THE BEACON

Florida Fusion Center #22-111 December 2022 Issue #28

Table of Contents

2 EDITOR'S CORNER
2 Happy 20th Anniversary to Secure Florida

3 CYBER THREATS
3 A Nation-State Actor Profile: Iran
5 Network Traffic Jams: Protect Your Organization from RDDoS Attacks
7 Don't Let Fake Retail Prevail! Avoid Online Shopping Scams
9 Don't Let Cybercriminals Tie Up Your Lines: VoIP Attacks

11 CYBER HIGHLIGHTS
11 Don't Be Left to Your Own Devices: Secure Your IoT at Home
13 Divided, Not Conquered: A Look at Network Segmentation

15 DISPATCH HIGHLIGHTS

17 WHAT IS TLP?

CONTACT THE FIPC:
Phone: (850) 410-7645
Email: FIPC@fdle.state.fl.us

EDITOR'S CORNER

Happy 20th Anniversary to Secure Florida!

It may be hard to believe, but the Florida Department of Law Enforcement's Secure Florida initiative is twenty years old and still going strong! The Florida Infrastructure Protection Center (FIPC) was created in 2001, and was designed to anticipate, prevent, react to and recover from acts of terrorism, sabotage, cybercrime and natural disasters. In 2002, Secure Florida was created to serve as the cyber education and awareness component of the FIPC. Secure Florida's mission is to provide resources to and educate local organizations, businesses and private citizens throughout Florida on how to protect their computers and information systems from cyber threats.

In its twenty years of existence, Secure Florida has provided over 200 presentations and trained more than 13,000 people from local government agencies, school districts, businesses and non-profit organizations, among others.

In its twenty years of existence, Secure Florida has provided over 200 presentations and trained more than 13,000 people from local government agencies, school districts, businesses and non-profit organizations, among others. Trainings consisted of multiple relevant topics such as online workplace safety, family online safety, online scams and fraud trends, as well as customized topics requested by organizations. Secure Florida has also disseminated over 1,000 FIPC Dispatches, which are our bi-weekly cyber news bulletins, and 26 editions of The Beacon, which is our quarterly cyber trends publication. We are so thankful to our subscribers, our community partners and organizations throughout the state for supporting this initiative!

Cyber threats continue to evolve as time goes on, which means Secure Florida continues to evolve as well. We not only continue to provide our free presentations and written products, but we also have cybersecurity safety videos for the public to view! You can find them on our Secure Florida website. Whether it's providing a presentation on avoiding online scams, or one on how to secure your mobile devices, the Secure Florida team looks forward to continuing to educate communities throughout Florida on best practices and ever-changing cyber threats. Here's to continuing to keep our cyber environments safe and another twenty years for Secure Florida!

CYBER THREATS

A Nation-State Actor Profile: Iran

Cyber threat actors have multiple motivations, including supporting a nation-state government's objectives. One such nation-state that supports malicious cyber operations is Iran.

Cyber threat actors have multiple motivations, including supporting a nation-state government's objectives. One such nation-state that supports malicious cyber operations is Iran. The Iranian Government's Islamic Revolutionary Guard Corps (IRGC) is one of the more well-known cyber threat actors backed by the Iranian government. The IRGC and other Iranian cyber threat actors have used various tactics, techniques and procedures (TTPs) such as website defacement, spear phishing, distributed denial-of-service attacks and personal identification information (PII) theft. They have carried out cyberattacks against a number of victims, including the United States, and they have continuously improved their cyber capabilities.[1] Some of the more advanced TTPs that Iranian threat actors have used include exploiting software vulnerabilities in widely used programs created by Fortinet, VMWare and Microsoft Exchange.[2] Iran is likely motivated to carry out these attacks due to U.S. sanctions and U.S. presence in Iraq and other Middle Eastern countries.[3]

In September 2022, three Iranian nationals were charged with conducting a scheme used to gain unauthorized access to computer systems of hundreds of victims in multiple countries around the world, including the United States. Those impacted by this hacking campaign consist of a wide array of organizations including small businesses, government agencies, educational facilities, healthcare centers and utility providers, among others. The perpetrators exploited known software vulnerabilities in commonly used network devices and software to gain access to the networks. They also stole data and information from the victims' computer systems and attempted to extort the victims for ransom payments.[4]

In November 2021, two Iranian nationals were charged for participating in a cyber campaign focused on intimidating and influencing American voters as it relates to the 2020 U.S. presidential election. The campaign was coordinated to undermine faith and confidence in the election. Additionally, approximately 11 state voter information and registration

It is important for organizations to be aware of the many malicious threat groups and TTPs associated with Iran.

websites were targeted with cyberattacks. This resulted in one state's computer system being exploited and the downloading of information for about 100,000 of the state's voters. The conspirators subsequently used the stolen information to send threatening emails that impersonated the Proud Boys. The emails were sent to registered Democrats and threatened to cause physical injury if they did not change their party affiliation and vote for President Trump.[5]

Iran's cyber capabilities continue to evolve. They have carried out attacks against many countries, not just the U.S., and have targeted private, public and government entities. It is important for organizations to be aware of the many malicious cyber groups and different TTPs they use. There are multiple steps organizations and users can take to mitigate Iranian cyber threats including pathing and updating systems, implementing backup and restoration policies and procedures, implementing multifactor authentication, using strong passwords for logging in and using antivirus programs for all users.[6]

[1] https://www.cisa.gov/uscert/iran
[2] https://media.defense.gov/2022/Sep/14/2003076379/-1/-1/0/CSA_IRGC.PDF
[3] https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf
[4] https://www.justice.gov/opa/pr/three-iranian-nationals-charged-engaging-computer-intrusions-and-ransomware-style-extortion
[5] https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-enabled-disinformation-and-threat-campaign-designed#:~:text=An%20indictment%20was%20unsealed%20in,the%202020%20U.S.%20presidential%20election.
[6] https://media.defense.gov/2022/Sep/14/2003076379/-1/-1/0/CSA_IRGC.PDF

Network Traffic Jams: Protect Your Organization from RDDoS Attacks

A distributed denial of service (DDoS) attack is a large-scale cyberattack used by criminal actors to flood a server of an organization with internet traffic and fake requests to overwhelm online services or websites rendering them inaccessible for users. In order to initiate an attack, criminal actors utilize a large network of computers and devices that are infected by malware and fall under their control. This network of compromised devices is known as a botnet.[1]

In recent years, there has been an increase in ransom DDoS (RDDoS) attacks.[2] This involves the use of DDoS along with extorting an organization for a ransom payment in exchange for not attacking the organization or stopping an ongoing attack. Typically, the criminal actors will request payment in virtual currency.[3] It is important to note that this is not the same as a ransomware attack, which involves the use of malware that encrypts or locks up files on a device, rendering those files unusable, as well as a demand for a ransom payment.[4]

In recent years, there has been an increase in ransom DDoS (RDDoS) attacks. This involves the use of DDoS along with extorting an organization for a ransom payment in exchange for not attacking the organization or stopping an ongoing attack.

A RDDoS attack can have damaging effects on an organization. In November 2021, it was reported that a global communications software company based in North Carolina, known to provide Voice over Internet Protocol (VoIP) services, was hit with a multi-day RDDoS attack along with many other VoIP service providers around the world in September 2021.[5][6] This attack led to many of the North Carolina-based company's customers to experience service outages and disruptions to their phone systems. While the company reportedly did not pay a ransom, the company reportedly expected to lose between $9 and $12 million in revenue during the fourth quarter of 2021, which is a high amount of financial damage. Additionally, some critical infrastructure entities in foreign countries were impacted by the campaign, including law enforcement agencies and healthcare organizations.[7]

Indicators of a RDDoS attack may be hard to identify as they may resemble issues users encounter on a regular basis. Warning signs of a DDoS attack may include:

- Delayed access to files
- Inability to access a particular website or any websites
- Internet connection issues
- Inordinate amount of spam emails[8]

Organizations should secure their networks using firewalls, antivirus software, employee cybersecurity awareness training and other methods.

Organizations should secure their networks using firewalls, antivirus software, employee cybersecurity awareness training and other methods. Here are a few more tips to help protect your organization against a RDDoS attack:

- **Determine your organization's normal internet traffic pattern –** This will provide a baseline and make it easier to identify possible abnormal internet activity.
- **Develop a DDoS response plan –** In the event of an attack, having procedures in place, developing a communication plan and designating a response team can help ensure a quick and efficient response occurs.
- **Consider increasing your network's bandwidth –** This may not necessarily stop a RDDoS attack, however, it could help lessen the effects of the attack.[9] [10]

If hit with a RDDoS attack, organizations should check with their internet service provider to see if there is any possible assistance they can offer, such as changing your IP address[a] or offering a DDoS mitigation service.[11] It is not recommended to pay the ransom if your organization is hit with a RDDoS attack. Following the tips described above can help organizations identify and prepare for potential RDDoS attacks and lessen the impacts to organizations' services and operations.

[a] An IP address is similar to the address of a house. It consists of a string of numbers assigned to an internet-connected device.

[1] https://www.fortinet.com/resources/cyberglossary/ddos-attack#:~:text=DDoS%20Attack%20means%20%22Distributed%20Denial,connected%20online%20services%20and%20sites.
[2] https://www.zdnet.com/article/ddos-attacks-that-come-combined-with-extortion-demands-are-on-the-rise/
[3] https://www.cloudflare.com/learning/ddos/ransom-ddos-attack/
[4] https://www.cisa.gov/stopransomware
[5] https://therecord.media/bandwidth-com-expects-to-lose-up-to-12m-following-ddos-extortion-attempt/
[6] https://investors.bandwidth.com/news-releases/news-release-details/bandwidth-issues-statement-recent-ddos-attack
[7] https://therecord.media/industry-group-warns-of-coordinated-ddos-extortion-campaign-against-voip-providers/
[8] https://us.norton.com/internetsecurity-emerging-threats-ddos-attacks.html
[9] https://www.fortinet.com/resources/cyberglossary/ddos-protection
[10] https://securityscorecard.com/blog/best-practices-to-prevent-ddos-attacks
[11] https://www.zdnet.com/article/what-is-a-ddos-attack-everything-you-need-to-know-about-ddos-attacks-and-how-to-protect-against-them/

Don't Let Fake Retail Prevail! Avoid Online Shopping Scams

In today's day and age, online shopping seems to be the norm for most people, especially during the holiday season. Unfortunately, online shopping can lead to scams that leave consumers without their purchased products and/or their money.

In today's day and age, online shopping seems to be the norm for most people, especially during the holiday season. According to a U.S. Census Bureau report, consumers spent approximately $100 billion in retail e-commerce sales in the first quarter of 2017.[1] In the first quarter of 2022, these sales totaled about $250 billion, which is a 150 percent increase.[2] Unfortunately, online shopping can lead to scams that leave consumers without their purchased products and/or their money.[3] In 2021, there were 43,000 complaints referencing online shopping scams that started on social media reported to the Federal Trade Commission (FTC) . This is much higher when compared to 24,000 similar complaints reported in 2020, and 7,000 in 2019.[4]

Some of the most common online shopping scams include:

- **Social media shopping scams:** Scammers will pose as a seller on popular websites such as Etsy or Facebook Marketplace. Once you inquire about an item, which is likely fake or a knockoff, they will ask you for your personal and financial information as well as send you fake invoices or receipts.
- **Fake online retail stores:** Scammers will either send an email or text message or use an online ad that will lead you to a fake website that looks legitimate. From there, scammers will take your payment and never send your product and the website may disappear shortly after your purchase.
- **Fake package delivery scams:** Scammers send an email or text message indicating there is an issue with a package. You are asked to pay for shipping and handling of a product you purchased, however your product never arrives.

There are many ways to protect yourself from these scams. Here are a few suggestions that can help you avoid becoming a victim.

1. **Be cautious of extremely large discounts:** It is possible that the discount or deal you see is too good to be true.
2. **Research the company:** Use a search engine and search for an unfamiliar company's name along with words like "review," "scam" or "complaint" to see what other users have posted online. If the reviews sound generic or unnatural, these sites may be fraudulent.
3. **Look closely at the company's URL[b]:** The domain may

While it's exciting to take advantage of great deals and discounts on items you covet, it's important to be aware of potential online shopping scams to ensure you protect yourself from being victimized and losing your money.

be very close to the original business but be aware of misspellings (e.g. secureflorida.org vs. securefiorida.org). Also look for "https" and a closed padlock symbol in the address bar. This likely means payments can be made securely.

4. **Use a credit card instead of debit card:** Credit cards can offer greater fraud protection and are not tied to your checking account.

5. **Confirm there are delivery, exchange, refund and return policies:** Verify the online store has a delivery, exchange, refund and return policy that is fair. Additionally, these stores should have a detailed complaint or dispute handling process in case something is wrong with the order.[7][8][9]

Criminal actors continue to increasingly use online shopping scams. While it's exciting to take advantage of great deals and discounts on items you covet, it's important to be aware of potential online shopping scams to ensure you protect yourself from being victimized and losing your money. Don't fall for online shopping scams! For more information on protecting yourself while shopping online, visit Secure Florida's website.

[a] E-commerce or electronic commerce refers to the buying and selling of goods or services using the internet.
[b] URL stands for Uniform Resource Locator, but essentially refers to a web address.

[1] https://www2.census.gov/retail/releases/historical/ecomm/17q1.pdf
[2] https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf
[3] https://cyberflorida.org/safe/
[4] https://www.forbes.com/advisor/personal-finance/online-shopping-scams/
[5] https://fightcybercrime.org/scams/financial/online-shopping-scams/
[6] https://cyberflorida.org/safe/
[7] https://www.verifythis.com/article/news/verify/scams-verify/5-tips-avoid-onling-shopping-scams/536-20db68f1-7d96-42d5-b4e6-83b0c5bfa5a6
[8] https://www.forbes.com/advisor/personal-finance/online-shopping-scams/
[9] https://www.fdacs.gov/Consumer-Resources/Scams-and-Fraud/Online-Shopping-Scams#:~:text=Online%20shopping%20scams%20involve%20scammers,to%20rip%20off%20unsuspecting%20shoppers

Don't Let Cybercriminals Tie Up Your Lines: VoIP Attacks

Do you know how the desktop phone in your office works? Many organizations use a technology known as Voice Over Internet Protocol or VoIP, which allows their employees to make phone calls using a broadband internet connection rather than regular phone lines. Organizations are constantly working to protect their networks from cyber threats and this includes their VoIP systems.[1] [2] It's not every day that you hear about cyberattacks on a VoIP system, but they can happen. VoIP attacks happen when hackers infiltrate your business phone system. These hackers can cause different forms of damage once they have access to the system. They can listen to phone calls or steal sensitive information belonging to the company and its customers. Criminal actors may also take over compromised employee accounts and use them to impersonate the business they have hacked.[3]

There have been some notable cyberattacks on VoIP systems in recent years as a result of threat actors targeting critical VoIP software or hardware vulnerabilities.

There are multiple methods threat actors use to attack VoIP systems, including Distributed Denial of Service (DDoS) attacks[a], malware[b] and vishing[c].[4] There have been some notable cyberattacks on VoIP systems in recent years as a result of threat actors targeting critical VoIP software or hardware vulnerabilities. In November 2020, it was reported that threat actors conducted a nearly year-long campaign that compromised VoIP systems at over 1,000 companies around the world. The campaign was designed to allow the threat actors to make money by selling access to the compromised accounts, which could allow other criminals to either conduct their own cyberattacks or listen in on the organizations' calls.[5]

There are multiple steps organizations can take to protect themselves from VoIP attacks, including the following:

1. Conduct user awareness training on social engineering schemes on a regular basis.
2. Consider using virtual private networks (VPNs)[d] or end-to-end encryption[e] to secure your conversations.
3. Implement a secure firewall on your VoIP system.
4. Try to restrict the attack area by limiting the number of requests a server can receive.
5. Patch and update your software on any device that uses the VoIP system.[6] [7] [8]

Threat actors continue to evolve and find ways to target organizations' VoIP systems to compromise networks, disrupt

VoIP attacks can be dangerous.

operations and steal data or financial information. Organizations that use VoIP systems must ensure that protecting their VoIP infrastructure is a priority and ensure their employees are trained to detect any potential threats.

[a] Distributed denial of service (DDoS) attacks happen when threat actors flood an organization's network with an overwhelming amount of data or connection requests that the network cannot handle, making its servers inoperable.
[b] Malware refers to malicious software developed by cybercriminals to steal data and damage or destroy computers or computer systems.
[c] Vishing or voice phishing involves spoofing a phone number to make it appear to come from a legitimate phone number or source, with the intent of getting individuals to share sensitive information such as passwords or important financial information.
[d] A VPN provides a protected network connection for remote connections to the extent that even an internet service provider is unable to see what websites are visited or what data is sent.
[e] Encryption is a method that involves scrambling data so that only authorized parties can understand the information. Essentially, it involves taking readable data and altering it so that it appears in random form.

1 https://www.fcc.gov/general/voice-over-internet-protocol-voip
2 https://www.nextiva.com/blog/voip-advantages-and-disadvantages.html
3 https://www.nextiva.com/blog/voip-hacking.html
4 https://getvoip.com/blog/2020/05/06/voip-security/
5 https://www.zdnet.com/article/hackers-are-exploiting-unpatched-voip-flaws-to-compromise-business-accounts/
6 https://www.getsafeonline.org/business/blog-item/how-to-protect-your-voip-phone-system/
7 https://thecyphere.com/blog/voip-security/
8 https://www.linkedin.com/pulse/protecting-your-voip-infrastructure-from-ddos-attacks-brahmbhatt?trk=pulse-article_more-articles_related-content-card

CYBER HIGHLIGHTS

Don't Be Left to Your Own Devices: Secure Your IoT at Home

Like other technology connected to the internet, Internet of Things devices have vulnerabilities that can be exploited whether it's through the software, user accounts or other methods.

Internet of Things (IoT) devices are internet connected devices which are often labeled or marketed as smart devices. These devices can be controlled using smartphone apps and include televisions, refrigerators, doorbells, thermostats, security cameras and more. While meant to help make life and home management easier, these devices can become targets for cybercriminals. Like other technology connected to the internet, these devices have vulnerabilities that can be exploited whether it's through the software, user accounts or other methods. Cybercriminals may use known or discovered software vulnerabilities to gain access or control of a device.[1] User accounts can also pose a vulnerability if their password can be easily guessed, is obtained through other criminal means such as phishing, password guessing or if they purchase leaked user data on the dark web. Access to IoT at-home devices can give criminals access to your home and family without your knowledge. For example, a smart front door lock connected to the internet may require you to use an account when setting it up and the device will be linked to your home Wi-Fi network. If cybercriminals gain access to your account they could gain control over the lock and unlock function on your home's door which could potentially lead to your home being burglarized.[2] Cybercriminals may also try to take over your IoT devices and use them for malicious activities, such as stealing personal or financial information or for cryptojacking[a] for their personal gain.[3] [4]

There are multiple ways to keep these devices secure, which include:

- When setting up an IoT device, ensure each user name and password is unique for user accounts for each device. Reusing passwords or usernames can leave your account vulnerable if that information was already obtained by cybercriminals in a previous data breach.
- If the device application allows, set up two-factor authentication to add an extra layer of protection. When setting up your device, pay attention to the security set up

questions and whenever possible, use security features that add extra protection.

- If the device has features you don't want to use, turn off or disable them and be sure to disconnect any IoT devices you no longer use.
- Make sure your device's software or firmware is up to date and patched. This may require you to go to the manufacturer's website for instructions on how to apply updates or patches.[5]
- If your device allows, check your account or device's access log regularly to spot unrecognized IP addresses or logins.

While cybercriminals may seek to take advantage of IoT device vulnerabilities, the proper security measures can help keep your home network and devices secure.

Ensuring your router is set up securely with a strong password and using extra layers of protection such as a VPN, strong encryption or firewalls can also help protect IoT devices on your home network.[6] While cybercriminals may seek to take advantage of IoT device vulnerabilities, the proper security measures can help keep your home network and devices secure.

[a] Cryptojacking is a technique used to mine cryptocurrency by taking over a victim machine without permission and exploiting its computer power.

[1] https://www.infosys.com/insights/iot/security-iot.html
[2] https://www.trendmicro.com/vinfo/fr/security/news/internet-of-things/inside-the-smart-home-iot-device-threats-and-attack-scenarios
[3] https://www.darkreading.com/iot/as-iot-attacks-increase-experts-fear-more-serious-threats
[4] https://www.csoonline.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html
[5] https://consumer.ftc.gov/articles/securing-your-internet-connected-devices-home
[6] https://www.iotforall.com/securing-your-home-network#:~:text=That%20means%20the%20first%20step%20to%20keeping%20IoT,devices%2C%20so%20that%E2%80%99s%20a%20good%20place%20to%20start

Divided, Not Conquered: A Look at Network Segmentation

Cybercriminals are always looking for ways to hack into computer networks to steal data or commit cyberattacks. Whether it is at home or at your office, it is important to implement security measures to protect connected devices and data present on your network. One technique users or organizations can use to enhance security is network segmentation. This involves separating a physical network into different sub-networks. Once the network has been divided into smaller and more manageable parts, customized controls can be applied to each individual segment as needed.[1] For example, one segment could be for users and another could be for Internet of Things (IoT) devices such as cameras or identification card scanners.[2]

Whether it is at home or at your office, it is important to implement security measures to protect connected devices and data present on your network.

There are multiple reasons why network segmentation is useful, but the main one is that segmenting the network into separate contained parts effectively prevents a single point of compromise. Cybercriminals will attempt to move around a network once they gain access. Segmentation improves security by reducing the potential attack surface of any network, and limiting the ability of attackers to move through the entire network. If they deploy malware on any device, network segmentation would ensure that the malware infection remains confined to that device's segment and does not affect other network segments. Essentially, attackers will only be able to access the section they breached initially, which could give an organization's IT staff time to locate the intrusion and minimize its impact.[3] In addition to reducing cyberattack risk, network segmentation can also improve network performance by reducing congestion and help you protect vulnerable devices, especially those devices that may not have advanced security features or limited options for patching security weaknesses.[4]

Organizations should take the following steps to initiate the segmentation process:

1. **Determine the value of your data and assets –** This can help organizations identify data and assets that are essential to operations.
2. **Classify your assets –** This will allow you to label assets based on the type and level of sensitivity of the data they possess (i.e. public or highly restricted).[5]

Organizations can implement network segmentation using internal firewalls, access control lists and virtual local area network

Users and organizations should consider implementing this security measure to protect their networks from cyber threats and to improve network functionality.

(VLAN) settings on networking equipment. Another method organizations can utilize is creating software-defined perimeters, which allows them to group and tag certain traffic on the network, which may be less complicated than changing configurations on network equipment.[6] [7] For users at home, security settings on your home router will differ and network segmentation may be an option depending on the model you have. At the very least, most users should be able to create a guest Wi-Fi network for anyone that visits their homes. If visitors download malicious files and/or their devices are infected with malware, this can help prevent your main home network from being compromised. Check with the manufacturer or your internet service provider to see what security features are available to use for your home network router.[8] [9] Whether you are at home or work, utilizing network segmentation can help you avoid severe damage from cyberattacks including data breaches and ransomware attacks. Users and organizations should consider implementing this security measure to protect their networks from cyber threats and to improve network functionality.

[1] https://www.vmware.com/topics/glossary/content/network-segmentation.html
[2] https://www.comptia.org/blog/security-awareness-training-network-segmentation
[3] https://www.strongdm.com/blog/network-segmentation
[4] https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html
[5] https://www.checkpoint.com/cyber-hub/network-security/what-is-network-segmentation/network-segmentation-security-best-practices/
[6] https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html
[7] https://learn.microsoft.com/en-us/azure/architecture/framework/security/design-network-segmentation
[8] https://www.cnet.com/home/internet/how-to-protect-your-home-wi-fi-network-from-hackers/
[9] https://www.cnet.com/home/internet/how-to-set-up-guest-wi-fi/

DISPATCH HIGHLIGHTS

This section highlights articles from past issues of FIPC's *The Dispatch* that our analysts think are noteworthy based on trends we're seeing in Florida. *The Dispatch* is a list of open-source articles compiled for the law enforcement, cyber intelligence and information security communities that is sent out twice weekly. To sign up for the *The Dispatch*, visit SecureFlorida.org and click "**Get Connected**" at the top of the homepage or send an email to **FIPC@fdle.state.fl.us**.

CISA, NSA AND ODNI RELEASE PART ONE OF GUIDANCE ON SECURING THE SOFTWARE SUPPLY CHAIN

https://www.cisa.gov/uscert/ncas/current-activity/2022/09/02/cisa-nsa-and-odni-release-part-one-guidance-securing-software

» Multiple Federal agencies collaborated to create a joint publication focused on providing recommended practices for software developers to ensure software supply chains remain secure from cyberattacks.

Analyst Note: Cybercriminals will often target vulnerabilities in widely-used software to compromise multiple organizations' networks. It is important for organizations to patch their software as soon as security updates are available.

BLACKCAT RANSOMWARE CLAIMS ATTACK ON EUROPEAN GAS PIPELINE

https://www.bleepingcomputer.com/news/security/blackcat-ransomware-claims-attack-on-european-gas-pipeline/

» A ransomware group known as BlackCat/ALPHV claimed responsibility for an attack on a natural gas pipeline and electricity operator company in Luxembourg.

» The attack resulted in taking down the organization's customer portals, however, there was no interruption in any provided services.

Analyst Note: BlackCat/ALPHV is believed to be a rebrand of DarkSide, which was reportedly responsible for the attack on a major U.S. fuel pipeline in May 2021. Organizations should visit StopRansomware.gov for ransomware protection tips.

RUSSIAN CYBERATTACKS HIT WEBSITES FOR LAX, LAGUARDIA AND O'HARE

https://gizmodo.com/russian-hacks-lax-laguardia-ohare-atlanta-killnet-1849639249

» A pro-Russian hacktivist group known as KillNet claimed a large-scale DDoS attack on websites of several major U.S. airports, causing some sites to be inaccessible.

Analyst Note: KillNet has recently targeted critical infrastructure throughout Europe

and expanded their attacks to include U.S. entities. These attacks are likely retaliatory attacks due to the countries supporting Ukraine.

CYBERCRIMINALS USE HURRICANE IAN AS LURE FOR SCAMS, THEFT OF FEMA FUNDS

https://therecord.media/cybercriminals-use-hurricane-ian-as-lure-for-scams-theft-of-fema-funds/

- Cybersecurity researchers noticed an uptick in scammers targeting individuals impacted by Hurricane Ian as well as filing fraudulent claims for FEMA relief funds.
- Scammers have also been observed using phishing emails centered around offering contractor repair services as well as impersonating government employees.

Analyst Note: It is common for scammers to use disasters to form targeted social engineering schemes including government impersonation. Individuals should not share their personal information with unverified individuals.

STATE-SPONSORED APTS DANGLE JOB OPPS TO LURE IN SPY VICTIMS

https://www.darkreading.com/remote-workforce/state-sponsored-apts-dangle-job-opps-lure-spy-victims

- Foreign nation-state actors are using phishing emails and messages centered around fake job offers and targeting individuals in multiple critical infrastructure sectors.
- Targeted sectors include the Chemical and Defense Industrial Base sectors and the goal is to steal intellectual property, confidential information or financial assets.

Analyst Note: Threat actors often use social media and messaging apps to supplement phishing emails. Users should avoid clicking on unknown links or downloading unknown documents in suspicious emails or messages they receive.

EX-NSA EMPLOYEE CHARGED WITH VIOLATING ESPIONAGE ACT, SELLING U.S. CYBER SECRETS

https://www.cyberscoop.com/nsa-former-employee-espionage/

- A former National Security Agency (NSA) employee reportedly attempted to share classified national defense documents with a foreign operative.
- The former NSA employee reportedly had access to information related to foreign targeting of U.S. systems and information regarding cyber operations.

Analyst Note: Malicious insider threats can be current or former employees that have access to an organization's systems or data. Organizations should consider utilizing behavioral monitoring tools to identify authorized access misuses.

WHAT IS TLP?

The Traffic Light Protocol (TLP) is a set of designations used to ensure that sensitive information is shared with the correct audience. It employs four colors to indicate different degrees of sensitivity and the corresponding sharing considerations to be applied by the recipient(s).

This *Beacon* is TLP:CLEAR and is intended for wide distribution. If you would like to read past issues of the *The Beacon*, visit the Secure Florida website.

TLP:RED	For the eyes and ears of *individual* recipients only, no further disclosure. Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.
TLP:AMBER	Limited disclosure, recipients can only spread this on a need-to-know basis within their *organization* and its *clients*. Note that TLP:AMBER+STRICT restricts sharing to the organization only. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note: if the source wants to restrict sharing to the organization *only*, they must specify TLP:AMBER+STRICT.
TLP:GREEN	Limited disclosure, recipients can spread this within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when "community" is not defined, assume the cybersecurity/defense community.
TLP:CLEAR	Recipients can spread this to the *world*, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

THE BEACON

ABOUT THE FIPC AND *THE BEACON*

The Florida Infrastructure Protection Center (FIPC) was established in 2002 to anticipate, prevent, react to and recover from acts of terrorism, sabotage, cybercrime and natural disasters.

The Beacon is the Florida Fusion Center's cyber and critical infrastructure publication, produced by the FIPC. Designed to highlight information of interest, *The Beacon* features events and trends that occur in Florida or specifically affect Florida.

This addresses DHS HSEC-SIN-1; FDLE SINs 1.1.1, 1.1.2, 1.1.4, 1.1.6, 1.1.6.1, 1.2.1, 1.2.2, 1.5.2, 1.8.2, 1.10 and 1.13; and FFC-SINs 1.1, 1.3, 1.4, 1.5 and 1.7