The Beacon

Florida Fusion Center #21-122 | Cyber and Critical Infrastructure Report | October 2021 Issue #25

Summary

More Than Remotely Possible: RDP Attacks
We discuss this emerging tactic and how users can protect their devices.

Finding Inner Peace: Fortifying Against Insider Threats
We provide an overview of this threat and how it can impact organizations.

Get Off My Land!: Living Off The Land Attacks
Learn about this term's meaning in the information security field.

A Nation-State Actor Profile: North Korea
A profile of a nation-state and their cyber activity.

Securing The Internet of Things is Really…Everything
There are billions of devices in the world connected to the internet. We examine how to protect those devices and the information stored on them.

Lasting Impressions: What's your Digital Footprint Look Like?
A description of a digital footprint and ways to protect yours.

Contents

About *The Beacon*

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

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

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

SecureFLORIDA.org

TLP: WHITE

Editor's Corner

Moving Forward: Cybersecurity Tips for a Hybrid Workforce

October is Cybersecurity Awareness month and this year's theme is "Do Your Part. Be Cyber Smart." It is a great time to remind people what they can do to maintain cyber hygiene. In 2020, many organizations decided to allow their employees to work remotely in an effort to slow the spread of COVID-19. While organizations adapted to the pandemic, cybercriminals also adapted when it came to finding ways into networks and stealing sensitive information. Recently, some organizations who were teleworking have transitioned back to the office as state and local COVID-19 restrictions began to phase out. While telework status may vary across the country and across job functions, it is always important to protect your organization from cyberthreats and understand that employees play a major role in cybersecurity.

With so many employees working remotely and using different networks over the last year, cybercriminals increased their exploitation of cyber vulnerabilities.[1] Researchers saw a 131% increase in malware infections and about 600 new phishing attacks per day when the pandemic and remote working started in March 2020.[2] Cybercriminals also used sophisticated COVID-19 related social engineering schemes to target victims in 2020.[3] Even during the pandemic, cybercriminals have continued to evolve and find new ways to conduct their attacks.

While not all organizations are able to support continued work-from-home

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

operations, some have decided to continue to give their employees the option to work remotely for part of the remainder of 2021.[4] Other employees may be back in travel status and working remotely from business meetings, conferences, or other locations. If your organization has decided to continue to allow remote work as an option, there are certain actions that you can take to reduce vulnerabilities. Here are some cybersecurity tips to consider while working remotely:

Consider strengthening your home wi-fi network password by using a 'pass phrase' to make it difficult for cybercriminals to guess and make it easier for you to remember. If you don't have a password to connect to your wi-fi, create one. If you are using the default password, change it as soon as possible.

Stay up-to-date with your organization's security training and follow any BYOD (Bring Your Own Device) policies if you are using your personal phone, computer or tablet for work.

Stay current on software updates and patches; do not ignore those reminders to update and restart your device.

Use a Virtual Private Network[i] (VPN) if your organization offers one.

Watch out for social engineering attacks via phishing emails.

Do not connect to public wi-fi while working.[5][6][7][8]

Use multi-factor authentication if your organization offers it.

Whether you are working from home or another location outside of your office, you have to remember that working remotely comes with cybersecurity risks and to use the resources your organization has available. If you ever have questions about cybersecurity while working remotely, consider reaching out to your IT staff for assistance.

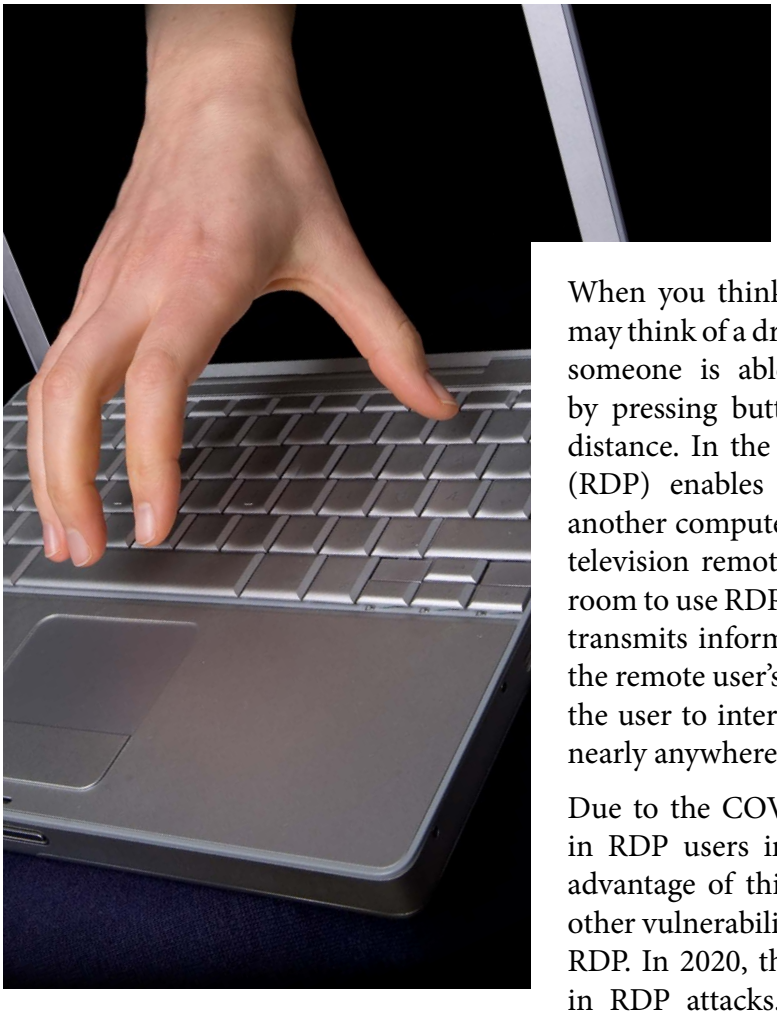
[i] A VPN provides a protected network connection for remote connections, to the extent that even an internet service provider can't see what websites are visited or what data is sent.

[1] https://www.zdnet.com/article/ransomware-vs-wfh-how-remote-working-is-making-cyberattacks-easier-to-pull-off/
[2] https://threatpost.com/2020-work-for-home-shift-learned/162595/
[3] https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
[4] https://www.businessinsider.com/companies-asking-employees-to-work-from-home-due-to-coronavirus-2020#reuters-the-international-news-organization-told-employees-they-can-work-from-home-until-january-2021-10
[5] https://www.zdnet.com/article/7-cybersecurity-tips-for-small-businesses-especially-those-with-remote-workers/
[6] https://www.techrepublic.com/article/how-to-handle-security-risks-in-a-hybrid-work-environment/
[7] https://www.zdnet.com/article/vpns-two-factor-authentication-and-more-keeping-your-data-safe-from-hackers-while-working-from-home/
[8] https://us.norton.com/internetsecurity-emerging-threats-working-from-home-due-to-coronavirus.html

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

Cyber Threats

More Than Remotely Possible: RDP Attacks



Remote access can be really useful. It allows employees to be able to work from a remote location and still have access to the organization's systems and files. For Information Technology professionals, it also offers the ability to access a remote system to perform a variety of functions or fixes. However, using RDP comes with cybersecurity risks as cybercriminals look to exploit weaknesses in it.

When you think of a remote controlled object, you may think of a drone or maybe a television. Essentially, someone is able to control that object or device by pressing buttons or entering commands from a distance. In the same vein, remote desktop protocol (RDP) enables computer users to gain access to another computer in a different location. Unlike your television remote, you don't need to be in the same room to use RDP. All you need is RDP software, which transmits information from the computer's server to the remote user's computer. Once connected, it allows the user to interface with the remote computer from nearly anywhere.[1] [2]

Due to the COVID-19 pandemic, there was a surge in RDP users in 2020.[3] Cybercriminals have taken advantage of this surge in remote users, along with other vulnerabilities, that can be exploited when using RDP. In 2020, there was an estimated 768% increase in RDP attacks.[4] Cybercriminals will often exploit vulnerabilities in an RDP entry point. One tactic they use is phishing, which usually involves sending emails in an attempt to trick users into clicking links and entering their credentials and passwords into fraudulent websites, allowing cybercriminals to steal the information. Cybercriminals may also exploit technological vulnerabilities such as an unsecure RDP port (particularly port 3389, which is typically the port used to enable the RDP connection).[5] Some cybercriminals may also use RDP to gain access to system files and other information to deploy a

As people continue to work remotely, cybercriminals will likely continue to seek out ways to exploit RDP vulnerabilities. With mitigation, RDP can be secured and continue to offer a productive solution to remote working.

multitude of cyberattacks including ransomware[i] attacks.[6]

There are actions organizations can take to secure remote desktop services, and it is imperative to recognize the human element when it comes to cybersecurity. It is important to stay up-to-date on any cybersecurity training and computer policies to understand how to avoid social engineering, develop unique and complex passwords, safeguard login information, and avoid clicking on malicious links.[7] Users can use a virtual private network (VPN) and multi-factor authentication as an extra layer of security, if it is available. Additionally, users should make sure to log out of their RDP sessions when they are not in use, rather than leaving them idle and potentially open to being hijacked by cybercriminals. It is also vital for users to ensure that all RDP software is updated when new patches and updates are released. Organizations can also employ and configure a network-based firewall,[ii] restrict the access of nonapproved external systems and explore limiting the number of employees with access to RDP to those that truly need it.[8]

[i] Ransomware is a form of malware that encrypts the files in a system and cybercriminals demand a ransom payment in order to have the files released.

[ii] A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

[1] https://searchenterprisedesktop.techtarget.com/definition/Remote-Desktop-Protocol-RDP
[2] https://www.cloudflare.com/learning/access-management/what-is-the-remote-desktop-protocol/
[3] https://www.zdnet.com/article/rdp-and-vpn-use-skyrocketed-since-coronavirus-onset/
[4] https://www.zdnet.com/article/big-jump-in-rdp-attacks-as-hackers-target-staff-working-from-home/
[5] https://www.cloudflare.com/learning/access-management/rdp-security-risks/
[6] https://blog.malwarebytes.com/malwarebytes-news/2021/02/rdp-the-ransomware-problem-that-wont-go-away/#:~:text=A%20majority%20of%20all%20ransomware,the%20way%20it%20is%20deployed.&text=In%202020%2C%20security%20researchers%20found,RDP%20clients%20used%20by%20businesses
[7] https://www.cisecurity.org/white-papers/exploited-protocols-remote-desktop-protocol-rdp/
[8] https://www.techrepublic.com/article/how-to-protect-your-remote-desktop-environment-from-brute-force-attacks/

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

Finding Inner Peace: Fortifying Against Insider Threats

Organizations face a variety of external cyber threats from cybercriminals, to criminal groups, or even nation-states, but what about threats from the inside? Sometimes the largest damage can be caused by someone with authorized access to an organization or its systems. This is known as insider threat.

"Insiders" can be employees, business associates, contractors or others who use your network. Within cybersecurity, insider threats can result in harm to an organization's information, systems, operations, personnel, and customers. The risk is greater than it might seem: insider threat breaches cost organizations millions each year, and according to Verizon, insiders caused between 20 and 40 percent of all recorded data breaches each year from 2011 to 2020.[1] [2] [3]

Insider threats may be the result of knowing actions by malicious actors or unknowing actions or errors. In some instances, insiders may intentionally act against the interests of an organization for personal gain or in reaction to grievances. Among other activities, some malicious insiders have stolen proprietary information for use by competitors, customer information for use in scams, and coworker information in retaliation for being fired.[4] [5] [6] The access and damage done by malicious insiders has not gone unnoticed by external threat actors. Nation-states, such as Russia and China, have attempted to recruit insiders in order to gain access to some sensitive information and systems.[7] [8] Malicious insiders may exhibit behavioral indicators observable to coworkers, such as disgruntlement or aggressiveness, unexplained financial gains, trying to gain access to sensitive information outside the scope of their normal duties, or working odd or late hours without reason or authorization.[9]

Insider threats can also arise from unintentional human error or complacency regarding security policies. Examples include opening a link or attachment from a phishing email, accidentally sending an email with sensitive information to a person or group without authorized access, ignoring messages to install new updates or security patches, or storing sensitive information on unapproved personal or unsecure devices.[10] While these incidents are not malicious, they can still do major harm to an organization. In recent years, high-profile data breaches at a range of organizations have also had elements of human error from within

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

the organization.[11] [12] [13] Behavioral indicators of an employee more susceptible to unintentionally threatening an organization may include patterns of carelessness, impulsiveness, or a lax attitude towards established security rules and procedures. However, nearly anyone can create unknowing vulnerabilities.[14]

There are several steps that can be taken to fortify an organization against insider threats, both intentional and unintentional. The Cybersecurity and Infrastructure Security Agency (CISA) recommends creating and maintaining a dedicated insider threat mitigation program that identifies key assets, threats, and vulnerabilities, and builds a culture of reporting, prevention, and secure behavior.[15] Additional ways to improve security against insider threats include: addressing the insider threat in periodic security training, implementing strict password policies, ensuring that sensitive information is limited to those who require it, and electronically monitoring network activity on official systems.[16] It is also essential that anyone with access to your systems understands the importance of safeguarding your information and property. For example, employees should make sure they protect their devices and passwords, implement updates in a timely manner, and avoid emailing sensitive documents to the wrong person.

While outside hackers continue to be a threat, the damage done to organizations by insiders, both accidental and malicious, continues to highlight the importance of taking insider threat protection just as seriously.

[1] https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
[2] https://enterprise.verizon.com/resources/reports/dbir/
[3] https://www.cisa.gov/sites/default/files/publications/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf
[4] https://www.fbi.gov/news/stories/two-guilty-in-theft-of-trade-secrets-from-ge-072920
[5] https://www.darkreading.com/attacks-breaches/suntrust-ex-employee-may-have-stolen-data-on-15-million-bank-clients/d/d-id/1331610
[6] https://chicago.cbslocal.com/2018/11/02/cps-data-breach-fired-employee-kristi-sims-charged-stolen-database-personal-information-identity-theft/
[7] https://www.justice.gov/opa/pr/russian-national-indicted-conspiracy-introduce-malware-computer-network
[8] https://www.justice.gov/opa/pr/former-boeing-engineer-convicted-economic-espionage-theft-space-shuttle-secrets-china
[9] https://www.cisa.gov/sites/default/files/publications/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf
[10] Ibid.
[11] https://www.cbsnews.com/news/twitter-hack-phishing-attack/
[12] https://www.gao.gov/assets/gao-18-559.pdf
[13] https://threatpost.com/boeing-notifies-36000-employees-following-breach/123942/
[14] https://www.cisa.gov/sites/default/files/publications/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf
[15] Ibid.
[16] https://www.cisa.gov/sites/default/files/publications/Insider%20Threat_1.pdf

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

Get Off My Land!: Living Off the Land Attacks

Did you know cybercriminals can use your computer's own systems against you? Traditionally, cybercriminals have targeted networks and used their own tools such as backdoors,[i] rootkits,[ii] and others, to attack networks. Recently, cybercriminals have increasingly turned to living off the land (LotL) attacks, which are also known as fileless malware or zero footprint attacks that use your computer's resources as part of the attack. Cybersecurity researchers saw a nearly 900% increase in fileless malware attacks in 2020.[1] A LotL attack allows cybercriminals to subtly gain access to a system using a computer's existing tools without having to install malware from another source. This makes it difficult to detect since the cybercriminals can remain in the environment long-term and avoid detection by blending in with regular activity. Some capabilities of LotL attacks are downloading files, code compiling,[iii] hiding payloads,[iv] and code execution.[v] [2] [3] [4] [5] However, antivirus software programs may be limited in their ability to detect these attacks because there are no outside connections trying to intrude.

Cybercriminals typically start a LotL attack by engaging in social engineering to encourage the target to visit compromised websites, open phishing emails, or click on malicious links. The attack usually undergoes three stages:

1. **Gaining access –** Fileless malware drops a payload into a computer's memory, which establishes contact with a cybercriminal remotely. They will scan for vulnerabilities and look for places to hide within the network.[6]

2. **Moving laterally –** The cybercriminal uses systems, compromised credentials, and tools on the computer to access other data or systems on the network. Examples of commonly exploited tools are PowerShell scripts, VB scripts, and Mimikatz. These are trusted administrative and troubleshooting tools that usually won't set off alerts when used.[7] Cybercriminals may also create a backdoor so they can return to the environment later.[8]

3. **Network damage and data theft –** The cybercriminal has access to the tools, directories and permissions needed to execute their attack and remain undetected, which may then be used to steal personal data or disrupt operations.[9]

There have been many attacks involving the use of LotL techniques. One well-known example with a global impact was the 2017 to 2018 outbreak of Petya/NotPetya ransomware. The attack focused on the software supply chain, infiltrating the update process in a software accounting program, which caused billions of dollars in damages.[10] [11] In April 2021, cybersecurity

researchers also discovered cybercriminals delivering a fileless backdoor through a spear-phishing campaign targeting professionals on LinkedIn with fake job offers. When malicious files sent with the job offer were clicked, cybercriminals gained access to victims' networks.[12]

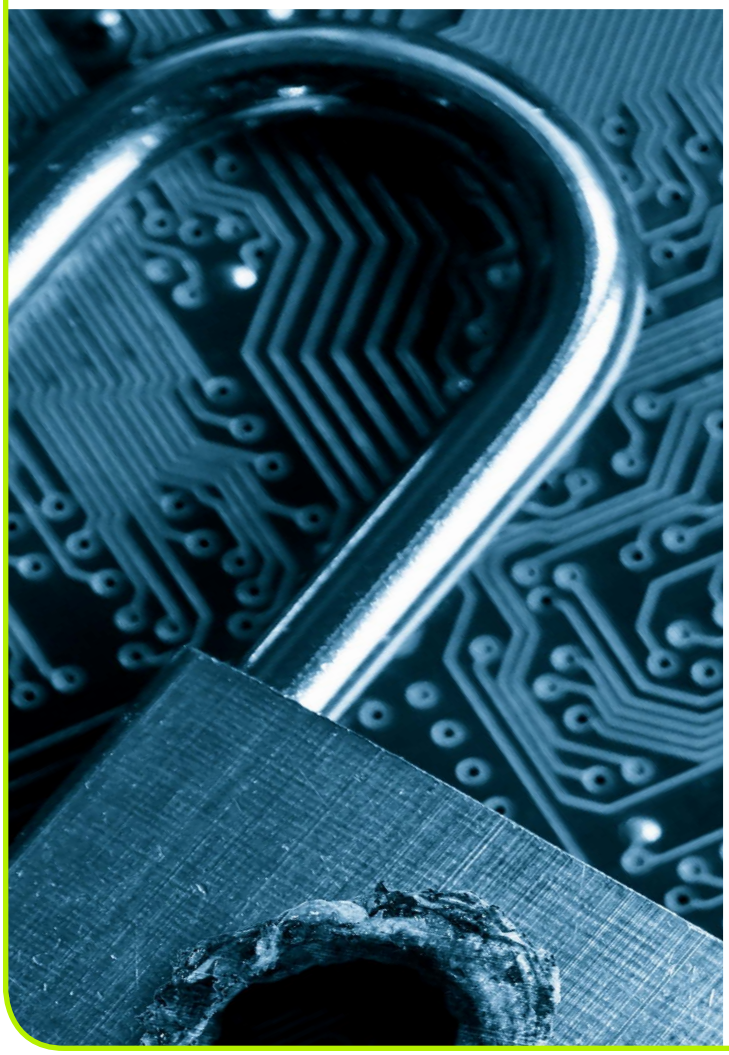
LotL attacks are difficult to detect since they take advantage of commonly used tools, but there are processes organizations can implement to protect their networks and increase the chances of detecting them. These attacks often rely on human vulnerability, which means users should use multi-factor authentication, if it is available, create strong passwords, be cautious of phishing emails, and stay up-to-date with security patching and application updates. Users should also be careful when downloading and installing unknown applications. Organizations can help with this. Prevention activity may include focusing on detecting criminal behaviors and setting up alerts when user account activities differ from normal. For example, organizations can implement alerts that indicate a remote desktop connection occurred at an unusual time for a user so it can be tracked by IT staff.[13] [14] Application whitelisting[vi] should be considered as well.[15] A combination of focusing on the human element, automated software, and threat hunting can help organizations prevent LotL attacks as fileless malware attacks continue to rise.

[i] A backdoor is an undocumented way of gaining high-level access to a computer system that allows cybercriminals to get around normal security measures that are in place.
[ii] A rootkit is a type of malware designed to be hidden, however, it remains active and can give cybercriminals the ability to remotely control a computer.
[iii] Code compiling allows cybercriminals to take high-level programming language they developed and translate it into machine language and eventually combine all of the language to create an executable program.
[iv] A payload is the component of a cyberattack that causes harm to the victim, and it can contain more than one type of malware.
[v] Code execution allows cybercriminals to upload malicious code onto a targeted computer by exploiting a software vulnerability and tricking the computer into running that code to execute tasks such as giving them access to sensitive data or modify files on that computer.
[vi] Whitelisting is a strategy that that ensures a user can only take certain actions on their computer if approved by an administrator.

[1] https://www.infosecurity-magazine.com/news/fileless-malware-detections-soar-1/
[2] https://blog.malwarebytes.com/glossary/payload/#:~:text=In%20cybersecurity%2C%20a%20payload%20is,not%20the%20email%20or%20document)
[3] https://www.ironnet.com/blog/what-are-living-off-the-land-attacks#:~:text=One%20common%20tactic%20is%20called,exist%20in%20the%20computing%20environment
[4] https://www.cynet.com/attack-techniques-hands-on/what-are-lolbins-and-how-do-attackers-use-them-in-fileless-attacks/
[5] https://www.venafi.com/blog/beware-cyber-attackers-living-land
[6] https://www.ironnet.com/blog/what-are-living-off-the-land-attacks#:~:text=One%20common%20tactic%20is%20called,exist%20in%20the%20computing%20environment
[7] https://www.varonis.com/blog/fileless-malware/
[8] https://www.darkreading.com/edge/theedge/how-to-evict-attackers-living-off-your-land/b/d-id/1337420
[9] https://www.crowdstrike.com/cybersecurity-101/malware/fileless-malware/
[10] https://www.varonis.com/blog/fileless-malware/
[11] https://www.darkreading.com/edge/theedge/how-to-evict-attackers-living-off-your-land/b/d-id/1337420
[12] https://www.cbsnews.com/news/lessons-to-learn-from-devastating-notpetya-cyberattack-wired-investigation/
[13] https://threatpost.com/linkedin-spear-phishing-job-hunters/165240/
[14] https://www.varonis.com/blog/fileless-malware/
[15] https://us.norton.com/internetsecurity-malware-what-is-fileless-malware..html
[16] https://www.darkreading.com/edge/theedge/how-to-evict-attackers-living-off-your-land/b/d-id/1337420

A Nation-State Actor Profile: North Korea

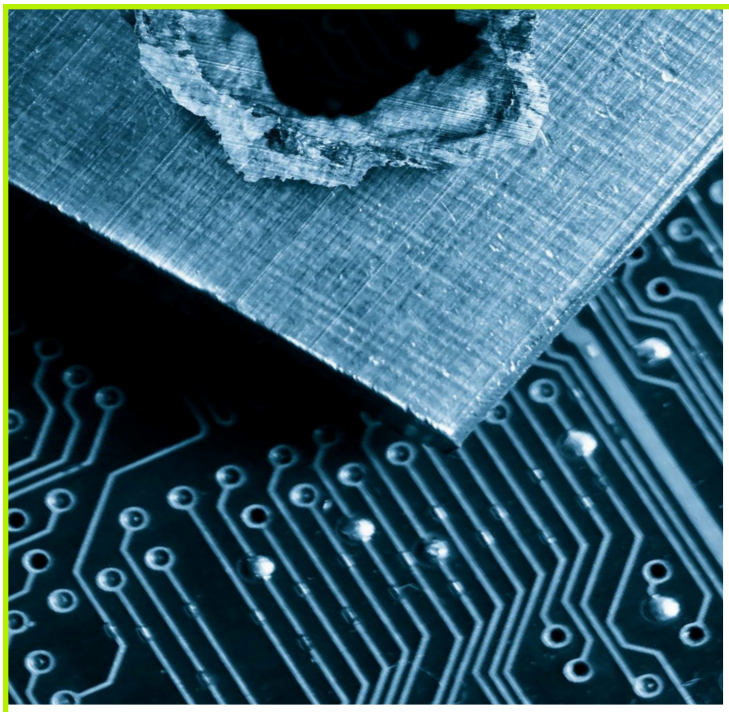
Have you ever thought about where malicious cyber actors come from or what their goals are? The reality is that cyber criminals can be from anywhere, and some malicious cyber actors have ties to nation-states, including Russia, China, and North Korea. Malicious cyber actors connected to the government in North Korea, formally known as the Democratic People's Republic of Korea (DPRK), have conducted several notorious cyberattacks in recent years. U.S. officials have expressed growing concern over the DPRK's increasingly sophisticated cyber capabilities, which could be used for espionage and financial gain.[1] The DPRK is under heavy economic sanctions from the U.S. and the United Nations, and cybercrime is one way the regime generates money while subject to these sanctions.[2]



In February 2021, a federal indictment that charges three North Korean computer programmers with stealing over $1.3 billion via cyberattacks was unsealed. These illicit cyber activities have allegedly targeted the entertainment industry, banking institutions, cryptocurrency companies, and others. The indictment states that the programmers employed a variety of tactics, including spear-phishing and ransomware.[3]

In January 2021, it was reported that a North Korean group was posing as a legitimate cybersecurity firm. The group created a sophisticated online presence, complete with high-quality websites and several social media accounts. They targeted cybersecurity researchers, luring legitimate cybersecurity professionals into sites with malicious code. Later, this same group created a fake company, complete with the trappings of a legitimate firm, that offered cybersecurity testing to companies. These offerings were actually ways for the group to deploy browser-based exploits when their "customers" attempted to use the fake firm's services.[4] In other words, if cybersecurity researchers visited compromised

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



websites, the exploits would use weaknesses in the browser's software to allow malicious cyber actors to infect the researchers' computers.

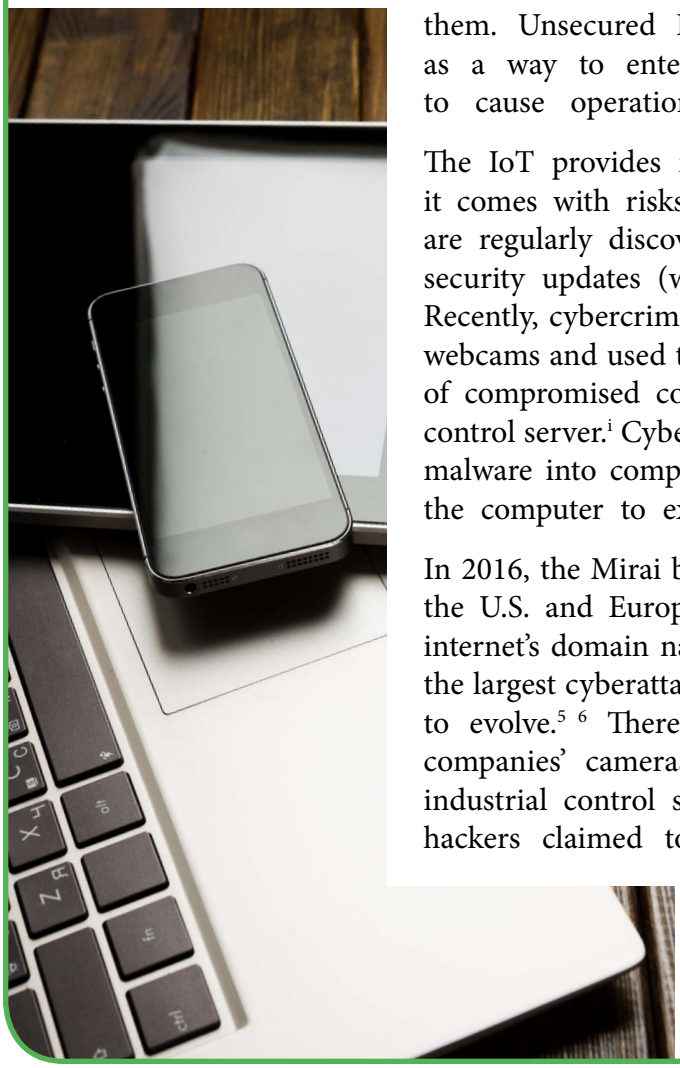
The most well-known hacking group connected to the regime in North Korea is the Lazarus group. This group excels at finding and exploiting vulnerabilities in cybersecurity systems, and is growing more sophisticated. The DPRK's cyber capabilities rival those of many countries, and they have shown a high willingness to engage in malicious cyber activities.[5] Some tactics used by the Lazarus group and others include financial theft, money laundering, extortion campaigns, and "cryptojacking"- a technique to mine cryptocurrency by taking over a victim machine and exploiting its computing power.[6]

As DPRK's cyber capabilities continue to evolve, it is important to note there are several ways to mitigate the cyber threats they pose. Among them are: increasing awareness of the DPRK's cyber activities among government and private sector entities, implementing cybersecurity best practices, and notifying law enforcement if a suspected cyberattack occurs.[7] As always, individuals should be cautious when clicking on links embedded in emails, entering personally identifiable information (PII) online, and keep antivirus software up to date.

[1] https://crsreports.congress.gov/product/pdf/IF/IF10246/14
[2] https://us-cert.cisa.gov/ncas/alerts/aa20-106a
[3] https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and
[4] https://www.zdnet.com/article/google-north-korean-hackers-targeting-researchers-now-pretend-to-be-from-offensive-security-firm/
[5] https://foreignpolicy.com/2021/03/15/north-korea-missiles-cyberattack-hacker-armies-crime/
[6] https://us-cert.cisa.gov/ncas/alerts/aa20-106a
[7] Ibid.

Cyber Highlights

Securing the Internet of Things Is Really... Everything



The term "Internet of Things" (IoT) was coined in 1999, but it took nearly a decade before the IoT began to develop into what it is today. The IoT refers to the billions of physical devices around the world that are connected to the internet, all collecting and sharing data. It started in business and manufacturing with machines communicating and sharing data wirelessly, but now, many people associate the IoT with smart home devices like appliances and thermostats.[1] Businesses in nearly every industry use the IoT for tasks like detecting and troubleshooting issues remotely, tracking production and efficiency, security, and many others.[2] With the IoT being a part of our daily lives, whether we are at home or in the office, it is important to focus on securing them. Unsecured IoT devices may be targeted by cybercriminals as a way to enter organizations' networks without authorization to cause operational disruptions or steal sensitive information.

The IoT provides many benefits to businesses and consumers, but it comes with risks. New flaws or vulnerabilities in device software are regularly discovered, even if devices have the ability to receive security updates (which is something not all IoT devices can do). Recently, cybercriminals have targeted IoT devices such as routers and webcams and used them to create giant botnets.[3] A botnet is a network of compromised computers that are supervised by a command and control server.[i] Cybercriminals use them to conduct attacks by injecting malware into compromised computers, stealing credentials, or asking the computer to execute certain tasks to give them an advantage.[4]

In 2016, the Mirai botnet caused a massive internet outage throughout the U.S. and Europe, using IoT devices to launch an attack on the internet's domain name system (DNS) infrastructure.[ii] This was one of the largest cyberattacks of its kind, and cybercriminals' tactics continue to evolve.[5] [6] There have been reports of cybercriminals hijacking companies' cameras, hospitals' medical devices, and compromising industrial control systems over the last few years.[7] In March 2021, hackers claimed to have gained access to over 150,000 security

Florida Department of Law Enforcement (FDLE)
Florida Fusion Center (FFC)
Florida Infrastructure Protection Center (FIPC)

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

cameras and surveillance footage from major private sector companies, hospitals, prisons, police departments and schools.[8] Footage from major companies and institutions was leaked as a result of this breach.[9]

Protecting IoT devices adds another layer for information technology security, but it is important to consider IoT device security and explore ways to improve it as cybercriminals continue to target them.

Cybercriminals will continue target IoT devices, and it is important for organizations' security practices to be strong. One of the first steps organizations should take is conducting inventory of the IoT devices running on their network and the data they contain. This can give an organization the ability to control when devices are running and enable and disable certain features to limit vulnerabilities. Once inventory is taken, it may be necessary to turn off older devices that rely on older versions of operating systems. Changing passwords on devices regularly is also an essential step. Additionally, there are more advanced actions that can be taken, such as using multi-factor authentication, firewalls, and network segmentation.[iii] It is also important to keep device software and security patches updated.[10] Similar actions, such as changing passwords and knowing what devices connect to the internet, can be taken at home as well. The main consideration for home users should be their router, which is like the "front door" of a "smart home." Users can consider using a security-focused router that can scan for vulnerabilities and supports network segmentation.[11] [12]

[i] Command-and-control servers are the machines cybercriminals use to maintain communication with the compromised systems in a target network.
[ii] DNS is basically the phonebook of the internet. People access information online through domain names, like secureflorida.org. Web browsers interact through Internet Protocol (IP) addresses and DNS translates domain names to IP addresses so browsers can load Internet resources.
[iii] Network segmentation divides a network into smaller parts, isolating some devices from others, to protect those that are critical to operations.

[1] https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/
[2] https://www.techrepublic.com/article/internet-of-things-iot-cheat-sheet/
[3] https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/
[4] https://www.crowdstrike.com/cybersecurity-101/botnets/
[5] https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet
[6] https://www.cloudflare.com/learning/dns/what-is-dns/
[7] https://www.darkreading.com/edge/theedge/how-to-build-a-resilient-iot-framework/b/d-id/1340566
[8] https://threatpost.com/breach-verkada-security-camera-tesla-cloudflare/164635/
[9] https://www.cbsnews.com/news/verkada-hack-tesla-nissan-equinox-cloudflare/
[10] https://www.darkreading.com/edge/theedge/how-to-build-a-resilient-iot-framework/b/d-id/1340566
[11] https://us.norton.com/internetsecurity-iot-smart-home-security-core.html
[12] https://www.forbes.com/sites/forbestechcouncil/2020/02/05/keeping-your-smart-home-secure-14-tips-to-help-protect-iot-devices/?sh=47d9bdc62bb1

Lasting Impressions: What's Your Digital Footprint Look Like?

Have you ever thought about what it would be like to live on an island without any electronic devices or internet availability? That may not seem practical for many people today. Given how much technology has evolved in recent years, it is increasingly necessary for people to use the internet as part of their daily lives. Much of our online activity creates a digital footprint, which is the personal data and information available about you online.[1] Despite best intentions, you may be unknowingly exchanging personally identifiable information (PII) and patterns of behavior as you search the web or post on social media, which may be used by cybercriminals to target you. In addition, criminals may use information you post on social media sites or other online locations for malicious purposes like identity theft, targeting you in an email scam, or for social engineering purposes.[2] This could include using personal information you posted, information about where you live, your family, pets, or other information as part of a scam. There are things that you can do to minimize your digital footprint, but keep in mind that patience will be key.

It is likely you will leave some sort of digital footprint online, but there are actions you can take to reduce it .

Next time you're online, check out your digital footprint by visiting a search engine of your choice and enter your name and location. Some of what you will find cannot be deleted; however, your digital footprint can be minimized over time. Consider the following tips as a starting point:

- Check your privacy settings on social media and consider restricting who can see your posts.
- Think about information contained in your posts and remove anything that might be sensitive before you make them public.
- Disable and erase online accounts you no longer use (e.g., online shops, social media sites, email accounts).
- Consider opting out of allowing websites to use or sell your data, where possible. The opt-out process can vary depending on the website, but you can usually find this information in their privacy policy, which describes how they collect, handle, and process website visitor data like your password, address, phone number, or payment information among other things.
- If you identify content that makes you uncomfortable but you cannot edit directly, contact the webmaster to see if they can remove your PII and undesired posts/content from their sites.[3][4][5][6]

[1] https://www.businessinsider.com/what-is-a-digital-footprint
[2] Ibid.
[3] Ibid.
[4] https://staysafeonline.org/blog/owning-your-privacy-by-managing-your-digital-footprint/
[5] https://www.bbb.org/article/news-releases/21390-bbb-tip-writing-an-effective-privacy-policy-for-your-small-business-website
[6] https://www.cnet.com/how-to/remove-delete-yourself-from-internet/

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

Dispatch Highlights

This section highlights articles from past *FIPC Dispatches* that our analysts think are noteworthy based on trends we're seeing in Florida. *The FIPC 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 *FIPC Dispatch*, visit SecureFlorida.org and click "**Get Connected**" at the top of the homepage or send an email to **FIPC@fdle.state.fl.us**.

Cyber attack on U.S. government may have started earlier than initially thought - U.S. senator

https://www.reuters.com/article/us-global-cyber-usa-senator/cyber-attack-on-u-s-government-may-have-started-earlier-than-initially-thought-u-s-senator-idUSKBN29501K

- In December 2020, U.S. officials disclosed a major cyberattack on a large number of high profile U.S. government and private sector networks.
- Cybercriminals gained access to various networks by hiding malicious code in information technology management software created by a Texas-based company.

Analyst Note: Cybercriminals understand that organizations rely heavily on certain software to operate and they are looking to conduct supply chain attacks by hiding malware in legitimate software developed by third-party vendors that serve a large number of customers. This is done in an effort to remain hidden on victims' networks, move around the network, and steal sensitive information.

Verkada Breach Demonstrates Danger of Overprivileged Users

https://www.darkreading.com/vulnerabilities---threats/verkada-breach-demonstrates-danger-of-overprivileged-users/d/d-id/1340403

- A major provider of surveillance cameras suffered a data breach that exposed the contents of live camera feeds from a large number of clients from various sectors and some private residences.
- Employees of third-party vendors having overprivileged access to customer data and devices has been highlighted in past incidents with major service providers.

Analyst Note: Cybercriminals reportedly gained access through a compromised "super administrative account" used by the major service provider to gain access to tens of thousands of cameras from more than 100 internal users. Organizations should vet their vendors to gain an understanding of their cybersecurity practices and what level of access vendors need to maintain their products and services.

Computer intruder tried to poison drinking water for a small Florida city

https://arstechnica.com/information-technology/2021/02/computer-intruder-tried-to-poison-drinking-water-for-a-small-florida-city/

- In February 2021, a cybercriminal hacked into a water treatment plant's network and attempted to poison the water supply of a Florida municipality through remote access.
- Fortunately, the attack was quickly spotted and mitigated before any changes were made to the water supply.

Analyst Note: There are actions that critical infrastructure providers can take to protect their networks, including but not limited to, updating software, using multi-factor authentication, and requiring strong and complex passwords for remote desktop login credentials.

A company paid millions to get their data back, but forgot to do one thing. So the hackers came back again

https://www.zdnet.com/article/ransomware-this-is-the-first-thing-you-should-think-about-if-you-fall-victim-to-an-attack/

- Cybercriminals attacked an organization with ransomware and the organization paid the ransom to gain access to their files.
- However, the organization reportedly failed to analyze how their network was infiltrated and the network was hit with ransomware again less than two weeks later.

Analyst Note: If your organization is attacked by ransomware, it is important to work to get systems back up and running and also examine how the network was impacted by malware in the first place to help mitigate potential security weaknesses. Additionally, paying the ransom is not recommended because it does not guarantee you will regain access to your system or data, and it does not prevent future attacks from happening.

White House details $20B fund to 'cyber modernize' energy infrastructure

https://www.cnet.com/news/white-house-details-20b-to-cyber-modernize-energy-infrastructure/

- A recent high-profile ransomware attack targeted a major pipeline company that provides 45% of the east coast's fuel.
- In an effort to "modernize" cybersecurity for energy infrastructure across state, local, and tribal governments, certain entities will be eligible to apply for grants and obtain funding if they meet certain requirements indicating their plans for improving their cybersecurity practices.

Analyst Note: Cyberattacks on energy infrastructure can disrupt the distribution of electricity, the operation of physical networks of oil and natural gas pipelines, and disrupt transportation elements like marine and rail transportation.

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

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

www.SecureFlorida.org/SF/The-Beacon

The following is from the United States Computer Emergency Readiness Team (US-CERT):

Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information.

Recipients may share TLP: GREEN information with peers, partner organizations, and with their sector or community, but not via publicly accessible channels.

TLP: WHITE information may be distributed without restriction, subject to copyright controls.