The Beacon

Florida Fusion Center #19-168 | Cyber and Critical Infrastructure Report | July 2019, Issue #20

Summary

Security When It Counts -
With the official population count on the horizon, we examine some possible threats to the 2020 U.S. Census.

A Little Off the Top: The State of Card Skimming -
We take a look at the current card skimming landscape and how you can protect yourself from having your credit or debit card compromised.

Dark Web Out of the Dark -
A deep dive into the dark web and its history, protocols, and uses.

Stalkerware Beware -
Certain apps can be installed on a cell phone to allow all activity to be tracked. Learn how to protect yourself from these invasive programs.

Cybersecurity and Online Gaming -
Our guide for keeping kids safe while videogaming.

Spearing Industrial Security: A Look at Triton Malware -
A look at how Triton targets the safety controls in industrial settings and the potential deadly implications.

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

Editor's Corner

Where Are You Leaving Your Data?

Recently, a number of city governments have found themselves at the mercy of malicious cyber actors and the results have been understandably concerning. In March 2018, the City of Atlanta, Georgia, suffered a crippling ransomware attack (later identified as SamSam). The ransomware impacted more than a third of the city's 424 necessary programs. In the end, the city spent millions of dollars in recovery efforts and lost many devices that couldn't be recovered, while the police department permanently lost their dash cam recordings.[1]

In 2019, the cities of Stuart and Lake City, Florida, were impacted by a ransomware virus that reports indicate most likely made it onto the city's servers through a phishing email. The Ryuk ransomware forced city employees to switch to paper and pencil while attempts were made at recovery. The outage impacted city services, police, and fire departments. Stuart refused to pay the ransom, meaning that the encrypted files may never be recovered and the network would need to be rebuilt; Lake City eventually paid the ransom.[2] The city of Baltimore, Maryland, also suffered a ransomware attack in May 2019, that affected voicemail, email, a parking fines database, and system used to pay water bills, property taxes, and vehicle citations. The city also refused to negotiate with the perpetrators. Unlike some cities hit by ransomware, Baltimore did not have an insurance policy that covered cyber incidents, and the recovery has been slow.[3]

There are several quandaries concerning ransomware that affect public entities. A ransomware fund is not usually a part of the budget, so when it does strike, there is not an account to pull money from quickly. Most ransomware demands payment in Bitcoin (or a similar cryptocurrency), and most entities do not keep this currency on hand. It also presents an ethical dilemma for government entities, as payment could include further criminal activities and also serve to make agencies attractive targets for future attacks.

While such policy considerations are up for debate at the executive level, municipalities as well as private sector companies are encouraged to remember that the best defense is not to be caught flat-footed. A robust and diverse antivirus solution, along with keeping up with updates, will thwart many ransomware attempts. Network segmentation and regular backups (stored separately) means that a network can be brought back up with minimal losses.[4] Paying the ransom is ill-advised, as the criminals responsible may elect not to send the decryption key or may ask for more money.

Cybercriminals may elect to continue targeting municipalities and cities in the future, knowing that the loss of public services will apply pressure to managers to remediate the fastest way possible: paying the ransom. It's more important than ever to make sure public and private cybersecurity posture is rigid enough to defend against these threats.

[1] https://www.engadget.com/2018/06/06/atlanta-ransomware-attack-struck-mission-critical-services/
[2] https://www.tcpalm.com/story/news/local/martin-county/2019/04/22/city-halls-ransomware-attack-may-linked-phishing-email-scam-ryuk/3540067002/
[3] https://nakedsecurity.sophos.com/2019/05/23/the-city-of-baltimore-is-being-held-hostage-by-ransomware/
[4] https://www.us-cert.gov/ncas/tips/ST19-001

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

Cyber Threats

Security When It Counts

With the focus in 2020 being on election cybersecurity, it may be easy to overlook another event happening the same year: the 2020 Census. The official headcount of people residing in the U.S. isn't just a survey to find out how many people are in the country; the Census is used to determine the distribution of U.S. Representatives across states, redraw district boundaries, and allocate funding for areas in need. The Census also provides a lot of demographic data, and it is considered the leading source of statistical information on the U.S. population.[1] The Census occurs every 10 years, and the next Census will be the most technologically advanced count to date. There are plans for internet-based self-reporting, enumerators (Census Bureau members who canvas to record data) equipped with mobile devices, and more traditional information collection methods (paper records) being used to collect data.[2]

Technological advancements may make the Census more efficient and perhaps more accurate, but can also leave it open to cyber threats. The importance of the Census in determining funding and the distribution of Representatives could make it an attractive target for data tampering. With the online collection portal being used for the first time, threat actors may have potential access to tamper with results if the repository databases are not adequately secured.[3] Bad actors could also hamper the collection of data, such as happened in Australia in 2016 when the government suffered a Distributed Denial of Service attack while attempting to upload census information to their servers.[4] Further, disinformation campaigns, similar to the ones that plagued the election in 2016, could attempt to undermine public trust in the results of the Census.[5] While the Census may seem like nothing more than an official survey, the results often show a snapshot of the U.S.'s changing demographic. Some of these results often cause controversy and could represent social pressure points that could be exploited.[6]

Exposure of respondent information could also lead to identity theft. While the Census does not collect information like Social Security numbers or other important identifying numbers, it does collect names, sex, dates of birth, race and ethnicity information, addresses, and telephone numbers.[7] This is a wealth of information that could be used by nefarious actors for other purposes. Public confidence in the federal government is considerably low for data protection. Leaks and breaches in recent years from the Office of Personnel Management (2013) and the Federal Emergency Management Agency (2019) that exposed millions of sensitive records, plus the stability problems of the healthcare.gov site (2013), have given many researchers doubts in the process of online data collection.[8] The U.S. Census Bureau has responded to these concerns, noting that the data will be stored on Amazon Web Services' GovCloud, which has systems that will continuously monitor incoming data for suspicious activity.[9]

Respondents to the survey should also be wary of social engineering campaigns that may seek to gain information or money from them. The U.S. Census Bureau warns to be on the lookout

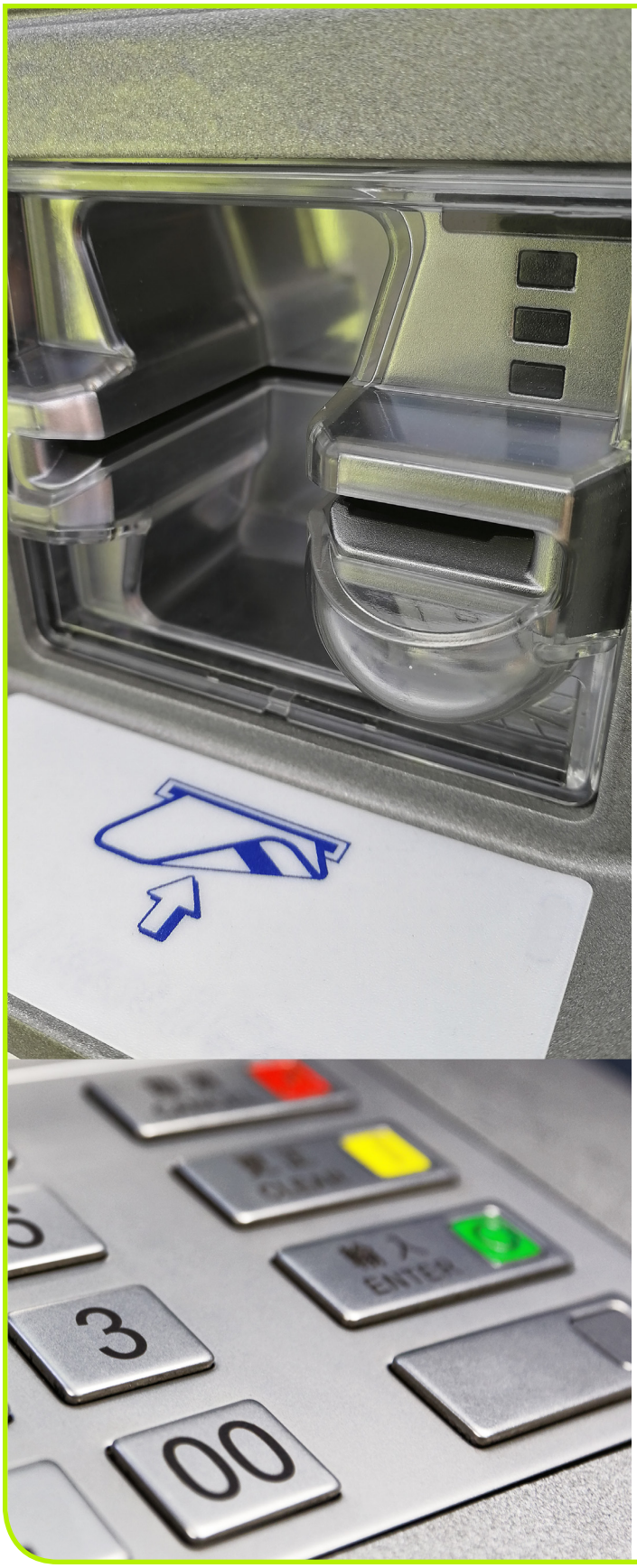
for malicious actors posing as someone from the Bureau asking for Social Security numbers (the Census does not ask for it and it is not needed for any part of the survey), money or donations, anything on behalf of any political party, bank or credit card information, or your mother's maiden name (which could be used to verify identity).[10] If you suspect fraudulent activity, they ask that you verify mailings come from a return address in Jeffersonville, Indiana, or contact their regional office in your area. If someone calls or shows up at your home to complete the survey and you want to be sure that they are legitimate, you may contact the National Processing Center via phone (1-800-523-3205) or email (NPC.Call.Center.Info@census.gov). Always check to make sure the person has a valid U.S. Census Bureau badge before disclosing any information about you or your household. For emails that you suspect are fraudulent, they can be forwarded to ois.fraud.reporting@census.gov.[11, 12]

The decennial U.S. Census can provide a wealth of information about the American population, but just as the U.S. Census Bureau works to secure the collection of the data, ordinary citizens must be vigilant to not give that information to bad actors as well.

[1] https://www.census.gov/topics/population.html
[2] https://www.fedscoop.com/census-cybersecurity-protections-2020-count/
[3] https://www.theatlantic.com/politics/archive/2018/07/census-2020-russia-citizenship/566384/
[4] https://www.washingtonpost.com/local/social-issues/2020-census-likely-target-of-hacking-disinformation-campaigns-officials-say/2019/03/31/12e8d416-522d-11e9-88a1-ed346f0ec94f_story.html?noredirect=on&utm_term=.4b511cbc54b3
[5] https://www.theatlantic.com/politics/archive/2018/07/census-2020-russia-citizenship/566384/
[6] Ibid.
[7] https://www.census.gov/history/www/through_the_decades/index_of_questions/2010.html
[8] https://www.washingtonpost.com/local/social-issues/2020-census-likely-target-of-hacking-disinformation-campaigns-officials-say/2019/03/31/12e8d416-522d-11e9-88a1-ed346f0ec94f_story.html?noredirect=on&utm_term=.4b511cbc54b3
[9] Ibid.
[10] https://www.census.gov/programs-surveys/are-you-in-a-survey/fraudulent-activity-and-scams.html
[11] Ibid.
[12] https://www.census.gov/about/npc.Contact_Us.html

A Little Off the Top: The State of Card Skimming

You may have seen alerts recently regarding card skimming devices on gas pump card readers and Automated Teller Machines (ATM), or received a new credit or debit card with an improved security chip to prevent fraud. Card skimming has become a real concern for financial institutions and consumers alike. The average ATM skimming incident costs $600 per card and a single compromised gas pump can capture data from 30 to 100 cards a day.[1] Skimmers are small devices that can fit over a legitimate card slot or be placed inside the slot and remain hidden from view. Card skimming initiates when a person scans their credit card or debit card at a gas pump or ATM. The skimmer is a small device that captures the data contained in the magnetic strip on the back of a debit or credit card. The skimmer is placed over the card swipe insert device



on gas station pumps, ATMs, or other card reading devices. With skimmers implanted in ATMs, small hidden cameras accompany the skimmer to capture entry of the personal identification number (PIN).[2] The skimmer can be external or internal, which can make it difficult to detect.[3] The data contained in the magnetic stripe includes the cardholder's full name, the card expiration date, and the credit card number; all of which is required to make purchases or withdraw money.[4] Threat actors sometimes use Bluetooth-enabled skimmers to transmit the information to their cell phones via text messages, so as to avoid being caught retrieving the data at the site of the skimmer. Thieves use this information to create new counterfeit cards or make purchases online with the card information (which doesn't require the use of a physical card).[5] "Shimming" is a newer technology that allows a small skimmer device to read data off of the new chip-based cards.[6] These smaller skimmers are very hard to detect, but luckily they are also very rare.[7]

Since 2015, approximately 2,250 devices were identified by or reported to the Florida Department of Agriculture and Consumer Services throughout the state.[8] South Florida seems to be heavily impacted by credit card skimming, with Broward County accounting for more than a third of the cases. Miami-Dade and Palm Beach County were also among the top counties for skimmers.[9] There have been some notable recent cases in Florida, some of which have been linked to known organized crime groups:

> In 2019, a judged sentenced a couple from Miami, FL, to prison for stealing hundreds of account numbers using skimmers placed in gas pumps. Skimmers were placed in a gas pump in Virginia and a laptop was used to extract the data. The

subjects then created fraudulent fake cards using the stolen information.[10]

In 2018, two subjects were arrested by the Okaloosa County Sheriff's Office for placing skimmers in ATMs. The subjects traveled from state to state installing the devices and were identified on surveillance video.[11]

These devices can be difficult to spot, but there are a few ways that consumers can protect themselves from falling victim:

- Pay cash or use your credit card.
- When withdrawing cash at a bank, go inside to a teller or use ATMs located inside the bank.
- Discontinue a transaction if you encounter resistance when inserting your card into a reader.
- Monitor your bank statements and look for suspicious charges.[12]
- Contact the merchant, your bank, and/or card issuer if you suspect your card has been compromised.[13]

While credit and debit cards have made checkout faster, easier, and more secure, it's important to keep in mind that bad actors are attempting to gain access to that information. Exercising caution while using card reading devices can keep you secure from falling victim to a skimmer.

[1] https://www.aba.com/Products/Endorsed/Documents/Rippleshot-State-of-Card-Fraud.pdf
[2] www.thebalance.com/how-credit-card-skimming-works-960773
[3] www.amarillo.com/news/20190303/swiping-data-apd-cautions-about-credit-card-skimmers-found-at-gas-pumps-atm.
[4] krebsonsecurity.com/category/all-about-skimmers/.
[5] www.thebalance.com/how-credit-card-skimming-works-960773.
[6] www.consumerreports.org/scams-fraud/thieves-get-craftier-with-skimmers-debit-cards-credit-cards/
[7] https://www.creditcards.com/credit-card-news/new-card-skimming-is-called-shimming.php
[8] www.wuft.org/news/2019/03/06/ag-commissioner-nikki-fried-warns-of-widespread-gas-pump-skimming-fraud/
[9] www.orlandosentinel.com/business/os-bz-credit-card-skimmers-20181108-story.html.
[10] https://www.justice.gov/usao-wdwi/pr/florida-man-sentenced-9-years-fraud-scheme-involving-gas-pump-skimmers
[11] www.nwfdailynews.com/news/20180510/romanian-fraudsters-caught-after-installing-atm-skimmers
[12] https://www.creditcards.com/credit-card-news/8-ways-protect-against-atm-skimming-1282.php
[13] https://www.creditcards.com/credit-card-news/new-card-skimming-is-called-shimming.php

Cyber Highlights

Dark Web Out of the Dark

It seems like every time any cybercrime happens, the term "dark web" inevitably comes up. The name itself sounds nefarious and evil, but mainly refers to the dark web's ability to obfuscate the identity of who is on it and who is using it. In popular culture, it's displayed as a seedy place to find illegal goods, hire a hitman, and as a hangout for hackers. Before we can begin to understand the dark web, we must first understand where it fits in in the internet ecosystem as a whole.

The internet that we are most familiar with is called the "surface web;" this term refers to any internet page that you can find using a search engine (Google, Bing, etc.). It makes up about 10 to 16% of total internet sites and may also be known as the "Indexed Web" (because sites that can be found on search engines are said to be "indexed").[1] The Deep Web is the next subset of the internet and also the largest. It makes up the rest of the internet (84-90%) and refers to pages that cannot be indexed by search engines.[2] Think of it this way: If you Google your bank's website, you will find the bank's main page (a surface web page), but once you log in to see your account statement, you have accessed a Deep Web page (that is, your specific account page that cannot be accessed through Google). The Deep Web includes just about every site that you need to log into (like email, banks, social media, and the shopping carts of retail sites) along with company intranets; 95% of it is publicly accessible somehow.[3] The dark web is contained within what is categorized as the Deep Web, but they are not quite the same thing.

In order to access the dark web, you need specialized software called a router (note: this is different from the hardware router you use to access the internet at home). This means that, without this software, you would not accidentally stumble onto a dark web site. The dark web is a completely separate network from the surface web, and navigating it requires the use of different protocols from what mainstream browsers use. One of the most common dark web routers is The Onion Router (more commonly known at Tor), which sets up the specific connections you need to access the dark web.[4] Sites on the Tor network may have the appearance of any regular internet site, though their addresses end in .onion instead of .com or .net.[5] The internet is a relatively new phenomenon in human history and it is only recent generations that can't remember a time when it wasn't available, but the dark web is even younger than that. Technically, the most basic routing protocols that it runs on were born along with the internet in the

1980s. The U.S. Naval Research Lab (NRL) first started researching "onion" routing in 1995, patented the concept in 2000, and released the first codes under an open-source license in 2003.[6] In 2004, the Office of Naval Research (ONR) cut funding, but the NRL continued to work on the project internally along with cooperation from the Electronic Frontier Foundation (EFF). Finally, in 2006, Tor became a non-profit organization and is obligated to disclose its funding.[7] It was originally developed as a way to safeguard U.S. intelligence communication online.[8] But why is it called "onion" routing?

The name isn't just a random moniker, but rather a metaphor for how the routing happens. The dark web, like the rest of the internet, is made of up a network of servers. On the surface web, the entire route that your information packet takes to get to the destination is visible to anyone (unless the information is encrypted, such as through a VPN). With onion routing, it's helpful to visualize an onion with its many layers; the center is the information or request that you're sending and its contents are fully encrypted. Only the destination site can see this data. The header of the onion packet contains routing information for each leg of the journey between your computer and the destination that can be decrypted in "layers". As the packet reaches each server along the route, a portion of the header is unencrypted and read for routing, then discarded. The server (called a relay) only sees the last point the packet came from and the next point to send it to. The process repeats as the packet reaches each relay, until it reaches its final destination.[9] The relays change each time you travel across the dark web, so a pattern cannot be established. The servers are located across the globe, meaning that you may be taking a very roundabout way to get to the site you're trying to access. You may notice that it takes a little longer to get to a site than when using a conventional browser, and that's because your usual browser is taking the shortest route possible while Tor (and other dark web browsers) are bouncing between relays that are potentially in other countries.[10]

Perhaps the most well-known use for the dark web is for visiting online marketplaces. At first glance, these sites seem indistinguishable from any other mainstream retail site. Independent vendors listed their wares along with prices, much like eBay or Amazon. The most striking difference between those sites and their dark web counterparts are the illegal and illicit products and services for sale. There have been several high-profile takedowns of these types of sites over the years, including Silk Road in 2013,[11] Alphabay in 2017,[12] and Wall Street Market and Valhalla

in 2019.[13] But for every marketplace that gets taken down, new ones sprout up to take its place. The advent of cryptocurrency has only spurred the growth of these sites by making tracking both vendors and buyers more difficult (but not impossible).[14] In 2016, a dark web site that offered hitman-for-hire services, Besa Mafia, was hacked and revealed to be a scam. Potential customers paid Bitcoin with the expectation that their targeted person would meet an unnatural end, unaware that there were no hitmen and the person behind the site was stealing their money.[15]

It certainly seems as though the dark web is full of illegal and, perhaps, even frightening activity, but there are legitimate uses for it. A lot of people use Tor to surf the internet while protecting their identity; not just for nefarious purposes, but to make sure they are not being tracked by websites. Additionally, people living or working in countries that have restrictive internet access may use the dark web to visit sites they may not be able to visit normally (several large social media sites, for example, maintain a .onion site).[16] Similarly, journalists leverage the encryption and anonymity of the dark web to protect their identity, as well as that of their sources.[17] Notably, the U.S. federal government has been the source of a majority of The Tor Project's funding each year since it was created.[18] This may seem surprising, but remember that the dark web was created in part by a U.S. government entity that was attempting to secure intelligence communications. Why might the U.S. want to fund a program this type of program? The dark web provides many opportunities for testing and research, as well as blanketing intelligence communications and investigative activities that need to be safeguarded for the protection of our nation with the same level of anonymity that cybercriminals employ. Quite simply, it is a powerful tool, even if it has its dark side.

Despite all the attention paid to the dark web, it is relatively small. A recent mapping of .onion sites found roughly 55,000 domains, of which only about 8,400 were active. Of those, only about 100 were active in criminal activities (criminal forums, dark net markets, etc.).[20] If you've considered using a dark web or Tor connection with privacy in mind, but you aren't sure you'd like the association it carries, there are several things you can do. The easiest method would be to use a Virtual Private Network (VPN) service, which will encrypt all of your traffic. If you're worried about search engines tracking you

for marketing purposes, there are certain engines available that claim to not use these methods. Additionally, there are a number of fully encrypted email services that will secure your data, should that be a concern.[21]

With all of this in mind, it is wise to remember that no method of obscuring your identity is ever fool-proof and there are many risks associated with venturing onto the dark net.

[1] https://resources.infosecinstitute.com/what-is-the-difference-between-the-surface-web-the-deep-web-and-the-dark-web/#gref
[2] Ibid.
[3] Ibid.
[4] https://computer.howstuffworks.com/internet/basics/how-the-deep-web-works4.htm
[5] https://www.csoonline.com/article/3287653/what-is-the-tor-browser-how-it-works-and-how-it-can-help-you-protect-your-identity-online.html
[6] https://www.informationsecuritybuzz.com/news/secret-history-tor/
[7] Ibid.
[8] https://www.webhostingsecretrevealed.net/blog/web-tools/tourist-guide-to-dark-web-accessing-the-dark-web-tor-browser-and-onion-websites/
[9] https://www.tomsguide.com/us/what-is-tor-faq,news-17754.html
[10] https://www.csoonline.com/article/3287653/what-is-the-tor-browser-how-it-works-and-how-it-can-help-you-protect-your-identity-online.html
[11] http://nation.time.com/2013/10/04/a-simple-guide-to-silk-road-the-online-black-market-raided-by-the-fbi/
[12] https://www.theverge.com/2019/2/17/18226718/alphabay-takedown-drug-marketplace-federal-arrest
[13] https://www.wired.com/story/dark-web-drug-takedowns-deepdotweb-rebound/
[14] https://www.theverge.com/2019/2/17/18226718/alphabay-takedown-drug-marketplace-federal-arrest
[15] https://www.vice.com/en_us/article/3d434v/a-fake-dark-web-hitman-site-is-linked-to-a-real-murder
[16] https://www.darkowl.com/blog/2017/darknet-series-who-uses-the-darknet-and-why
[17] Ibid.
[18] https://www.businessinsider.com.au/claims-tor-funded-by-us-government-agencies-2018-3
[19] https://www.washingtonpost.com/news/the-switch/wp/2013/09/06/the-feds-pays-for-60-percent-of-tors-development-can-users-trust-it/?utm_term=.a1415412242f
[20] https://www.cyberscoop.com/dark-web-marketplaces-research-recorded-future/
[21] https://www.webhostingsecretrevealed.net/blog/web-tools/tourist-guide-to-dark-web-accessing-the-dark-web-tor-browser-and-onion-websites/

Stalkerware Beware

In an age where privacy is a top priority, we often do not realize that stalking has evolved with modern technology to become stealthier and harder to detect. Stalkers no longer have to creep in the bushes or follow you in the streets to know everything about you. Simply downloading and installing a stalkerware app on a phone gives them access to everything.

Stalkerware, a form of spyware, is primarily used for spying. Advertised as "legal spyware", apps (such as FlexiSpy or iSpyoo) have the

capability to log everything you do on your device; from the websites you visit, to the texts you send and calls you make. Some apps also have the capability to allow the user to turn on your camera and see what you are doing in real time.[1] The program will send all of this information to whoever installed the app.

Legally-registered companies advertise these apps as a way to monitor your child or track what your employee is doing on company-issued work devices. However, sometimes these apps are bought by people with malicious intent, such as a jealous ex or a suspicious or abusive spouse. The difference between a legitimate monitoring app and a stalkerware app is that a legitimate app lets you know that you are being watched, whereas stalkerware apps hide themselves among other apps on your device without showing any signs that they have been installed.[2]

Most stalkerware apps require a user to install it on your device (meaning they must be in possession of it); however, on rare occasions a stalkerware app can be installed by an infected link sent to you via email or text if you click on it. If your device has a stalkerware app installed on it you may start noticing some performance issues. Stalkerware uses a lot of central processing unit (CPU) power to stay hidden and continually run in the background of your device. Due to this, your device may lose battery charge faster than usual or begin to lag.[3]

As if being stalked wasn't bad enough, a number of the developers of these apps have suffered data leakage from poorly configured servers, spilling victims' personal data onto the internet. Data is also usually available to the employees of the app makers, not just to the stalkers alone.[4]

Since most of the time, a potential stalker must have access to your phone to install the software, the best way to thwart them is to set your phone to lock and have a good, strong password set up. Having a strong and reliable password is the first way you can protect yourself. Passwords that are at least fifteen characters long and incorporate random uppercase and lowercase letters, numbers, and special characters will give you a complex combination that would take years to crack.[5] If you are having trouble coming up with a strong password or your password is not strong enough, you can use password generating websites to create a unique password. Remember to NEVER share your password with anyone.

Regularly check the apps that are installed on your devices. Deleting the ones that you no

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

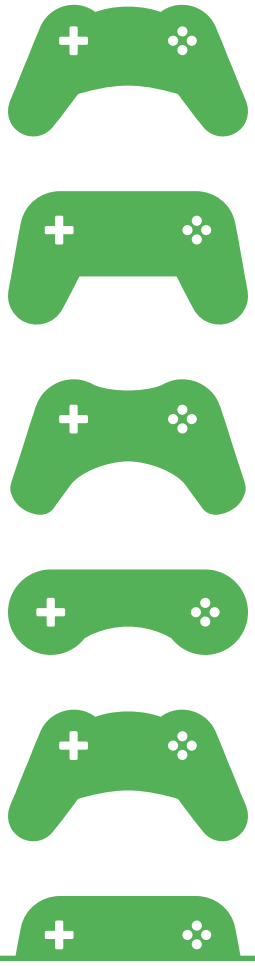
longer need will help you pay attention to what you have installed on your devices as well as free up memory space. Look for strange apps that weren't there before (remember that some stalker apps try to hide and will not be obvious) or processes that are taking up a lot of memory.

Use a reliable anti-virus provider to scan your phone for malicious apps. This will also keep your devices safe from various types of viruses and malware. Most antivirus providers detect stalkerware and alert you of a potential threat to your sensitive information, though they may not alert you to the presence of tracking apps that don't attempt to hide themselves. This is another reason why it's important to check your phone regularly and be aware of what's on it.[6]

[1] https://callnerds.com/spot-remove-stalkerware/
[2] https://www.zdnet.com/article/over-58000-android-users-had-stalkerware-installed-on-their-phones-last-year/
[3] https://callnerds.com/spot-remove-stalkerware/
[4] https://www.zdnet.com/article/over-58000-android-users-had-stalkerware-installed-on-their-phones-last-year/
[5] https://www.cnet.com/how-to/the-guide-to-password-security-and-why-you-should-care/
[6] https://www.zdnet.com/article/over-58000-android-users-had-stalkerware-installed-on-their-phones-last-year/

Cybersecurity and Online Gaming

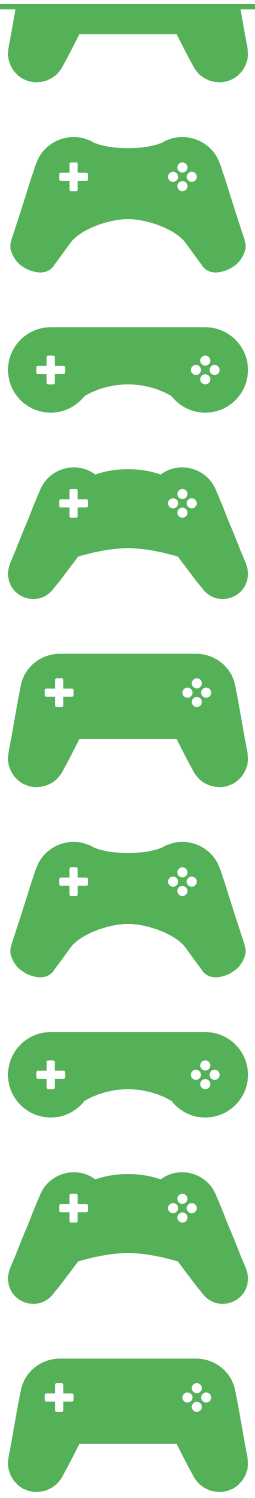
Gaming: a popular pastime for all ages that seems to only be getting more popular as technology advances. Gone are the days where all relevant players needed to be present in one room for a game to take place. Utilizing internet connectivity, a group of players is capable of raiding a dungeon together, even though they may be miles and time zones apart from each other. While games can be popular with players of any age, a percentage of gamers are children, and parents should be aware that there are potential dangers in the online games their children may be playing.



Before a child has a chance to play an online game, parents should know what the game is rated. Rating systems vary from country to country, but the U.S. primarily uses the Entertainment Software Rating Board (ESRB), in addition to recommended age-range systems for some apps. The ESRB ratings "provide concise and objective information about the content in video games and apps so consumers, especially parents, can make informed choices.[1]" They provide a letter rating that suggests an appropriate age the player should be to play the game, content descriptors the letter rating is derived from, and an elements list that highlights interactive/online elements of the game.[2] The ESRB is a fairly detailed, but not totally comprehensive, alert to what a game contains; parents can use this as a baseline when considering whether a game is appropriate for their child. Mobile app stores employ a system that similarly has a recommended age for use,[3] though parents should always do their own research into any game or

app and decide for themselves if it's appropriate for their child to play.

Most games children are likely to play online have some form of communication function, whether the game focuses more on a one-on-one environment, a massively multiplayer environment, or anything in-between. Children can be at risk of seeing or hearing things parents may not want them to see or hear. Children may also be presented with opportunities to say things they shouldn't say, such as information regarding user accounts or personal information about themselves or others. Parents can't dictate what other people can or can't say to their kids, but a combination of a game's built in filtering controls as well as parental controls on the consoles themselves can help cut down on what toxic material children are exposed to.[4] Most games also have systems in place for reporting chatter, both text and speech-based, that goes against their terms of service (which commonly includes inappropriate or bullying behavior).[5] Children should act with the same discretion they would in any chatroom. Remind them not everyone is who they say they are; don't give out any personal information; and if they see or hear something that makes them feel uncomfortable, they should document the exchange to the best of their ability (safely), quit the game, and alert an adult.



Parents should also be aware of where the games their children play come from. Hard copies of games are still sold in stores, but games and apps can also be purchased and downloaded directly onto a console. To be safe, children and parents should only download from trusted and verified sources; not doing so introduces the potential for buying and downloading pirated software and/or for malware to come bundled with the download. This also goes for any "cheats" or "add-ons" that can be applied to a game: use only trusted and verified sources.[6]

In order for children to enjoy their games and for parents to know they're being enjoyed as safely as possible, parents should continuously make an effort to communicate with their children regarding them. Where are they buying and downloading their games from? Are they playing with friends or with strangers? Are they talking to other players and are they being talked to? What are they talking about? While there are opportunities for children to get into trouble playing games, taking proactive steps to ensure safety can keep it a fun and wholesome pasttime.

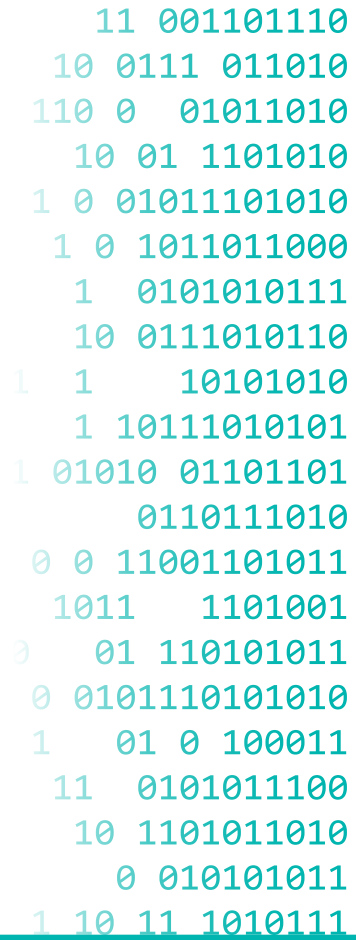
[1] https://www.esrb.org/ratings/ratings_guide.aspx
[2] Ibid.
[3] https://support.google.com/googleplay/android-developer/answer/188189?hl=en
[4] https://www.consumer.ftc.gov/articles/0270-kids-parents-and-video-games
[5] https://www.theguardian.com/games/2018/aug/17/tackling-toxicity-abuse-in-online-video-games-overwatch-rainbow-seige
[6] https://www.wired.com/2016/12/never-ever-ever-download-android-apps-outside-google-play/

Critical Infrastructure

Spearing Industrial Security: A Look at Triton Malware

Triton has been dubbed "the world's most murderous malware" by cybersecurity experts because of its potential to impact safety systems that protect the public from potentially lethal disasters.[1] The malware was detected after it infected a petrochemical plant in Saudi Arabia in 2017, but it was not able to cause damage as the malware's own activity shut down the facility.[2] Since this malware affects safety control systems, successful deployment of Triton could have potentially led to the release of deadly hydrogen sulfide gases or caused explosions, adding real casualties to a cyberattack.[3]

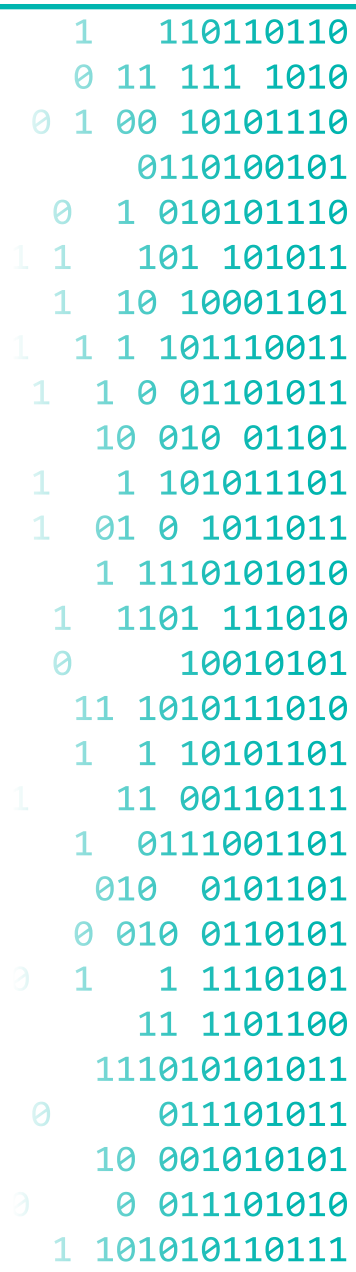
Triton has yet to be successful in carrying out an attack, but the actors behind recent attempts appear to be intent on targeting critical infrastructure that have the potential for serious implications. As of 2019, firms that specialize in industrial cybersecurity have found evidence that the hacking group behind Triton is using the same technology to research targets in North America amongst other locations.[4] A private cybersecurity analysis firm has asserted that Russia may be behind the Triton malware, but this has not been confirmed.[5]



How it works:

Triton, also known as Trisis (named for the Triconex safety controller model that it targets), is a form of malware that targets industrial control systems (ICS). Although Triton has only been documented a few times, ICS compromise is not uncommon. In 2018, a study of ICS cybersecurity at manufacturing, construction and engineering, and oil and gas facilities found that 54% of responding companies experienced an ICS security incident.[6] Triton is similar to the Stuxnet malware, which targeted Iranian nuclear facilities in 2010, and CrashOverride, which targeted Ukraine's power grids in 2016.[7]

Triton malware attacks ICS in order to tamper with emergency systems and cause process shutdowns.[8] Once this malware has infiltrated a network, it is designed to overwork systems leading to an accelerated rate of wear and tear.[9] In the incident at the Saudi petrochemical plant, the actors behind Triton accessed the industrial plant's network nearly a year before gaining access to the Safety Instrumented System (SIS), slowly and patiently deploying parts of the malware as well as conducting network reconnaissance and moving laterally across systems. This careful and extended deployment process made changes to the system more difficult to detect.[10]



Who is targeted:

This malware is designed to target and compromise the SIS and distributed control systems of oil, gas, nuclear, water treatment, transportation, and manufacturing facilities. These critical safety systems prevent catastrophic industrial incidents by returning systems to normal levels or shutting them down entirely when they detect dangerous conditions.[11] With access to the control systems of these infrastructure components, threat actors had the ability to tamper with and cause physical damage to these critical safety systems.

Notable Events:

In 2017, the first petrochemical plant to be attacked in Saudi Arabia was targeted by Triton malware. The attack was meant to physically damage the site but was unsuccessful in carrying out the attack. Instead, a bug in the malware's coding led to the plant entering a fail-safe state and abruptly shutting down. It is believed that the Triton malware first infiltrated the corporate network in of the plant in order to gain access to the industrial network.[12]

In April 2019, a second site reported evidence of activity by the Triton threat group. The company that owns the plant declined to name the plant name, location, or year of the attack.[13]

Mitigation:

Standard security procedures like complex passwords and vulnerability patching are recommended to protect ICS systems. Facilities employing Triconex safety control systems should take extra precautions to ensure that their network is secured. Additionally, security measures like segregating industrial networks from business networks and restricting ICS user privileges can help in protecting these systems from compromise.[14]

[1] https://www.technologyreview.com/s/613054/cybersecurity-critical-infrastructure-triton-malware/
[2] https://www.scmagazine.com/home/security-news/malware/second-triton-trisis-critical-infrastructure-attack-spotted/
[3] https://www.technologyreview.com/s/613054/cybersecurity-critical-infrastructure-triton-malware/
[4] Ibid.
[5] Ibid.
[6] https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html
[7] https://www.technologyreview.com/s/613054/cybersecurity-critical-infrastructure-triton-malware/
[8] https://www.zdnet.com/article/triton-hackers-return-with-new-industrial-attack/
[9] https://www.thethreatreport.com/triton-hacker-group-attacks-saudi-petrochemical-company-again/
[10] https://www.scmagazine.com/home/security-news/malware/second-triton-trisis-critical-infrastructure-attack-spotted/
[11] https://www.technologyreview.com/s/613054/cybersecurity-critical-infrastructure-triton-malware/
[12] https://www.zdnet.com/article/triton-hackers-return-with-new-industrial-attack/
[13] https://techcrunch.com/2019/04/09/triton-malware-strike/
[14] https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/triton-malware-spearheads-latest-generation-of-attacks-on-industrial-systems/

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

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 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.

Young people are overconfident with online security, survey says

https://mashable.com/article/young-old-people-security/?utm_campaign=hp-n-1&utm_source=internal&utm_medium=onsite

- A poll found that 78% of users aged 16 to 24 admitted that they used the same password for multiple online accounts. Seventy-one percent of users in the same age range expressed confidence that they wouldn't fall for a phishing scam.
- Older users tended to have better password security and less confidence about their ability to spot phishing scams.

Analyst Note: Reusing passwords for multiple accounts can give bad actors an easy way in if they can figure out a single password. Use different, strong passwords for different accounts and use multifactor authentication where you can.

"WHAT HAPPENED????" How a remote tech writing gig proved to be an old-school scam

https://arstechnica.com/gadgets/2019/06/scamming-the-scammers-how-i-sniffed-out-and-fought-a-cash-hungry-employment-scam/

- The author believed he had been hired for a remote tech writing job after a long stint of unemployment.
- His new "employer" asked him to deposit several checks into his account, but the checks were from other companies and business entities.
- The fraud actor was attempting to use a tactic known as Remote Deposit Capture (RDC), wherein in depositing the check allows the fraud actor access to the victim's bank account.

Analyst Note: Times of heightened emotional stress (such as being unemployed) can make anyone more susceptible to scams. Remember that if something doesn't feel right, take a step back and assess before you give away any personal information or money.

Facebook, Instagram, Twitter have a dark side. Here's how to anonymously report abuse

https://www.cnet.com/how-to/youtube-facebook-instagram-twitter-have-a-dark-side-heres-how-to-report-abuse/

- Social media platforms can be useful in connecting people and sharing positive moments, but can also be spaces where cyberbullying and abusive behavior take place.
- Approximately 73% of adults report seeing cyberbullying and 40% report being a target.
- There are established ways to report abusive content on all social media platforms.

Analyst Note: It's a good idea to be familiar not only with the privacy settings of any social media platform you're using, but also how to report troubling content. Every platform has its own way to report content; be sure to check it out before posting anything or interacting with other users.

Game Over for GandCrab: New free decryption tool allows victims to unlock all versions of this ransomware

https://www.zdnet.com/article/game-over-for-gandcrab-new-free-decryption-tool-allows-victims-to-unlock-all-versions-of-this-ransomware/

- A new decryption tool that counters all versions of GandCrab ransomware has been released for free on the internet.
- The key works on versions 5.0 through 5.2 as well as allowing for the retrieval of encrypted files from older versions of the ransomware.
- It is estimated that GandCrab has affected over 1.5 million Windows users at a loss of over $2 billion since it emerged in January 2018.

Analyst Note: The release of any decryption key that works is good news in the fight against ransomware, but there are still many types that don't have it. As always, make sure your antivirus is up to date, your files are backed up, and be careful with suspicious emails and links.

Update Your Dell Laptop Now to Fix a Critical Flaw in Pre-Installed Software

https://gizmodo.com/update-your-dell-laptop-now-to-fix-a-critical-security-1835732883

- A security flaw in pre-installed SupportAssist maintenance software on Dell brand laptops could have allowed malicious actors to replace files on the device.
- Dell has issued a fix for the flaw and advised consumers to update the SupportAssist software.

Analyst Note: Sometimes new electronic devices come with support software that provides firmware and BIOS updates. While this software is very helpful, it's important to keep it updated like any other program.

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/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 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.

THE BEACON

Editing by: Ashley Grover
Designed by: Maria Olivella

July 2019

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