About The Beacon

The 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 FIPC 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 protection analysts. FIPC analysts work to protect Florida’s infrastructure through FDLE’s Internet safety and awareness effort (Secure Florida), and the website SecureFlorida.org.

If you see a topic where you would like more detailed reporting, or have seen something you think we need to know about, Let Us Know.

We welcome your feedback.
www.surveymonkey.com/SFBeacon4
Contact SecureFlorida.org at: Admin@SecureFlorida.org
Editor’s Corner

CSAFE

Cybersecurity analysts in the Florida Fusion Center offer free cyber security presentations to Florida citizens, businesses, and organizations. We offer a number of established presentations and create new ones all the time. They generally run from one hour to one-and-a-half hours and we tailor them to fit your needs. We offer this at no cost inside the state of Florida. The idea is to further the cause of cyber resilience for individuals and organizations. We know that preventing cybercrime is the most effective way of fighting cybercrime.

Learn more at SecureFlorida.org/C_SAFE

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

Google Dorking

We would like to introduce a new information delivery method that we will start using in the coming months. The cyber group in the Florida Fusion Center understands that we collect and analyze cybersecurity intelligence and Internet safety information for a broad audience. We developed what we call the FIPC Extra. We will use this delivery mechanism to put out documents that are more technical in nature and require more in-depth analysis than would fit in The Beacon. We will also push out stand-alone FIPC Extras as the need develops.

Here is an example of recent research we completed on Google Dorking. To see the complete document go to www.secureflorida.org/risks/google_dorking

Summary

Google Dorking, or Google Hacking, is the creative use of Google, or any search engine, to find sensitive information that organizations and individuals may not realize is publicly available. Network, system, and website administrators need to understand the risk and steps they can take to limit their exposure.
Cyber Highlights represent issues cyber analysts have seen active in Florida. The following articles are intended to serve as overviews of issues we feel the citizens of Florida would benefit from knowing.

**Fraudulent Procurement Orders**

We have observed a trend across several states concerning fraudulent purchases of large amounts of highly resalable merchandise including computers, routers, cameras, office supplies, and medical equipment. These transactions result from fraudulent purchase orders or the use of a victim’s line of credit. The high volume and routine orders made to large vendors create gaps in security that lead to the success of the fraudulent purchases.

Targeted entities used to facilitate the scams include state and local agencies, private companies, and state universities. There are different methods used to conduct the schemes to defraud; however, there are similar identifying characteristics. In a majority of the cases the subjects contact the merchandise vendor while posing as purchasing personnel from the victim organizations. The subjects use an email address with a domain almost identical to the victim entity allegedly making the purchase. They submit either a fictitious purchase order or use a stolen line of credit to complete a large order of equipment.

Initially the vendors were directed to deliver the products to a drop location, usually controlled by someone hired as part of a “work from home” scam. Traditionally, this person (also a victim) would be directed to reship the equipment overseas. The scam is thus completed, and the merchandise vendor suffers the loss of their merchandise with no payment.

More recent variations of the scam change the delivery address to the organization allegedly making the equipment order. This helps to legitimize the order and avoids using suspicious third party delivery locations. After delivery, the subjects contact the organization and act as representatives of the vendor company claiming the order was shipped in error. The organization is then requested to ship the equipment to the “rightful owner” at a domestic address. These domestic addresses frequently belong to a “work from home” or “romance” scam victim. Several of the victims reported receiving poorly-written emails from the subjects. Victim entities have been reported in Florida, California, Massachusetts, Pennsylvania, Ohio, Texas, Nevada, and Oklahoma.

Recommendations:

- Have protocols in place for employees to report suspicious activity as well as mitigating steps once fraudulent activity is identified.
- Limit information posted online about the procurement process and procurement personnel.
- Routinely check for out-of-sequence or duplicate purchase order numbers.
Man-In-The-Middle

With Cyber Security Awareness month upon us, the Florida Fusion Center wants to highlight a particularly problematic type of network security issue observed in numerous cyber-crime cases throughout Florida: Man-In-the-Middle attacks. Man-In-the-Middle, or MITM as discussed in security circles, is electronic eavesdropping by unauthorized personnel. The activity frequently results in the theft of user credentials and victim identities.

MITM attacks happen exactly like they sound; an attacker will use one of numerous techniques to insert themselves into the middle of a communication stream between a user and their connection to a trusted entity such as their email provider, bank, or Facebook account. Even secure protocols such as SSL can be compromised when bad actors physically insert themselves into the data stream, stripping security layers, inserting their own security credentials, and channeling traffic to the appropriate destinations. This happens so fast and so transparently that the end user and the trusted third party are unlikely to notice anything unusual.

While specific hacking techniques can vary, this exploit primarily takes advantage of the anonymity offered by unrestricted and unaccountable access to a network used by the victim—in most cases victims. Attackers will typically hop on a free (read: “insecure”) network such as those available in fast food restaurants, school libraries, and airports.

In general, the bad actors tend to prefer locations with a high volume of users and little or no usage restrictions. Once on the network, and upon the successful implementation of their hacking tools of choice, the attacker simply waits. Users tempted by the convenience of free Internet in our now hyper-connected world come along and, if the attacker is lucky, log into their sensitive accounts and pass along sensitive communications.

There are numerous technologies a user can leverage to protect their communication (HTTPS, VPN, PKI infrastructures, etc.). However, the best and most effective practice is simply don’t use public or open networks for sensitive communications. The more sensitive the communication is to you, the more certain you should be of the network’s security. At the same time, using free public WiFi or other public networks is not always a bad thing. Just behave and ‘surf the net’ as though someone might be watching and govern your activities accordingly. For instance, jumping on the local McDonald’s or Starbucks WiFi to check the latest sports scores, read your favorite blog, or checking the weather shouldn’t cause any heartburn. However, don’t use it for logging into your secret Swiss bank account to transfer around the family fortune.

Caveat Utilitor
Internet access is everywhere; not just “everywhere.” Everywhere. You can easily find wireless (WiFi) Internet in airports, hotels, restaurants, libraries, doctors’ offices, airplanes, buses, park benches.\(^1\) EVERYWHERE. In fact, I have a WiFi hotspot in my pocket right now. Not only is the Internet everywhere, most of the time it is free. As a society, we have all come to appreciate being connected everywhere we go. The problem we face is that the more we connect, the more bad guys (hackers, scammers, identity thieves) are connecting, too.

And the problem with wireless is…wait for it…NO WIRES. This means that anyone with the right equipment can intercept your communications from within the room, outside the room, or even across the street.

We want to help. Here are some tips for staying safe the next time you visit the coffee shop (or park bench) with your WiFi-enabled device.

1. **Always remember that open wireless networks are not secure.**
   If you can log into a network without a password, that means anyone else can too. Even more concerning is that reassembling the data transmitted on unlocked WiFi networks is possible by anyone who can receive the signal. Never send personal information over a public WiFi network.

2. **If you need a secure connection, use a VPN (virtual private network).**
   A VPN provides a secure way of connecting to a remote network by encrypting your transmission so that, even if intercepted, it can’t be read. Many work places offer the service for their employees to use at remote locations. You can also purchase the service for private use.

3. **Make sure you have a software firewall and keep your antivirus program updated.**
   Firewalls help keep out hackers, while antivirus programs detect and remove many types of malicious software. While not a cure-all, the use of these protections makes your information more difficult to steal.

4. **Watch out for shoulder surfers.**
   Most public networks are in areas where there are a lot of people (makes sense). Make sure that no one is looking over your shoulder while you conduct your business or read your email.

5. **Verify the name of the network you are connecting to.**
   Just because you can connect to a network does not mean you may. If the owner of a network has left it open to the public by mistake, it could still be illegal to use it. (Chapter 815 of the Florida Statutes makes it illegal to access a network without permission.) Not to mention, a hacker can setup another network with a similar name such as Starbucks Free Internet vs. Starbucks Customer Internet. Which one is the right one?

---

\(^1\) Literally, in 2013 Microsoft set up WiFi enabled park benches to advertise Microsoft 365.
Cloud Safety

Over the past few weeks, there has been much talk of security in the cloud. When “Jennifer Lawrence nude pic” started showing up in EVERY news outlet (and now our little publication), everybody started getting worried about their stuff getting loose. Turns out the cloud, that vast something that exists somewhere and holds all our stuff, is now dangerous. Suddenly, the vague became tangible and we all looked up in a mixture of dread and excitement.

The question everybody asks is, “What is the cloud?” Simply put, it is several really big rooms housing a lot of computers and hard drives. Depending on which cloud you are talking about, they might be located in any number of places. Seems simple enough...until you realize the way it all connects can be wildly complicated.

Sure, we all agree it’s great to have your information synced between your phone, tablet, and PC. The cloud is far from our minds, until someone other than us figures out how to get our stuff out of it.

So, what do you do? Most of us are not going to change anything about how we use cloud services. They are simply too convenient. But we can take steps to make our stuff harder to get.

1. Don’t let passwords intimidate you.
   We know that we end up sounding like a broken record when it comes to passwords. Consider this: you have no control whatsoever over security practices used by service providers. (They might leave the door to the datacenter open to ventilate the break room fridge twice a month.) However, you can control your password strength. Make them good; shoot for length and complexity. We can help with that: http://secureflorida.org/staying_safe/strong_passwords/

2. If the cloud service offers two-factor authentication – use it.
   You may not need that much security. Consider what you have stored in whichever cloud service you are using. A recipe database probably doesn’t need two-factor authentication. But, if you have intimate photos stored in the cloud, it’s probably time to start thinking two factors. For more information on two-factor authentication check out http://www.secureflorida.org/staying_safe/two_factor_authentication.

3. Do the best you can to understand how cloud services interconnect.
   Depending on the service, this can be nearly impossible. So it is up to you to research whom you are allowing to store your information and what steps they take to protect it. Some companies are better than others.

4. Manage the information you put in the cloud.
   Some things might be best protected at home or in the office. Granted, the cloud offers great protection from destruction, but it sometimes fails in its protection from disclosure.

5. Keep track of the accounts you create.
   Use a database, legal pad, email, whatever works for you. You can even use it to keep up with password hints. There is nothing like forgetting you have some forgotten cloud service tied to another and then reading about that service in the news.

6. Never assume security on the part of a cloud provider.
   You never know. I mean, someone figured out a way around Apple’s security for iCloud. You can count on the fact that, if it is connected to the Internet, someone is trying to get in to it.
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.

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

Home Depot Hit By Same Malware as Target

Summary:
- Point of sale terminals were infected with a new variant of “BlackPOS.”
- BlackPOS is malware designed to siphon data from cards when swiped at an infected terminal.
- Stolen card numbers turned up underground cybercrime shops that sold cards stolen from Target.

Analyst Note:
This was the first article we saw concerning the Home Depot breach. Many more followed and there will probably be more to come. We highlight this because we believe there are more of these types of breaches coming. Home Depot reported 54 million cards compromised. However, this type of breach is relatively common, just smaller in scale. Home Depot, or any large retailer, is a large stationary target. Until credit card processing practice changes, we will only see more of this.

Update: What Jennifer Lawrence Can Teach You About Cloud Security

Summary:
- Hackers stole nude photos of up to 100 celebrities allegedly from Apple’s iCloud service.
- Turned out Apple’s iCloud cloud service was susceptible to brute force attacks.
- The incident exposed critical flaws seemingly inherent in cloud security.

Analyst Note:
This is only one of many, many, articles covering this subject. Nonetheless, it is as good a place as any for us to make our point. People love convenience. The availability of Internet bandwidth means we are connecting to and using remote storage more now than ever. The amount of security vulnerabilities inherent in cloud technologies is significant. How many truly understand exactly how their photos are shared and stored in Apple’s (or anybody’s) cloud service. We always encourage our readers to study the services they use. Do the best you can to understand the risk before you post something to the cloud.
Hackers Take Control of Internet Appliances

Summary:
- Many mundane digital devices connect to the Internet and are easy to find.
- Hackers use automated programs to find Internet connected devices.
- Once found the devices are sometimes corrupted and used for nefarious purposes.

Analyist Note:
Everything connects to the Internet. The computing power in many of these devices, though it may be limited, is a prime target. In the future, more devices will connect and the problem will only become worse as we transition over to IPv6 and the untold undicillions of devices connected. The article mentions the use of these devices in payment card fraud and botnets. Imagine the possibilities.

FBI Used ‘Leaky Captcha' To Catch Silk Road's Hidden Servers

Summary:
- The FBI managed to locate and seize the underground marketplace Silkroad.
- The FBI maintains they found the Tor hidden service server because of misconfiguration on the site.
- The article gives a very good synopsis of how the FBI discovered and located both the hidden server and the person responsible for the site.

Analyst Note:
This is a very interesting case. It highlights one way to surmount encryption and anonymizing techniques in investigations. Granted, in many ways, the FBI was lucky that Silkroad was set up with an overlooked misconfiguration; those types of investigative leads make many cyber cases. In addition, this case illustrates the new reality of cyber investigation. Jurisdictional and technological barriers truly require creative approaches.