The Beacon

Florida Fusion Center #17-104 | Cyber and Critical Infrastructure Report | July 2017 Issue #14

Summary

Botnets - All about how botnets are created, spread, and wreak havoc.

WannaCry: All Smoke, No Fire? - You may have heard about WannaCry in the news, but how badly did it impact networks?

Net Neutrality: UPDATE - A brief overview of the latest in the debate over a free and open internet.

Facial Recognition - As this technology gains widespread adoption, we discuss some possible risks.

VPNs: FAQ - People are more concerned about their internet privacy than ever. VPNs are a great way to insure that privacy.

Dark Web vs. Deep Web - There are deep and dark areas of the World Wide Web out there, and we explain the differences.

Malware - Healthcare organizations retain a lot of valuable information for hackers, making them ripe targets.

Space: Blank, but Balanced - Layout matters when creating written products. Here's why.

Contents

About *The Secure Florida Beacon*

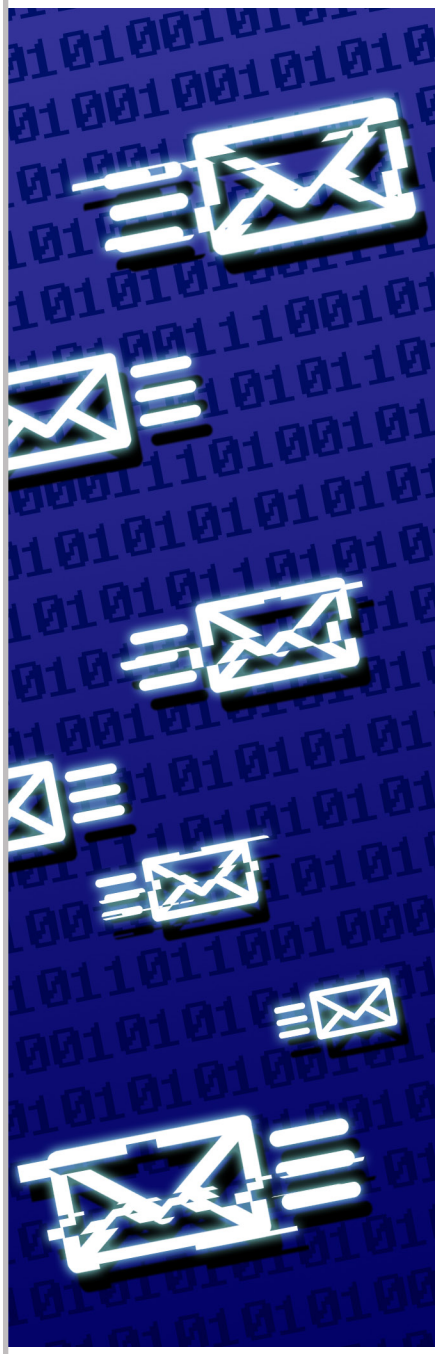
The Secure Florida Beacon is published by Secure Florida to highlight cyber and critical infrastructure security information and awareness. Secure Florida is an internet safety and awareness effort of the Florida Department of Law Enforcement's Florida Infrastructure Protection Center (FIPC).

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

Contact Secure Florida at:
Phone: (850) 410-7645
Email: admin@secureflorida.org

Editor's Corner

The Risky Non-Click



One of the best practices we regularly mention at the FIPC is "be suspicious of email links and attachments." While that remains a best practice, the threat landscape has shifted…and hackers are using savvier tactics to trick users. In some malware cases, you may not even have to open or click on the emails or attachments for the malware to execute.

Researchers recently discovered a type of malware using subtitles in open source media software. Vulnerabilities in software such as VLC or Popcorn Time allow bad actors to create subtitles for media content, embedded with malware. The process for the malware to execute is simple: a user opens the program, and loads content (like a movie). Then, when subtitles are turned on, malicious subtitles execute malware and give the attacker remote access to the victim's machine.[1]

Another new twist on the traditional phishing scheme involves Microsoft PowerPoint. Most savvy computer users these days know not to click on a suspicious link/attachment when they get a weird looking email. To verify the URL, many users navigate their cursor over the link to see if it appears like it would send you somewhere malicious…and that's the tactic the bad guys are exploiting with this scheme. When users *mouse over* the suspicious link, the malware executes, no click required.[2]

Of course, you can't discuss unique malware methods without also mentioning WannaCry ransomware, which is the first ransomware type to act like a worm (that is, propagating without user interaction). The malware easily spread across entire networks, even if users did not click on anything to cause the infection. For more information on WannaCry check out **WannCry: All Smoke, No Fire?** on page 5.

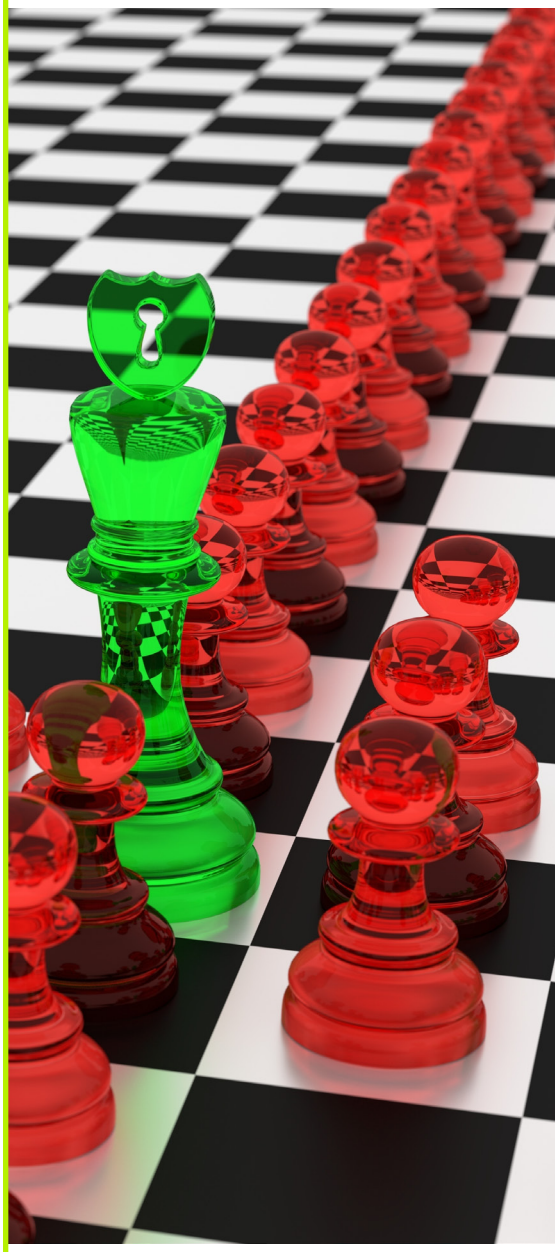
Bad actors are always on the lookout for the vulnerabilities they can exploit, as well as new and unique ways to deliver malware. This issue highlights some of these schemes, as well as some risks to take into account when it comes to securing your tech.

[1] http://www.csoonline.com/article/3197774/security/malicious-subtitles-in-popular-media-players-could-lead-to-remote-compromise.html
[2] https://www.engadget.com/2017/06/11/malware-downloader-infects-your-pc-without-a-mouse-click/

Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

Cyber Threats

Botnets: The Impact of Manipulating Non-Secure Devices



In the first half of 2017, many cybersecurity firms finalized reports on the cyber issues that defined 2016. Most of these reports cite botnets, which enslave Internet of Things (IoT) devices,[1] as a major threat to both private and public networks in the near future.

A botnet is a network of compromised computers and devices infected with malware and remotely controlled by a hacker.[2] Botnets may be used for a number of functions, such as launching Distributed Denial of Service (DDoS) attacks[3] as well as facilitating spam email campaigns. Spam makes up nearly two-thirds (65%) of total email volume, and global spam volume is only expected to grow as a result of these thriving, spam-sending botnets.[4]

Experts estimate more than 200 billion IoT devices will be in operation by the end of 2020. Because IoT device manufacturers typically place functionality and speed of production over safety, many products retain default security settings that are easily exploited by cybercriminals. With over 15 billion IoT devices in use today, this means cybercriminals can create powerful botnets with thousands vulnerable devices.[5]

IoT botnets came into the spotlight in 2016 with the emergence of the Mirai botnet. The Mirai botnet was responsible for the largest DDoS in history to date, targeting domain name service company Dyn. The disruption of Dyn's services affected many widely-used web services such as Netflix and PayPal. Cybercriminals created a botnet large enough to carry out this DDoS attack by exploiting non-secure IoT devices, namely routers and security cameras. Mirai operates by continuously scanning for IoT devices, infecting them

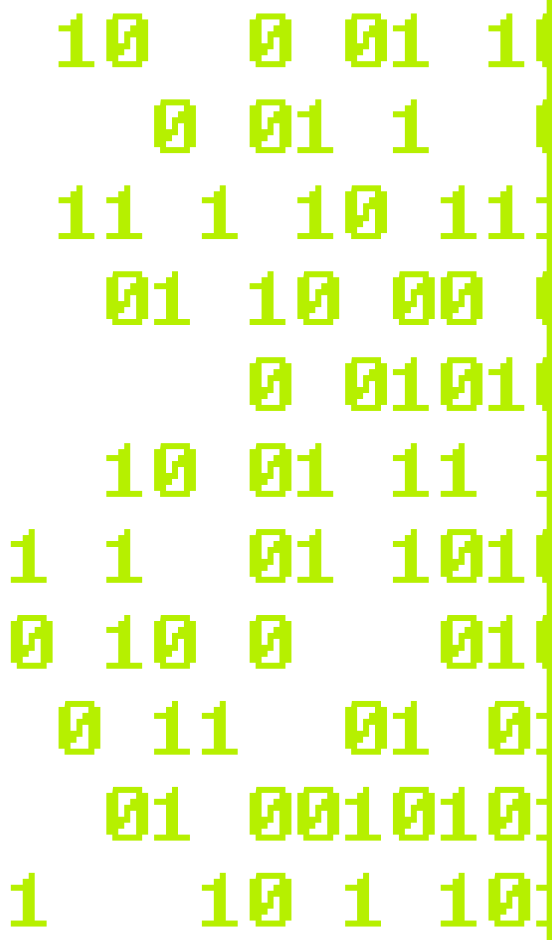
[1] Internet of Things: The network of everyday objects embedded with computing devices, enabling internet connectivity via wireless or wired connections.
[2] Trend Micro. *Trend Micro – Botnet*. 2017. https://www.trendmicro.com/vinfo/us/security/definition/botnet
[3] A cyber attack designed to temporarily disable access to a web service.
[4] Cisco. *2017 Annual Cybersecurity Report*. 2017.
[5] McAfee Labs. *McAfee Labs Threat Report, April 2017*. April 2017.

Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

with malware, and forcing the devices to communicate with a central control server for future DDoS attacks.[6] In October 2016, the source code for Mirai was publicly released, and other cybercriminals used the code to create smaller botnets and offer "DDoS-as-a-service," with posts advertising Mirai botnet services from as little as $30 to as high as $7500.[7] In addition to leveraging these devices into a botnet, another risk to consumers is that attackers could render their compromised devices unusable by changing the default login credentials, which many leave unchanged.[8]

Other botnets with unique characteristics have been discovered by researchers since Mirai.

- In May 2017, security researchers at Trend Micro identified over 1,000 different models of internet-connected cameras at vulnerable to the botnet dubbed Persirai. 122,069 internet-connected cameras (primarily in China) were assessed to be at risk of being controlled by malicious actors.[9]
- The Necurs botnet, which originally surfaced in 2012, reappeared this year to facilitate a spam scheme that tries to artificially boost a company's stock market price. This spam campaign sends massive amounts of spam to convince users to buy stocks for a particular company.[10] The price of that company's stock then surges due to an influx of new buyers. The botnet operators then proceed to sell their stocks at the higher price and net an overall profit (a scheme commonly known as "pump and dump").[11]
- Over two million devices were compromised by the Brickerbot botnet. Its mission was to create a permanent denial of service (PDoS) attacks against non-secure devices. PDoS is an attack that damages a system so badly that it requires replacement or reinstallation of hardware.[12]



[6] Symantec. *Internet Security Threat Report Volume 22*. April 2017. https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

[7] McAfee Labs. *McAfee Labs Threat Report, April 2017*. April 2017.

[8] McAfee Labs. *McAfee Labs Threat Report, April 2017*. April 2017.

[9] Cluley, Graham. *Persirai IoT botnet threatens to hijack over 120,000 IP cameras*. Tripwire. May 11, 2017. https://www.tripwire.com/state-of-security/featured/persirai-iot-botnet-hijacks-over-120000-ip-cameras/

[10] Cimpanu, Catalin. *Spam Sent by Necurs Botnet is Trying & Succeeding in Altering Stock Market Prices*. Bleepingcomputer. March 21, 2017. https://www.bleepingcomputer.com/news/security/spam-sent-by-necurs-botnet-is-trying-andamp-succeeding-in-altering-stock-market-prices/

[11] Cimpanu, Catalin. *Spam Sent by Necurs Botnet is Trying & Succeeding in Altering Stock Market Prices*. Bleepingcomputer. March 21, 2017. https://www.bleepingcomputer.com/news/security/spam-sent-by-necurs-botnet-is-trying-andamp-succeeding-in-altering-stock-market-prices/

[12] Radware. April 5, 2017. https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/

The Brickerbot network in particular questions in the cybersecurity community about the ethics behind the destruction of botnets. The alleged author of Brickerbot, who operated under the alias 'janitor,' claimed the goal was to destroy non-secure IoT devices before they could be compromised by real criminals.[13] In an interview, Janitor stated:

> *I hope the unconventional actions by 'Brickerbot' have helped in buying another year of time for governments, vendors and the industry in general to get the current IoT security nightmare under control.*[14]

Cybersecurity researchers recognize that IoT devices will likely continue to remain non-secure so long as these private manufacturers have no incentive to bolster security measures. The best course for consumers is to set good passwords and keep all IoT devices behind a firewall on their network.

[13] Cimpanu, Catalin. *BrickerBot Author Claims He Bricked Two Million Devices*. Bleepingcomputer. April 21, 2017. https://www.bleepingcomputer.com/news/security/brickerbot-author-claims-he-bricked-two-million-devices/
[14] Ibid.

WannaCry: All Smoke, No Fire?

Ransomware was yet again in the news with the spread of WannaCry, a ransomworm that used some of the tools from the NSA leak late last year (Editor's Note: In our **January 2017 issue**, we predicted that the ransomworm might be on the rise). On May 12, 2017, WannaCry went live and infected an estimated 300,000 computers across 150 countries, and, perhaps most terrifyingly, disabled the National Health Service (NHS) in the United Kingdom. The cryptoworm operated by using an exploit of Windows' Server Message Block (SMB), locking and encrypting all files associated with a computer or network. WannaCry also included a transport mechanism in its code, which enabled the malware to automatically spread to other computers on the network (meaning that even if it was another coworker who initially opened the malware, your computer could still get infected). Once the files were encrypted, a dialog box would appear and instruct the user to pay $300 in Bitcoin to get their files back.

Microsoft addressed the vulnerability in March 2017,[1] releasing several critical security patches, but due to lags in patching or outdated software, many entities remained vulnerable. Microsoft even took the unprecedented step of releasing an emergency patch for Windows XP and Server 2003, which have not had any updates since 2014.

This certainly had the makings of a cyber-doomsday scenario, but were the issues as terrible as news reports made them out to be? Within hours of its initial attack, MalwareTech, a malware researcher, inadvertently found the "killswitch" for WannaCry and effectively ended all new infections. This bought precious time for organizations to patch their systems and check for other vulnerabilities. The researcher noted that usually, such programs use the same procedure: query a

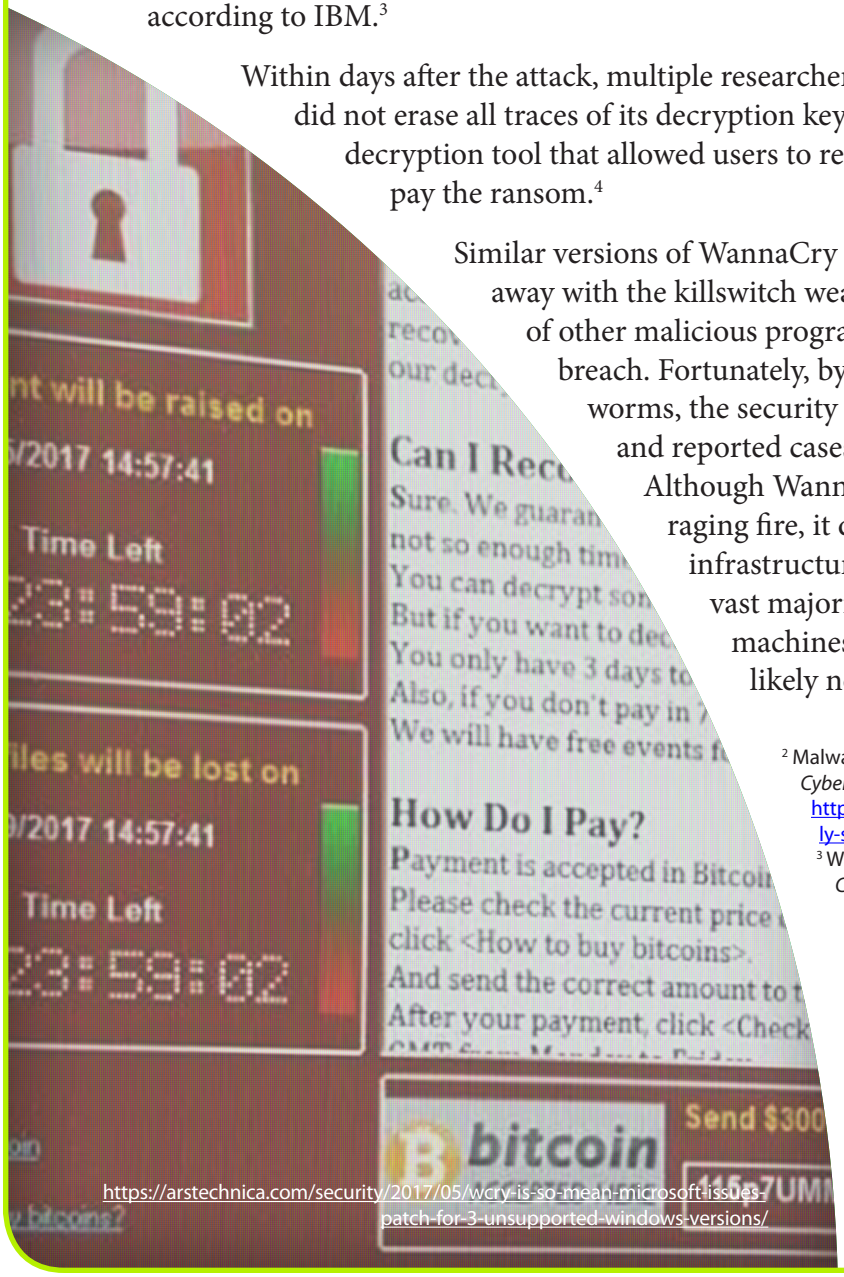
[1] Goodin, D. (2017, April 15). *Mysterious Microsoft patch killed 0-days released by NSA-leaking Shadow Brokers*. Retrieved June 2, 2017, from ArsTechnica: https://arstechnica.com/security/2017/04/purported-shadow-brokers-0days-were-in-fact-killed-by-mysterious-patch/

number of random domains (which usually don't exist); if they all return the same answer, the program will either move forward with infection or quit the process. WannaCry's code only had one domain to query, and when MalwareTech purchased the domain and activated it, this prompted the malware to stop executing the payload and halted additional infections.[2]

Analysis of the amount of profit WannaCry made for its creators provides another insight into its lackluster performance. As of May 18, it was estimated that the program had netted around $80,000 USD. Examination of the three addresses provided to make payments for WannaCry reveal a total of 288 payments, amounting to 43.92 bitcoins. With roughly 300,000 confirmed infections, this means that about one-tenth of one percent of victims made an attempt at any payment. To contrast, about 70% of companies paid a ransom to get their files back in 2016, according to IBM.[3]

Within days after the attack, multiple researchers studying WannaCry noticed that it did not erase all traces of its decryption key and were able to effectively create a decryption tool that allowed users to retrieve their files without ever having to pay the ransom.[4]

Similar versions of WannaCry have emerged, including one that did away with the killswitch weakness. There have also been reports of other malicious programs using other tools from the NSA breach. Fortunately, by the time hackers deployed these new worms, the security community improved their posture, and reported cases of infection have slowed to a trickle. Although WannaCry was a flash in the pan instead of a raging fire, it did expose serious security infrastructure flaws across a number of targets. The vast majority of infections (98%) occurred on machines running Windows 7 that were most likely not patched.[5]



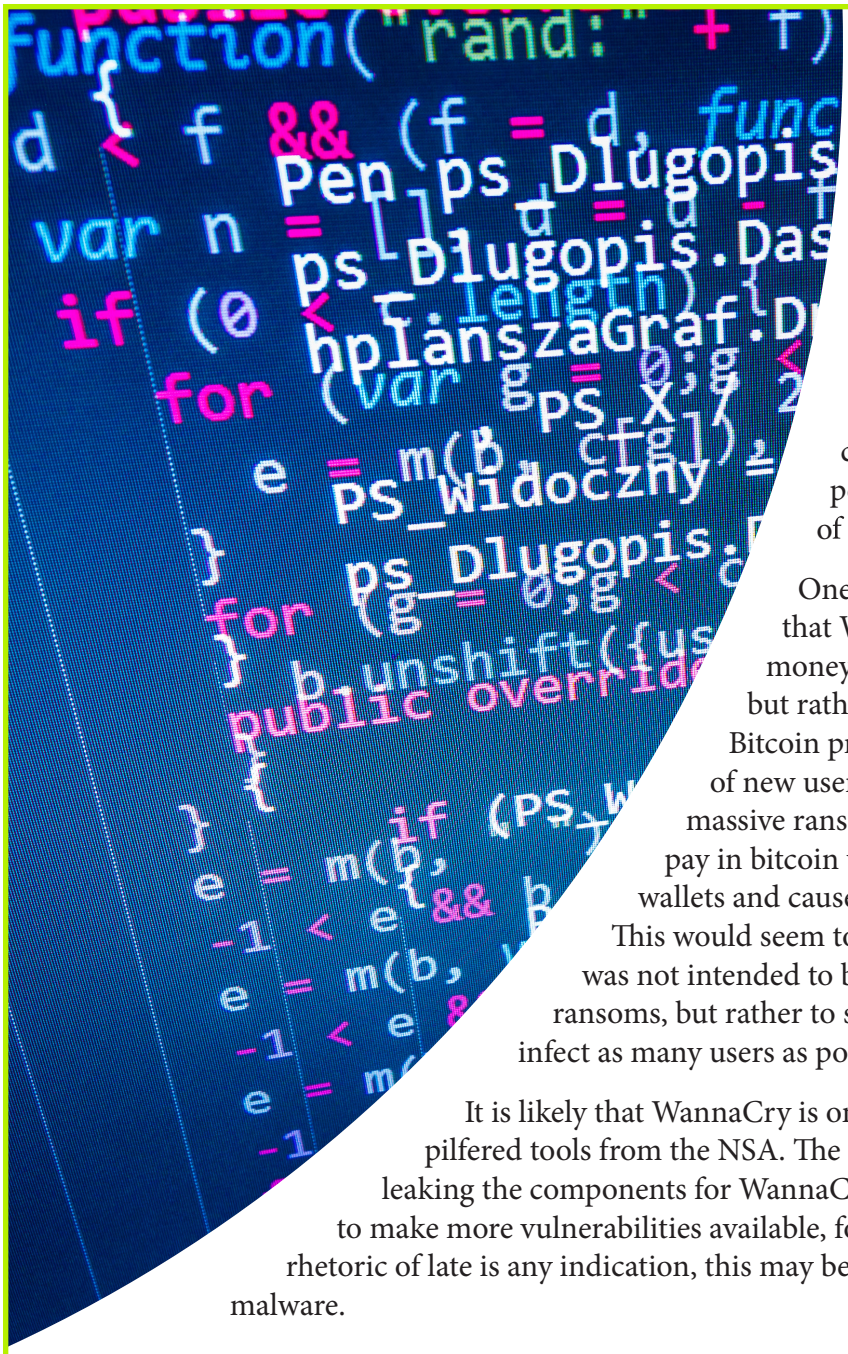
https://arstechnica.com/security/2017/05/wcry-is-so-mean-microsoft-issues-patch-for-3-unsupported-windows-versions/

[2] MalwareTech. (2017, May 13). *How to Accidentally Stop a Global Cyber Attacks*. Retrieved June 2, 2017, from MalwareTech: https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html

[3] Warner, G. (2017, May 18). *WannaCry: Ransomware Catastrophe or Failure?* Retrieved June 2, 2017, from DARKReading: https://www.darkreading.com/attacks-breaches/wannacry-ransomware-catastrophe-or-failure/a/d-id/1328900

[4] Khandelwal, S. (2017, May 18). *WannaCry Ransomware Decription Tool Released; Unlock Files Without Paying Ransom*. Retrieved June 2, 2017, from The Hacker News: http://thehackernews.com/2017/05/wannacry-ransomware-decryption-tool.html

[5] Cimpanu, C. (2017, May 20). *Over 98% of All WannaCry Victims Were Using Windows 7*. Retrieved June 2, 2017, from Bleeping Computer: https://www.bleepingcomputer.com/news/security/over-98-percent-of-all-wannacry-victims-were-using-windows-7/



The consensus seems to be that WannaCry had all the tools and makings of a cyber monster, but thankfully its design was poorly executed. Although it took a country's entire health care system offline temporarily, the implications of an attack could have been far worse. However, WannaCry signals a new era ransomware, wherein the cyber intelligence community's most powerful weapons are now in the hands of rogue actors.

One of the more interesting theories posits that WannaCry was not about making money through the payment of the ransom, but rather through currency manipulation. Bitcoin prices can rise based off of the number of new users (called "wallets") that join. A massive ransomware attack that forces victims to pay in bitcoin would theoretically boost the number wallets and cause a rise in the value of existing bitcoins. This would seem to support the position that WannaCry was not intended to be foolproof, or to make money off ransoms, but rather to spread as quickly across the world and infect as many users as possible.[6]

It is likely that WannaCry is only the first major attack using the pilfered tools from the NSA. The group claiming responsibility for leaking the components for WannaCry, the ShadowBrokers, is working to make more vulnerabilities available, for malware developnebt. If their rhetoric of late is any indication, this may be the dawn of a new age in malware.

What can I do to protect myself against WannaCry?

The steps to protect oneself from WannaCry or other types of ransomware remain the same:

- Keep current on security patches for operating systems and applications.
- Avoid clicking on suspicious emails or attachments.
- Back up files and test the backups regularly.

[6] Cimpanu, Catalin. *BrickerBot Author Claims He Bricked Two Million Devices*. Bleepingcomputer. April 21, 2017. https://www.bleepingcomputer.com/news/security/brickerbot-author-claims-he-bricked-two-million-devices/

Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

Cyber Highlights

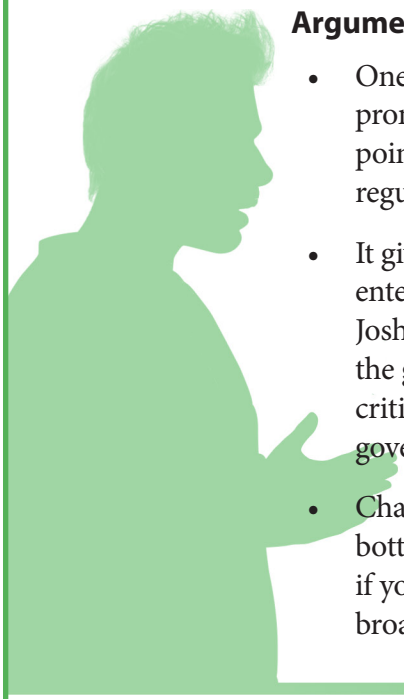
Net Neutrality: UPDATE

In our April 2015 issue, the **FIPC Beacon** *included an article titled* **"Net Neutrality: What it is, and Why You Should Care."** *This is an update to that discussion.*

If you assumed, back in February 2015, that the issue of net neutrality was settled for the near future, unfortunately you were wrong. This past May, the FCC (Federal Communications Commission) voted to end the net neutrality order enacted in 2015. For some, the decision eliminates excess government regulation that stymies businesses. For others, it is the death knell of a free and open internet.

In its simplest form, net neutrality is the concept that all internet traffic should be treated equally—your internet service provider (ISP) can change neither the speed of your service nor the cost, based on what sites you visit. Think of it like a utility: the electric company has no say over how you use your electricity—a hospital incubator or a refrigerator full of beer—they only get to charge you for providing it. Net neutrality will do something similar with your internet service.

The issue is not simple, but below are some of the reasons that seem to be universal within the two sides.

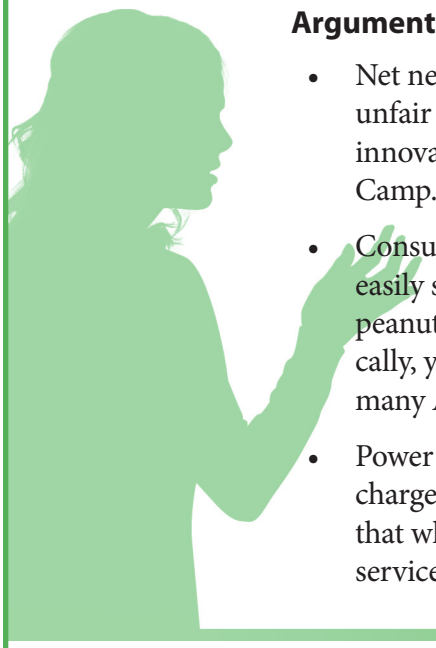


Arguments AGAINST

- One of the cornerstones of Donald Trump's presidential campaign was the promise to decrease excess government regulation. FCC Chairman Ajit Pai points to the twenty years that the internet has worked just fine without such regulation. In other words, if it ain't broke, don't fix it.
- It gives the government more control over the internet, which could stifle free enterprise and compromise individual privacy. Writing in Forbes, entrepreneur Joshua Steimie warned, "Don't be surprised if [net neutrality regulation] means the government needs to be able to install its own hardware and software at critical points to monitor [internet traffic]. Once installed, can we trust this government, or any government, to use that access in a benign fashion?"[1]
- Charging the same price for everyone is not fair. Internet bandwidth is not a bottomless pit; it must be allocated in some way. Using the utility comparison, if you use more electricity, you have to pay more. If you generate or use more broadband traffic, should you also not have to pay more?

[1] https://www.forbes.com/sites/joshsteimle/2014/05/14/am-i-the-only-techie-against-net-neutrality/#63dfca2b70d5

Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org



Arguments FOR

- Net neutrality allows for true freedom of access on the internet by precluding unfair pricing practices on the part of the ISP. It also fosters free enterprise and innovation from entrepreneurs like Snapchat's Evan Spiegel or Uber's Garret Camp.
- Consumers do not have freedom of choice when it comes to ISPs; they can't easily switch to a better provider. For example, let's say you prefer Peter Pan peanut butter, but the one grocery store in your area stocks only Jif. Theoretically, you could always shop elsewhere, but it's not practical. This is the situation many Americans find themselves in when it comes to internet access.
- Power in the hands of ISPs could be abused. Although Comcast refutes the charge, in 2010 they were accused by Level 3 Communications[2] of doing exactly that when it came to adjusting internet speeds for customers streaming Netflix services.[3]

It seems to come down to this question: which are you more concerned about—control in the hands of the government or in the hands of the ISPs?

The FCC plans to take comments on its plan until August 16 and then make a final decision sometime after that. The Secure Florida staff urges you to make your views known to the FCC. The Verge provides instructions: https://www.theverge.com/2017/5/23/15681434/net-neutrality-how-to-comment-fcc-proposal-released

[2] http://www.washingtonpost.com/wp-dyn/content/article/2010/11/29/AR2010112907024.html
[3] https://arstechnica.com/tech-policy/2010/11/how-comcast-became-a-toll-collecting-hydra-with-a-nuke/

Facial Recognition: Emerging Uses and Concerns

How does facial recognition work?

There are several techniques that can be used in facial recognition systems. The traditional, and most commonly used, method uses 'landmarks' or features on the face and head of an individual as the basis for analysis. Facial recognition systems can compare these features geometrically (looking at distinguishing features) or photo-metrically (using statistics to break a photo or video image into mathematical values that can be compared.)

Facial recognition technology factors a number of different parts to verify a face. This includes using 3D data; the entire head (not just the face) as reference; skin texture analysis, which turns the unique lines, patterns, and spots on someone's skin into a mathematical space; and in some cases thermal fingerprinting (using thermal cameras to detect the shape of a person's head). A combination of one or all of these calculations increase the percentage chance of a successful

facial recognition attempt.

How is facial recognition used?

Facial recognition market use is growing rapidly worldwide, projected to be a $6.8 billion industry by 2021.[1] Due to high costs, previously, the primary users of facial recognition systems have been law enforcement and government agencies. These systems have mostly been used to assist in controlling driver license fraud and immigration control. Times change, and as the technology has gotten cheaper we are seeing it being tested or used more often in private companies and businesses.

Banks have started using these systems to verify purchases through cell phones and ATMs,[2] and airlines are testing using a similar system for baggage checks.[3] Even our cell phones can now be unlocked using selfie cams. Marketing firms are joining in, eager to capitalize on the direct marketing that facial recognition could provide.[4]

The Flip Side

Sure, facial recognition could make your life easier, but what are the tradeoffs for privacy and security that could arise regarding this new technology?

First and foremost is privacy: data used to identify you could also be used to track you. The fear of "total" surveillance and the lack of any retention or use standards are concerning civil rights and privacy organizations. An even more significant concern is the slow shift from using private data (a password) for security, to public data (your face). You can always change a password, but changing your face may be more difficult.

The technology is also not perfect. Failure rates for successful identification are well documented; misidentifications can and do occur, especially for those with dark skin tones.[5] The lack of industry-wide standards, lighting levels, clothing, hair, and even expressions can often make using or verifying facial recognition problematic. And of course, the more systems using your facial data means a higher likelihood that your facial data could be hacked or stolen.

Currently, there are no real mechanisms in place if your facial data is stolen or breached. There is a silver lining, however: facial recognition data over six years old is not usable, thanks to the aging process (see: wrinkles) our faces undergo naturally.[6]

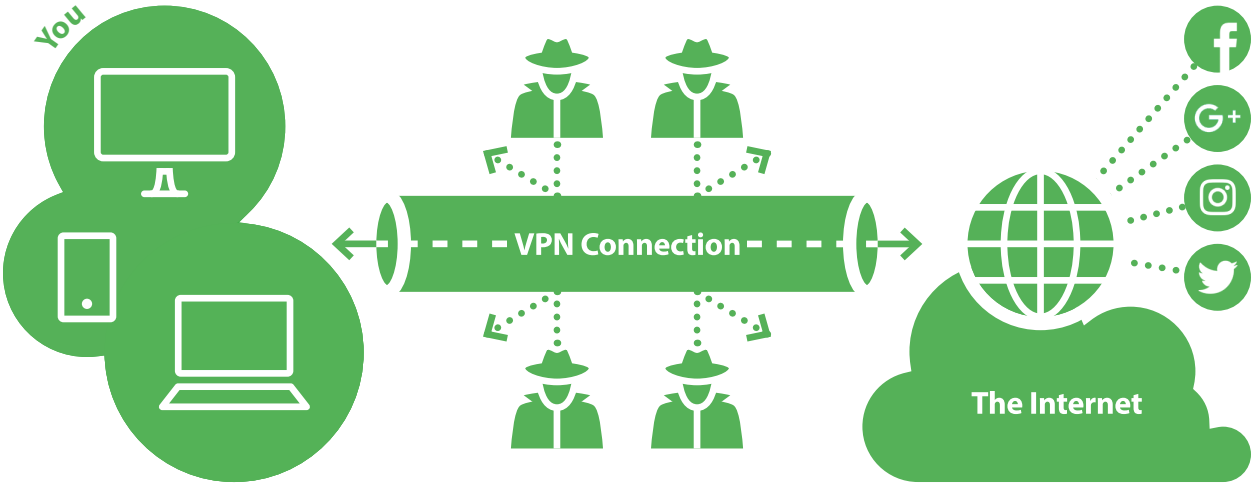
[1] http://www.marketsandmarkets.com/PressReleases/facial-recognition.asp
[2] http://fortune.com/2016/09/06/hsbc-facial-recognition-biometrics-digital-revolution/
[3] http://www.cbsnews.com/news/delta-airlines-facial-recognition-technology/
[4] https://www.inc.com/molly-reynolds/how-facial-recognition-is-shaping-the-future-of-marketing-innovation.html
[5] https://www.digitaltrends.com/photography/google-apologizes-for-misidentifying-a-black-couple-as-gorillas-in-photos-app/
[6] http://www.cbsnews.com/news/delta-airlines-facial-recognition-technology/

VPNs: Frequently Asked Questions

What are they?

You may have heard of VPNs (Virtual Private Networks), or perhaps even been required by your organization to use one when working remotely. With the rise in privacy debates surrounding internet use[1] (for more information on that, see **Net Neutrality: UPDATE** on page 8), we thought it might be useful to provide some background on what a VPN is, and why you may want to use one regularly as an extra way to increase your cyber security posture.

So how does a VPN work? When you use a VPN, it creates a private, controlled network through which you connect to the internet. You connect to a VPN server, and that then transmits your information out to the internet. Think of a VPN in this way: it creates an encrypted tunnel from your computer to the public internet, so no one can spy on where you are browsing, or what sensitive information you may be entering (like passwords or bank information).[2]



VPNs also cloak your IP address, which protects that information from third parties like advertisers who target you based on location. A VPN adds that extra layer of protection when you connect to open Wi-Fi networks as well, so that your web browsing cannot be observed by another person connected to that network.

What's the difference between VPN and HTTPS?

When you visit most reputable websites, they have an 's' after 'http' in the URL for the site. That 's' stands for secure, and means that there is a secure, encrypted connection from your computer to that site, shielding any activity from outsiders. However, your Internet Service Provider (ISP) can capture some details about what you are doing, despite the secure connection: that you visited the site, the date and time of the visit, and how long you stayed there. Coupling a VPN when you navigate to HTTPS sites helps you be sure that your data will continue to be encrypted.

[1] https://arstechnica.com/gadgets/2017/05/how-to-build-your-own-vpn-if-youre-rightfully-wary-of-commercial-options/
[2] https://www.wired.com/2017/03/want-use-vpn-protect-privacy-start/

Why/When you should use one?

Use of a VPN is a best practice any time you are concerned about the security of your internet connection, and want to protect the privacy of your activities. The best example of this is when you need to connect to an unsecured Wi-Fi (think coffee shop or hotel) where there is either no password or a default password, and you have no idea who else may be connected to the same network. VPNs afford that extra bit of privacy, and help safeguard against many of the risks associated with unsecure Wi-Fi.

With the debate over net neutrality, consumers have grown concerned about how their web-based communications or browsing habits could be gathered, used, or monitored by ISPs or other third parties. The risk is two-fold, and boils down to two major categories: ISPs and hackers.

A lot of the time, ISPs and third parties use that data to target ads (have you ever noticed that after you book a hotel room, many ads that appear on other web pages are for that hotel company?). If you connect to public Wi-Fi, anyone else on that network may also have access to what you're browsing…and potentially do something more nefarious with that.

How do I obtain a VPN?

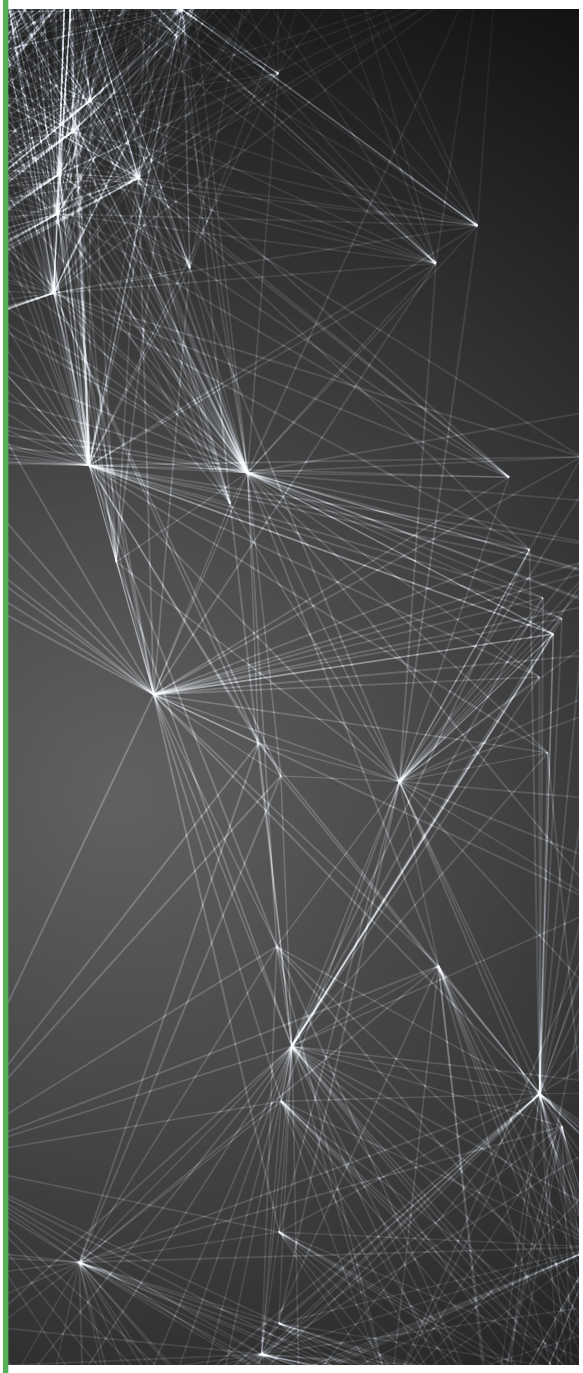
You may have used a VPN in conjunction with your work device, but how do you get a VPN for your personal devices? There are a number of free and subscription-based services out there, for computers as well as mobile devices. Make sure you do your research on a product before you download or purchase. There are many sites (such as this one: http://www.pcmag.com/article2/0,2817,2403388,00.asp) that compare different VPN services.

Keep in mind that if a service is free, then you are the product: a company offering a free VPN service may still access (and use) your browsing information, thereby compromising any security you seek by using the service in the first place.[3] If you decide to use a VPN, choose one that has a good track record on security, is well-known, and read their privacy policy.

[3] http://www.pcadvisor.co.uk/test-centre/internet/best-free-vpn-services-2017-3613860/

Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

Beyond the World Wide Web



When most people think of the internet, the sites that come to mind are popular ones such as Facebook or Amazon. To find these sites, you use a pointer site, also known as a search engine (like Google). The sites and information you can access using a search engine are part of the surface web.[1,2,3] Beyond the surface is a ***deeper*** and ***darker*** web, each with distinguishing characteristics. These portions of the internet cannot be located by search engines.

The deep web is the second level beyond the surface web. In brief, the deep web is anything that a search engine cannot find.[1,2] Perhaps the best example of the deep web is content from databases within a governmental organization, such as your agency's internal website.[1,2] It is difficult, or impossible, to locate deep web sites using a search engine because any associated results will be links to login pages—you must know how to access the content (usually by having login credentials).[1]

You may also have heard about the dark web, also known as the Darknet.2 Like the deep web, dark web content cannot be found using a typical search engine. In fact, the content is intentionally hidden and inaccessible: you must download specific browsers (like The Onion Router, or TOR) to get to dark web sites.[1,2,3] These browsers incorporate anonymity into the network, allowing users to cloak their identity. This also facilitates illegal activities, which is why you may hear the dark web in conjunction with criminal activities such as selling drugs, child pornography, gambling, or human trafficking.

The World Wide Web is more complex than many people realize, and the sites most commonly accessed on the surface are just a portion of what is out there.

[1] "Clearing Up Confusion – Deep Web vs. Dark Web." BrightPlanet Corporation, 27 Mar. 2014, https://brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/.
[2] Miessler, Daniel. "The Internet, the Deep Web, and the Dark Web." Daniel Miessler, https://danielmiessler.com/study/internet-deep-dark-web/.
[3] Thompson, Cadie. "Beyond Google: Everything you need to know about the hidden internet." Business Insider Inc, 16 Dec 2015, http://www.businessinsider.com/difference-between-dark-web-and-deep-web-2015-11.

Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

Critical Infrastructure

Malware: Infecting the Healthcare Industry

The healthcare sector has been a desirable target for hackers due to the sensitive nature of patient information contained in their systems. The stakes are very high in the healthcare industry because any disruption in operations and care can have significant repercussions for patients. As such, this industry offers ideal victim for ransomware and data breaches, These attacks are likely to continue—exposing patient data and potentially disrupting employee access to important documents and systems.[1]

In 2016, several hospitals including those in California, Kentucky, and Indiana were attacked with Locky ransomware, spread through malicious email attachments. Locky-related emails include instructions such as 'you can download and view a copy of your invoice from the attached document.[2]' Ultimately, the California hospital was forced to pay nearly $17,000 in bitcoin to restore their records and control of the system, but other affected hospitals with a more robust backup system were able to access their systems and data without paying ransom.[3,4,5,6]

There have also been several reports of other types of malware disrupting employee access to systems which would hamper the ability to provide critical services—creating a public safety concern.

- In late March, a single-user's files were infected with ransomware at a hospital. An infected email with the subject line "invoice" contained the name of the hospital's new printer and fax machine in the "From Field", paired with its official email domain. Systems were intentionally placed offline for approximately 48 hours while the infected device was cleaned.
- Some hospitals in Baltimore, Maryland, were infected with malware that prevented log-ins. The healthcare facilities shutdown their system to prevent the virus from spreading throughout the organizations.

[1] www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets.
[2] Kentucky Office of Homeland Security and Kentucky Intelligence Fusion Center; Situational Awareness Bulletin; "Ransomware Targeting Kentucky Healthcare Providers"; 25 MAR 2016.
[3] www.digitaltrends.com/computing/hollywood-hospital-ransomware-attack.
[4] www.technologyreview.com/s/600817/hospital-forced-back-to-pre-computer-era-shows-the-poer-of-ransomware/.
[5] www.nzherald.co.nz/wanganui-chronicle/news/article.cfm?c_id=1503426&objectid=11594628.
[6] Kentucky Office of Homeland Security and Kentucky Intelligence Fusion Center; Situational Awareness Bulletin; "Ransomware Targeting Kentucky Healthcare Providers"; 25 MAR 2016.
[7] www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets.
[8] http://kdhhs.netreturns.biz/NewsReleases/Article_Detail.aspx?id=e067d2ba-d9ca-4174-b789-144d34d83075.
[9] Kentucky Office of Homeland Security and Kentucky Intelligence Fusion Center; Situational Awareness Bulletin; "Ransomware Targeting Kentucky Healthcare Providers"; 25 MAR 2016.
[10] www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets.

Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

In 2016, Florida had the second-highest number of healthcare data breaches exceeding 500 records.[11] The 27 reported breaches exposed more than 2.8 million records; of those, nearly 37% were reported as the result of unauthorized access/disclosure, 30% hacking/IT incidents, 22% as theft, 7% as loss and 4% as improper disposal. At least one of the instances was determined to have been the result of a ransomware infection; the facility has since strengthened their firewall protections and taken other corrective action.[12]

Florida has a variety of healthcare facilities and other types of critical infrastructure that could become targets of these types of malware. Here are some best practices to protect your organization from these types of threats:

- Employ a data backup and recovery plan for all critical information.
- Use application whitelisting—a computer administration practice used to prevent unauthorized program from running—to help prevent malicious software and unapproved programs from running.
- Keep your operating system and software up-to-date with the latest patches. Vulnerable applications and operating systems are the target of most attacks, ensuring these are patched with the latest updates greatly reduces the number of exploitable entry points available to an attacker.
- Maintain up-to-date anti-virus software and scan all software downloaded from the Internet prior to executing.
- Restrict users' ability (permissions to install and run unwanted software applications, and apply the principle of "least privilege" to all systems and services.

[11] http://www.hipaajournal.com/2016-healthcare-data-breach-report-ranks-breaches-by-state-8692/
[12] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Design 101

Space: Blank, but Balanced

Blank space, when it's used efficiently, is unremarkable to the reader; but it makes for uncomfortable reading when it's used improperly. However, when multiple copies of like things, such as magazines, are next to each other, the problems are easier to spot. As an example, below are two sample magazine pages. The left side is using blank poorly, and the page suffers because of it. A reader is likely to skip over that page in favor of the right page, which uses blank space much more efficiently.

There are no glaring errors on the first page, but comparing it to the second gives a good idea of what effective use of blank space can do for your text. The first page has more content, but it trades-off approachability and ease of readership to fit it in. The second has less content, but what it has it lays out cleanly and efficiently.

When used correctly, blank space is breathing space for your eyes. Much like how athletes will take strageic breaks during a marathon, blank space acts as rest areas for your eyes as they traverse around a spread. Blank space is more than just unused space on the page. It includes the space between lines and characters, the space between text blocks and the edges of a page, as well as strategic areas of empty space.

Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

Blank space can be active, even if there's nothing in it. At first glance, it may appear that the space is going completely unused if there isn't a primary physical element in the space, but that's not always the case.

https://media.nga.gov/public/objects/1/2/3/6/1236-primary-0-740x560.jpg

As a different example, here is Vermeer's *Woman Holding a Balance*. The woman and her work-station are the primary elements in this painting, creating something like a right triangle of interest for your eye in the bottom right corner of the composition. This leaves the rest of the space, mostly empty space, to balance out the positive space she takes up. This balance is an initial aspect of what makes the painting aesthetically pleasing to look at. Good use of blank space can be an invitation to continue looking at your product. If used inefficiently, however, it can drive people away from it. Why bother devoting your attention to something that takes more effort to read through when there are alternatives?

In text-based products, there's only so much you can do when it comes to using space, since most of your space will either be taken up by text or difficult to edit directly. When laying out your information, ask yourself this: will this be visually enticing? Getting as much information as you can into a product is important, but you want to avoid the "wall of text," which discourages readers by suffering visually; there's nowhere for their eyes to take a breather. Good use of blank space can really give your products a visual edge, and that edge could lead to an increase in readership.

Padding and Margins

Text boxes like this are a popular addition to text based products, but getting them to fit seamlessly into a product can be difficult. ***Padding***, the space between a text block and the edge of its container, is an editable feature for these boxes, and changing it up could create some breathing space around them, making them much more visually approachable. This same technique can also be applied to ***margins***, which are essentially padded space between your main text block and the edge of a page.

Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

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 and fill out the sign-up sheet 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.

Backdoors: When Good Intentions Go Bad

http://www.darkreading.com/endpoint/backdoors-when-good-intentions-go-bad/a/d-id/1328796

- The number of terrorist incidents in the past couple of years in western countries has resulted in some calling for the ability to create back doors into technology as a means to gather intelligence on terrorists.
- While the ability to identify and stop terrorists before they act, using backdoor technologies, may be useful, there could be some major drawbacks…like leaving that same backdoor open for hackers.

Analyst Note: Weakening the security on our devices means law enforcement and bad guys alike can get access to your data, and it is important to weight the benefits and costs of creating such a feature.

Even tech-savvy Gmail users are getting fooled by this phishing scam

http://www.komando.com/happening-now/393678/old-google-login-phishing-scam-is-still-fooling-people

- Hackers have increasingly sought sophisticated ways to trick users into thinking that a scam email is legitimate.
- The most recent Gmail scam is quite convincing, tricking users into clicking on attachments purportedly sent by people in their own contact lists.

Analyst Note: Even if it's someone with whom you correspond regularly, make sure to always confirm that the email you received is genuine and not a hoax.

Why it's a good idea to clear your browser history and cookies

https://www.grahamcluley.com/good-idea-clear-browser-history-cookies/

- Every time you visit a site on the web, there is data stored in your browser and on your computer...some helpful, and some not so helpful.
- This article discusses some tips on data that you should consider clearing from your computer regularly.

Analyst Note: Whether to speed up a computer that's been lagging or keep ad trackers from knowing your browsing habits, it is a best practice to clear out data associated with your internet use.

WannaCry Ransomware Decryption Tool Released; Unlock Files Without Paying Ransom

http://thehackernews.com/2017/05/wannacry-ransomware-decryption-tool.html

- The latest and greatest ransomware, WannaCry, quickly damaged thousands of networks across the world in a few short days.
- Tech researchers quickly discovered how to retrieve encryption keys from the malware, which prevented many individuals from having to pay a ransom to get their files back.

Analyst Note: As we have said before, ransomware isn't going away any time soon. Many got lucky with this variant, but may not be so lucky in the future.

What home products are most susceptible to cyber burglars?

http://www.csoonline.com/article/3186808/security/what-home-products-are-most-susceptible-to-cyber-burglars.html

- Many "smart" devices may not be smart enough to withstand a cyber attack on their own. It is important as a device owner to ensure that you have passwords and firewall protections in place.
- As more devices around your home become part of the Internet of Things, understand what some of the risks are associated with them, from signal jammers to hackers remotely accessing and changing settings.

Analyst Note: We talk a lot about the Internet of Things…because they are never going away, and you will thank yourself later for adopting best practices as you incorporate more of these devices into your everyday life.

Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

Secure Florida's Best Practices for Office Security

1 Be suspicious of email links and attachments.

Emails designed to trick you into clicking links and downloading files come to inboxes daily. It is a practice called phishing and it's surprisingly effective. The easiest way for someone to get unauthorized access to your network is for you to give it to them. Never click on email links and never download attached files unless they are from trusted sources.

2 Use strong passwords and keep them private.

Your password is one part of the information security process that you control. Remember that you are protecting your accounts not only from someone trying to guess your password, but also from someone who steals password files to crack them. A strong password can take so much time to crack that it's not practical to keep trying, so the stronger your password is, the safer you are.

3 Back up your files regularly.

That spinning plate on your hard drive is an accident waiting to happen, and Florida is the lightening capital of the country. Hard drive crashes, electrical surges, and operator errors lead to many lost files. So do stolen laptops. Make sure you have backups of your important files.

4 Be careful when using public Wi-Fi.

When you connect to public Wi-Fi, or an "open network," anything you transmit can be seen by others. This includes usernames, passwords, account numbers, and confidential work information. Using a "secure" connection (such as HTTPS, SSL, or VPN) helps lessen the risk.

5 Use password protected screen savers.

It can only take a few minutes for someone to take advantage of a computer left idle.

6 Download only from approved sources.

As with email attachments, never download files from untrusted sources. Be especially suspicious of free software; it often has malicious software bundled with it.

7 Don't give out information to unverified individuals.

Social engineers try to fool you into giving out confidential information. Sometimes the information they ask for seems harmless, so their request doesn't raise any red flags. Before giving out any office-related information, be sure the person making the request is authorized to receive it.

8 Know and follow your organization's information security policies.

Your organization has its own security rules on matters such as using USB drives and personal devices on your work computer. Follow them carefully.

Information Resources

The Florida Infastructure Protection Center was established in 2002 to anticipate, prevent, react to, and recover from acts of terrorism, sabotage, cyber crime, and natural disasters. The FIPC is a team of cyber intelligence and critical infrastructure analysts who work to protect Florida's infrastructure.

SecureFlorida is an Internet safety and awareness outreach effort of the FIPC. Designed for the majority of computer users, Secure Florida covers all areas of computer, network, and communication security.

To sign up for alerts and other notices, **visit www.secureflorida.org/members/signup/**

The Beacon

The Beacon is published quarterly by Secure Florida to highlight cyber and critical infrastructure security information and awareness. **The Beacon** seeks to provide privacy and security information to all Internet users.

To read issues of **The Beacon**, visit **www.secureflorida.org/news/the_beacon/**

To sign up for **The Beacon**, visit **www.secureflorida.org/members/signup/**

The Dispatch

The FIPC Dispatch is compiled twice weekly by cyber intelligence analysts in the Florida Fusion Center. The content is intended as an informative compilation of current open-source cyber news for law enforcement, cyber intelligence, and information security communities.

To join **The Dispatch** mailing list, write to **FIPC@fdle.state.fl.us**

The **CSAFE** effort provides Internet safety presentations for organizations, clubs, schools, and businesses anywhere in Florida. For more information, visit **www.secureflorida.org/c_safe**

Class topics include:

- Best Practices for Internet Security
- Family Online Safety
- Combating Cyberbullying
- Online Safety for Seniors
- Identity Theft
- Mobile Communications
- Email Safety
- Internet Laws & Regulations