# CYBER SECURITY BRIEFING

A Monthly Recap of Technology & Information Risk

PINKERTON®

JANUARY 2018

## Authorities Warn Of Increased Cyber-Frauds In December

### The National Commission for the Protection and Defense of Users of Financial Services (Condusef) has warned of an increase in cases of cyber-fraud in the current month.

According to the authorities, this phenomenon occurs because workers receive more money as a result of their annual bonuses. Per the Condusef, the most common crimes are cloning of credit cards, unrecognized money transfers, identity theft or falsification of personal information, as well as deceptive practices at ATMs to obtain personal data. Specifically, December 15, 30, and 31 were the riskiest days, claimed the authorities.

Pinkerton finds that the rate of cyber-crimes in Mexico has increased considerably in recent months. Cyber-crimes present threats to clients in at least two ways; they might affect the physical security of personnel, and could harm the finances of clients and companies with investments in the country. To avoid frauds and other cyber-crimes, Pinkerton encourages clients in Mexico to strengthen their cyber-security protocols following a set of preventive measures. When paying for a product or service, it is essential to keep a visual track of bank cards. Further, it is advisable to keep the payment tickets in case of any clarification. Before conducting any online purchase, it is important to verify the authenticity of the website and using antivirus software. Another essential measure is to avoid sharing personal and financial data. Pinkerton found two recent cases of theft of personal information of BBVA Bancomer and HSBC bank users in Mexico. Fake telephone operators called users of these banks alleging unrecognized charges to obtain confidential information and bank card PINs.

## Hacker Group Targets At Least Six Governments

### Researchers confirmed that a group called Sowbug developed a malware aimed at attacking and spying mainly on government entities in South America and Southeast Asia.

According to reports, the malware has so far stolen government information in countries such as Argentina, Brazil, Ecuador, Peru, Brunei, and Malaysia. The modus operandi of the attacks has been through the propagation of the Felismus virus, which enables remote access to government systems by sending and downloading arbitrary commands that facilitate the theft of information. The researchers estimate that these attacks could affect the 3 private sector as well.

Although cyber-attacks commonly affect targets in the U.S., Europe, and Asia, Pinkerton finds that cases of cyber-attacks targeting Latin American countries are becoming more frequent. The emergence of Sowbug confirms that no region and public or private entity is safe from cyber-crime. Regarding the attacks of Felismus malware, Pinkerton finds that the compromised information could be related to financial or political data. Recently, cyber-security firm Symantec revealed that attacks in Latin America are more common in democracies undergoing political transitions. Although the modus operandi of Sowbug has not been confirmed, the researchers have found that it could operate through false updates of government software.

# Exposed VPN Credentials In FortiClient

## Security researchers at SEC Consult announced the discovery of vulnerabilities in FortiClient, an endpoint protection product from Fortinet.

The specific vulnerabilities relate to virtual private network (VPN) authentication credentials, as they are stored in a configuration file on systems running on Linux or macOS, or in the registry on Windows machines. These storage locations are easily accessible to potential attackers. A second issue regarding the VPN vulnerabilities is that while the VPN credentials are encrypted, all installations of FortiClient use the same decryption key that is hardcoded in the application, and therefore allows for easy decryption of maliciously acquired VPN credentials. This vulnerability is being tracked as CVE-2017-14184 and is classified as a high severity issue. Internally, Fortinet has rated the risk as 4 out of 5. Fortinet is aware of the issue and has issued patches to address the vulnerability. While there is a FortiClient App for Android and iOS mobile devices, it is not affected by this vulnerability.

While the vulnerability in FortiClient has been identified, there is no current evidence that it has been exploited, rather the vulnerability has only been exposed through the proof-of-concept test by SEC Consult. The basis of the vulnerability could prove catastrophic to business clients using FortiClient, as a compromise of their VPN could allow malicious actors access to sensitive data, as well as credentials to internal systems and networks. Pinkerton advises any clients operating FortiClient on Windows, Linux, and macOS systems to ensure to download and install the latest security patches.

# Keylogging Software Creates Security Gap In Hewlett Packard Models

## Last month, news outlets expanded on cybersecurity researcher Michael Myng's blog post about a keylogger found in Hewlett Packard's (HP) Synaptics Touchpad software.

The keylogger is deactivated by default but could be used against the laptop user if an attacker has access. The keylogger's original use was to help debug errors. If an attacker exploits it, the keylogger could be used to open the device up to malware and record what the user types, such as passwords. HP published an update that removes the keylogger from over 460 models it affects.

The keylogging software presents a threat to users' privacy and exposes the laptop to malware if activated by an attacker. However, its default status as deactivated means it is a security gap rather than an ongoing malicious threat. Pinkerton recommends HP users check the list of affected devices HP published to determine if their model is compromised. Additionally, clients with an HP model compromised with the keylogging software are advised to update their software with HP's patch. Pinkerton suggests users routinely check their 5 computer brand's security bulletins for possible security vulnerabilities and patches.

# 50% Companies Do Not "Fully" Inform Clients Of Data Breaches, Says Survey

## According to a survey conducted by CyberArk, a cyber-security firm, it is common for companies to not "fully" inform clients of data breaches that may have compromised clients' details.

As many as 50% of the 1,300 interviewed, including IT decision makers and cyber-security leaders, reported that this was the case at their organization. The study follows reports that Uber refrained from informing customers about a data breach that occurred in 2016, as reported in the Pinkerton Insights Intelligence Brief on November 30.

Pinkerton finds that organizations operating in Europe, which currently do not fully inform customers of data breaches that jeopardize clients' information and accordingly change standard operating procedures, risk breaching the EU General Data Protection Regulation's (GDPR) 72-hour breach notification mandate in the medium to long term. The mandate will enter into force on May 25, 2018. Pinkerton further notes that a recent study by Honeywell and LNS Research shows that only 55% of industrial companies have a designated cyber-security leader. Pinkerton assesses it likely that firms which do not adopt cyber-security best practices, including having an established head IT decision maker, are more likely to fail in preventing and informing clients of data breaches. Pinkerton, therefore, advises clients to ensure that best practice is part of their standard operating procedure, and that a designated IT role is established.

## Starbucks WiFi Used Customers Systems To Mine Cryptocurrency

Per reports on December 13, 2017, the devices of visitors to one of Starbucks' Buenos Aires, Argentina, outlets were unknowingly exploited for a cryptocurrency "mining" operation.

Mining requires enormous processing power as it involves solving complicated mathematical equations to verify cryptocurrency transactions. In a statement, Starbucks said that "as soon as we were alerted of the situation … we took swift action to ensure our third-party support provider resolved the issue." Further, it assured that the issue was limited to the one outlet, as it originated from the Internet service provider. It is not yet known how many customers were affected, or the duration for which the malware was operational.

Pinkerton assesses that the incident highlights the inherent risk of using public WiFi connections. Clients are recommended to mitigate such attacks by following precautionary measures, including using up-to-date protective software; look for suspicious activity such as slow processing on particular websites, and use applications and websites that utilize encryption by default.

Further, Pinkerton assesses that cryptocurrency mining operations are likely to increase in the near term as hackers are increasingly hijacking computer processors to search for virtual currency not being traded on the open market. To this end, hackers install a script on popular websites that infect the computers of visitors. Clients experiencing slow browsing on particular websites are recommended to delete their browser cache and scan their system for security threats.

## Banking Trojan Discovered In Google Play Store

According to information released by a team of security researchers at Avast, about 160 banking apps available in the U.S., Latin America, Europe, and the Asia-Pacific versions of Google's Play Store have been affected by a Trojan called BankBot.

In September 2017, Google announced it had made sure that no apps containing Trojans were available on their App Store, but recent information indicates that several apps were able to continue being available to the general public up to mid-November this year. This Trojan hides in apparently benign apps such as games and flashlight apps, and once it has been installed, it downloads the effective payload from an external source and proceeds to steal banking credentials from a smartphone. In its Insights Intelligence Brief on July 25, Pinkerton had first reported the discovery of this form of Android malware, which steals financial data and passwords from smartphones.

Pinkerton finds it likely that the process of identifying all the users who were affected by the Trojan will continue in the near to medium term. Pinkerton, therefore, recommends clients with Android phones to change their banking credentials as soon as possible. Clients currently using Android devices are advised to limit, as much as possible, their use of banking apps and perform routine backups. Pinkerton further recommends clients to revise their cybersecurity protocols, as well as to make sure that their employees have a basic understanding of safe web-navigation practices to avoid possible cyber-security attacks.

## Vulnerability Exposes Android Developers And Reverse Engineers

Per media reports on December 6, 2017, researchers at the Check Point Research Team discovered vulnerabilities in Android developer tools that are both downloadable and cloud-based.

The flaw, codenamed ParseDroid and technically called XML External Entity (XXE) vulnerability, tries to parse an AndroidManifest.xml file that allows attackers to steal files, remotely run malicious code on the targeted systems, and execute commands on the target's system. According to reports, the vulnerability affects Android Integrated Development Environment (IDE), which is commonly used by application developers.

Pinkerton assesses that in the medium term the ParseDroid vulnerability will increase the threat of cyber-attacks on organizations that engage in Java/Android development. It exposes their products to design defects that may result in direct exposure of the client, as well as financial losses and suboptimal performance. Moreover, it poses a high risk of theft of company database and product information. Programmers that are operating on the affected systems are advised to update their tools. Companies are recommended to review their business applications to check if the work of security analysts and reverse engineers has been compromised. Pinkerton finds that most tool developers launch patched versions and, hence, recommends programmers to update their systems as soon as these are made available.

## Department Of Homeland Security Says Drones Being Used To Spy

Per reports on December 4, 2017, the U.S. Department of Homeland Security (DHS) has issued a memo stating that drones produced by Da-Jiang Innovations (DJI), a Chinese manufacturer, are being used to provide critical information regarding American infrastructure and law enforcement to the Chinese government.

Suspicions regarding DJI were published earlier by the office of Immigration and Customs Enforcement (ICE) in August 2017. ICE suspects that applications used with the drones store information like images and location even when the function is turned off. The data is then uploaded to cloud-based storage, where Chinese authorities could gain access. DJI denied the claims and said that while some geographical information is being collected to comply with Chinese regulations, it is only to determine whether the user is in China or not.

Pinkerton assesses that the DHS memo has escalated the issues associated with DJI drones in specific and foreign-produced technology with a possible state connection in general. Additionally, such issues have become increasingly relevant following the DHS ban on Kaspersky Lab's products due to the allegations that the company has close relations with the Russian state, just as DJI allegedly has to the Chinese state. Pinkerton assesses an even chance that DHS will implement a ban against DJI products that are being used by official organizations, as it has already banned its use by the military. In such an event, it is also likely that the use of the drones in the private sector will be affected. Further, it is likely that scrutiny of foreign-manufactured products will increase in the medium term. Clients who use DJI products are recommended to follow developments in the case and adhere to any governmental decision.

## Intelligence Agencies Warn Against Mobile Applications

Per reports on December 1, 2017, the Indian government announced a list of mobile applications that have been identified by intelligence agencies, including the Research and Analysis Wing (RAW) and National Technical Research Organisation (NTRO), as "Chinese spyware" with the potential to conduct cyber-attacks.

At least 42 applications on both Android and iOS are being used to send data back to servers in China. The armed forces have been recommended not to use these applications. However, TrueCaller, one of the applications listed, responded by saying that it is "not a malware, and all our features are permission-based and are disabled by default." In a related development, in August, the Indian government tightened its rules for equipment used in the power and telecommunication sectors to check for malware amid concerns regarding China's advance into sensitive sectors.

Pinkerton assesses that given the increasing concern regarding Chinese cyberattacks, the Indian government is likely to impose stringent checks for hardware and software linked to China. There is also an even chance that other countries will follow suit to protect their data. Further, security organizations in the private sector that work with the government are likely to take similar measures. Cybersecurity firm Symantec's Internet Cyber Security Threat Report of 2017 ranked India the fifth-most vulnerable to cyber-attacks in the world. Further, according to Indian Computer Emergency Response Team (CERT-In), more than 27,000 cyber-security incidents were reported in India in 2017. Pinkerton recommends clients with business interests in India to liaison with the government and report security breaches to contain the impact of any attack, while also ensuring operational continuity. For latest cyber-alerts by CERT-In, refer to the link: http://www.cert-in.org.in/.

## New Ursnif Trojan Malware Tested; Australian Banks First Victim

Per media reports, researchers have warned about a recently detected Trojan, which is a new version of the "Ursnif" malware.

The new version employs a tactic of redirection to divert victims to a fake website hosted on a server controlled by the attackers. Reportedly, researchers observed that the new variant also employs malicious thread-local storage (TLS) callback techniques to achieve process injections, an anti-analysis trick easily missed by automated security tools. The first detected use of the malware was silently aimed at Australian banking customers, and authors of the malware seemingly choose to keep a low profile by limiting the distribution.

Pinkerton assesses that the new version of the Ursnif Trojan will pose an increased threat of redirection-attacks in the near to medium term. Previous attacks indicate that clients in the financial and banking sectors are at risk of being targeted by the malware. Pinkerton finds that the code configurationv which previous versions of the malware utilized was the most actively used to attack the financial sector in 2016, and harmed banks and credit unions in Japan as well as North America, Europe, and Australia. Pinkerton finds that the increased risk of attacks requires clients to ensure that proper security measures are in place. All suspicious movements on an account should be reported to the financial enterprise's security department to prevent exploitation.

# Golden SAML Technique Allows Attackers To Forge Authentication To Access Cloud Apps

## Per media reports, researchers have warned about a newly-created post-intrusion violation technique called a Golden Security Assertion Markup Language (SAML).

The Golden SAML, a technique which is used after an intrusion attack has been launched against a company, allows attackers to use a fake identity and forge authentication requests to access cloud-based apps. The aggressor can pass two-factor authentication, and issue forged tickets for user accounts even after the authorized user has changed the password. According to researchers, the technique is particularly concerning for companies that use domain controllers compatible with SAML..

Pinkerton assesses that the new Golden SAML technique likely will increase the risk of data loss and system manipulation in companies that operate with SAML protocol in the medium term. Pinkerton finds that using a SAML protocol is common standard when exchanging authentication and authorization data between identity providers and service providers, and therefore assesses that such attacks expose companies to critical risks. Pinkerton recommends clients to keep security systems up-to-date and periodically change token-signing private keys to limit the time an attacker can exploit company data.

# GPayPal Subsidiary Breach Exposes 1.6 Million Customers Data

## On December 1, 2017, PayPal announced that hackers might have accessed personal information for 1.6 million customers through PayPal's subsidiary TIO Networks.

TIO Networks is based in Canada and services approximately 16 million of PayPal's customer billing accounts. PayPal stated that the breach was due to a sub-standard data security program at TIO Networks. On November 10, after discovering the breach, PayPal suspended TIO Networks' operations in an attempt to mitigate any threats from the stolen data. The breach may have allowed hackers to access personally identifiable information for 1.6 million PayPal customers. Customers and companies who may have had their information stolen will be emailed by PayPal and offered Experian free credit monitoring services. PayPal assured users that TIO Networks would not be brought back online until they are confident all threats have been resolved and the network has been secured.

While PayPal assures that their platform and network are still secure, Pinkerton finds it likely that there may have been more accounts breached than PayPal is initially sharing. Due to the malicious actors' success in infiltrating one of PayPal's largest subsidiaries, it is likely that other attacks will follow on other PayPal subsidiaries to see if the same weaknesses can be exploited. Pinkerton advises clients and companies who use PayPal on a regular basis to change their password, to a complex password, immediately out of an abundance of caution and sign up for credit monitoring services to ensure their data was not included in the breach.

# Serial-To-Ethernet Devices Leak Telnet Passwords

## On December 1, 2017, a cyber-security researcher at NewSky Security discovered thousands of Serialto-Ethernet devices are leaking Telnet passwords online that could be used to attack the connected equipment.

The vulnerability varies between several Serial-to-Ethernet device servers that are manufactured by Lantronix. The password exposure is caused by an old vulnerability from 2012 that allows attackers to retrieve the setup configuration of Lantronix devices by using a malformed request on port 30718. Companies use the device servers as a way to connect to remote equipment. Products like the external device server universal device server (UDS) or Serial-To-Ethernet device server xDirect allow users to plug an RS-XXX serial connector on one end and an RJ-45 Ethernet connector on the other. This manages the device via a local area network (LAN) or wide area network (WAN) connection.

Pinkerton assesses that, due to the long timeframe that the vulnerability has been available, malicious actors are likely obtaining passwords via this method. Once an actor has the password, it is highly likely they will take control over the device via Telnet, affecting clients by sending serial commands to connected devices. Pinkerton assesses that this vulnerability will most likely affect clients that use device servers in the Industrial Control Systems (ICS) sector, as this is where most equipment features serial ports. However, any client that uses serial ports is likely to be affected by the vulnerability. Pinkerton recommends clients that use Lantronix Serial-to-Ethernet device servers ensure that their devices have been updated with the latest firmware to best prevent an attack using this vulnerability.

# MacOS High Sierra Vulnerability Allows Root Access To Device

## On November 29, 2017, cyber-security researchers identified that macOS High Sierra has a critical vulnerability that can be exploited by malicious actors to gain root access to a device without needing a password.

After users complained that their admin accounts became standard accounts after updating the operating system, one user suggested logging in with the username "root" with no password on November 13. This was then discovered to be a critical vulnerability with the operating system. Researchers at Security Week confirmed it is easy to reproduce this flaw, but multiple attempts are required. While it appears that the vulnerability could only be exploited by having physical access to a device, macOS hacker Patrick Wardle, along with others, managed to reproduce the vulnerability remotely as well if sharing services were enabled. Apple is in the process of creating a patch to the vulnerability.

Pinkerton assesses that malicious actors are likely using the vulnerability to gain access to a device since the suggestion for using root to log in has been known for almost three weeks. Pinkerton assesses that malicious actors are likely scanning Apple Remote Desktop for devices online to gain remote access to the device. To best avoid potential attacks, Pinkerton recommends clients who have upgraded to macOS High Sierra manually set a password for the root user. In the event that clients operating macOS High Sierra need to login to the root user, Pinkerton recommends clients avoid connecting to online networks as well as Apple Remote Desktop. Pinkerton also recommends clients using the identified operating system disable sharing services to best prevent remote exploitation. When the patch is released, it is recommended to update all Mac devices as soon as possible.

# Global Shipper Hit By Ransomware Attack

## On November 29, 2017, the global maritime shipping company, Clarksons, reported that they had been the victim of a ransomware attack.

The company noted that they have refused to pay the ransom and confidential data is likely to be released. The nature of the confidential data has not been disclosed. Access to the data was gained through a single user account that has since been disabled. Clarksons is working with law enforcement and lawyers to attempt to prevent the release of the stolen confidential data.

Pinkerton assesses the shipping industry is a high-value target for cyberattacks. Malicious actors could cause a number of operational disruptions including halting shipping operations, spoofing ship positions, gaining access to cargo lists for targeted seizures, and gaining access to the switchboard to render ships inoperable or provoke a collision. Ransomware attacks on the shipping industry are likely to increase as many shipping companies are likely to opt to pay ransoms to mitigate the profit losses associated with operational delays. In June 2017, the shipping company Maersk was a victim of the NotPetya cyber-attack, which cost the company USD 300 million (EUR 155 million) in profits. Pinkerton recommends clients in the maritime shipping industry ensure that regular penetration testing is performed to ensure the security of their network. Additionally, Pinkerton recommends clients ensure that external media ports are disabled, and institute complex passwords that are regularly changed, especially following hostile terminations.

# 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

©2018 Pinkerton Consulting & Investigations, Inc.
d.b.a. Pinkerton Corporate Risk Management. All Rights Reserved.