CYBER SECURITY BRIEFING

A Monthly Recap of Technology & Information Risk

PINKERTON®

AUGUST 2018

Security Loopholes Reported In Car-Sharing Applications

Per reports on July 25, researchers from Kaspersky Lab have identified security loopholes in 13 car-sharing mobile applications available on Google Play for Android devices.

Malicious actors can reportedly exploit the security vulnerabilities of these applications to access the personal information of users; they can also steal and misuse car-sharing account credentials to use the services without paying, commit crimes, and steal cars. According to Kaspersky, cyber-criminals are already selling hacked car-sharing accounts. Per reports, these applications have recorded more than 1 million downloads primarily in the U.S., Europe, and Russia.

Pinkerton assesses it likely that the user accounts of car-sharing applications will be stolen and misused in the medium to long term due to the weak cyber-security standards of these applications. The existence and exploitation of such security loopholes will likely affect the operational continuity and brand reputation of businesses running these car-sharing applications. Further, it is highly likely that individuals using car-sharing applications are identified, as their information including phone numbers are listed publicly on these applications for engagement with other users. Pinkerton recommends personnel to use stronger passwords for their car-sharing application accounts and update them regularly. Personnel are recommended to monitor any irregularities in their transport history log and bank transactions. Businesses operating car-sharing applications are recommended to enhance the cyber-security measures employed to sustain brand reputation.

New Cyber-Espionage Group Discovered

Per media reports on July 27, a new cyber-espionage group has been discovered, and its attacks analyzed.

The group, unofficially named Leafminer, had an active Advanced Persistent Threat (APT) since early 2017, detected on at least 44 computers in Israel, Kuwait, Lebanon, and Saudi Arabia. The country of origin of the malware has not been detected, but suspicions indicate that the group is based in Iran. Researchers from Symantec managed to gain access to one of the hacker's operational servers, used for phishing and malware distribution, and discovered a list of 809 organizations across Saudi Arabia, the United Arab Emirates, Qatar, Kuwait, Bahrain, Egypt, Israel, and Afghanistan. Leafminer is believed to scan the targeted organizations to identify weak points in preparation for future attacks. Reportedly, while the group is considered inexperienced, it is seemingly quickly responding and adapting to new hacker trends and developments.

Pinkerton assesses that the cyber-threat to organizations operating in, or originating from, the Middle Eastern countries on the list is likely to increase over the medium term. As only one hacker's server has been accessed, Pinkerton notes that the full potential of the Leafminer group has not yet been determined. In the medium term, organizations should expect intensified APT attacks, which aim to achieve ongoing and maintained access without discovery, allowing an intruder to steal data rather than to cause damage to the system. In a wider perspective, collected information is likely to allow hackers to prepare an attack damaging the network's or organization's operational system. Preventive measures should be based on the most recent security system updates as the hackers tend to modify and use newly discovered malware tools rather than creating their own.

Increase In Cyber-Attacks Reported During Helsinki Summit

Per reports on July 19, an increase in the number of cyber-attacks targeting Internet of Things (IoT) devices was recorded during the Helsinki Summit between U.S. President Donald Trump and Russian President Vladimir Putin.

Per reports, the majority of these attacks emanated from China and were aimed at stealing information from "targets of interest" in Finland. The ports primarily targeted include Session Initiating Protocol (SIP) port 5060 associated with Voice over Internet Protocol (VoIP) phones and video conferencing systems, and Structured Query Language (SQL) port 1433 and Telnet port 23 used for remote administration of the IoT devices. Other ports targeted in the attack include Secure Shell (SSH) port 22 and Server Message Block (SMB) port 445 used by IoT devices, and HTTP port 80, SQL port 3306, SQL port 8090, and Remote Desktop Protocol (RDP) port 3389.

A similar increase in the number of cyber-attacks was reportedly recorded during the summit between President Trump and North Korean Leader Kim Jong-un held in Singapore in June 2018. According to researchers at cyber-security firm F5 Network, the attacks during the Singapore summit primarily targeted SIP port 5060. The researchers further noted that given the importance of these events, a combination of state-sponsored and other malicious non-state actors could likely have perpetrated these attacks.

Pinkerton assesses that the cyber-attacks reported in Finland will likely result in the compromise of data and communication of businesses operating in the vicinity of the summit location in the short term. The attacks are also likely to disrupt the operational continuity and systems integrity of businesses in the identified area in the short term. Clients are recommended to practice caution with regard to the IoT devices deployed in the country for operations and reset their configuration to ensure that they are not compromised. Pinkerton recommends businesses to ensure that the personal IoT devices used by employees at the workplace are also reconfigured. Further, Pinkerton notes that the hackers can use the IoT devices to gain access to the main network integrated with the IoT devices; clients are recommended to perform a business-wide scan to avoid any security breach in the immediate to short term. Additionally, Pinkerton finds that cyber-attacks increase significantly during events such as the summits at Finland and Singapore; businesses in the vicinity of such events are recommended to undertake additional cyber-security measures.

Extortion Scam Exploits Leaked Account Credentials

On July 11, Bleeping Computer reported an extortion scam involving claims of malware being installed on the computers of adult website users after stealing their logon information and email contacts; emails sent to victims of the scam also indicated that videos of the users had been created while they were using the sites.

Perpetrators further stated that if the recipient failed to comply with demands for a Bitcoin payment of USD 2,900 (EUR 2,481) within one day of receipt, they would share the damning video with all of the user's contacts. According to Bleeping Computer, the hackers' claims of installing malware and filming users of adult websites appear to be unsubstantiated. However, the culprits do seem to have gained access to legitimate user passwords via recent data breaches, making emails to the intended victims of the scam appear at least somewhat authentic.

Pinkerton assesses that the breaches that enabled access to sensitive information like account credentials underline the growing urgency for heightened data security. Until increased regulation forces website administrators to bolster security measures to protect against these breaches, they will likely continue to occur with progressive frequency. While this phenomenon is beyond the control of individual users, there are several measures they can take to better guard their own data—especially their passwords. Cyber-security experts recommend the following steps for improving password strength and security: create passwords that are a complex mixture of letters, numbers, and special characters; disable the "autocomplete" browser feature that stores site credentials for future use; change passwords frequently; and delete the browser data cache after using a public computer.

Banks On Alert Over Threat Of Cyber-Attacks

On July 6, financial authorities asked banks in Mexico to strengthen security measures due to a high risk of cyber-attacks.

According to an official statement, the authorities have found irregular operations that could harm the banking system. The recommended measures for banking operations include areas of telecommunications, information security, as well as financial transactions systems. The authorities also reported that although the monetary funds of banking users are safe, the security protocol estimates the temporary deactivation of the virtual asset retirement system.

Pinkerton finds that cyber-threats have increased considerably in recent months in Mexico particularly against the financial sector, which recently recorded a massive attack on the inter bank transfer system. In this regard, Pinkerton found that in 2017, 92% of companies in Mexico were victims of a cyber-security incident. It has been found that cyber-attacks have mainly occurred against the banking, telecommunications, as well as the manufacturing sector through malicious software that steals or removes information. In this context, the most vulnerable information is related to employee registration, customer records, and financial assets of companies. Consequently, Pinkerton encourages clients in Latin America to raise their security awareness of cybernetics and to strengthen more specific measures to ensure the IT security of their assets.

Airport Security Access Advertised For Sale On Dark Web

The McAfee Security Research team announced on July 11 that they found online shops selling Remote Desktop Protocols (RDP) to access computer systems responsible for security and other critical infrastructure.

Access to a major U.S. international airport's security, building automation system, and video surveillance sold for about USD 10 (EUR 8.60) at an identified Russian RDP online shop. RDP allows a user to access another computer through a graphical interface. Attackers scan for systems that allow RDP and then use password hacking tools made of password dictionaries and information from large, previous data breaches to gain access through brute force. After access is made, it is then sold. The team found the hacked systems were from Windows XP to Windows 10 with the majority from the Windows 2008 and 2012 Server.

Pinkerton evaluates that compromised computer access to security systems would highly likely cause businesses, particularly facilities involved with infrastructure, to experience a critical threat to operations and information security. Pinkerton assesses that any business with computer systems within the mentioned range will highly likely benefit from a thorough security review. The low cost of supposedly accessing a major U.S. international airport's security does not seem to match with the high-value of its advertisement, but this does not negate the possible threat. Pinkerton recommends businesses to ensure that their IT departments have enabled password policy controls that require complex passwords, are not reused, and require change within a 90-day window to mitigate against brute force password hacking. Additionally, businesses with computer systems in the mentioned range are recommended to immediately follow the McAfee Security Research team's advice by searching a computer system's registry for recordings of user accounts being hidden by attackers, and the Windows event and security log for alterations to the registry and any uploaded file that allows simultaneous remote desktop access. Lastly, Pinkerton recommends adding these steps to information security reviews if they are not already included.

Cyber-Attack Targeting Chlorine Distillation Station Stopped

Per reports on July 12, the Ukrainian Secret Service (SBU) stated that it foiled a cyber-attack targeting its chlorine distillation plant in Aulska in the Dnipropetrovsk region.

Per a statement released by the SBU, "the continuation of the cyber-attack could have led to a breakdown of technological processes and possible crash;" the SBU has accused Russia of planning the cyber-attack through the VPNFilter malware. Pinkerton notes that VPNFilter is a malware that targets router models. Once it infects the system, the malware cannot be removed by rebooting the system; further, per reports, the malware is capable of cyber-espionage, stealing files, confidential data, website credentials, and physically destroying the device. Further, per cyber-security experts, the persons responsible for the VPNFilter malware are highly likely state actors, and per the Federal Bureau of Investigation, linked to Russia's military intelligence services. Per reports, the chlorine distillation plant in Aulska is the only one in Ukraine and provides drinking water and sewage treatment facilities for the country.

Though the planned cyber-attack no longer poses a threat to business operations, Pinkerton finds that it underscores the trend of critical infrastructure systems being targeted in cyber-attacks to increase the scope of damage. Pinkerton notes that cyber-attacks targeting Ukraine's infrastructure have been recorded annually since Russia's annexation of Crimea in 2014; major incidents include the attack on Ukraine's power grid in 2015 and 2016, and the NotPetya and Bad Rabbit ransomware attacks. Given this trend, Pinkerton finds that the IT infrastructure of businesses are at a continued risk of cyber-attacks as geopolitical tensions increase between countries. While initiatives to curb such attacks are limited, clients are recommended to ensure that they have a contingency plan in the event that critical infrastructure systems, such as power and water, are attacked.

Twitter Suspends Over 1 Million Accounts Per Day, Says Report

Twitter has increased its crackdown on fake user accounts and bots, suspending over 1 million accounts a day.

The rate of account suspensions has reportedly more than doubled since October 2017 when the company revealed that fake Russian accounts were used to interfere in the 2016 U.S. presidential election; a “troll factory” based in St. Petersburg reportedly used social media platforms to manipulate voter preferences, thereby increasing social and political tensions during the election period. The tweets included, but were not limited to, instructions to Hillary Clinton supporters on invalid voting procedures and promotional posts for then-candidate Donald Trump. Per reports, Twitter suspended 70 million accounts through May-June 2017.

While the Twitter crackdown is targeted at removing fake accounts, Pinkerton finds that it poses a threat to businesses with operations primarily concentrated on digital and social media platforms. The mechanisms to identify fake accounts or bots is yet to be specified by the company; a real person can also operate a fake account that engages in malicious activity while several legitimate accounts such as those by weather reporting agencies are bots. Pinkerton finds that this ambiguity poses a threat to businesses that largely conduct marketing activities on social media platforms such as Twitter. Given the ongoing increased scrutiny on fake news, there is an even chance of other media platforms such as Facebook and WhatsApp engaging in account suspensions over the medium term.

Further, Pinkerton assesses an even chance that the suspension of user accounts will have an adverse impact on the company’s revenue that in some cases depends on the number of active users and reposting of tweets, thereby posing a threat to Twitter’s brand reputation and investor perception in the long term. In the medium term, businesses engaging in digital marketing activity are recommended to review their internal protocols to ensure that their accounts are in compliance with platforms’ policies to avoid suspension of their accounts and disruptions to business continuity.

Upgraded GandCrab Ransomware Targets Even Older Systems

Per reports on July 10, the GandCrab ransomware family has been updated several times in the recent past and is now attempting to infect Windows XP machines; it is using the National Security Agency-linked EternalBlue exploit.

GandCrab 4, the latest variant, is using compromised websites for spreading and appends the “.KRAB” extension to the encrypted files. Further, the latest variant has significantly changed the terms of code structure and has switched to the Salsa20 stream cipher for data encryption. According to the cyber-security firm Fortinet, several infected websites injected with malicious pages were found, which redirect the user to a separate page with the link to the GandCrab executable. Another researcher found that the ransomware is also attempting to spread via the NSA’s EternalBlue SMB exploit. As a consequence, Windows XP and Windows Server 2003 systems are at risk along with modern operating systems.

Given the dynamic nature of the threat from GandCrab ransomware as it is constantly updated, Pinkerton assesses the risk is likely to persist in the medium term. As mentioned in the Pinkerton Insights Intelligence Brief on February 9, the GandCrab ransomware was first reported in January 2018 and was distributed through malware advertising (malvertising). Per the researchers working on the ransomware, the best defense against GandCrab ransomware is to update operating systems with the latest security patches, especially for older operating systems like Windows XP and Windows Server 2003 as several anti-virus software do not support them. Further, clients are recommended to be careful when opening attachments and advised to confirm the source.

Google Confirms Third-Party Application Staff Read Gmail Messages

Per reports on July 3, Gmail users who have connected their email accounts to third-party applications risk unknowingly having their emails read by the staff of the third-party app.

According to Google, this is possible as the email holder is asked to grant the external service certain permissions when creating an account with the app, such as the permission to read and manage the account holder’s email. Reportedly, the practice does not go against Google’s policies, and per a Wall Street Journal interviewee, it is common that software developers scan the inboxes of people who have signed up for email-based external services.

Pinkerton assesses that clients who have connected their email accounts to third-party applications continuously risk having their emails read unless Google enforces more stringent rules toward third-party application developers. Even though Pinkerton finds it likely that the main reason for scanning through Gmail-users’ inboxes is to personalize commercials, clients are advised to avoid including sensitive information in emails, particularly in headings. Pinkerton further notes that, as reported in an Insights Intelligence Brief on September 29, 2017, there is a security gap between primary organizations and third-parties that are increasingly likely to be at risk of data breaches.

Exactis Data Breach Exposes 340 Million Records

On June 2, Wired reported that a security researcher had uncovered a data breach made by marketing and data-aggregation firm Exactis that exposed the personal information of U.S. citizens contained in an estimated 340 million files, divided between approximately 230 million consumers and 110 million businesses.

Comprised of nearly two terabytes of data, the leak is believed to have affected hundreds of millions of U.S. citizens; the exact number of persons involved was unconfirmed as of June 27. While credit card information and social security numbers did not appear to have been included in the breach, other highly-personal information was discovered in the files, such as the genders of individuals' children, health habits like smoking, and personal interests and hobbies; 400 such variables were reportedly contained in the exposed profiles. According to Wired, Exactis acted promptly to protect their data after being notified of the publicized files.

Pinkerton assesses that marketing-related datamining and analytics, which have become increasingly pervasive in digital advertising practices throughout the past decade, appear to have been at the root of several recent breaches. While these practices are unlikely to become less secure as they evolve, highly-publicized breaches by companies like Equifax and Facebook have drawn widespread attention and inspired increased scrutiny of data security standards in general, expanding public awareness of existing practices. The Exactis leak, which is believed to be the largest of its kind since the 2017 Equifax breach, is yet another domino that has fallen in a beeline toward increased governmental regulation of data privacy practices in the U.S. Occurring on the heels of Europe's implementation of the landmark General Data Protection Regulation legislation, the Exactis incident is likely to draw attention to the growing disparity in data privacy regulations between the U.S. and other industrialized nations.

Tasmanian Voters' Details Stolen In Typeform Data Breach

Per reports on July 1, the personal information of approximately 4,000 voters from Tasmania has been stolen through five forms developed by Typeform used on the website of the Tasmanian Electoral Commission (TEC).

Per reports, the name, date of birth, email address, and enrolment address of the voters who applied for an express vote at the 2018 Legislative Council and state elections have been stolen. TEC chairman Mike Blake stated that the Commission would conduct an internal investigation to identify the vulnerability that resulted in the breach. Per reports, several incidents of data breaches have affected federal and state agencies in the past two years, although the data was stolen from a third party in most cases.

Pinkerton assesses that the personal data uploaded on forms developed by Typeform will highly likely remain prone to theft until the vulnerabilities exploited in the TEC data breach are identified and fixed. Pinkerton finds that Tasmanian voters with stolen personal information will likely receive a higher number of phishing emails from unidentifiable addresses. Pinkerton recommends Tasmanian electors who had applied for an express vote on the TEC website in 2018 to avoid responding to emails received from unknown sources. Pinkerton recommends businesses using forms developed by Typeform on their web-based platforms to seek details of the data breach from Typeform to avoid data theft.

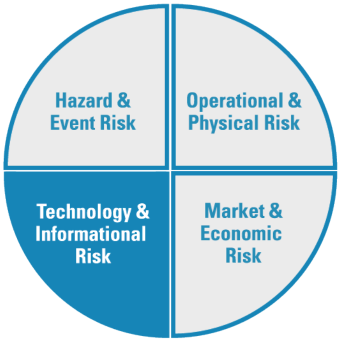
4G Network Flaw Compromises Personal Information

A recent investigation by security researchers from Ruhr-Universitat Bochum and New York University Abu Dhabi reportedly revealed that the Longterm Evolution Network (LTE), commonly known as the 4G network, presented a flaw on the data link layer.

The data link layer is in charge of the connection between the device and the network, encrypting data, organizing communications between users, and stabilizing transmissions. By attacking the layer, the researchers were able to identify the web pages the user browsed and redirect them to a malicious server or website to infect the device with malware. The researchers have already notified the GSM Association, telephone companies, and the 3rd Generation Partnership Project (3GPP) to minimize the future implications.

Pinkerton assesses that a massive attack using this flaw is not likely to occur, as it will require specialized training as well as expensive and sophisticated technology; however, a focused attack may result in severe consequences for a victim. There are no updates or patches to solve the problem because the flaw is inherent to the 4G network design, but 3GPP and 5G developers are working on its design to avoid the deficiency from appearing in the new network design. Nevertheless, major carriers have already begun implementing the 5G protocol without the requisite design update.

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