CYBER SECURITY BRIEFING

A Monthly Recap of Technology & Information Risk

PINKERTON®

SEPTEMBER 2018

Cryptocurrency Platform Atlas Quantum Compromised

As reported on August 28, 2018, hackers breached cryptocurrency platform Atlas Quantum. Over 260,000 user's information was stolen.

Through Atlas Quantum, users can add Bitcoin to accounts and make profits by trading it on various platforms. Atlas Quantum stated it has 240,000 users in over 50 countries, with over USD 30 million (EUR 25.6 million) in assets. Leaked information included names, phone numbers, email addresses, and account balances. The company stated they are monitoring the affected accounts as well as working to add more protection to the site. Atlas indicated some features on the platform have been temporarily disabled, but users will be notified when services are reactivated.

Pinkerton assesses that cryptocurrency and companies that manage crypto services are likely to remain a target for hackers over the medium- to long-term. The breach will likely generate discussion over security concerns with a decentralized currency. As many had personal information exposed, Pinkerton assesses that even if the malicious actors did not steal the cryptocurrency, users are still at risk. Pinkerton recommends clients who use Atlas Quantum monitor their accounts in the short- to medium-term. Pinkerton advises other businesses that have a similar platform to Atlas Quantum ensure their cyber-security measures are up to date to best prevent against a cryptocurrency attack.

Malware Known as Dark Tequila Affecting Users Since 2013

Recently, the cyber-security firm, Kaspersky Lab, identified a malware known as Dark Tequila that has been affecting users in Mexico since 2013.

The virus is capable of obtaining sensitive information such as bank account's credentials and personal data through spam e-mails and USB memories. The malware is generally installed in desktop computers as applications after been in contact with infected devices. According to the Kaspersky Lab, the most affected cities by the cyber-attack have been Guadalajara, Monterrey, and Mexico City. The main objective of Dark Tequila is to commit financial fraud. However, it is also used to obtain access to personal sites such as social networks, online shopping sites, and online storage accounts.

Pinkerton recommends clients to be particularly careful with the external devices they plug into their computer equipment as the most common way of Dark Tequila propagation is through USB memories. Also, the installation of new apps in desktop and laptops computers must be supervised and preferably approved by the IT department experts. Clients currently operating in Mexico are encouraged to delete their spam and junk-email inbox on a regular basis to avoid being the target of this malware. If the equipment shows any suspicious activity, it should be reported to the IT department, especially before making any online banking transactions. Finally, it is recommended not to store any sensitive information related to online banking or bank accounts information in electronic devices.

Corporate Networks Affected By Mining Malware

On August 1, 2018, a computer security company released a report about a new mining malware called PowerGhost that is attacking corporate networks.

This malware is especially tricky to detect because it works without installing files on the device where it is hosted and once established, it begins to take advantage of the operating system vulnerabilities to start the cryptojacking process. As with any other malware of this kind, PowerGhost monopolizes the processing power of the infected devices and directs it to decipher the algorithms that validate transactions with cryptocurrencies. This malware could cause overheating and slowness on affected devices. PoweGhost, specifically, focuses on corporate networks and also attacks server performance and accelerates wastage, generating replacement costs. The countries with more detected cases of PoweGhost attacks are Brazil, India, Colombia, and Turkey.

Pinkerton assesses that this will be a relevant matter in the near- to medium-term for all clients using corporate networks for their daily operations. This is because it is not clear yet how to detect a malware that works without installing files in the devices and when it becomes evident that the processor is being attacked, the malware has already caused irreversible damage. Pinkerton recommends all clients ensure antivirus systems are installed on all their devices and to be alert to any kind of abnormal operations as frozen screens, overheating, or slowness. Additionally, it is advisable to stay informed about any discoveries regarding this matter as a more effective solution could be found.

Cryptomining Malware Attack Detected By Microsoft

Recently, Microsoft announced that in January-March 2018, a multi-tier attack against supply chains was detected in a PDF editor.

These attempts compromised the shared infrastructure between the editor vendor and one of its font-provider partners, causing serious vulnerabilities for six other sellers that were collaborating with the vendor. The attack was first identified as a common infection, and the system blocked it. However, more than 70,000 cases were reported and linked with coin-mining processes. The investigation showed that a malicious installer package (MSI) was downloaded by the editor during installation. This way, the PDF editor became an unexpected carrier of the malware and users installed the coinminer along with the original app. The attack attempted to use the infected machine's resources to mine for Monero cryptocoin and to block all communication with the update servers.

Pinkerton assesses that the development will highly likely pose a credible concern in the short to medium term for clients using Microsoft in their operations. This is because coin-mining attacks have become increasingly recurrent and are a standard way for attackers to access sensitive information. Even though this specific malware was detected and stopped, it is likely that attacks of this nature arise at the slightest indication of system vulnerabilities. Pinkerton recommends clients to keep administrative ports closed and maintain a regular password rotation policy to keep the network locked against the deployed mining malware. Additionally, it is advisable to limit users' permissions to applications and services and stay informed of any official announcements related to this attack-type.

Malicious Actors Target Payment Processing Services

As reported on August 6, 2018, cyber-security researchers released a report detailing Border Gateway Protocol (BGP) hijacking attacks on the Domain Name Service (DNS) servers of three U.S. payment processing companies.

Through these attacks, malicious actors attempted to reroute traffic to steal data associated with the payment processors. Cyber-security researchers identified three dates in July (July 6, July 10, and July 13) where malicious actors targeted Datawire, Mercury Payment Systems, and Vantiv. Two of the attacks appeared to originate in Luhansk, Ukraine and routed to IP addresses in Curacao. Cyber-security researchers noted similarities between these attacks and attacks conducted against Amazon Web Services (AWS) in April 2018.

As both attacks were conducted out of Luhansk and used similar methods, Pinkerton assesses that the same malicious actors are likely behind the attacks. Pinkerton assesses that further attacks utilizing the same methods are likely in the medium-term. Pinkerton recommends clients in the payment processing industry monitor web traffic for any suspicious server activity, particularly any activity that routes from Luhansk

New Remote Spectre Attack Detected

Recently, a group of security researchers discovered a new Spectre-class vulnerability that can be launched over the network.

Previous versions of this attack required the local code execution to function, but the new NetSpectre can be used to overcome randomizations on the remote system. This means that attackers could be allowed to read arbitrary memory from the systems available in the network, as long as it contains a code that performs specific operations that leave sensitive data vulnerable. If this happens, the attacker could have access to either the memory of the entire corresponding application or the whole kernel memory. This is the third variation of Spectre-class vulnerabilities after Spectre 1.1 and 1.2 were discovered earlier this month.

As we reported in our Insights Intelligence Brief on July 12, it is likely that more vulnerabilities will be found in the medium term, as flaws have been detected mainly in the design of the most recent generations of processors. Since the NetSpectre version will be fixed with a new security update, Pinkerton recommends clients to ensure that the latest version is installed on their devices as soon as it is made available. Additionally, it is advisable to stay informed about any new flaws and discoveries that could affect operations and to monitor all updates and patches released to fix them.

New Version of AZORult Malware Has Improved Capabilities to Infiltrate Cryptocurrency Wallets

Per reports on July 31, 2018, a new version of AZORult information stealer and downloader is being used by cyber-criminals in an email phishing campaign since it became available on July 17.

Researchers at cyber-security firm Proofpoint have revealed that version 3.2 of the AZORult malware is used to spread Hermes ransomware version 2.1 to extract the credentials of targets. The new version of the malware has improved capabilities of stealing with support for infiltrating cryptocurrency wallets. The emails sent in the phishing campaign had subject lines associated with employment, such as “About a role” and “Job Application.” An email sample examined by the researchers had the message “My name is Napoleon and I’m interested in a job. I’ve attached a copy of my resume. The password is 789.” The malware is downloaded when a victim opens the password-protected document using the provided credentials and enables embedded macros, which downloads AZORult 3.2. Further, the researchers have attributed the campaign to a known perpetrator called TA516, who have previously used similar tactics to distribute banking Trojans and Monero miners.

Pinkerton assesses that the reported email phishing campaign, as well as the malware, poses a threat to data and communications security in the immediate to short term, especially since the malicious emails are likely to remain in circulation. Pinkerton notes that the emails used employment-related terms since businesses receive a high volume of such emails; clients are recommended to scrutinize and filter job applications with similar content reported by the researchers. Pinkerton recommends clients to specify certain terms to be included in the application, as well as the format of the acceptable attachments in their employment notifications to help filter the potentially infected emails. When accessing documents protected with password, clients are recommended to ensure that the document does not contain embedded macros.

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