# CYBER SECURITY BRIEFING

A Monthly Recap of Technology & Information Risk

PINKERTON®

OCTOBER 2018

## Cryptocurrency Miner Apps Identified On Google Play Store

### Cyber-security researchers have identified 25 cryptocurrency mining applications on the Google Play Store for Android.

Many of the malicious applications were masquerading as educational applications, games, and utilities. As of the time of writing, approximately 120,000 users had downloaded and installed the malicious applications. The majority of the malicious applications contained Coinhive code, a JavaScript implementation that mines Monero cryptocurrency. According to cyber-security researchers, mining capabilities are easily added to any app using a WebView embedded browser requiring only a few lines of code. Malicious actors are able to use CPU throttling to prevent the owner from noticing. A single developer, Gadgetium, published 11 of the applications, all under the guise of U.S. test preparation. Google has already removed some of the applications from the store.

Pinkerton assesses that the use of cryptocurrency miners in applications on the Google Play store is likely to increase over the long term. Pinkerton finds it likely that the applications are designed for download by individuals who may not scrutinize the applications, increasing the threat. Pinkerton further assesses that Google is unlikely to wholly prevent the publication of malicious cryptocurrency applications on its Android store. Pinkerton recommends that clients with enterprise Android devices monitor applications for any suspicious activity.

## Adwind RAT Targets Linux, Windows, And MacOS Systems

### A new Adwind remote access Trojan (RAT) has been detected that targets Linux, Windows, and macOS systems.

ReversingLabs and Cisco Talos cyber-security researchers discovered the attacks feature Adwind 3.0 RAT and employ a variant of the Dynamic Data Exchange (DDE) code injection. The campaign started on August 26, targeting most users in Turkey, although some in Germany were also targeted. The malicious actors used two different droppers for malicious payload, a CSV and XLT file. Both files leveraged a new variant of DDE code injection attack. Cisco Talos reported the dropper uses over 30 different file extensions. However, there are three warnings before fully opening the file. If the user accepts all warning, the application is executed and the code is injected to create and execute Visual Basic Script using “bitasdmin” to fetch the final payload. After, Adwind RAT allows attackers to execute commands, log keystrokes, take pictures and screenshots, and transfer files.

Pinkerton assesses that since the Adwind RAT has been successful in Turkey and Germany, the malicious attackers are likely to start targeting users in additional countries. As users have been affected, it is likely that the malicious actors have modified the formats to avoid detection from antivirus systems. The cyber-attack highlights the importance of understanding download warnings, as three are given before final execution of code. Pinkerton recommends clients ensure employees understand the type of documents they are downloading and educate employees about best practices for mitigating phishing scams.

## Pegasus Spyware Accounts Still Active In The Country

### A report released by Citizen Lab has revealed that there are several active accounts of the spyware Pegasus being used in Mexico.

The report explains how the software has been used from within the country to spy on lawyers, journalists, human rights defenders, anti-corruption activists, and politicians. Moreover, the report reveals that the Mexican government is allegedly still operating the spyware with at least three user accounts. The program, developed by the Israeli company NSO Group, allows the user to gather information from the cell phones of its victims. According to the researchers, the Maybereckless user has been working in Mexico since September 2017, Pricklypear started in October 2016 and continues active, as well as the Aguilareal user, that operates since September 2016.

Pinkerton assesses that this will be a relevant matter for all clients operating in Mexico as this is not the first time that this kind of attacks has been found. Pinkerton had reported similar attacks on February 27, 2018, Daily Insight Review as this software infiltrates smartphones and other devices to monitor details of a target's daily life, whether through calls, SMS messages, emails, passwords, contacts, and calendars. Pegasus can even use the microphone and camera phones to perform surveillance and to turn the victim's phone into a hidden microphone. Based on the information gathered on previous attacks, Pinkerton assesses to avoid becoming the target of a mobile device attack by not opening unrecognized SMS or e-mails with suspicious links on them, not downloading uncertified mobile applications on the mobile devices, and not storing sensitive data in smartphones. Pinkerton encourages clients in Mexico to raise their cybersecurity awareness levels and that of their employees, as well as to strengthen all of their IT internal security protocols.

## Cyber-Security Researchers Identify Critical Vulnerability In IoT Devices

### Researchers have identified a critical flaw in NUUO software that renders hundreds of thousands of Internet of Things (IoT) devices vulnerable to remote viewing and feed tampering.

According to Tenable, the cyber-security researchers who identified the flaw, the vulnerability could be present in over 100 brands and 2,500 models of cameras with NUUO software. NUUO software is present in devices used for a variety of industries, including education, government, banking, and retail. The vulnerability, CVE-2018-1149, is an unauthenticated stack buffer overflow and enables malicious actors to conduct remote code executions. After exploiting the vulnerability, malicious actors could gain access to control management systems (CMS) and the credentials for all connected video surveillance cameras. With root access, malicious actors could then tamper with feeds or disconnect them altogether. As of the time of writing, there is no patch to address the flaw. Cyber-security researchers identified a second vulnerability in NUUO software, a backdoor leftover debug code. The backdoor requires a file called / tmp/ moses. If this file is present, malicious actors can gain access to a list of all user accounts on the system and change passwords.

Pinkerton assesses that NUUO is highly likely to release a patch in the medium term to remove the vulnerabilities. However, Pinkerton finds it likely that malicious actors will likely leverage the flaw to gain access to IoT devices. Pinkerton assesses that malicious actors will highly likely leverage the devices in distributed denial of service (DDoS) attacks and for other malicious purposes. Pinkerton recommends that clients using NUUO IoT devices determine whether the identified file exists on their systems and remove it if present. Further, Pinkerton recommends clients using these devices update the software when a patch becomes available.

## Multinational Tech Companies Preparing To Fight India's Planned Data Law

### India is the latest country to move toward a data law that will require tech firms with operations there to store the firms' customer data in-country as well.

A move that would affect Indian global tech giants as much as it would U.S.-, UK-, or EU-based technology firms operating in the country. A coalition of lobby groups representing companies such as PayPal and Facebook has drafted a letter it will deliver to the minister of information technology by September 30, which will present tech companies' concerns over infrastructure and compliance costs and petition the government to reconsider. The Washington DC-based Information Technology Industry Council (ITI), India-based NASSCOM, the U.S.-India Strategic Partnership Forum, and London-based techUK reportedly support the letter and the effort behind it to prevent data localization regulations. An unidentified official from the information technology ministry told Reuters that the regulatory law was necessary for the government to conduct investigations and prevent data breaches. Referring to tech industry giants, the official also said "They are too ambitious to think that this won't become a law within a year."

While China and Vietnam's recently installed cyber-security laws, among others, are impacting multinational corporations' in-country infrastructure and operational practices to varying degrees, Pinkerton assesses that India's data localization law would more deeply affect global companies, whether they fall into the tech industry category or not. Like the EU's General Data Protection Regulation (GDPR), Pinkerton finds it likely that Indian data localization requirements would affect all companies with customer service, software development, back-office operations, and manufacturing divisions outsourced in India. These would include auto manufacturers, accounting firms, chemicals and plastics manufacturers, online and brick-and-mortar retailers, and more.

## Firmware Vulnerabilities Create Cold Boot Threat

Cyber-security researchers have announced that firmware present on “nearly all” computers renders the devices vulnerable to cold boot attacks.

Cold boot attacks enable malicious actors with physical access to a device to obtain highly sensitive data from the device’s memory, including passwords and encryption keys. Malicious actors are able to gain access to data in a device’s random access memory (RAM) following a cold or hard reboot, anywhere from seconds to minutes. Malicious actors are able to extend this process by cooling memory modules with compressed air or liquid nitrogen. Device manufacturers reportedly were aware of the vulnerability and implemented mitigation methods to prevent such attacks. However, cyber-security researchers discovered that the mitigation mechanisms could be bypassed. The bypass requires malicious actors to make physical changes to device hardware, requiring an external device.

As the attack method requires physical access to a device, Pinkerton assesses that these styles of attacks will likely be rare. Pinkerton finds it likely that the attack method poses the greatest threat to enterprise laptops due to their portability. To best mitigate the threat of cold boot attacks, Pinkerton recommends clients enable BitLocker PIN prompts, shutting down or hibernating devices when not in use, and creating an incident response plan for lost or stolen devices.

## MEGA Chrome Extension Hack Steals Credentials and Cryptocurrency

Cyber-security researchers have discovered that the MEGA Chrome extension was compromised to steal login credentials and cryptocurrency keys.

When the extension is installed, it will monitor for specific login form submissions to various sites like Amazon, Github, Google, and Microsoft. It also monitored for when the URL contained strings “Register” or “Login” or variables with username, user, email, login, pass, passwd, password, or usr. If the extension detected these variables, it would then send the credentials to a host in Ukraine. The extension also looked for URLs for MyEtherWallet, MyMonero, and Idex Market, and would execute JavaScript to steal cryptocurrency private keys. Approximately 1.6 million users installed the extension. Once the hack was discovered, Google removed the extension.

Pinkerton assesses that malicious actors are likely hacking other extensions in similar ways. Since 1.6 million users had downloaded the extension, the hack has the potential to have a large impact. The company is likely looking into how the Chrome web store was hacked. Pinkerton recommends clients who use the MEGA Chrome extension immediately remove it. Out of an abundance of caution, Pinkerton advises clients to change passwords at any accounts that may have been used with the extension, especially banking, financial, shopping, and government institution sites. If clients use cryptocurrency, Pinkerton recommends they monitor their accounts as well.

## 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.

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

### 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