From: "Reiff, Darrell (MM) (FBI)" <dreiff@fbi.gov>
To: Southeast Florida Fusion Center <seffc@mdpd.com>, "bso_intel@sheriff.org" <bso_intel@sheriff.org>, "pbregionalfusion@pbso.org" <pbregionalfusion@pbso.org>, FusionCenter FL - CFIX <cfix@ocfl.net>, "Florida Fusion Center" <FFCenter@FDLE.state.fl.us>
Cc: "NCTC at Miami (miami@nctc.gov)" <miami@nctc.gov>
Subject: Cyber Highlights for January 16 - 23, 2018
Date: Tue, 23 Jan 2018 18:30:39 +0000
Importance: Normal

To the South Florida JTTF, and the Florida Fusion Centers, and the Private Sector Security Partners,

The following list of cyber highlights articles are intended for information only, and not as official FBI opinion:

Cyber Highlights January 16 – 23, 2018

NEWS ITEMS:

Legislation /Policy:

NA

Critical Infrastructure / SCADA:

NA

Ransomware:

1 - World's Largest Spam Botnet Is Pumping and Dumping an Obscure Cryptocurrency

https://www.bleepingcomputer.com/news/cryptocurrency/worlds-largest-spam-botnet-is-pumping-and-dumping-an-obscure-cryptocurrency/

- Necurs, the world's largest spam botnet, is currently sending millions of spam emails that push an obscure cryptocurrency named Swisscoin.
- Such spam emails are known as pump-and-dump, and the technique relies on sending large quantities of spam to drive interest up towards a particular penny stock.
- Necurs, a spam botnet believed to have millions of bots, has been known to engage in pump-and-dump spam campaigns for years, being one of its primary activities, besides spreading the Dridex banking trojan, and several ransomware families.
- The cryptocurrency in question is Swisscoin, an altcoin that's been described as a Multi-Level-Marketing (MLM) ponzi scheme in a report last year, and for which trading was recently suspended.
- It was also seen sending dating spam and emails carrying files that spread the GlobeImposter ransomware.

2 - City Of Farmington Recovering After SamSam Ransomware Attack

http://www.daily-times.com/story/news/local/farmington/2018/01/18/farmington-recovering-after-ransomware-attack/1044845001/

- The City of Farmington is returning to normal after a variant of the ransomware known as SamSam shut down the computer systems.
- City Manager Rob Mayes said via text message that the FBI advised the city not to pay the 3 bitcoin — worth more than $35,000 — ransom that was demanded. Mayes said the city was able to recover the encrypted information without paying ransom.
- Many of the business operations computers were encrypted on 03 JAN by a variance of the SamSam ransomware.
- According to a press release from the city, no customer or employee personal information was extracted and the public administration system was not affected. The ransomware also did not breach any electric utility operations systems and there was not an interruption of public safety services. The city email systems were not affected by the virus.

3 - Ransomware Attack Targets Adams Memorial Hospital

http://wane.com/2018/01/18/ransomware-attack-targets-adams-memorial-hospital/

- Adams Health Network, which runs Adams Memorial Hospital, has confirmed that a ransomware attack targeted some of its computer servers on 11 JAN.
- An employee brought the problem to the attention of administrators after certain files did not look correct according to Susan Sefton, a spokesperson for Adams Memorial Hospital. Sefton said the network was slow and then went blank before files on the system read "sorry."
- The Berne Outpatient Clinic and three physicians in the network could not access patient history or appointment schedules Friday as a result of the breach. Sefton said this impacted about 60 to 80 patients. Adams Health Medical Offices were closed Friday and a Facebook post attributed the closure to weather conditions.
- Doctors now have access to scheduling however it is unclear if access to patient history has been restored. Sefton said the IT department still working to fully restore the servers.

4 - Allscripts Recovering from Ransomware Attack That Has Kept Key Tools Offline

https://www.csoonline.com/article/3250246/security/allscripts-recovering-from-ransomware-attack-that-has-kept-key-tools-offline.html

- Allscripts, the billion-dollar electronic health record (EHR) company headquartered in Chicago, IL said they were still working to recover from a ransomware attack that left several applications offline after data centers in Raleigh and Charlotte, NC were infected on Thursday
- In a conference call for customers on Saturday, which Salted Hash listened-in on, Allscripts' Jeremy Maxwell, director of information security, said their PRO EHR and Electronic Prescriptions for Controlled Substances (EPCS) services were the hardest hit by the ransomware attack.
- The ransomware attack started on Thursday, January 18 at around 02:00 a.m. EST, and by 06:00 a.m. EST it was a full-blown ransomware incident, which required that incident response teams from Microsoft and Cisco be called in to assist.
- Backup systems were not impacted by the ransomware, thus enabling Allscripts to restore systems one-by-one from backup. Full backups are made on Friday, and incremental backups are done nightly at 10:00 p.m. EST. So as the systems are restored, the expectation is that there will be minimal – if any – data loss.
- The variant of SamSam that infected Allscripts was a new variant unrelated to the version of SamSam that infected systems at Hancock Health Hospital in Greenfield, Indiana and Adams Memorial Hospital in Decatur, Indiana.

Malware:

1 - MaMi Malware Targets Mac OS X DNS Settings

http://www.zdnet.com/article/mami-malware-targets-mac-os-x-dns-settings/

- A researcher has discovered a strain of malware in the wild which targets Mac OS X users. The malware, dubbed MaMi, was first spotted by security researcher Patrick Wardle.
- The only indicator spotted by Malwarebytes software at the time was reported as "MyCoupon" software, which is often labeled as nuisanceware. However, the hijack of DNS entries suggested that something more sinister was happening.
- MaMi is not sophisticated. The unsigned Mach-O 64-bit executable has been marked as app version 1.1.0, which suggests the malware is fresh from development.
- However, the creator of MaMi has included functionality including DNS hijacking, screenshot capture, generation of simulated mouse events, the download and upload of files, the execution of arbitrary code, and may also persist as a launch item.
- In a blog post, Wardle said that while infection methods remain a mystery, the malware is hosted on a number of domains.

2 - Phishers Push Malware Disguised as Meltdown Fix

https://www.infosecurity-magazine.com/news/phishers-push-malware-disguised/

- Cyber-criminals are using interest in the recent Meltdown and Spectre chip vulnerabilities to trick users into downloading malware disguised as security patches, according to Malwarebytes.
- The SSL-enabled phishing site is spoofed to look like one managed by the German Federal Office for Information Security (BSI), explained the vendor's lead malware intelligence analyst, Jérôme Segura.
- This fake domain links to a ZIP archive which appears to contain a patch for the recently disclosed chip flaws (Intel-AMD-SecurityPatch-10-1-v1.exe) but is in fact malware.
- "Upon running it, users will infect themselves with Smoke Loader, a piece of malware that can retrieve additional payloads. Post-infection traffic shows the malicious file attempting to connect to various domains and sending encrypted information," Segura explained.

3 - New 'AdultSwine' Malware Displays Adult Images To Children

https://www.inc.com/joseph-steinberg/new-adultswine-malware-displays-pornography-to-children.html

- Malware that displays graphic, adult images has been found in multiple Android apps targeting children.
- The new strain, dubbed *AdultSwine* by researchers, was found in 60 Android apps, many with child-focused names -- such as *Spinner Toy for Slither* and *Drawing Lessons Angry Birds* -- by researchers from the cybersecurity firm, Checkpoint. According to Google app store estimates, the infected programs were downloaded between 3.5 and 7 million times.
- When run, the malware causes the apps in which it resides to displays popups - some of which include advertisements containing sexual imagery and others containing ads for fake security software and other problematic items.
- Because the malware works by downloading target links from a malware command-and-control server, it could also be extended to take other harmful actions.

4 - Skygofree — a Hollywood-style Mobile Spy

https://www.kaspersky.com/blog/skygofree-smart-trojan/20717/

- We recently discovered one such cinematic Trojan by the name of Skygofree. Skygofree is overflowing with functions, some of which we haven't encountered elsewhere. For example, it can track the location of a device it is installed on and turn on audio recording when the owner is in a certain place. In practice, this means that attackers can start listening in on victims when, say, they enter the office or visit the CEO's home. Skygofree can also secretly turn on the front-facing camera and take a shot when the user unlocks the device, and intercept calls, SMS messages, calendar entries, and other user data.

- Another interesting technique Skygofree employs is surreptitiously connecting an infected smartphone or tablet to a Wi-Fi network controlled by the attackers — even if the owner of the device has disabled all Wi-Fi connections on the device. This lets the victim's traffic be collected and analyzed. In other words, someone somewhere will know exactly what sites were looked at and what logins, passwords, and card numbers were entered.
- The malware also has a couple of functions that help it operate in standby mode. For example, the latest version of Android can automatically stop inactive processes to save battery power, but Skygofree is able to bypass this by periodically sending system notifications. And on smartphones made by one of the tech majors, where all apps except for favorites are stopped when the screen is turned off, Skygofree adds itself automatically to the favorites list.
- We discovered Skygofree recently, in late 2017, but our analysis shows the attackers have been using it — and constantly enhancing it — since 2014. Over the past three years, it has grown from a rather simple piece of malware into full-fledged, multifunctional spyware.
- The malware is distributed through fake mobile operator websites, where Skygofree is disguised as an update to improve mobile Internet speed. If a user swallows the bait and downloads the Trojan, it displays a notification that setup is supposedly in progress, conceals itself from the user, and requests further instructions from the command server. Depending on the response, it can download a variety of payloads — the attackers have solutions for almost every occasion.

5 - Microsoft Office Vulnerabilities Used to Distribute Zyklon Malware in Recent Campaign

https://www.fireeye.com/blog/threat-research/2018/01/microsoft-office-vulnerabilities-used-to-distribute-zyklon-malware.html

- FireEye researchers recently observed threat actors leveraging relatively new vulnerabilities in Microsoft Office to spread Zyklon HTTP malware. Zyklon has been observed in the wild since early 2016 and provides myriad sophisticated capabilities.
- Zyklon is a publicly available, full-featured backdoor capable of keylogging, password harvesting, downloading and executing additional plugins, conducting distributed denial-of-service (DDoS) attacks, and self-updating and self-removal. The malware may communicate with its command and control (C2) server over The Onion Router (Tor) network if configured to do so. The malware can download several plugins, some of which include features such as cryptocurrency mining and password recovery, from browsers and email software. Zyklon also provides a very efficient mechanism to monitor the spread and impact.
- We have observed this recent wave of Zyklon malware being delivered primarily through spam emails. The email typically arrives with an attached ZIP file containing a malicious DOC file (Figure 1 shows a sample lure). The following industries have been the primary targets in this campaign: Telecommunications; Insurance; Financial Services
- Attack Flow: 1: Spam email arrives in the victim's mailbox as a ZIP attachment, which contains a malicious DOC file. 2: The document files exploit at least three known vulnerabilities in Microsoft Office, which we discuss in the Infection Techniques section. Upon execution in a vulnerable environment, the PowerShell based payload takes over. 3: The PowerShell script is responsible for downloading the final payload from C2 server to execute it.
- Conlclusion: Threat actors incorporating recently discovered vulnerabilities in popular software – Microsoft Office, in this case – only increases the potential for successful infections. These types of threats show why it is very important to ensure that all software is fully updated. Additionally, all industries should be on alert, as it is highly likely that the threat actors will eventually move outside the scope of their current targeting.

6 - New Botnet Infects Cryptocurrency Mining Computers, Replaces Wallet Address

https://arstechnica.com/information-technology/2018/01/in-the-wild-malware-preys-on-computers-dedicated-to-mining-cryptocurrency/

- Satori—the malware family that wrangles routers, security cameras, and other Internet-connected devices into potent botnets—is crashing the cryptocurrency party with a new variant that surreptitiously infects computers dedicated to the mining of digital coins.
- A version of Satori that appeared on January 8 exploits one or more weaknesses in the Claymore Miner, researchers from China-based Netlab 360 said in a report published Wednesday. After gaining control of the coin-mining software, the malware replaces the wallet address the computer owner uses to collect newly minted currency with an address controlled by the attacker. From then on, the attacker receives all coins generated, and owners are none the wiser unless they take time to manually inspect their software configuration.
- It's not clear precisely how the new variant is infecting mining computers. At least one vulnerability has been reported in the Claymore Mining software, along with a corresponding vulnerability. Wednesday's post said Satori isn't exploiting it. Instead, Wednesday's post said Satori "works primarily on the Claymore Mining equipment that allows management actions on 3333 ports with no password authentication enabled (which is the default config)."
- Satori is a modified version of the open source Mirai botnet malware. Mirai took control of so-called Internet-of-Things devices and caused them to participate in distributed denial-of-service attacks that paralyzed large swaths of the Internet in 2016. When Satori appeared in December, the underlying code was significantly overhauled. Instead of infecting devices that were secured with easily guessable default passwords, it exploited programming vulnerabilities in the device firmware. In early December, Satori had infected more than 100,000 devices and reportedly grew much bigger in the following weeks.

7 - Crypto-Mining Attack Targets Web Servers Globally

http://www.securityweek.com/crypto-mining-attack-targets-web-servers-globally

- Dubbed RubyMiner, the threat was discovered last week, when it started launching massive attacks on web servers in the United States, Germany, United Kingdom, Norway, and Sweden. Within a single day, the attackers behind this malware attempted to compromise nearly one third of networks globally.
- The purpose of the attack, which is targeting both Windows and Linux servers, is to install XMRig, a Monero miner, by exploiting old vulnerabilities that have been published and patched in 2012 and 2013. The attackers weren't looking for stealth compromise, but attempted to compromise a large number of vulnerable HTTP web servers as quickly as possible.
- The infection campaign is targeting vulnerabilities in PHP, Microsoft IIS, and Ruby on Rails. Despite the large number of compromise attempts observed, only 700 servers worldwide have been successfully enslaved within the first 24 hours of attacks. The attack on Ruby on Rails attempts to exploit CVE-2013-0156, a remote code execution vulnerability. A base64 encoded payload is delivered inside a POST request, expecting the Ruby interpreter on the server to execute it.
- The payload is a bash script designed to add a cronjob that runs every hour and downloads a robots.txt file containing a shell script, designed to fetch and execute the crypto-miner, but not before checking whether it is already active on the host. Not only the mining process, but the entire download and execution operation runs every hour.
- One of the domains used in the newly observed infection campaign is lochjol.com, which was previously used in an attack in 2013. That attack abused the Ruby on Rails vulnerability as well, and also had some features common with the current incident, but the researchers couldn't determine further connections between the two, especially with their purpose seemingly different.

8 - EFF And Lookout Uncover New Malware Espionage Campaign Infecting Thousands Around the World

https://www.eff.org/press/releases/eff-and-lookout-uncover-new-malware-espionage-campaign-infecting-thousands-around

- The Electronic Frontier Foundation (EFF) and mobile security company Lookout have uncovered a new malware espionage campaign infecting thousands of people in more than 20 countries. Hundreds of gigabytes of data has been stolen, primarily through mobile devices compromised by fake secure messaging clients.

- The trojanized apps, including Signal and WhatsApp, function like the legitimate apps and send and receive messages normally. However, the fake apps also allow the attackers to take photos, retrieve location information, capture audio, and more.
- The threat, called Dark Caracal, may be a nation-state actor and appears to employ shared infrastructure which has been linked to other nation-state actors. In a new report, EFF and Lookout trace Dark Caracal to a building belonging to the Lebanese General Security Directorate in Beirut.
- "People in the U.S., Canada, Germany, Lebanon, and France have been hit by Dark Caracal. Targets include military personnel, activists, journalists, and lawyers, and the types of stolen data range from call records and audio recordings to documents and photos," said EFF Director of Cybersecurity Eva Galperin. "This is a very large, global campaign, focused on mobile devices. Mobile is the future of spying, because phones are full of so much data about a person's day-to-day life."
- Dark Caracal has been operating since at least 2012. However, one reason it has been hard to track is the diversity of seemingly unrelated espionage campaigns originating from the same domain names. The researchers believe that Dark Caracal is only one of a number of different global attackers using this infrastructure. Over the years, Dark Caracal's work has been repeatedly misattributed to other cybercrime groups. In fact, EFF's Operation Manual report from 2016 misidentified espionage from these servers as coming from the Indian security company Appin.

9 - Evrial Trojan Switches Bitcoin Addresses Copied to Windows Clipboard

https://www.bleepingcomputer.com/news/security/evrial-trojan-switches-bitcoin-addresses-copied-to-windows-clipboard/

- A new information stealing Trojan called Evrial is being sold on criminal forums and being actively distributed in the wild. Like most infostealing Trojans, Evrial can steal browser cookies and stored credentials, but this Trojan also has the ability to monitor the Windows clipboard for certain text, and if detected, modify it to something else.
- First discovered and tracked by security researchers MalwareHunterTeam and Guido Not CISSP, by monitoring the Windows clipboard for certain strings, Evrial makes it easy for attackers to hijack cryptocurrency payments and Steam trades. This is done by replacing legitimate payment addresses and URLs with addresses under the attacker's control.
- According to MalwareHunterTeam, Evrial is currently being sold on Russian criminal forums for 1,500 Rubles or ~ $27 USD. In the advertisement, the seller states that after purchasing the product, an attacker gains access to a web panel that allows them to build an executable. This web panel also keeps track of what clipboard modifications have taken place and allows an attacker to configure what replacement strings should be used.
- Evrial's most interesting feature is that it will monitor the Windows clipboard for certain types of strings and replace them with ones sent by the attacker. This allows the attacker to reroute a cryptocurrency payment to an address under their control.
- In addition to monitoring and modifying the clipboard, Evrial will also steal bitcoin wallets, stored passwords, documents from the victim's desktop, and a screenshot of the active windows. All of this information will be compiled into a zip file and uploaded to the attackers' web panel.

10 - Triton Malware Exploited Zero-Day Flaw in Schneider Electric Safety Controllers

https://securityboulevard.com/2018/01/triton-malware-exploited-zero-day-flaw-in-schneider-electric-safety-controllers/

- Schneider Electric has confirmed that a recently uncovered malware program that was used to attack industrial infrastructure exploited a vulnerability in its Triconex safety controllers.
- The malware, dubbed Triton, was uncovered in December by researchers from security firm FireEye after it triggered an emergency shutdown event at a critical infrastructure organization. It was the first case of malware designed to specifically infect industrial controllers after Stuxnet, which was used to destroy uranium enrichment centrifuges at Iran's Natanz nuclear plant in 2010.

- Schneider is developing a security enhancement for the Tricon controllers, a tool to detect the malware's presence and a procedure to remove it when discovered. These are expected to be released in February.

DDoS:

1 - Mirai Okiru: New DDoS Botnet Targets ARC-Based IoT Devices

https://www.csoonline.com/article/3247794/security/mirai-okiru-new-ddos-botnet-targets-arc-based-iot-devices.html

- Mirai malware and its many variants which have targeted CPU architectures in the past, is now targeting the second most popular type of CPU core – ARC processors.
- Meet Mirai Okiru, the Mirai variant targeting ARC processors, which are embedded processors used in IoT, auto, mobile, TVs, cameras and a nearly endless list of products – CPUs reportedly shipped in over a billion products per year. Brace yourself for the botnet targeting ARC-based IoT devices.
- You may remember hearing about the Mirai malware variant Satori (pdf) back in December; it was sometimes also called Okiru. Satori was used to attack "hundreds of thousands" of Huawei routers. The exploit was released for "free" on Christmas by what NewSky Security dubbed a blackhat Santa.

Despite the similarities of the two type of Linux IoT DDoS malware, Mirai Okiru is "very different" from the Mirai Satori variant.

Breach / Hacking / Phishing:

1 - Official: Hancock Regional Hospital Information System Hacked, Patient Info Not Affected

https://www.indystar.com/story/news/2018/01/12/official-hancock-regional-hospital-information-system-hacked-patient-info-not-affected/1030542001/

- A Hancock Regional Hospital official has confirmed that the hospital's information system is being held hostage as part of a ransomware attack, but said patient information does not appear to have been compromised.
- Rob Matt, the hospital's chief strategy officer, said the hack occurred around 10 p.m. Thursday and was noticed by hospital employees immediately. The hack affects the hospital's email system, electronic health records and other internal operating systems, he said.
- It's unclear who or what is hacking the system, Matt said, but they are asking for an unspecified amount of bitcoin, a form of cryptocurrency. Matt said the hospital has not paid that ransom.

Matt said hospital staff had been adequately trained and was able to continue to provide patient care Friday without electronic system access.

2 - Latvia's E-health System Hit By Cyberattack From Abroad

https://sg.news.yahoo.com/latvias-e-health-system-hit-cyberattack-abroad-174710799.html

- Latvia said its new e-health system was on Tuesday hit by a large-scale cyberattack that saw thousands of requests for medical prescriptions pour in per second from more than 20 countries in Africa, the Caribbean and the European Union.
- No data was compromised, according to health officials, who immediately took down the site, which was launched earlier this month to streamline the writing of prescriptions in the Baltic state.
- "It is clear that it was a planned attack, a widespread attack -- we might say a specialised one -- as it emanated from computers located in various different countries, both inside the European Union and outside Europe," state secretary Aivars Lapins told reporters.
- The site was back up and running within a couple of hours but with reduced functionality, forcing Latvia to provisionally revert to the previous paper system that was kept as a backup after digital prescriptions became compulsory on January 1.

3 - 4 Malicious Chrome Extensions Put 500k Users at Risk of Click Fraud

https://www.hackread.com/malicious-chrome-extensions-click-fraud-risk/

- According to a report from ICEBRG, four Google Chrome extensions have been identified as malicious and targeting more than half a million Chrome users as well as workstations of a majority of high-profile organizations operating globally. The four extensions include: Change HTTP Request Header, Lite Bookmarks, Nyoogle, and Stickies.
- As per the report, these malicious extensions contain suspicious coding that affected over 500,000 users worldwide including corporate workstations. The extensions are used to carry out "click fraud" and "search engine optimization (SEO) manipulation."
- Moreover, these offer a strong foothold to threat actors because they can leverage these extensions to obtain access to corporate networks and user information. These extensions were discovered while the team of researchers at ICEBRG was investigating the sudden increment in outbound network traffic between a European VPS provider and a customer's workstation.
- Researchers noted that these four extensions didn't contain an obvious coding but used a combination of two different features that allowed attackers to inject and execute arbitrary, malicious JavaScript code whenever a permission request to retrieve JSON was received by an update server from an external source. When injected the malicious script creates a WebSocket tunnel using the change-request.info and then the extension uses it to proxy browsing traffic through the browser installed on the targeted machine.
- Currently, it is not clear whether same attackers are involved or there are different threat actors behind each of the four malicious extensions but it is evident that similar TTPs (techniques, tactics, and procedures) have been used. Researchers noted that these techniques can also allow sophisticated hackers to establish a beachhead into "target networks."

4 - Espionage Behind Health Care Hack

http://www.newsinenglish.no/2018/01/18/espionage-behind-health-care-hack/

- Norway's police intelligence unit PST suspects that a "serious" hacking attack on the computer systems of the country's largest regional health care agency was carried out on behalf of a foreign state. The 08 JAN attack on Helse Sør-Øst may have put the health care files for more than 2 million Norwegians at risk.
- PST has said they don't know who's behind the attack, which was discovered by *Sykehuspartner*, the company responsible for all of the state-owned Helse Sør-Øst's computer systems. The regional public health agency for southeastern Norway covers all hospitals and health care records for around 2.8 million residents of Østfold, Akershus, Oslo, Hedmark, Oppland, Buskerud, Vestfold, Telemark and the Agder counties.
- It was on 08 JAN that Sykehuspartner registered "abnormal activity" against Helse Sør-Øst's systems all over the southeastern region. Helse Sør-Øst was informed immediately and efforts were made to halt the intrusion. The abnormal activity was described as being "quite advanced and professional."
- "There is a suspicion that someone, on behalf of a foreign state, is gathering information that, if it becomes known for such a state or can be revealed, can damage fundamental national interests regarding state infrastructure," Line Nyvoll Nygaard, prosecutor for PST, said earlier in the week. "That can include information about health care preparedness."

5 - Data Breach At Testing Vendor Questar Exposes 52 NY Students

http://www.miamiherald.com/news/business/technology/article195434494.html

- A data breach at testing vendor Questar Assessment exposed personal information of about 52 students in five New York schools, state Education Commissioner MaryEllen Elia said Thursday.
- Questar, headquartered in Apple Valley, Minnesota, reported that someone accessed a small amount of "personally identifiable" information from 30 DEC to 02 JAN, Elia said. The data included some student names, identification numbers, grade levels and teachers' names, but not student addresses, social security numbers, disability status or test scores.

- The data breach affected one other state, Questar Chief Operating Officer Brad Baumgartner told The Associated Press. He declined to identify it, saying he could not disclose client information.
- New York Attorney General Eric Schneiderman's office has opened an investigation, spokeswoman Amy Spitalnick said.

6 - 53,000 Patient Records Breached After Phishing Hack on Onco360, CareMed

http://www.healthcarefinancenews.com/news/53000-patient-records-breached-after-phishing-hack-onco360-caremed

- A hacker breached employee email accounts of Onco360 and CareMed Specialty Pharmacy, exposing the data of 53,173 patients, according to Onco360.
- Those emails contained patient demographic information, medical and clinical data, health insurance information, and Social Security numbers for some patients of Onco360 and CareMed Specialty Pharmacy.
- The breach notice appears to imply the breach occurred by employees opening phishing emails, a common method used by hackers to leverage their way into a health system's network.

7 - National Stores Inc Says Customers Notified of Data Security Incident

https://www.reuters.com/article/brief-national-stores-inc-says-customers/brief-national-stores-inc-says-customers-notified-of-data-security-incident-idUSFWN1PH16O

- National Stores, Inc. has been a victim of a malware attack, enabling unauthorized parties to access payment card information.
- National Stores, Inc. contacted FBI about possible "criminal activity".
- National Stores, Inc. says affected payment card information may have included names, payment card numbers, expiration dates, and security codes.
- National Stores, Inc. based on investigation appears payment cards used at some stores locations between July 16 and Dec 11, 2017 may be involved.

8 - MDE Says Tupelo Schools Impacted by Data Breach

http://www.djournal.com/news/mde-says-tupelo-schools-impacted-by-data-breach/article_36182beb-3f6e-57d2-809e-0c15fa17364e.html

- The Mississippi Education Department's assessment vendor, Questar Assessment, Inc., reported today that 562 students in the Tupelo Public School District were impacted by the data breach the company discovered last week.
- Questar's preliminary analysis found that an unauthorized user viewed student assessment records between Dec. 31, 2017 and Jan. 1 from Tupelo Middle School, Tupelo High School and Jefferson County Junior High School.
- The MDE does not share student addresses and social security numbers with Questar; and therefore, this information was not accessible.
- Following the discovery of a similar breach in New York, Questar has closed the accounts of all former employees and has hired a third-party audit firm to perform a security audit of its systems.
- Questar first notified the MDE about the breach on the afternoon of Jan. 18. On Jan. 19, Questar provided additional information, and on Monday, Questar provided the MDE with the names of the impacted students and schools.
- Tupelo Public School District superintendent Gearl Loden said although the breach is concerning, he is glad that no social security numbers, addresses or other potentially harmful data was accessed.

Telephones/Apps:

NA

Other:

1 - North Korea Targeted South Korean Cryptocurrency Users and Exchange in Late 2017 Campaign

https://www.recordedfuture.com/north-korea-cryptocurrency-campaign/

- Recent reporting regarding North Korean attacks against cryptocurrency exchanges and using Pyeongchang Olympics as a lure describe techniques that are unusual for the Lazarus Group. These include leveraging PowerShell, HTA, JavaScript, and Python, none of which are common in Lazarus operations over the last eight years. The campaign we discovered showcases a clear use of Lazarus TTPs to target cryptocurrency exchanges and social institutions in South Korea.
- This campaign leveraged four different lures and targeted Korean-speaking users of the Hangul Word Processor (.hwp file extension), a Korean-language word processing program utilized widely in South Korea. North Korean state-sponsored actors have used Hangul exploits (CVE-2015-6585) and malicious .hwp files in the past, including during a phishing campaign in early 2017, to target South Korean users.
- Beyond Korean-speaking HWP users, targets of this campaign appear to be users of the Coinlink cryptocurrency exchange, South Korean cryptocurrency exchanges at large (or at least those that are hiring), and a group called "Friends of MOFA" (Ministry of Foreign Affairs), which is a group of college students from around South Korea with "a keen interest in foreign affairs."
- This campaign relies on a known Ghostscript exploit (CVE-2017-8291) that can be triggered from within an embedded PostScript in a Hangul Word Processor document.
- The attack chain occurs in multiple stages with the PostScript deobfuscating a first stage shellcode that's been XORed with a hardcoded four-byte key. The shellcode in turn triggers the GhostScript vulnerability in order to execute an embedded DLL that has also been XORed. A PwnCode.Club blogpost details the deobfuscation of the shellcode and loading of the DLL into memory.

2 - $400,000 Stolen in Lumens BlackWallet Theft

http://www.zdnet.com/article/400000-stolen-in-lumens-blackwallet-theft/#ftag=RSSbaffb68

- Unknown threat actors have compromised the BlackWallet application and stolen $400,000 in user funds.
- The Stellar Lumen (XLM) cryptocurrency was the target of the attack and by redirecting the DNS server to a server controlled by the attacker, close to 670,000 Lumens was stolen.
- When the theft took place, over $400,000 was contained in the attacker's wallet. At the time of writing, roughly $48,000 in funds has been left following a number of transfers taking place over the past two days.
- The exploit used was a code injection. If over 20 Lumens was held by users, the funds were automatically transferred over to the attackers' wallet.
- In a statement, the creator of BlackWallet said that an unknown individual had managed to access their hosting provider account, leading to the DNS changes and compromise of user funds.

3 - OnePlus Suspends Credit Card Payments After Customers Report Fraudulent Purchases

https://www.theverge.com/2018/1/16/16895858/oneplus-credit-card-details-stolen-cybersecurity-fraud

- OnePlus has temporarily shut down credit card payments on its website following reports that customers' payment details were stolen after they bought goods through its online store. The company says it's disabling credit card payments "as a precaution," but will still be accepting purchases through PayPal. OnePlus also says it's looking for "alternative secure payment" options.

- The investigation began after a poll posted by users on OnePlus' forums found that many customers had experienced the same problem. In the poll, 174 respondents said they had discovered fraudulent transactions on their cards after making a purchase from OnePlus. One customer who bought a OnePlus 5T wrote that he was alerted by the bank as someone tried to make an unauthorized purchase at Walmart worth $790.
- In its response, OnePlus outlines various protocols the company uses to safeguard users' payment information, including sharing data over encrypted connections. However, an analysis of the site's payment processing by security firm Fidus suggests there is a brief window "in which malicious code is able to siphon credit card details before the data is encrypted."
- OnePlus says the site is undergoing a complete audit in order to look for such potential faults. The smartphone maker says customers who are affected by fraud should contact their bank immediately to initiate a chargeback.

Thanks,

Darrell Reiff
FBI Miami Division
Intelligence Branch
South Florida JTTF
Southeast Florida RDSTF
Southeast Florida Fusion Center
754-703-2688 (desk)
305-218-3064 (cell)
dreiff@fbi.gov (New)

-

-