NJCCIC
NJ CYBERSECURITY & COMMUNICATIONS INTEGRATION CELL

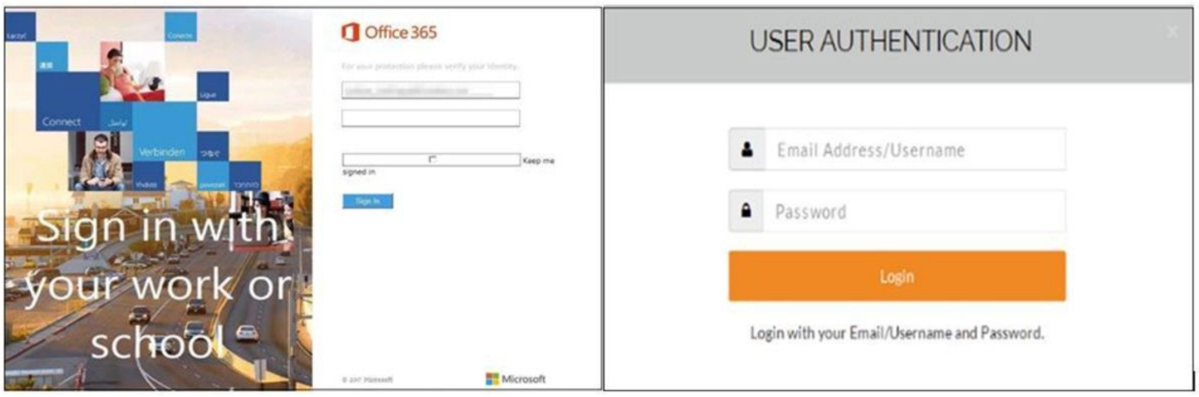
THE WEEKLY BULLETIN | December 14, 2017

Garden State Cyber Threat Highlights

Providing our members with a weekly insight into the threats and malicious activity directly targeting New Jersey networks.

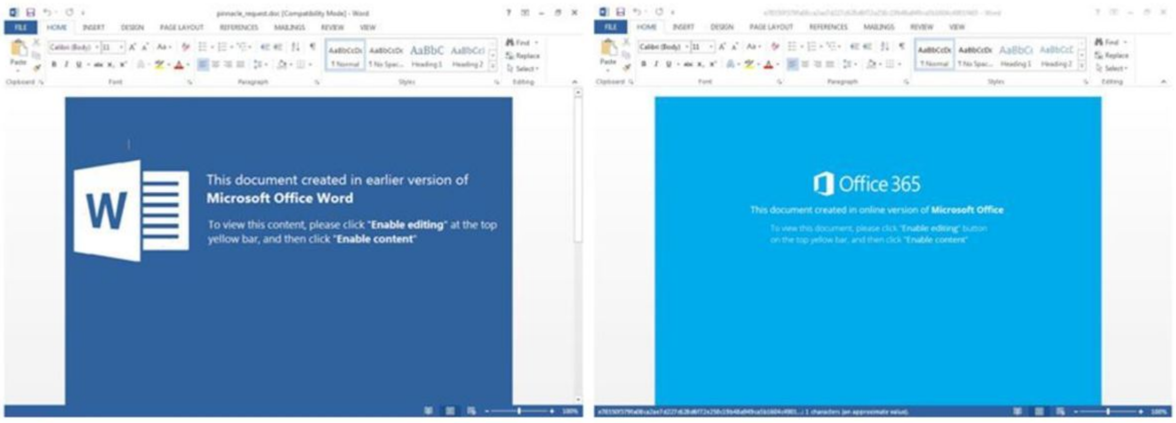
Phishing Campaign Targets Office 365 Account Credentials

The NJCCIC has been alerted to a phishing campaign attempting to steal Office 365 account credentials. Emails related to this attack may display subject lines including “Account Notification” or “Patch Alert” and contain a URL link or HTML attachment that redirects users to a fraudulent Office 365 login page. Once account credentials are entered into the phishing website, victims are redirected to an authentic Office 365 website with a message indicating that the initial login attempt was unsuccessful. ***The NJCCIC strongly recommends never using links provided in unsolicited emails to visit websites requiring the input of account credentials, particularly those for sensitive accounts such as corporate and personal email and online banking. Instead, visit the account’s associated website by typing the legitimate address directly into the URL field of your web browser.***



Ursnif Banking Trojan Detected in Malicious Email Campaign

The NJCCIC has observed a malicious campaign attempting to deliver emails containing the Ursnif banking trojan to state email accounts. These emails are being distributed with malicious attachments that often include “request.doc” in the name. When the document is opened, an Office365 or Microsoft Word notice is displayed requesting the user to “Enable Content” to allow macros to run. If the user enables the malicious content, the Ursnif trojan will then download and install onto the user’s system via PowerShell. ***The NJCCIC strongly recommends educating end users about this and similar threats and reminding them never to click on links or open attachments delivered with unexpected or unsolicited emails. Additionally, if end users have received and taken action on these emails, isolate the affected systems from the network and perform a full system scan using a reputable anti-malware solution. Proactively monitor and change passwords to any financial, personal, or business accounts accessed on infected systems and enable multi-factor authentication where available.***


This document created in earlier version of **Microsoft Office Word**

To view this content, please click "**Enable editing**" at the top yellow bar, and then click "**Enable content**"

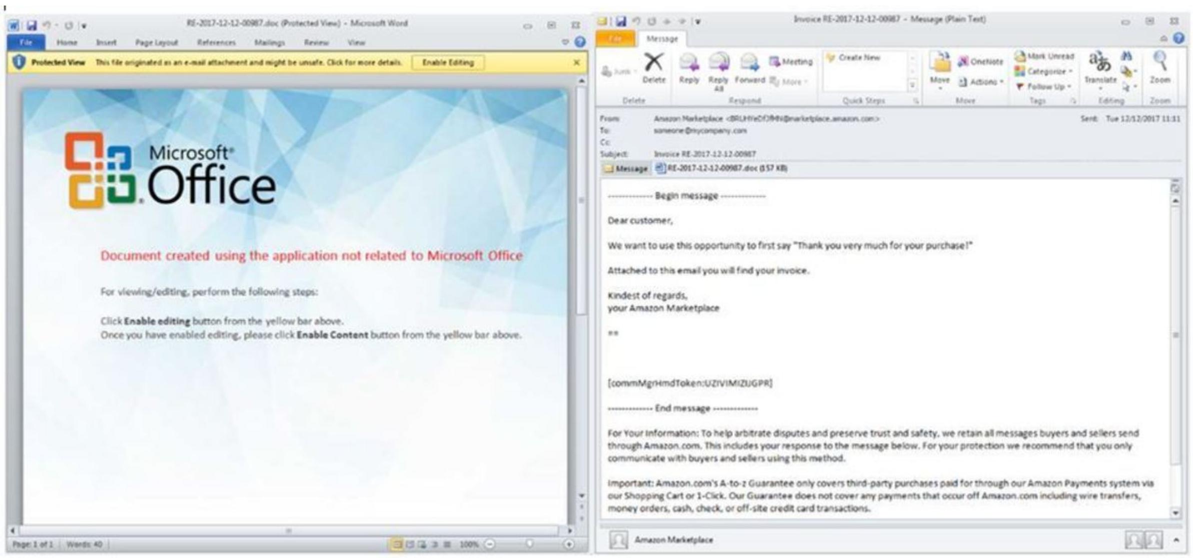
Office 365

This document created in online version of **Microsoft Office**

To view this document, please click "**Enable editing**" button on the top yellow bar, and then click "**Enable content**"

Fraudulent Amazon Invoice Email Distributes TrickBot Banking Trojan

The NJCCIC has detected a recent uptick in malicious emails attempting to deliver the TrickBot, or Trick, banking trojan to New Jersey government accounts. The emails appear to be from Amazon Marketplace and are sent from an email address comprised of random letters and *@marketplace.amazon.com*. The subject line lists "Invoice" followed by the date the email was sent and randomly generated numbers. A malicious MS Word document with a filename matching the subject line is attached. If recipients open the attached document and enable macros to run, TrickBot will install onto their system and download additional malware and modules. ***The NJCCIC strongly recommends educating end users about this and similar threats and reminding them never to click on links or open attachments delivered with unexpected or unsolicited emails. Additionally, if end users have received and taken action on these emails, isolate the affected systems from the network and perform a full system scan using a reputable anti-malware solution. Proactively monitor and change passwords to any financial, personal, or business accounts accessed on infected systems and enable multi-factor authentication where available.***



Protected View This file originated as an e-mail attachment and might be unsafe. Click for more details.

Document created using the application not related to Microsoft Office

For viewing/editing, perform the following steps:

Click **Enable editing** button from the yellow bar above.
Once you have enabled editing, please click **Enable Content** button from the yellow bar above.

From: Amazon Marketplace <BRUHYeDfJfMN@marketplace.amazon.com>
To: someone@mycompany.com
Cc:
Subject: Invoice RE-2017-12-12-00987
Sent: Tue 12/12/2017 11:11
Message RE-2017-12-12-00987.doc (157 KB)

-------------- Begin message --------------

Dear customer,

We want to use this opportunity to first say "Thank you very much for your purchase!"

Attached to this email you will find your invoice.

Kindest of regards,
your Amazon Marketplace

==

[commMgrHmdToken:UZIVIMIZUGPR]

-------------- End message --------------

For Your Information: To help arbitrate disputes and preserve trust and safety, we retain all messages buyers and sellers send through Amazon.com. This includes your response to the message below. For your protection we recommend that you only communicate with buyers and sellers using this method.

Important: Amazon.com's A-to-z Guarantee only covers third-party purchases paid for through our Amazon Payments system via our Shopping Cart or 1-Click. Our Guarantee does not cover any payments that occur off Amazon.com including wire transfers, money orders, cash, check, or off-site credit card transactions.

NJ Native Pleads Guilty to Co-Authoring Mirai Botnet

On Wednesday, former Rutgers University student and Fanwood, NJ resident Paras Jha, 21, plead guilty in Federal court in Trenton to conspiracy to violate 18 US Code § 1030(a)(5)(A) in violation of 18 US Code § 371, charges associated with his role in the creation of Mirai, a botnet comprised of hundreds of thousands of infected internet-connected devices. The Mirai botnet was used to launch several massive distributed denial-of-service (DDoS) attacks, including the October 21, 2016 DDoS attack that targeted the internet infrastructure firm Dyn, degrading internet service and causing disruption to many major websites across the US. Jha also plead guilty to computer fraud charges for repeatedly disabling Rutgers University's network beginning in 2014, timing the attacks to greatly impact the online activities of students, faculty, and staff. Additionally, Jha and his co-conspirators leveraged Mirai to generate online ad revenue through fraudulent clicks, known as click-fraud, making a total of 200 Bitcoin, valued at $180,000 in January but worth approximately $3.4 million today. Jha and his co-conspirators also rented the botnet to other hackers for additional revenue. Jha faces up to 10 years in prison and a $250,000 fine. He has agreed to forfeit 13 Bitcoin, worth over $220,000, as restitution. In January 2017, cybersecurity expert and investigative journalist Brian Krebs published a post on his KrebsOnSecurity blog detailing his investigation into the Mirai botnet authors, citing Jha and co-conspirator Josiah White as culprits. In late September 2016, just weeks before the massive Dyn DDoS attack, Kreb's site was the victim of a Mirai botnet DDoS attack. ***For additional information, please review the NJCCIC Mirai botnet threat profile and NJCCIC threat analysis product DDoS: Internet-of-Things Likely to Fuel More Disruptive Attacks*****.**

Event Announcement

2018 NJCCIC Secure NJ Cybersecurity Summit

Hosted by the New Jersey Cybersecurity & Communications Integration Cell and the Kean University Cybersecurity Center

Date: January 12, 2018
Time: 7:30 AM - 4:00 PM
Location: Kean University/STEM Building

In keeping with the mission of the NJCCIC, the purpose of the 2018 NJCCIC Secure NJ Cybersecurity Summit is to provide attendees with practical strategic and tactical information that can be used to make them more resilient to cyberattacks.

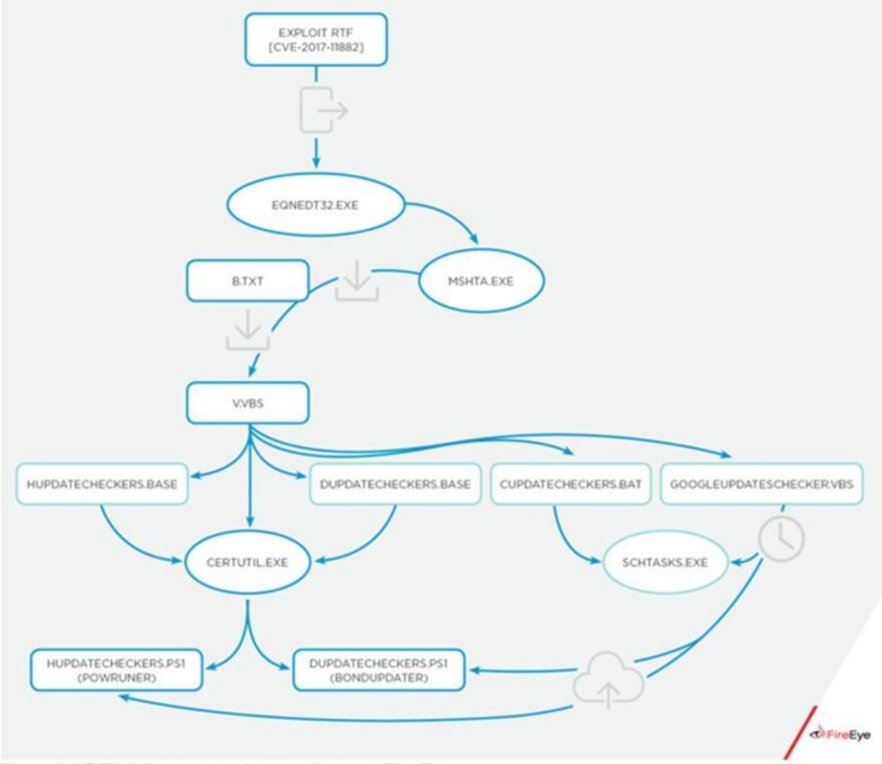
- **Audience:** Public and Private Sector Cybersecurity Professionals
- **Cost:** Free, breakfast and lunch will be provided

Please go to www.cyber.nj.gov/calendar/securenj2018 for more information on agenda, speakers, and registration. Seating is limited.

Threat Alerts

APT34 Activity Targets Critical Infrastructure

Researchers at FireEye have detailed the activity of a cyber-espionage group they dubbed "APT34" after observing a threat actor using an exploit for the Microsoft Office memory corruption vulnerability CVE-2017-11882 patched by Microsoft on November 14, 2017. Researchers believe the threat actors are Iran-based, either working directly for the Iranian government or as contractors, selling their access to various networks of interest, and loosely align with a group commonly referred to as "OilRig." APT34 works towards the interests of the Iranian government and largely focuses on reconnaissance activity targeting organizations in the financial, government, energy, chemical, and telecommunications sectors in the Middle East. APT34 uses a variety of tools and tactics, including public and non-public backdoors, and spear-phishing operations using compromised accounts to gain access to additional networks. The latest campaign leverages CVE-2017-11882 to deploy a PowerShell-based backdoor, POWRUNER, and a downloader with domain generation algorithm (DGA) functionality, BONDUPDATER. Additionally, FireEye attributes two previously reported cyber operations to APT34: A May 2015 spear-phishing campaign that used malicious attachments to distribute the POWBAT malware to banks in the Middle East; and a July 2017 incident that used malicious .rtf files exploiting the Microsoft Office/WordPad remote code execution vulnerability CVE-2017-0199 to deliver POWRUNER and BONDUPDATER to a Middle East organization. APT34 operations, along with APT33 activity, highlight Iran's added efforts and resources dedicated to increasing cyber-espionage activity and its effectiveness. The group's targeting of critical infrastructure sectors is especially concerning as access could possibly be used for future disruptive or destructive operations. ***The NJCCIC recommends critical infrastructure sector organizations review the FireEye report for additional technical details and scan their networks for malicious activity using the Indicators of Compromise (IoCs) provided to determine if malicious activity associated with APT34 was observed within their network. If detected, this activity should be given the highest priority for mitigation and reported to the NJCCIC as soon as possible.***



Recent APT34 Campaign. Image Source: FireEye

Patchwork Cyber-Espionage Campaign

Patchwork, also referred to as Dropping Elephant, is a cyber-espionage group that targets diplomatic and government agencies and private businesses. As the name suggests, the group is known for rehashing tools and malware in its campaigns. Based on Patchwork's targets and operations, the group's primary objective is to obtain sensitive and confidential data. They employ social engineering tactics, use backdoors, and exploit recently reported vulnerabilities using Dynamic Data Exchange (DDE) and Windows Script Component (SCT). The group uses spear-phishing emails and website redirects, links, and malicious attachments to gain access to the target's network. The malicious documents used vary from Rich Text Format *.rtf* files, PowerPoint Open SML Slide Show *.ppsx* files, and PowerPoint *.ppt* files and contain exploits for a variety of vulnerabilities. Additionally, the group abuses DDE to retrieve and execute the Android xRAT malware. The group also delivers the following malware: NDiskMonitor, Socksbot, Badnews, Taskhost Stealer, and Wintel Stealer. The group misuses publicly available PHP scripts to retrieve files from their server without disclosing its real path, likely to prevent researchers from finding open directories. They also temporarily remove files and replace them with legitimate files and display a fraudulent 302 redirection page on their servers' home pages to fool researchers. Patchwork has targeted organizations in China and South Asia, and they have recently targeted the UK, Turkey, and Israel with spear-phishing emails. The group targeted business-to-consumer (B2C) online retailers, telecommunications and media companies, aerospace researchers, and financial institutions. The UN Development Programme was also targeted. ***The NJCCIC recommends organizations review Trend Micro's report; educate their users on spear-phishing and other social engineering tactics; deploy proactive defenses, such as email gateways, firewalls, and endpoint protection; employ the Principle of Least Privilege on all user accounts; and always keep hardware and software updated. Symantec published a blog post detailing Patchwork activity in 2016 here.***

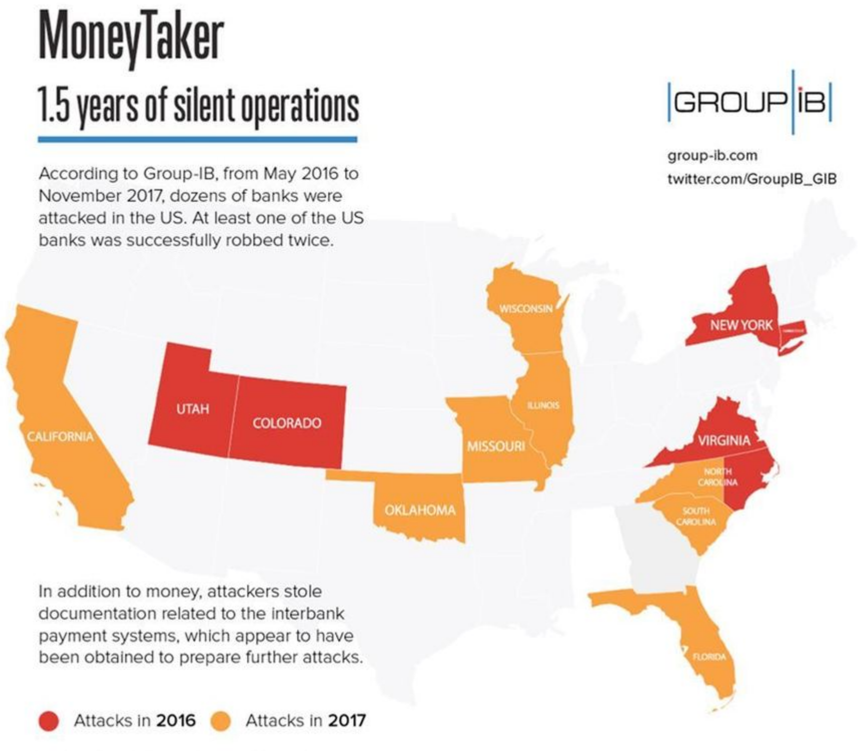
Image Source: Cymmetria

GratefulPOS: The Grinch Who Stole Your Payment Data

GratefulPOS, a new point-of-sale (PoS) malware variant, is targeting PoS systems running Microsoft Windows OS versions 7 or later. The malware exfiltrates payment card data via encoded and obfuscated DNS queries that are sent to a hard-coded domain controlled by the threat actor. This DNS exfiltration method effectively bypasses firewalls and circumvents PoS system controls designed to block the system's access to the internet. The infected PoS system sends the payment card data to an internal DNS server that then passes the data encoded in the DNS queries to the threat actor, eliminating the need for the infected PoS system to have a direct connection to the internet. ***The NJCCIC recommends all merchants using PoS systems review the RSA report and the NJCCIC profile on GratefulPOS and scan systems and networks for the associated IoCs. Merchants who have not yet upgraded to EMV chip card terminals are highly encouraged to use hardware-enabled point-to-point encryption for the storage and transmission of payment card data. On chip-enabled terminals and readers, disable the magnetic strip reader processes and components, if possible, to reduce the risk of payment data compromise.***

MoneyTaker Has Targeted at Least 16 US Organizations

MoneyTaker, a cyber-criminal hacking group likely operating out of Russia or a Russian-speaking country, has reportedly stolen over 10 million dollars after targeting at least 20 financial institutions and legal firms. Researchers at the cybersecurity firm Group-IB believe MoneyTaker operations began in 2016, first infiltrating a Florida bank in May of that year, and have since targeted 14 additional US banks, a US service provider, a UK company, three Russian banks, and a Russian law firm. The group steals funds by infiltrating inter-banking money transfer and card processing systems, such as First Data STAR Network and Russia Central Bank's AWS CBR system. MoneyTaker actors use legitimate apps and several types of malware to carry out malicious operations, including fileless malware, making investigations much more difficult. The group has targeted card processing systems and ATM networks, has used the ScanPOS malware against PoS systems, the Citadel and Kronos banking trojans for lateral movement, and custom screenshotting and keylogging tools. The threat actors delete their entry points, preventing researchers from determining the initial infection vector. MoneyTaker actors appear to initially steal internal documentation to learn about bank operations prior to initiating their cyber operations and have stolen documents on the inter-banking money transfer system, SWIFT, and the card processing system, OceanSystems' Fedlink, deployed across Latin America, indicating financial institutions in Latin America may be the groups' next target. ***The NJCCIC recommends users and administrators at financial institutions review the Group-IB report for additional information and scan their networks for malicious activity associated the MoneyTaker group using the IoCs provided.***



According to Group-IB, from May 2016 to November 2017, dozens of banks were attacked in the US. At least one of the US banks was successfully robbed twice.

In addition to money, attackers stole documentation related to the interbank payment systems, which appear to have been obtained to prepare further attacks.

● Attacks in **2016** ● Attacks in **2017**

MoneyTaker US Targets. Image Source: Group-IB

Increase in Phishing Attacks Targeting Cryptocurrency Owners

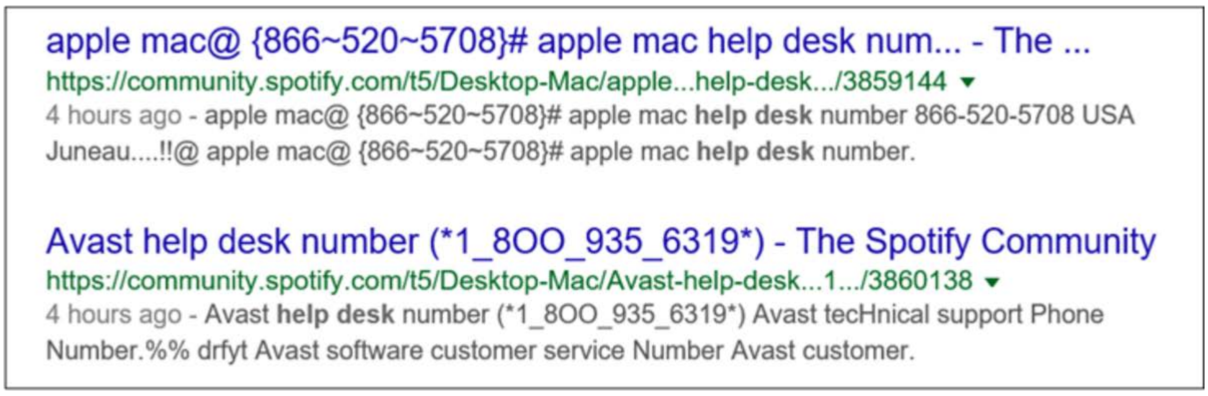
As the price of Bitcoin and other cryptocurrencies have drastically increased in recent weeks so, too, have the number of phishing campaigns targeting cryptocurrency owners. These campaigns are designed to steal login credentials for cryptocurrency apps and exchanges and trick victims into revealing their secret keys for cryptocurrency hot wallets so that the perpetrators can access the victims' digital funds. Some reported phishing campaigns contain malicious URLs masquerading as the online wallet service Blockchain and the trading site LocalBitcoins. Others were fraudulently promoting a cryptocurrency trading bot called GunBot. These types of social engineering attacks are likely to continue as the price and popularity of cryptocurrency surges. ***The NJCCIC recommends cryptocurrency owners maintain awareness of this and similar threats and avoid using links provided in emails or through social media platforms to visit websites that require the input of account credentials. Users are encouraged to visit cryptocurrency wallet and exchange sites by typing the legitimate address directly into the URL field of their web browsers and to exercise caution before downloading any cryptocurrency-related application or allowing full read/write API access to accounts from external sources. Lastly, we strongly recommend enabling multi-factor authentication on all accounts that offer it to prevent unauthorized access as a result of credential compromise.***

Malicious Email Campaign Threatens Recipients' Physical Security

This week, a Spiceworks forum user discovered an emerging email campaign in which the sender claims to have an order to kill the recipient, but offers to spare the recipient's life in exchange for a Bitcoin payment. The sender also warns recipients not to contact law enforcement and claims the kill order will be executed after two days of non-payment. Analysis of the Bitcoin wallet address included in the email reveals that, as of now, no one has paid the sender; however, email users unfamiliar with cyber extortion tactics such as this could easily fall for the scam, especially as the campaign appears to be using compromised email accounts of legitimate organizations. ***The NJCCIC recommends email users and administrators read the Sophos report, familiarize themselves with this cyber extortion scheme, and spread awareness to prevent others from potentially falling victim. Report any instances of this or other cyber extortion campaigns to your local police department, the FBI, and the NJCCIC.***

Tech Support Scammers Abusing Spotify SEO to Defraud Victims

Tech support scammers have been rapidly spamming Spotify's online forums with posts featuring phone numbers for fraudulent services abusing the site's search engine optimization (SEO) algorithm to achieve a high ranking within Google search results. These posts advertise support services for legitimate companies such as Avast, Apple, Microsoft, Turbotax, Amazon, Norton, and McAfee, among others; however, anyone who calls the posted phone numbers will be put in contact with scammers and risk compromising their personal and financial data. Although Spotify is currently trying to resolve the issue, these posts are still currently appearing within search results. ***The NJCCIC recommends users seeking support services from legitimate companies visit the companies' websites directly for contact information and avoid calling phone numbers that appear within search results.***



apple mac@ {866~520~5708}# apple mac help desk num... - The ...
https://community.spotify.com/t5/Desktop-Mac/apple...help-desk.../3859144 ▾
4 hours ago - apple mac@ {866~520~5708}# apple mac **help desk** number 866-520-5708 USA Juneau....!!@ apple mac@ {866~520~5708}# apple mac **help desk** number.

Avast help desk number (*1_8OO_935_6319*) - The Spotify Community
https://community.spotify.com/t5/Desktop-Mac/Avast-help-desk...1.../3860138 ▾
4 hours ago - Avast **help desk** number (*1_8OO_935_6319*) Avast tecHnical support Phone Number.%% drfyt Avast software customer service Number Avast customer.

AiTURE Fidget Spinner App Sends Device Data to Chinese Server

The AiTURE fidget spinner app developed by Chinese firm Shenshen Heaton Technology Co. Ltd. and available in the Google Play Store for devices running Android OS was reportedly observed collecting user device data and sending it in plaintext to a server in China without the user's consent or knowledge. This app is designed to pair a user's mobile device with the associated AiTURE Bluetooth-enabled fidget spinner and allow the user to control certain functions of the popular toy using the app's interface. However, a researcher observed that the app was transmitting a large amount of data to a server in China that included information about other apps installed on the device. Although the intent behind this data collection is currently unknown, this incident highlights the risks posed by downloading software and applications developed in countries outside the US and the increasing risks that Android users face when downloading apps from the Google Play Store. ***The NJCCIC recommends AiTURE app users immediately delete the app from their devices. We also recommend mobile device users exercise caution when downloading any application, paying special attention to permissions the app requests, and consider avoiding apps developed within countries that are known to conduct cyber-espionage against US targets.***

Vulnerability Alerts

Palo Alto Networks Firewalls Vulnerable to Remote Code Execution

A vulnerability in Palo Alto Networks firewall products running PAN-OS could allow a threat actor to remotely execute code with root privileges. The vulnerability, dubbed CVE-2017-15944, affects PAN-OS 6.1.18 and earlier, PAN-OS 7.0.18 and earlier, PAN-OS 7.1.13 and earlier, PAN-OS 8.0.5 and earlier. Networks are vulnerable to attack only if their web management interface is left exposed to the internet. A search on Shodan returned results indicating 46 Palo Alto firewalls in New Jersey are vulnerable. Palo Alto has released updates for this vulnerability, as well as fixes for four other flaws [1, 2, 3, 4]. ***The NJCCIC recommends users and administrators of Palo Alto firewall products apply the most recent updates as soon as possible. We also recommend limiting the access of Palo Alto firewall's web management interface to the local area network (LAN) only.***

ROBOT Attack Can Be Used to Decrypt HTTPS Traffic

A variation of the 19-year-old cryptographic Bleichenbacher attack can be exploited to obtain the private encryption key allowing threat actors to decrypt sensitive HTTPS traffic. In response to the original Bleichenbacher attack, instead of replacing the insecure RSA algorithm, designers of the TLS standard added countermeasures, detailed in Section 7.4.7.1 of RFC 5246, to increase the difficulty in conducting brute-force attacks. The countermeasures fail to sufficiently mitigate the attack and several variations of the Bleichenbacher attack have been published over the last 14 years, including the DROWN attack from May 2016. This new attack, dubbed ROBOT for "Return of Bleichenbacher's Oracle Threat," exploits server equipment that does not have the countermeasures properly implemented. According to the researchers, 27 out of the Alexa Top 100 websites are vulnerable to the ROBOT attack and several vendors, such as Cisco, Citrix, and Oracle, have products that are vulnerable to ROBOT attacks when the server owner encrypts the TLS session key with the RSA algorithm and uses the PKCS #1 version 1.5 padding system. The ROBOT attack could allow a remote, unauthenticated threat actor to obtain the TLS session key and decrypt HTTPS traffic. ***The NJCCIC recommends users and administrators of the affected products review the CERT/CC Vulnerability Note, ROBOT attack paper, and visit the ROBOT attack site for additional information and a full list of vulnerable products; use the Python script to scan for vulnerable hosts and the ROBOT vulnerability checker to test public HTTPS servers; disable TLS session key RSA encryption on affected devices; and apply updates to affected products as soon as they are available.***

TeamViewer

A vulnerability is present in the Windows OS, macOS, and Linux OS versions of TeamViewer, a type of remote access and presentation software. If exploited on the presenter's side, this vulnerability could allow an attacker to gain full unauthorized control of the viewer's system. If exploited on the viewer's side, it could allow an attacker to gain full unauthorized control of the presenter's system, despite the presenter's permissions settings. A patch for this vulnerability will be delivered automatically to users who have configured their instances of TeamViewer to accept automatic updates. Users who have not configured TeamViewer to accept automatic updates will be notified when the patch is available. ***The NJCCIC recommends all TeamViewer users and administrators apply the patch as soon as possible.***

Breach Notification

EcommerceBytes discovered that eBay customers' first and last names, the items those customers have purchased, and their product reviews were made publicly available on Google and Google Shopping. The leak of customer data occurred due to a flaw in the feed eBay provides to Google. After EcommerceBytes alerted eBay and Google of the privacy breach, Google masked the real names of eBay customers and all other users in the Product Reviews section of Google Shopping while eBay is reportedly working to resolve the security issue. ***The NJCCIC recommends eBay users remain vigilant as the personal information leaked may be used by threat actors to craft clever and convincing spear-phishing emails designed to trick users into divulging their account credentials or other sensitive information. The NJCCIC reminds users to never click links provided in unsolicited emails to visit websites requiring the input of account credentials and, instead, visit the account's associated website by typing the legitimate address directly into the URL field of the web browser.***

In last week's bulletin we reported that a PayPal company, TIO Networks, suffered a security breach. TIO Networks has notified PSE&G that the information of approximately 2.5 million customers may have been exposed as a result of the breach. PSE&G customers who made payments using automated kiosks in PSE&G's customer service centers between 2012 and 2017 may have had their bank account numbers and addresses compromised. ***The NJCCIC recommends customers of PSE&G that made payments using PSE&G's automated kiosks enroll in any free credit monitoring programs offered and review the TIO Networks website for additional information.***

Threat Profiles

Android Threat Profile: No **new** or **updated** variants were added.
Botnet Threat Profile: No **new** or **updated** variants were added.
Exploit Kit Threat Profile: No **new** or **updated** variants were added.
Industrial Control Systems Threat Profile: No **new** or **updated** variants were added.
iOS Threat Profile: No **new** or **updated** variants were added.
macOS Threat Profile: No **new** or **updated** variants were added.
Point-of-Sale Threat Profile: One **new** variant: GratefulPOS. No **updated** variants were added.
Ransomware Threat Profile: Two **new** variants: HC7, Tyrant. Three **updated** variants: CryptFile2, CrySiS, GlobeImposter.
Trojan Threat Profile: One **new** variant: UBoatRAT. One **updated** Ramnit variant.

ICS-CERT Advisories

PHOENIX CONTACT FL COMSERVER, FL COM SERVER, and PSI-MODEM/ETH
Rockwell Automation FactoryTalk Alarms and Events
Xiongmai Technology IP Cameras and DVRs
WAGO PFC200
Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump Vulnerabilities (Update A)

Throwback Thursday

Threat Analysis:

Remote Access: Open Ports Create Targets of Opportunity, Undue Risk (August 17, 2017)
Ransomware: Poised to Cause More Disturbance, Losses in 2017 (March 9, 2017)

Blog:

Time is of the Essence (March 30, 2017)
Hackers Are Circumventing 2FA and Here's What You Can Do About It (August 23, 2017)

Patch Alerts

Apache | Apple: AirPort Base Station | Apple: iOS and tvOS | Cisco WebEx | Fortinet FortiClient | HP Laptops | Microsoft | Mozilla Firefox | Palo Alto Networks PAN-OS | SUSE Linux Enterprise 12 SP2

Social Engineering Awareness

Phishers Are Upping Their Game. So Should You.

Comment: Although it is important to ensure the green padlock and HTTPS are displayed in the URL field of your web browser, the presence of these indicators alone does not guarantee your connection is safe. Threat actors are increasingly utilizing HTTPS domains to host phishing campaigns in an attempt to gain the trust of unsuspecting victims by appearing as legitimate websites. Be especially wary of messages that create a sense of urgency or panic and never open attachments or click on links contained within unsolicited emails.

Ridgewood Police Warn Residents About High School Phone Scam

Comment: Although this time of year may make you feel especially charitable, beware of scammers attempting to take advantage of your giving nature. If you receive an unsolicited phone call from someone identifying themselves as a representative of a charity or non-profit organization, ask the caller for a phone number so that you can donate at a later time. If the caller refuses to share the number or tries to pressure you into making a donation immediately, hang up the phone, as it is likely a scam. Before sharing payment information either online or over the phone, thoroughly research the organization. More information about how to verify the legitimacy of a charity is available on the FTC’s Charity Giving website.

Glen Rock Woman Avoids Being Victim of 'Grandparents Scam'

Comment: This article is a great example of just how effective education and awareness can be in preventing people from becoming victims of social engineering schemes. “Grandparent scams,” in particular, target senior citizens and attempt to extort money from them by eliciting a feeling of fear or urgency. Help keep friends and loved ones from falling victim to this and other scams by spreading awareness and encourage them to report incidents to their local police departments.

Cyber At a Glance

12 Threats of Christmas

Comment: As we prepare to begin a new year, now is the perfect time to reflect on the vulnerabilities, threats, and lessons learned throughout 2017. Ransomware remains a top concern, as are attacks stemming from unpatched, disclosed vulnerabilities. It is essential that organizations continue to educate employees on common social engineering and phishing campaigns and improve cyber hygiene practices to prepare for, and defend against, next year’s emerging threats.

Cybersecurity Incidents Hit 83% of US Physicians: Survey

Comment: A concerning percentage of healthcare facilities have experienced at least one cybersecurity incident. From malicious phishing campaigns designed to steal account credentials to crippling ransomware attacks that disrupt operations, the number of cyber threats that could potentially impact the healthcare sector are on the rise. Medical providers and organizations of all types are advised to allocate the proper amount of resources needed to identify, evaluate, and mitigate cyber risk in a timely and effective manner, as well as provide adequate cybersecurity education to staff.

Questions?

Email a Cyber Liaison Officer at
njccic@cyber.nj.gov.

Connect with us!

The Weekly Bulletin aggregates information about cyber threats, vulnerabilities, and other resources to promote shared awareness and the adoption of best practices. Designed for a general audience, the Bulletin aims to bridge the information sharing gaps between all levels of government, the private sector, and our citizens.