CYBER SECURITY BRIEFING

A Monthly Recap of Technology & Information Risk

PINKERTON®

OCTOBER 2019

Cyber-Criminals Render More Realistic Phishing Campaigns

New cybercriminal gang is targeting vendors with phishing emails that sends realistic invoices to their clients for money.

Cyber-security researchers of Agari issued a report about new phishing campaigns that target the victims' providers or vendors to render credible malicious invoices to steal money from their actual targets. Agari researchers named the group of cyber-criminals who began these campaigns in 2018 Silent Starling. Per Agari's report, Silent Starling has targeted at least 500 companies and compromised 700 business e-mails. The attack starts by sending fake e-mails to the target's vendors requesting to verify the e-mail credentials in the form of warnings about suspicious activity in their Microsoft account or alleged faxed documents. As malicious actors gain access to the e-mail data, they study the interactions with clients, timeframes of purchases, writing style, and graphic features of e-mails. Finally, malicious actors send a highly realistic invoice to their target and modify the bank account information to include one under the attackers' control. Cyber-security experts stated that these attacks have focused on North America, the UK, and Western Europe, and warned that other criminal groups had mimicked the approach of Silent Starling.

As business e-mail compromise (BEC) campaigns have proved efficient for malicious actors, Pinkerton finds it highly likely that individuals and criminal organizations will replicate similar attacks against companies worldwide. The 2018 Internet Crime Report of the Federal Bureau of Investigation (FBI) calculated losses of USD 1.2 billion (EUR 1.09 billion) due to BEC attacks in 2018. Similar campaigns target executive personnel and impersonate them to defraud the company. Pinkerton recommends that clients inform their staff about phishing campaigns and ensure that e-mails requesting credentials and other personal information are legitimate by contacting the involved institutions directly. Further, verification of the billing data likely will be required to avoid losses due to BEC attacks.

Report Identifies Top Sectors Targeted By State-Backed Hackers

Hackers from the Chinese government hit the largest number of industry verticals during the first half of 2019.

Crowdstrike, a cybersecurity company, revealed the sectors of most interest for cyberattacks to state-sponsored actors and financially motivated cybercriminals. Crowdstrike tracked sophisticated cyber-attacks against its customers in industry sectors from January-June 2019. According to Crowdstrike's report, Chinese government hackers lead the most significant number of attacks against eight out of 19 industry sectors. The Chinese hackers deployed the attacks across the chemical, gaming, hospitality, healthcare, pharmaceutical, manufacturing, technology, and telecommunications sectors. While Russian hackers mainly focused on non-governmental organizations (NGOs) from Crowdstrike's clients, such as think tanks. Although, according to Check Point and Intezer, two Israeli cyber-security companies, Russian state-sponsored hackers are distinguished as the most disruptive, active, and aggressive attackers worldwide. Vietnam-based hackers only targeted the automotive industries, and the Iranian attackers are focused on the transportation, aviation, and logistics sectors. North Korean hackers are leading campaigns against the academic, professional services, telecommunication, and NGO industries. Crowdstrike's report showed that 61% of cyber-attacks were associated with cyber-criminal activity, while state-sponsored actors executed 39%. E-criminals are targeting most of the sectors, including the previous ones and, financial, oil and gas, law enforcement, food and beverage, manufacturing, and retail. Pinkerton assesses that it is highly likely that the industrial sector will remain one of the favorite targets for hackers, and especially for e-criminals.

Following Crowdstrike's report, it is likely that the e-criminals are leading more hacking campaigns; which is why it seems to be an escalation. Pinkerton finds that it is likely that government hackers are most interested in confidential information and intellectual property, while the e-criminals are more likely to target sensitive, administrative, or financial information. Most e-criminals are expecting to get an economic reward, either through bank account theft or blackmail for confidential information. Therefore, it is highly likely that hackers are seeking to obtain passwords and access credentials. According to a Verizon report, 81% of the hacking breaches are done using stolen or weak passwords. Pinkerton recommends all clients enact a multi-layered defense that covers their entire enterprise, including mobile devices, applications, and Internet-connected devices. Pinkerton advises clients to create access policies with third-parties' vendors and to continually reviewing the use of credentials with third parties. Also, Pinkerton recommends all clients to continue back up their data and update their software. Pinkerton advises clients to whitelist software applications to avoid installing non-approved software. Pinkerton recommends clients considering acquiring anti-hacker insurance, to cover any loss in case of a hacking attack. Since an attack can mean significant monetary losses for the company, not just reputational ones. Pinkerton advises clients to consider hiring a managed security service provider (MSSP) to monitor and ensure the security of their network.

GandCrab Ransomware Resurfaces After Alleged Retirement

No retirement for GandCrab after authors have been linked to REvil/Sodinokibi ransomware.

Open sources reported that the GandCrab organization developed the new REvil ransomware despite that the cyber-criminals allegedly ceased operations in May 2019. Researchers from the Counter Threat Unit (CTU) of Secureworks analyzed samples of the REvil ransomware, also known as the Sodinokibi, and revealed that REvil shared code features typically associated with GandCrab. In addition to shared encoding logic, cyber-security experts found an almost identical URL building logic, a deed which is "outside the realm of possibility" to achieve without sophisticated reverse engineering. Finally, the files of the malware samples contained code names that referred to GandCrab and showed that the malware was initially intended to be the sixth version of the ransomware.

Pinkerton assesses that the reappearance of the GandCrab reflects the growing market available for malicious actors on the Dark Web as well as the potential revenues from coordinated cyber-attacks. Per reports, the GandCrab organization made USD 2 billion (EUR 1.8 billion) from January 2018 to late May 2019. Malicious actors rendered a coordinated campaign using the Sodinokibi malware against 22 local government offices in Texas on August 16, 2019. The vectors GandCrab used to infect private and public institutions turn more sophisticated with each new version. This type of malware can spread through system exploits, Remote Desktop Protocol (RDP) servers, and spam campaigns. The GandCrab uses ransomware-as-a-services (RaaS) models, allowing inexperienced actors to subscribe to GandCrab's malware to render similar attacks easier. Thus, Pinkerton finds it likely that the REvil ransomware will remain a credible information threat to clients in the long term as the organization continuously updates their products. Pinkerton recommends clients to back-up, encrypt, and fragment critical data to mitigate the damage of potential cyber-attacks.

XHunt Malware Campaign Targets Shipping Firms

Transportation and shipping companies are targeted by hackers in new trojan malware campaign.

Security researchers at Palo Alto Networks Unit 42 threat intelligence division identified a hacker campaign active since May 2019, which targets transportation and shipping firms that operate in the Persian Gulf. The campaign was named xHunt, as the malicious tools used by the attackers have the names of the characters of an anime series called Hunter x Hunter. The first victim was in Kuwait. The target's machine system was infected with a backdoor named Hisoka version 0.8, which allows other malware to get into the system. Gon, another tool, allows the hacker to scan for open ports on remote systems, upload and download files, take screenshots, find other systems on the network, run commands, and create its own Remote Desktop Protocol (RDP) function. Thus, the attackers are able to keep track of the victim's actions while accessing data. In June 2019, there was another attack on a Kuwait shipping and transport firm. In this attack, researchers detected a more advanced version of Hisoka, being able to transfer itself to other systems and login to Exchange services using legitimate credentials for accounts. Researches think it is likely that the hackers are related to OilRig, also known as APT (Advanced Persistent Threat) 35 and Helix Kitten, which has links to the Iranian government.

Pinkerton assesses that major firms, including those related to shipping and transportation, are likely to continue suffering cyber-attacks in the long term. Security researchers and international IT teams are not able to prevent the execution of hacking campaigns as their malicious tools become more sophisticated, especially if they are state-sponsored, and sometimes remain undetected for months. Moreover, security researchers have difficulties identifying ATP groups as they can carry out different campaigns in various locations. Palo Alto researchers found similarities between the malware used in Kuwait's attacks and another malicious tool called Sakabota, which was detected in July 2018. Some experts believe Sakabota is the predecessor of Hisoka and that the same author developed it. Gon also had similarities with Sakabota's code. Pinkerton recommends clients use security tools able to detect unusual activity on Exchange servers. Further, experts advise incorporating tools that can also detect DNS Tunneling. The leak of firms' data could likely compromise information from other clients in other regions, beside the Persian Gulf, that could be attractive to hackers. Therefore, Pinkerton assesses that many clients' data could likely be at risk as hackers could take advantage of remaining security breaches.

125 Vulnerabilities Identified In Routers Could Impact Millions

Connecting our lives to the internet is creating new ways for hackers to gain remote access to devices' shell or admin panel.

Open sources reported that researchers from the Independent Security Evaluators (ISE) found 125 web application vulnerabilities after testing 13 small office or home office (SOHO) routers and Network Attached Storage (NAS) devices, potentially affecting millions. According to cyber-security experts, the flaws allow attackers to gain remote access to the devices' shell or administrative panel. ISE researchers ascertained that routers and NAS devices from Xiamoi, Lenovo, Zioncom (Totolink), Netgear, QNAP, Seagate, ASUS, Asustor, Zyxel, Buffalo, Drobo, Synology, and TerraMaster manufacturers had at least one vulnerability. Out of the 13 devices, six of them allowed third parties to gain access without authentication. Researchers added that although manufacturers updated several security features for Internet of Things (IoT) devices, some lacked basic protection capabilities.

As IoT technology continues developing and building more extensive networks between devices, Pinkerton assesses that routers and NAS devices' security will remain a significant concern in the long term. In 2018, a Russian state-sponsored group developed the VPNFilter malware which launched a high-profile attack against routers. Pinkerton finds it likely that similar malware will exploit the identified vulnerabilities to render cyber-campaigns. When a malicious actor hijacks these devices, they can trigger distributed denial-of-service (DDoS) attacks, crypto-mining, and access the data sent and received through the network. Pinkerton recommends clients ascertain the brand and model of their routers and NAS devices in their households and at the workplace. More specific information about the model of the identified devices is available at https://www.securityevaluators.com/whitepaper/sohopelessly-broken-2/. Although the companies have been notified and some will release security patches, if the devices correspond to those mentioned in the ISE report, Pinkerton recommends clients contact the support team, update the firmware, and ensure that the device has strong passwords to mitigate cyber-security risks.

Malware Sent Via Text Message Could Impact Almost A Billion

Your data and location may be tracked without your knowledge by SIM card flaw.

Open sources have reported that AdaptiveMobile Security researchers found a spying malware that exploits the SIMalliance Toolbox Browser software (SaT Browser) of SIM cards in mobile devices worldwide. The Simjacker is the first malware sent via text message that operates without the victim's knowledge. The message sends commands to the SIM card, which allow attackers to obtain the location and IMEI of the device. Additionally, cyber-security experts stated that as the malware gives the attackers access to the STK command set, third parties can open browsers and search for malicious websites to spread damaging malware, use the phone as a listening device, send SMS and MMS, and dialing premium-rate numbers to defraud the user. Reportedly, operators in at least 30 countries use the SaT Browser, which potentially impacts a billion users. Moreover, the CEO of AdaptiveMobile stated that the developers of Simjacker are state-sponsored agents as they have access to "critical network backbone infrastructure."

As this is the first text-delivered malware, Pinkerton assesses that attacks of this kind will remain a significant threat to information and privacy security in the medium to long term. Researchers stated that malicious actors could render similar attacks against the Internet of Things (IoT) devices as they use eSIM cards. As state-sponsored agents highly likely devised the Simjacker malware, Pinkerton finds it likely that people involved in state-owned companies, government institutions, and transnational companies remain potential targets. Pinkerton recommends that clients contact their operators to ensure if their handsets use the SaT Browser and inform about the issue. Operators can look for suspicious Sat Browser commands and render specific strategies to block and prevent further attacks. Pinkerton advises following the Virus Bulletin Conference in London on October 3, 2019, in which further technical details about Simjacker will be revealed. Further, Pinkerton recommends that clients monitor the response of operators and telecommunications firms to assess the overall security level of mobile devices.

Data Breach Affects Southeast Asian Airlines

Malindo Air passengers' have personal information exposed after data breach.

Malindo Air, a Malaysian subsidiary of Indonesian biggest private airline Lion Air, suffered a massive data breach, which exposed millions of passengers' personal data from Malaysia and Thailand (Thai Lion Air) operations. The data included passport details, home addresses, and phone numbers. Customer payment details were not compromised. The information was being stored in a public cloud storage system (Amazon), and it was being leaked by a person or organization called Spectre, who runs a site on the dark web. Malindo Air CEO said the leak was detected last week and reported to the Malaysian Communications and Multimedia Commission (MCMC) on September 17. The company says it still does not know how the data breach occurred, but that it would hire an independent cyber-security firm to do forensic analysis. Additionally, Malindo's in-house team, together with Amazon Web Services and GoQuo, started an investigation. Malindo Air has 800 flights per week to 40 destinations.

Pinkerton assesses that significant leaks of data which could compromise millions of people's information are highly likely to continue as airports and airlines become more vulnerable to attacks while increasingly relying on digital technology for their daily operations. Moreover, several databases are not protected and are instead kept in public storage systems. In recent years, several airlines have been subject of data breaches. One of the most significant occurred in October 2018, when Hong Kong's Cathay Pacific Airways Ltd. reported that hackers accessed personal information of 9.4 million customers.

In August 2018, British Airways was affected by a data breach in which hackers stole the personal and financial information of 380,000 passengers, including names and credit card details. As airlines databases collect relevant information of millions of people which is attractive to hackers, Pinkerton assesses that many clients' data could likely be at risk as hackers could take advantage of remaining security breaches.

Local Company Leaks The Country's Population Personal Data

Database leaks personal data of Ecuador's citizens, which included over 6 million children.

Security researchers from vpnMentor discovered two weeks ago an Elasticsearch server exposed personal records of most of the Ecuadorian population, including children, as it was misconfigured. The incident is one of the most significant data breaches in the country's history, as the server contained approximately 20.8 million user records. The number is larger than Ecuador's population due to duplicated files or data from deceased people. The data spread included names, family members' information, civil registration, financial data, and work and car registration information. All the data was spread across the server indexes, and it appeared to have been gathered from updated government sources and private databases. Researchers found records for the country's president and even Julian Assange, who received political asylum for a short period. Some of the indexes were labeled with the acronyms of private and government entities such as BIESS, which stands for Banco del Instituto Ecuatoriano de Seguridad Social, and AEDE, for Asociacion de Empresas Automotrices del Ecuador. According to ZDNet and vpnMentor, the source of the leak is a local company named Novaestrat, which provides analytics services for the Ecuadorian market. The company's website did not display an email address or phone number, and when the researchers tried to access the support forum it yielded a PHP error. Consequently, they reached to the Ecuador CERT (Computer Emergency Response Team), which helped secure the database last week. Security researchers also contacted the server owner.

Pinkerton assesses that significant leaks of data which could compromise millions of people's information are highly likely to continue as several databases are not protected. In August 2019, voter information of more than 14.3 million Chilean citizens, almost 80%of the country's population, was exposed on the internet inside an Elasticsearch database. The information included names, addresses, gender, age, and tax ID numbers. Moreover, it is difficult for security researchers to know when a leak is taking place and since when, thus hindering the prevention of future cyber-intrusions. In this event, one of the biggest privacy concerns was the leak of children's' data as it exposes them to potential identity theft and puts them in physical danger as their home addresses were exposed online. Furthermore, criminals could also target the country's most wealthy citizens, based on their financial records, in case they had accessed the archives.

Power Outage Hits Four Countries

Massive power outage in Central America caused by failure in the connection network.

Recently, a major power outage affected Honduras, Nicaragua, El Salvador, and Guatemala, leaving them partly without electricity. Allegedly, the blackout, which lasted for about an hour, was caused by an error in the regional connection network that originated in the 230-kilowatt supply line in Honduras. Nicaragua's state-owned National Electricity Transmission Company (ENATREL) solved the problem while giving priority to hospitals, health centers, and the sewage system. Citizens in southern Guatemala, as well as people from Nicaragua and Honduras, reported the blackout via social media at the same time.

Pinkerton assesses that these kind of network failures are likely to happen again. In June 2019, Argentina and Uruguay suffered a massive electrical failure which left millions of people without energy and caused public transport disruptions. The outage also delayed local elections in Argentina in several regions. Moreover, parts of Chile and Paraguay were also affected. In this case, authorities did not identify the exact cause and even considered the possibility of a cyber-attack. As power outages are likely to halt cities' services and cause traffic disruptions, affecting logistics, Pinkerton recommends clients monitor the news for up to date information on blackouts locations as violence and crime are likely to occur in those places. Further, the press would allow clients to identify in which regions and countries this problem is expected to take place more frequently.

Experts Discover New Ransomware That Steals Sensitive Information

Malware discovered that looks for and steals confidential files from the military and law enforcement.

Reported earlier this month, the Malware Hunter Team discovered a new malware associated with the Ryuk Ransomware. The Ryuk Ransomware is characterized by encrypting the victim's files and demanding a ransom to be able to recover them. This new ransomware scans all the files and then uploaded the target ones to an attacker-controlled FTP site. The campaign first scans all the data available with the .doc or .xlsx extensions and then checks if the malware contains keywords, such as, 'military,' 'secret' and 'undercover.' Also, it searches for specific first names, which allegedly came from the U.S. Social Security Department's list of top names. According to experts, most antivirus does not protect against this type of malware because it is usually downloaded and installed by the victim from apparently legitimate links that are received by email. Even though it is not common, this type of virus can also affect cell phones, specifically androids. Since there have been code similarities between the new malware and Ryuk, it has led to the speculation that they are likely related in some way. But there is no clarity if the Ryuk group is behind this new malware, or if another group has access and modified the code. Although, the security researchers are still investigating how the ransomware infects and attacks their victims.

Pinkerton assesses that it is highly likely that this new malware is explicitly targeting confidential data for financial gain. Cyber-security experts noted following previous cyber-attacks by the group that the group is likely Russian cyber-criminals, not state-actors. Pinkerton finds that it is highly likely that this ransomware will target government offices, security companies, or companies with essential databases that can engage third parties. Although it is likely that other enterprises will also be attacked since this type of malware can target meaningful information about products and disrupt business operations.

This new malware is much more harmful than Ryuk since the attacker will possess the victim's information, and it highly likely could be leaked to third parties. Pinkerton recommends all clients to keep their computers and applications updated, as new versions are highly likely to bring better protection against possible attacks. Pinkerton advises all clients to avoid opening suspicious links, as well as downloading unknown documents. It is important to keep a backup copy of all the files and information since it is the only reliable way to recover the data. Therefore, Pinkerton recommends all clients to create a backup plan, in which at a specific time of day a backup of all the information is made. Pinkerton advises all clients to acquire a reliable antivirus, because, although it may not stop the malware, it can detect it; and make it easier to remove. Pinkerton recommends all clients to filter in your mail all files that contain an extension '.EXE', to avoid downloading harmful files. If any client has downloaded a suspicious file by mistake, it is advised to disconnect the computer from the internet network; to prevent third parties from downloading or accessing the information. Then Pinkerton recommends that a cyber-security expert checks the device and delete the file if it is a malware.

Report Shows Black Market On The Dark Web Encourages Cyber-Crime

Inexpensive hacking tools and services on the black market lead to increase in cybercrimes.

Recently, Armor's Threat Resistance Unit (TRU) issued the Black Market Report, which revealed that cyber-crime tools and services are widely available at affordable prices on the black market of the Dark Web. Armor's researchers found that cyber-criminals offer malicious tools and a variety of services to third parties. One of the most common products is detailed identity packets (fullz) containing personal and financial information of residents all over the world. The price varies depending on the origin of the data. For instance, fullz from the U.S. cost between USD 30-40 (EUR 27-36), while French fullz value on an average of USD 20-25 (EUR 18-23).

Additionally, cyber-criminals offer more complex services such as banking trojans (USD 1,000), Distributed Denial-of-Services (DDoS) campaigns (USD 60 per hour), and monthly subscriptions of USD 120 to request ransomware attacks. Cyber-criminals frequently target medical companies as their records contain valuable information. According to Privacy Rights Clearinghouse, 23.5 million medical records have been disclosed from 266 medical organizations during 2019. Other products available to malicious actors are access credentials for remote desktop protocols (RDP) which allegedly remain unhacked.

Pinkerton assesses that cyber-crime will highly likely remain a significant security threat for business worldwide. Researchers noted a 29% decrease of the price of stolen financial data from British accounts, suggesting a high supply of leaked information in the Dark Web. Amateur hackers obtain packets of data from various institutions and offer them to more skillful malicious actors that use the information to render more dangerous attacks like phishing campaigns and identity theft. Furthermore, buyers at the black market can purchase packets with malware and an attached tutorial, further increasing the cyber-security threats. As cryptocurrency lacks international legislation and most countries do not have an industry-specific regulation for the cryptocurrency market, Pinkerton finds that illicit transactions through the Dark Web to buy cyber-criminal tools and services will continue in the long term. Pinkerton recommends that clients ensure that the networks, database, and devices related to their business have update security protocols for a wide range of malware. Due to the high availability of sensitive personal information, Pinkerton advises reporting any suspicious financial activity to the corresponding authorities.

Telnet Vulnerabilities Affect Over A Million IoT Devices

Backdoor vulnerabilities allow a million IoT radio devices to be remotely exploited.

Open sources reported that a cyber-security expert from Vulnerability-Lab found significant vulnerabilities in Telestar Digital GmbH Intenet of Things (IoT) radio devices. The compromised stereos are from the Imperial & Dabman Series I and D, including digital audio broadcasting (DAB) stereos. An undocumented Telnet service, an active port forwarding, and a weak password let external agents gain access to the device with full privileges. According to cyber-security experts, this breach allows the attackers to save audio files, remotely or locally send audio as commands, and change the device name. After researchers informed Telestar Digital GmbH on June 1, 2019, the firm launched a patch by August 30 and stated that updates would be released to maintain an overall safe environment against cyber-attacks.

As future deployment will benefit the capabilities of IoT devices, Pinkerton finds it highly likely that cyber-campaigns targeting IoT devices will increase in the long term. Cyber-security experts have warned about high-impact cyber-attacks that hijack smart devices to distribute malware or render large-scale attacks. The Mirai botnets hijack devices with weak security protocols to perform denial-of-service (DDoS) attacks. As DAB stereos are widely distributed in Europe and the Asia Pacific, Pinkerton recommends clients using the identified devices to reset the radios to the factory settings and enable the downloads of the most recent firmware version to activate the automatic download of security patches. For more technical information about this issue, consult the two assigned common vulnerabilities and exposures, CVE-2019-1373 and CVE-2019-13474. Further, Pinkerton recommends clients operating with IoT technology to evaluate the devices' security protocols and customize strong passwords whenever possible.

Major Manufacturing Firm's Data Breach Due To An Open Database

DK-Lok's internal and external communications were breached exposing client data, newsletters, and emails.

The cybersecurity firm, vpnMentor has revealed the existence of an open database from DK-Lok, the South Korean industrial manufacturer. According to the researchers, they discovered the database during a vpnMentor's web mapping project. This project was created to find online systems that do not have any form of access restrictions or authentication. In this open database, it is found all the internal and external communications records of DK-Lok; including private emails, personal messages, online e-commerce orders, product bids, travel details, full staff and client names, telephone numbers and user IDs. The exposed database includes information of clients in the U.S., South Korea, New Zealand, South Africa, Australia, among other countries. Also, there is an email sent by the Australian government and at least 1,500 emails from the UK. VpnMentor notified DK-Lok about the open database on August 21, but the access was still open on September 5. Also, on September 3, vpnMentor discovered that Yves Rocher, the French retail consultancy, exposed the data of 2.5 million of its Canadian customers. Including names, email addresses, phone numbers, birth dates, and postcodes, ID's, transaction amount, the currency used, store location, and delivery date. This data breach was discovered through an unsecured Elasticsearch database, which let them access to Aliznet, a private database.

Pinkerton assesses that it is highly likely that more enterprises and corporations are not using any authentication form or access restriction in their Information Technology (IT) infrastructure. Which makes it easier for hackers or even competitors to obtain this information. Pinkerton finds that it is highly likely that this kind of data breach will affect the companies, in terms of reputation and future business since clients will not feel that their data or private information is secure. Pinkerton recommends all clients ensure that IT staff routinely review the company's IT infrastructure and solve any security problems they may encounter. Pinkerton advises hiring cybersecurity specialists to ensure that there are no problems or possible leaks of your information. Pinkerton advises all clients to act immediately if their company is notified of a data breach or cyber-attack.

Cyber-Attack Affected The Power Grid Causing A Blackout

Cyber attack on U.S. power grids is first of its kind causing five minute blackouts.

Cyber-terrorists attacked the U.S. power grid, affecting its control center and several sites across the country on March 5, 2019. The cyber-attack caused five-minute blackouts in the western U.S., and signal outages at the grid's low-impact control center. In January 2019, the former National Intelligence Director revealed that Russians hackers were capable of disrupting the power utilities in the U.S. because they had already done so in Ukraine in 2015 and 2016 for several hours. However, according to a Dragos Inc. cyber-security expert, there was no evidence that hackers intentionally targeted the power grid. Reportedly, the cyber-attack was likely performed by an automated bot scanning for vulnerable devices. Also, the North American Electric Reliability Corporation (NERC) reported that the firmware was not updated for the firewalls that got attacked, but patches have since been deployed.

Although this incident did not intentionally target the power grid, it is highly likely that attacks against critical infrastructure, including power grids, will continue to occur worldwide with increased frequency and sophistication. In the last ten years, the energy sector has experienced various attacks, affecting homes, institutions, and companies, to name a few. Pinkerton assesses that a cyber-attack on the electricity infrastructure will highly likely impacts on the country and world's economy; due to the interconnectivity and digitalization. A blackout would highly likely result in a loss of information, interruption in operations, and an even chance of theft or leak of data. Although all sectors would be affected, it is highly likely that the telecommunications, ports, and sewage sectors would have a more significant number of losses. Pinkerton finds that it is likely that such attacks will be carried out on a smaller scale to test penetration capabilities. Pinkerton advises all client to us Virtual Private Networks (VPNs) and regularly update and check your firmware. Also, Pinkerton recommends all clients to segment their network, and restrict the communication traffic to the expected, to reduce the impact of a breach. Pinkerton recommends all clients to keep primary and backup power systems in good condition to mitigate the impact of sudden blackouts on operations and data.

Successful Deepfake Voice Attack Impacts Energy Firm

AI-generated audio tricked a CEO into wiring money to a scammer's bank account.

Open sources have reported that malicious actors successfully deceived the manager of a UK-based energy firm into transferring EUR 220,000 (USD 242,704) using a deepfake voice attack. Deepfake developers gather audio or visual information of a subject and program artificial intelligence (AI) to modify the attacker's appearance or voice to pass as someone else. Chief executive officers (CEOs) or individuals with high exposure in media outlets are potential targets. During the reported incident, the attacker impersonated the CEO of the German parent firm and urged a British employee to make the money transaction to a Hungarian account. After the preliminary investigations, reports say that the malicious actor moved the money to accounts in Mexico and other locations.

As the development of AI is increasing, cyber-campaigns based on this technology will likely remain a significant threat to companies worldwide in the long term. According to cyber-security researchers of Pindrop, only one of 638 voice frauds in 2013-2017 was artificially generated. However, these numbers likely will increase as well as their efficiency in the short to medium term. Similar to phishing campaigns, the success of deepfake attacks rely on exploiting unknowing employees.Thus, Pinkerton recommends its clients to inform its personnel about the nature of these attacks and implement secondary verification procedures for instructions that involve sharing sensitive information or transferring money.

For instance, requesting an e-mail to confirm what has been instructed through a phone call. Further, Pinkerton recommends monitoring the development of cyber-security software to detect deepfake audio and video. The media forensics department of the U.S. Defense Advanced Research Projects Agency (DARPA) has offered financial support to research organizations to create more advanced deepfake detection tools.

Two Year Spyware Campaign Called Most Serious iPhone Hack To Date

Nation-state hackers infected Apple iPhones with spyware over two years ago.

Researchers say that suspected nation-state hackers had been infecting iPhones with spyware for over two years. On August 29, Google Researchers revealed five exploit chains that had been targeting iOS platform ranging from iOS 10 to iOS 12. The exploit chains are tools that link the security vulnerabilities, allowing the hacker to penetrate each layer of the iOS protections. Therefore, the chains took advantage of 14 security flaws and affected everything from the browser's isolation mechanism to the core of the operating system, gaining complete control over the phone. According to Google's researchers, several websites were programmed to assess devices, and then infect them with a monitoring malware. Some of the malicious sites were active from 2016 to July 2019, which was when the last one was found; and had thousands of visitors per week. Through this malware, hackers could monitor live location data, access photos, contacts, passwords, or even to end-to-end encryption apps like WhatsApp or Hangouts. Apple declined to comment on the operation but allegedly patched the vulnerabilities in the iOS 12.1.4, released on February 1.

Pinkerton assesses that it is likely that more chains and malware for the iPhone will emerge since in the latest iOS updates many vulnerabilities have been found that enable cyber-attacks. Due to the nature of the malware, it is highly likely that infected iPhone owners were unaware that their device was hacked and their communications compromised. Pinkerton advises all the iPhone users to update its software to the iOS12.4.1, which is the latest patched version, for this malware and the jailbreak flaw, that appeared on August 17. Also, Pinkerton recommends all clients use a professional antivirus, to protect their iPhone from any virus or malware from malicious websites or apps. Since hackers implanted the malware on pages without the Hypertext Transfer Protocol Secure (HTTPS) encryption; Pinkerton advises all clients browse pages with this encryption and avoid unofficial or illegitimate pages.

State-Sponsored Hacking Campaign Targets Uyghurs Ethnic Minority

Monitoring implants were installed on phones by China to target Uyghur Muslims.

Security researchers from Volexity discovered state-sponsored hackers compromised websites popularly used by ethnic minority Uyghurs. The hackers programmed these websites to install monitoring implants on the users' phones, infecting both iPhone and Android devices. The international community recently condemned China because of its treatment of Uyghur Muslims, which includes intense surveillance. Additionally, around a million Uyghur Muslims have been detained at detention "reeducation" camps by Chinese authorities in Xinjang province. Volexity researchers released a report on September 2, 2019, describing how certain websites frequently used by Uyghurs members, such as news sites and learning resources, automatically hacked the Android phones of the users who visited the sites. Researchers say hackers used "watering holes" attacks, which allow them to compromise sites their targets usually visit instead of seeking their victims out directly. Initially, Volexity researchers only detected the vulnerability on Android phones, however, thanks to a recent discovery made by Google's Project Zero and TechCrunch, Volexity members confirmed that iPhone users were also targets of some of the compromised URLs. The chairman of the Uyghur Human Rights Project told CNN he had been target of email-based hacking attempts before knowing about the affected websites.

Pinkerton assesses that more popular websites are likely to be hacked in the long term, so to obtain information from both iPhone and Android users linked to minorities or political opposition. Security researchers and international IT teams are not able to prevent the execution of state-sponsored hacking campaigns as their operation are not limited to a specific region or group. In 2014, China targeted Tibetan Buddhists through regular spear phishing attacks; thus they began a campaign to stop using email attachments. These events show how cyberespionage campaigns can be compelling when they are supports by governments and the latter deice to spy on particular groups. Nonetheless, by compromising many websites, the attacks hack indiscriminately the device of any user who accesses the affected sites, which tend to be used by thousands of individuals. Therefore, many clients are likely to be exposed. Furthermore, areas where targeted groups, in this case Uyghurs, locate are likely to have more security presence including cameras and facial recognition systems. Other Uyghurs important communities are located in Taoyuan County, in north-central Hunan, and countries such as Kazakhstan, Kyrgyzstan, Uzbekistan, and Turkey. Pinkerton recommends clients located in these zones to install the updated version at the earliest convenience, keep their devices up-to-date, and verify that their accounts do not present any unrecognized actions.

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