Summary

**BlueKeep Your Operating System Up To Date!** - A serious vulnerability affects many older versions of Windows operating software. What can you do to protect yourself?

**Swiped!: What is SIMSwapping?** - SIMSwapping is a routine service that allows you to port your phone number and information to a new mobile phone, but scammers are using it to bypass multifactor authentication. We examine their tactics.

**Mobile Device Security: How To Protect Your Data** - These days, we use our mobile devices for everything from banking to web surfing. Find out how to keep your data safe.

**A Primer on Privacy: Social Media Controls** - Sharing on social media can be an easy way to connect with friends or family, but take care that you aren’t giving away too much information.

**Why DDoS My Internet Connection Suck?** - Distributed denial of service attacks are getting bigger. See the newest trends and tips on how to protect your organization.

**Nihao Did I Get Hacked?: A Look at China’s Cyber Activities** - China is a major player in the cyber threat landscape. We take a look at their current activities.

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

This addresses the DHS Standing Information Need HSEC-SIN-1 and FDLE SIN-1 TLP: WHITE
New Year, New Secure Florida

The time around New Year’s is a great chance to start anew, clean things up, and make lasting resolutions. It’s no different here at the Florida Infrastructure Protection Center and Secure Florida. For the past year, we’ve been working towards updating and improving the Secure Florida site and we’re proud to announce that the revamped and revitalized site is now live.

For those who are unfamiliar with the Secure Florida program, it is an initiative of the Florida Department of Law Enforcement with the goal of teaching Floridians how to stay safe on the internet and protect your personal information. Secure Florida analysts have traveled the state to give in-person training to thousands of Floridians over the years; a feat we’re very proud of. The Secure Florida site is intended to supplement these trainings and act as a base of knowledge for the industry’s latest tips and best practices. With that in mind, we set out to update the site to reflect the changed cyber threat landscape and to address what we felt were some of the most pressing questions we received while out meeting with Floridians during training.

All of the features of the old site will still be available; you’ll still be able to sign up for The Beacon and The Dispatch, see a listing of Secure Florida classes, and you’ll be able to contact Secure Florida directly with questions about cybersecurity or training.

Over time, we intend for Secure Florida to grow and offer more information as cybersecurity situations change and evolve. We hope that you find the new layout easier to navigate and the information timely and relevant.

So, here’s to new beginnings and fresh starts as Secure Florida continues its resolution to keep Floridians safe online and to safeguard the Sunshine State’s economy, infrastructure, and government.
Cyber Threats

BlueKeep Your Operating System Up To Date!

BlueKeep, also known as CVE-2019-0708,1 is a remote code execution vulnerability that exists within the Remote Desktop Protocol (RDP) used by Microsoft Windows Operating Systems.1 The vulnerability can act like a worm (a type of malware that is spread without user interaction),2 similar to Conficker and WannaCry.3 Attackers can exploit this vulnerability by sending a specially crafted request command to the target system via RDP.4 The attackers can then install programs; view, change, or delete data; or create new accounts with full user rights.5

In May 2019, Microsoft issued a patchiii and warned Windows administrators and users of the BlueKeep vulnerability.7 In addition to the patch, there are several steps that administrators can take to reduce their vulnerability to BlueKeep:

- If Remote Desktop Services are not required, administrators can disable them as a security best practice and reduce their exposure to security vulnerabilities.8
- Network Level Authentication (NLA) can also be enabled on a system that supports editions of Windows 7, Windows Server 2008, and Windows Server 2008 R2. The NLA will require users (and potential attackers) to provide authentication when using a valid account on the system before the attacker can exploit the vulnerability.9
- Lastly, administrators can block TCP port 3389 at the enterprise perimeter firewall. The TCP port 3389 initiates a connection with the affected component, and when this port is blocked at

The BlueKeep vulnerability affects both 32- and 64-bit versions and all Service Pack versions of the following:6

- Windows 2000
- Windows Vista
- Windows XP
- Windows 7
- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2
Although there is a remedy for the BlueKeep vulnerability, there continues to be a risk for attackers to exploit it. In May 2019, a security researcher ran an internet-wide scan and found that 922,225 machines had not been patched against the vulnerability.\(^1\) Given the high number of systems remaining unpatched, the researcher issued a warning that attackers were likely to figure out a way to exploit the vulnerability within the next few months.\(^2\) As of November 2019, Microsoft confirmed that there had been increased activity around BlueKeep exploitation with successful attacks leading to the installation of a cryptocurrency miner.\(^3\)

Microsoft and other security researchers suspect that the BlueKeep exploitation will continue to impact machines in the future. The best way to protect against BlueKeep exploitation is to patch vulnerable systems and ensure that RDP is configured to only allow approved connections, if necessary. Ensure that antivirus software is up to date and that it can detect applications such as cryptocurrency miners. Additionally, be sure to check system logs to see if new accounts are being made or if suspicious software or applications are being downloaded.

---

1. A vulnerability that allows an attacker to run code on a target machine remotely.
2. A proprietary Windows protocol that allows users to remotely access a network.
3. A patch is a set of changes to a computer program or its supporting data designed to update, fix, or improve it.
4. [1](https://www.us-cert.gov/ncas/alerts/AA19-168A)
5. [2](https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/1865726/nsa-cybersecurity-advisory-patch-remote-desktop-services-on-legacy-versions-of/)
6. [3](https://www.microsoft.com/security/blog/2019/08/08/protect-against-bluekeep/)
9. [6](https://www.us-cert.gov/ncas/alerts/AA19-168A)
10. [7](https://www.forbes.com/sites/daveywinder/2019/11/03/windows-bluekeep-attack-that-us-government-warned-about-is-happening-right-now/#cc4e9d331a00)
11. [8](https://www.us-cert.gov/ncas/alerts/AA19-168A)
12. [9](https://blog.erratasec.com/2019/05/almost-one-million-vulnerable-to.html#.XeMB5OhKjIU)
control of their device. The first sign that a device has been compromised is often the inability to send or receive text messages or phone calls. Once the phone company completes the swap, the scammer will have access to the data and phone number of the customer. Many people use their cell phone for multifactor authentication on their online accounts; as a result, scammers may be able to access email, bank, social media, and even bitcoin accounts by requesting the password verification be sent to the phone number they now control. Once the passwords are changed and the accounts are compromised, the scammer gains access to all of the target's personal information, and/or money, which can be difficult to recover if the scam is not quickly discovered.

The primary way to protect yourself from SIMSwapping is to set up a PIN or strong password on your cellular account. Most phone companies already require this, but check with your provider to make sure your account has the maximum amount of security. Second, consider using strong authentication on accounts with sensitive or personal information. Last, do not reply to calls, emails, or text messages that request personal information and limit the personal information that you share online. In the event that SIMSwapping happens to you, immediately call your mobile service provider and report it. Then, call the agencies of accounts involved with the stolen phone number to try and recover your information, including your bank, email, and social media accounts. The more quickly the scam is discovered and reported, the more likely it is that your information can be saved.

SIMSwapping has been around for years, yet a recent reliance on phone authentication and the value of your device's data makes this scam enticing for criminals; therefore, strong security measures and paying close attention to your accounts and devices is extremely important and may save your important information and finances in the event that the unthinkable occurs.

3 https://stopsimcrime.org/faq/?active-tab=simcrime
4 https://www.consumer.ftc.gov/blog/2019/10/sim-swap-scams-how-protect-yourself
Cyber Highlights

Staying Safe on the Go: Mobile Device Safety

Downloading apps safely on your devices is a must. It is recommended that you review the features, permissions, and technical requirements of any new app before installing it on your device. Know what information the app will store about you, such as location, financial information, or personal contacts. Additionally, installing apps from official app stores is also vitally important, as these stores scan apps for malicious code and have stricter requirements for vendors.\(^1\) Downloading apps from third-party sites is risky and can expose you to apps that can adversely affect the operation of your device or have malicious code.\(^2\) In addition to doing your research before you download an app, maintaining the apps you already have is also key.

Experts recommend that you keep mobile apps and your device’s operating system up to date; that is the best defense against emerging online threats, viruses, malware, or any other malicious attacks.\(^3\)\(^4\) One of the best ways to combat cyber threats is to install anti-virus software on all of your mobile devices.\(^5\) Delete applications that you download for a specific purpose, such as when you are going on vacation and will only need it for a short period of time. It is also a good idea to go through the apps on your mobile devices every couple of months and delete any that you are no longer using. This not only frees up space on your device’s hard drive, but allows you to make sure you are not giving unwanted access to your personal information.

In addition to being conscientious about what you access and do on your mobile device, below are some suggestions of good habits to keep in mind:

- Avoid using public wireless networks (Wi-Fi) as much as possible as they are not secure and can open your device up to vulnerabilities. If you do need to access Wi-Fi, consider using a virtual private network (VPN) and remember to disconnect as soon as you are done.\(^6\)
- Disable the geo-tagging feature on your mobile device, which will turn off location and limit tracking through apps.\(^7\)
- Ensure that the passwords you use to access different apps are all unique, at least 15 characters in length, and include numbers, letters (upper and lower case), and special characters. It is also vitally important that you keep your passwords private.\(^8\)
- Encrypt sensitive data on your devices, when possible. By encrypting data, it stores sensitive data (such as financial information, emails, and contacts) in an unreadable form so they cannot be easily understood by bad actors.\(^9\) Set your device to lock when you aren’t using it. This will encrypt all of the data on your device and require a user to input a code in order to access it.

Mobile device safety is a necessity given all of the personal information stored on your laptops, tablets, and smartphones. Mitigating theft of personal identifiable information or loss of money requires good mobile device safety habits and regular application (app) maintenance.
• Close out of apps when you are done with them and also make sure to log out of accounts, such as bank accounts or social media sites.  

With over 194 billion apps downloaded worldwide in 2018 (a number that is sure to grow every year), it is imperative that you do your due diligence to safeguard your information and protect the integrity of your mobile devices.

A Primer on Privacy: Social Media Controls

Social media is a part of many people's daily lives. People share pictures of their families, health statuses, relationship statuses, vacations, and even opinions on controversial topics. Sometimes, those who use social media may share sensitive life details in order to stay connected to friends, family, and co-workers. If shared publicly, these private details can be used maliciously by cyber criminals looking to access sensitive accounts, create fraudulent identities, and exploit individuals.

In the past five years, nearly 1.3 billion social media users worldwide have had their social media accounts compromised.

As a result, some estimate that anywhere from 45 to 50 percent of all illicit trading of personal information – including stolen credit card information as well as username and password combinations – can be traced back to social media platforms.

Each platform has privacy control settings and features that users can implement to protect themselves. These settings and features can be
used to manage who may see your information, posts, and what third-parties will have access to that information. It is important to note that not all social media platforms are created equally and users should be aware of what privacy settings are available.

Facebook is the largest and most popular social network and allows users to connect with friends, post status updates, “check in” to various locations, send private messages, join common interest groups, and upload photos. Users can also share personal information like their birthdate, hometown, activities, and political preferences. Facebook has different privacy settings and features for many aspects of a user’s profile. Settings for photos, status updates, friends lists, and page likes must all be adjusted individually, which gives you the most control over who can see your content. Some of the settings that Facebook offers are the ability to turn off access to your location, turn off facial recognition, limit data collection from third-parties, and the ability to allow your profile to be found through search engines. Most of these settings can be accessed by going to the “Privacy Settings and Tools” panel. It is important to note that certain information will always be available to the public, including your name, profile picture, cover photo, gender, networks, username, and user ID.3

Twitter is the second largest social networking site in the U.S. and allows users to share 280-character updates, called “tweets,” with their friends and followers. Twitter also allows you to include links and photos in your tweets. There are some simple settings that can allow you to make your account private. A private account will ensure that only Twitter users approved by you can see your tweets. Your tweets will no longer appear in search engine results or be “retweetable.” Any replies you send will not be seen, unless you send them to your approved followers, but one of your approved followers could take screenshots of posts and share them elsewhere. These settings can be found under the Security and Privacy page under Settings. Additionally, users can elect to turn off location tagging in this same menu.4

Instagram is a smartphone-based app that allows users to upload photos and videos. Captions and comments are allowed, as well as private picture messaging. Users can modify their privacy settings to ensure only approved followers can see their posts by going to their profile and tapping on the three lines in the upper right corner of the app, and then selecting Settings > Privacy > Account Privacy and then turning on “Private Account.” Enabling this setting ensures that only preapproved users can see posts, and posts will no longer appear in public searches. Individuals wanting to connect with other users will need to send a request and receive approval before viewing their pictures and follower list. Users should remember that regardless of their privacy settings, any Instagram user will still be able to read their bio, and send a photo, video, or message to them directly.5

Facebook, Twitter, and Instagram are just three of the social media platforms available, but every social media platform should have privacy controls that allow you to limit what is shared. It is a good idea to learn what personal data social media sites store and share with third-parties. Users should also carefully consider what personal details they provide. No matter which platform you use, make sure you read their privacy policies and know how to adjust privacy settings. Even with privacy controls, individuals should be careful posting sensitive information and photos on any platform. Users should always be mindful of who can see, react, or comment on their posts, and take advantage of any opportunity you can to take control of the information that you share to protect yourself and your loved ones.6

1 https://identity.utexas.edu/everyone/how-to-manage-your-social-media-privacy-settings
3 Ibid
4 Ibid
5 Ibid
6 Ibid
Why DDoS My Internet Connection Suck?

Many cyber threats revolve around illegally accessing the information of others. However, some revolve around making computer systems and websites unavailable for those who should otherwise have access. The main way bad actors achieve this is through a distributed denial of service (DDoS) attack, in which a hacker floods a server with a large number of spurious requests, overloading and effectively taking the connected system offline. A server can only handle so many requests for a connection at a time, so these fake requests tie up valuable resources and eventually overload the system.

Once initiated, DDoS attacks are often successful in disrupting online services, with 91% of enterprises who experienced a DDoS attack reporting that at least one attack completely saturated their server's bandwidth. Additionally, although DDoS attacks cannot be used to steal personal or sensitive information, they still have a substantial financial impact on affected enterprises. Enterprises reportedly lost an average of $218,339 with each DDoS-related service outage in 2018. In addition to companies, DDoS attacks sometimes target government agencies, draining taxpayer dollars and suspending important services. In May 2019, a resident of Akron, Ohio, was arrested and has since been convicted for conducting several DDoS attacks against government agencies, including the city government website for Akron, Ohio, and their police department. After his arrest, the hacker told detectives he held grudges against the police department. The hacker also targeted websites for NATO, the National Institutes of Health, the U.S. Department of Defense, and the U.S. Department of the Treasury.
DDoS attacks remain prolific and varied. Although the number of DDoS attacks slightly decreased from 2017 to 2018, likely due to government takedowns of several DDoS service online marketplaces, they are still incredibly common. Worldwide an estimated 6.13 million attacks occurred in 2018, an average of 16,794 per day. Several different DDoS vectors exist, some of which are stronger or more effective than others. UDP flood attacks are relatively outdated, easy to detect, and considered the least dangerous type of DDoS attack. In contrast, TCP SYN flood attacks are capable of overloading a server and causing connection outages. In 2018, over one third of DDoS attacks used multiple vectors.

The number of DDoS attacks may have decreased but the attacks themselves are getting larger. In 2018, the two largest recorded DDoS attacks occurred within days of each other. The first reached 1.35 terabytes per second (TBPS) of illegitimate requests by using vulnerable or unsecure memcached servers (servers normally used to speed up websites by caching, or storing, data) to amplify the attack. This tactic allows for stronger attacks compared to the common DDoS technique of using botnets, which are executed by using multiple infected computers to send spurious requests. This suggests that DDoS attackers continue to develop new strategies for creating more effective attacks that can bypass existing security protocols.

To combat these new strategies, continued cybersecurity vigilance and adaptation is required by companies and agencies that may be targeted. DDoS attacks can be difficult to mitigate. However, anti-DDoS technology exists and can redirect or drop malicious traffic. Additionally, there are software and hardware solutions that can identify suspicious traffic and block IP addresses, which can slow the onslaught of a flood attack. The best practice is to have a plan in place to address service availability before such an attack occurs.

1 User Datagram Protocol, a communications protocol used to send information over the internet
2 Transmission Control Protocol, another protocol used to send information
3 SYN (synchronize) is a type of packet sent to a server to initiate a connection. A server sends back an acknowledgment, which the original machine also acknowledges. Once all handshakes are made, a connection is established.
5 https://www.netscout.com/report/
7 https://www.netscout.com/report/
10 https://www.netscout.com/report/
11 https://www.zdnet.com/article/github-was-hit-with-the-largest-ddos-attack-ever-seen/
12 https://www.cloudflare.com/learning/ddos/memcached-ddos-attack/
13 https://www.cloudflare.com/learning/ddos/memcached-ddos-attack/
In September 2015, the U.S. and China reached an agreement to address malicious cyber-attacks between the two countries. Within this agreement, both countries agreed primarily to avoid cyber activities that supported the theft of intellectual property, to follow agreed upon behaviors for nation-states, and to share information on malicious cyber activities. At the time, many felt that this agreement was a step towards real progress in protecting U.S. intellectual property and preventing the unauthorized access and exploitation of sensitive information. Although it appears that China has decreased some of its unauthorized cyber activity since the signing of the agreement, enough of this activity still occurs within the defense and information technology sectors to suggest actors affiliated with the Chinese government are still active.

China has largely avoided conducting any cyber campaigns that would resemble outright cyberwarfare and has largely relied on cyberespionage instead. Cyberespionage is the use of cyber-attacks for theft of classified or intellectual property information. China uses cyberespionage techniques as a useful tool in helping the country to reach its developmental goals of advancement in science and technology, military modernization, and economic growth. China has expressed intent in establishing a presence in cyberspace as a means of defending national interests.

In recent years, China has focused mainly on the acquisition of sensitive U.S. technology and trade secrets. In 2018, two alleged members of Advanced Persistent Threat 10 (APT10), a Chinese cyber espionage group, were charged with allegations of computer intrusion in multiple countries between 2006 and 2018. The two individuals allegedly conducted computer intrusion campaigns that targeted intellectual property and confidential business information. Groups named as APTs generally refer to nation-state operators who receive steady funding for new and emerging technologies to leverage against targets.

Unlike private cyber actors, they do not have to rely on generating income and may have access to steady hardware and software supplies. These groups may also receive advanced training through government programs or universities more readily. Multiple APT groups may be active at any given time, targeting various entities or furthering national goals. Attribution to these groups is tricky; they often operate independently from recognized government agencies and the sources of their income are obfuscated.
APT10 has targeted engineering, aerospace, and telecom firms in alleged support of Chinese national security goals for roughly a decade. The group is believed to be linked to China’s premier intelligence and security agency, the Ministry of State Security (MSS). MSS commonly targets entities in the U.S., Europe, and Japan. APT10 has been known to use spearphishing (targeted phishing) attacks to deploy different forms of malware, including Scanbox, Sogu, Poison Ivy, and PlugX.7,8

Although APT10’s actions are notorious globally for their cyber activities, China’s cyberespionage network is vast, varied, and comprised of military, security, and civilian components. In April 2019, the U.S. Department of Justice charged two individuals suspected of being members of APT10 with economic espionage and conspiring to steal trade secrets from General Electric (GE). One of the individuals, based in New York, was an employee of GE and allegedly stole multiple electronic files with sensitive information regarding the company’s turbine technologies. This information was then passed to an individual based in China with the intention of having the information shared with a number of Chinese companies to advance their business interests.9

This cyber-enabled theft of American-made intellectual property and sensitive information is a serious counterintelligence threat for the U.S. with no signs of stopping. Organizations that suspect they may have been targeted by China-affiliated actors should take steps to harden their cyber defenses and contact the Internet Computer Crime Center (IC3) at www.ic3.gov or the Cyber and Infrastructure Security Agency (CISA) at www.us-cert.gov.

China’s cyberespionage network is vast, varied, and comprised of military, security, and civilian components.

---

1 https://fas.org/sgp/crs/row/IN10376.pdf
7 https://blog.malwarebytes.com/cybercrime/2019/01/advanced-persistent-threat-files-apt10/
8 https://www.freeeye.com/current-threats/apt-groups.html
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 that is sent out twice weekly. If you are interested in receiving The FIPC Dispatch, let us know.

To sign up for the FIPC Dispatch, visit secureflorida.org and click the Sign up for The FIPC Dispatch link at the bottom of the homepage or send an email to FIPC@fdle.state.fl.us.

This content is intended as an informative compilation of current/open-source cyber news for the law enforcement, cyber intelligence, and information security communities.

**Maze ransomware was behind Pensacola “cyber event,” Florida officials say**

https://arstechnica.com/information-technology/2019/12/pensacola-city-government-was-hit-by-maze-ransomware-was-data-stolen/

- Ransomware that struck the city of Pensacola in December 2019 was the same malware used in an attack against a private security firm.
- The malware has been identified as Maze, ransomware that has been distributed via spam email campaigns in Italy.
- The threat actors advise that they steal sensitive information with the threat of posting it online as leverage to force organizations to pay the ransom.

Analyst Note: Stealing data that is encrypted by ransomware is not a common practice, so this presents a new strategy to watch out for. Updating security software and firmware, backing up your files, and training users to spot phishing is the best defense against ransomware. Remember: paying a ransom is no guarantee the perpetrators will send your decryption key.

**Office 365 Admins Targeted by Ongoing Phishing Campaign**


- The phishing campaign actively targets Microsoft Office 365 administrators with the goal of compromising entire domains to create accounts and deliver future phishing emails.
- The phishing emails are designed to look like they come from Microsoft. The emails are able to bypass spam filters as they come from compromised Office 365 accounts.
- The attackers did not target a particular industry sector, but did direct attacks at a certain user level.

Analyst Note: These types of spear phishing attacks are becoming more common. Email administrators have access to a lot of valuable resources that threat actors want, so it is imperative that they receive training to spot social engineering schemes and enable multifactor authentication on their accounts.
Pre-installed apps on low-end Android phones are full of security holes


- A DHS-funded report uncovered 146 apps, which come installed on inexpensive phones with Android operating systems, would eavesdrop using the microphone, change permissions, or transmit data back to the manufacturer without notifying the user.
- Some apps come bundled as part of larger app suites.

Analyst Note: It can be hard to control your security if your device is compromised before you even get it. Before deciding on a new device, research the apps that come with it. Consider permissions carefully and uninstall any apps you don’t need or use.

Here are the most popular robocall scams and how to avoid them


- The most common robocalls claim that your information was on debit cards sold illegally, your identity has been stolen, or that irregular activity has been flagged on your bank account.
- The best defense is to let unknown numbers ring without picking them up.
- The vast majority of U.S.-based robocalls originate in California and Florida.

Analyst Note: Robocalls can be bothersome but can also cost you if you fall for a scam. Screening your calls by letting them go to voicemail or using screening software available from your mobile carrier can help you spot trouble. Never give any sensitive personal information over the phone; hang up and find an official number to the institution calling you and call them to resolve any disputes.

Details of Attack on Electric Utility Emerge


- A Distributed Denial of Service (DDoS) attack in March 2019 impacted generating facilities and the electrical grid in three western U.S. states.
- An unpatched vulnerability in the utility provider’s firewalls was the target of the attack.
- The attack affected communications but did not cause service interruptions to any customers.

Analyst Note: Always keep up to date on manufacturer security and firmware patches. A lot of the malware infections seen after a patch is issued are due to lagging patch implementation.
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.

https://secureflorida.org/SF/The-Beacon

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

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

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

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

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