuters has reported that the Thai government would impose a cyber-security law that would allow the government to spy on Internet users and to restrict websites with "inappropriate content." So far, it has been announced that the National Cybersecurity Committee (NCSC) would be the authority in charge of implementing the new law. According to media reports, the new amendment would allow the NCSC to carry out arbitrary invasions of privacy without a court order and to make copies of information as well as search and confiscate computer systems without needing authorization. Moreover, the NCSC could also summon businesses or individuals for interrogation and force them to hand over information belonging to other parties. Facebook, Google, Apple, and Amazon stated through the Asia Internet Coalition (AIC), which represents the four U.S. giants and seven other major internet companies, that the country could lose businesses by implementing the law. This concern is being discussed in other countries as India, Vietnam, and Indonesia, as their governments are aiming for similar regulations.

Pinkerton assesses that this will be a relevant matter for all clients operating in Thailand in the medium to long term as companies could be forced to share confidential information from both themselves and their clients. Pinkerton recommends all clients to consider the possible new law while planning any declarations and operations in order to avoid any unusual events that could make them a target for the NCSC investigators. Additionally, it is advisable to stay informed about any official declarations regarding this matter, as only the draft of the law has been presented and changes could be implemented, varying the risks and stipulations that could affect companies operating in the area. Shall the law be approved, it would most likely cause western countries to reconsider their Asian hubs for investments and information storage.

Military Targeted By Sophisticated Cyber-Attack

An undisclosed threat actor is targeting nuclear-armed government and military in Pakistan with resources necessary to modify and refine tools and malware.

Recently, security researchers with Cylance provided information on cyber-attacks conducted against Pakistan's military. The attacks were conducted by a previously unknown threat group now known as "The White Company." The attacks were a year-long campaign dubbed "Operation Shaheen" which included evading detection from eight anti-virus/anti-malware products. The campaign used CVE-2012-0158 to install remote access trojans (RATs), followed by the use of maliciously altered documents to exploit CVE-2015-1641.

Pinkerton assesses that while there is no specific information on what systems were infected, given the extensive evasion tactics employed by The White Company, it is likely that significant information regarding Pakistan's military was obtained. Further, while only Pakistan is known to have been targeted by The White Company, given the difficulties in detection, it is likely that other countries have been targeted as well. Pinkerton advises clients who conduct business with the government of Pakistan to review CVE-2012-0158 and CVE-2015-1641 to ensure systems have all necessary and relevant security updates and patches to prevent exploitation.

Cyber Attacks Threaten Special Sales Weekend

Cyber-attacks expected during a sales weekend in Mexico that affected bank cards, and online financial services like PayPal.

Last month, an electronic payment firm warned that during the following weekend cyber-attacks could increase. The alert for Mexico was issued for November 16, 17, and 18, when a large number of sales are expected to take place in physical and online stores; according to the firm, two out of every three purchases during these days will be done with bank cards or via online financial services such as PayPal. It was also revealed, that the most common electronic frauds committed during these days tend to happen when people log their personal information to fake websites, and via phishing emails offering false special offers.

Pinkerton assesses that the risk of cyber-fraud could be extended for at least ten days after the special sales weekend takes place. As referred by the consultancy PricewaterhouseCoopers, nearly 87% of all the companies currently operating in Mexico had suffered a cyber-attack during the past 12 months, and according to data provided by the Presidency's Specialized Tech Strategy Unit, the country losses MXN 61.5 billion (USD 3 billion) each year due to cyber-crime activity. Pinkerton advises clients planning to make online payments and transfers, to make them through a secure internet connection, confirm the authenticity of the website before submitting any sensitive information, and to immediately report any unrecognized payment to their banking institution.

Industrial Control System Devices Vulnerable To Side-Channel Attacks

Side-channel attacks have been known for a long time, but few research papers describe their impact on industrial systems, until now.

Just recently, information from the October SecurityWeek's Cyber Security Conference regarding industrial control systems (ICS) has become available. At the conference, a lead engineer from Eaton presented an analysis of protection devices used in power distribution stations. The research indicated that many of the ICS were vulnerable to side-channel attacks on timing and power analysis. The side-channel attacks can be used to obtain passwords or encryption keys. The power analysis method utilizes analysis of power profiles measured by oscilloscope to discern the data from the power profile. The researcher noted that the equipment needed for a power analysis attack costs around USD 300 (EUR 262.86) and requires physical access to the ICS.

Pinkerton assesses that it is unlikely for side-channel attacks of ICS to be widespread due to the requirement for physical access to the systems. However, without mitigation, the vulnerability does leave significant data that is otherwise protected at risk of exposure. Pinkerton advises clients utilizing ICS, especially those in the power distribution sector, to ensure that access to systems is properly controlled as the best method of mitigating the dangers of side-channel attacks. who receive suspicious emails report them immediately to the relevant department. Pinkerton further recommends clients conduct education campaigns about suspicious website URLs and other phishing techniques to mitigate the threat.

Millions Of Voter Records For Sale Online

Ahead of the US Midterm elections, researchers found voter databases available for affordable prices on the dark web.

Cyber-security company Carbon Black identified voter records for sale on the dark web. The cyber-security researchers found millions of records available for at least 20 different state voter databases on the dark web. The information included for purchase are full names, voter IDs, current physical addresses, previous physical addresses, phone number, gender, and citizenship status. At the time of writing, it is unclear if the records are genuine as the Carbon Black report primarily focused on the numbers and type of data available.

If the data available is genuine, Pinkerton assesses that malicious actors are likely to buy and use the data for various reasons. The information available is highly likely sufficient enough to steal someone's identity. As so much information is available, malicious actors will likely use the information to create phishing scams. Pinkerton also assesses that the information could be used to influence the result of the campaign by sending targeted campaign information to a desired audience. Pinkerton assesses that further voter information is likely to become available on other dark web markets as well as outside of the dark web in the medium term. Pinkerton recommends clients monitor their information and accounts out of an abundance of caution for any suspicious activity.

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