The Beacon

SecureFlorida.org Monthly Cyber and Critical Infrastructure Report Jan 2014 Issue #1

Summary

Keyloggers — Florida Fusion Center cyber analysts received reports in December of hardware keyloggers on point-of-sale terminals at retail establishments in south Florida. In addition, we received unrelated reports of software keyloggers delivered to numerous Florida citizens via unknown malware.

CryptoLocker — CryptoLocker is malware that encrypts files until a ransom is paid. Since September, CryptoLocker has become active throughout the United States including Florida. Awareness is crucial to prevent data loss.

Citizen Issues — The most common complaints we hear involve cyber stalking and harassment. In addition, in the past few weeks we received two reports of individuals threatened by "law enforcement" for non-payment of payday loans that had in fact been paid off.

Physical Security — Physical security considerations are an important part of the cyber risk management process. Many information breaches result from theft of a computer, computer component, or paperwork.

Contents

About *The 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 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.**

The Secure Florida Beacon welcomes your feedback.
www.surveymonkey.com/s/TheSFBeacon1

Contact SecureFlorida.org at:
(850) 410-7400
Admin@SecureFlorida.org

Citizen Issues

Florida Fusion Center cyber analysts regularly receive citizen concerns and complaints. These calls vary greatly, but the following articles focus on developing trends.

Cyber Harassment

The chief complaints of citizens calling the cyber analysts are from victims of cyber stalking and harassment. The complaints range from defamation of character to posting of personal information to stalking through email, websites, social media sites, and text messages. In some instances, these include threats of physical violence against the victim.

Reports of harassment on social networking sites are increasingly common. Many times, when the victim reports the harassment to the website administrators the offending pages are taken down; however a new page will often be created to continually harass the victim. It is common for this activity to continue for an extended period of time. The nature of this activity results in time-consuming efforts on the part of the victim and law enforcement in an attempt to pursue an investigation.

Payday Loan Fraud

Cyber analysts have recently received calls referencing what appears to be a fraud that targets persons who have previously obtained, or inquired online about obtaining, a payday loan. The callers reported that they received phone calls, purporting to be from a law enforcement agency, claiming that the loans were past due. The so-called detective threatened to arrest them if they did not send the money immediately. In each case, the citizens either had inquired online about obtaining a payday loan, or had previously obtained and paid off a payday loan, roughly within the past year.

The calls were not from actual victims; the callers merely wanted to report the attempt and verify that they were not truly in trouble with the law.

The cyber group is trying to determine the common denominators in this fraud, and would appreciate hearing about any other cases that have occurred. **Let Us Know**

Cyber Highlights

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.

Key Loggers

Florida Fusion Center cyber analysts received two unique reports of keyloggers deployed within Florida. The reports illustrate two common keylogger uses in criminal activity.

Florida Fusion Center cyber analysts have received reports of keylogger activity in Florida. While keyloggers are not new technology, they pose a continued threat to computer users and businesses. Keyloggers can be used to collect credit card data from point-of-sale terminals as well as user names and passwords from home computers.

Hardware keyloggers are impossible to detect with an anti-malware scan. In addition, they are small and easily concealable; some even have WiFi capability. High-end models can be purchased online for $150.00, and most are designed to fit inline on a PS/2 or USB cable. Unencrypted card readers on point-of-sale terminals and public shared computers are particularly vulnerable.

Hardware based keyloggers can be mitigated on any computer by inspection of cable connections for any extra unexplained connectors and on point-of-sale terminals by insuring that card readers transmit encrypted data.

Software keyloggers are used to target end-users, likely because they are more successful than attempting a large-scale breach of a secured database. While susceptible to anti-malware scanning, these can sometimes slip by some consumer anti-malware software, quietly capturing login credentials for months.

Currently, there are two simple ways to defeat software keyloggers. **First**, make sure that your anti-malware program is up to date and that you scan your system frequently—every day is not too often. **Second**, use two-factor authentication whenever it is available. Two-factor authentication mitigates the effectiveness of both hardware and software keyloggers.

The use of two-factor authentication is gaining popularity as many large web sites offer the feature as an option. Two-factor authentication will likely become increasingly popular as it renders the possession of a stolen password useless without the possession of the second factor.[1]

If you have had an experience with keyloggers, Florida Fusion Center cyber analysts are interested in your story. Let Us Know

Two-factor authentication requires that you supply two (or more) of the three authentication factors: *a knowledge factor, a possession factor, and an inherence factor.* In other words

- Something you **know** (such as a password or PIN)
- Something you **have** (such as a swipe card or portable authenticator)
- Something you **are** (like a fingerprint or retinal scan).

[1] **Lessons Learned In Password Security 2013** **http://www.net-security.org/article.php?id=1933**

Florida Department of Law Enforcement
Florida Fusion Center
Florida Infrastructure Protection Center

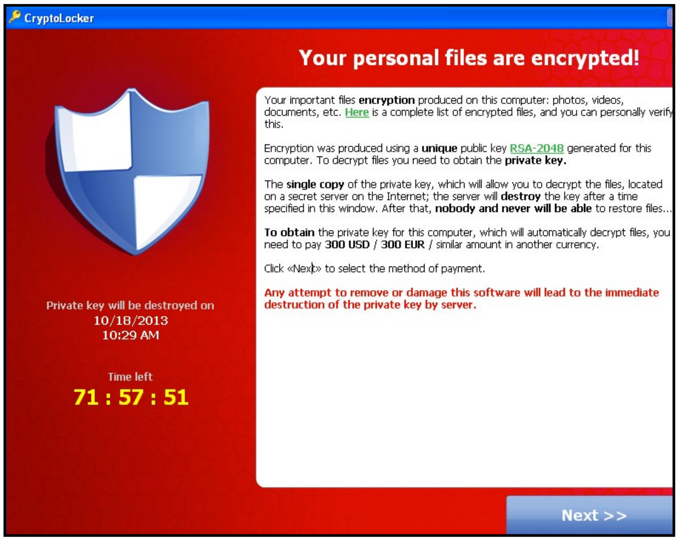
Let Us Know:
(850) 410-7400
Admin@SecureFlorida.org

CryptoLocker

The “ransomware” CryptoLocker showed up in September 2013 and spread to many businesses in the United States.

CryptoLocker is a relatively new malware discovered in early September 2013. The malware is still active and, according to open source reports, new variants are being developed.

CryptoLocker is a form of “ransomware” that prevents access to your files until you pay the ransom. This particular version encrypts the computer’s hard drive, making file access impossible until the decryption key is entered. The victim is then instructed to pay the ransom to get the key—usually $300 within 72 hours—after which the key is destroyed. At that point the data is permanently lost and the only solution is an uninfected backup file. After completion of the encryption process CryptoLocker displays a countdown message until the files are permanently destroyed.



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD** / **300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
10/18/2013
10:29 AM

Time left
71 : 57 : 51

CryptoLocker is generally delivered by spear phishing campaigns and reportedly targets businesses, however personal computers can be vulnerable. **Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data**. A typical infection method is a spear phishing email with a .zip file attachment containing a PDF file that, when opened, executes its payload. Like many malicious emails, it’s often crafted to look like a message from the victim’s “Payroll Department” or from a legitimate package delivery company. Every Windows-based computer is a potential victim.

By some accounts, there have been upwards of 250,000 CryptoLocker infections worldwide, the largest percentage of which have been in the United States. Once on a computer, this malware can encrypt available files on any connected computer or storage device.

To avoid this malware:

- Ensure computer users are aware of the threat.
- Be suspicious of emails from unknown senders and never open unexpected attachments.
- Backup your systems regularly to decrease the impact of this infection.
- Update your antivirus regularly; daily is not too often.
- Ensure that automatic updates are enabled to patch software vulnerabilities.
- Restrict access to sensitive files and, in a business environment, limit access to only those who need it to do their jobs.

If you believe your computer is infected:

- Immediately disconnect it from your network to prevent the virus from encrypting other storage mediums.
- Immediately turn off any data synchronization software that automatically synchronizes your backups. This will prevent CryptoLocker from writing over unlocked files with newly encrypted locked files.
- In a business environment, contact your IT manager.

If you have had an experience with CryptoLocker, or if you need more information **Let Us Know.**

For additional information:

CryptoLocker Ransomware
http://www.secureworks.com/cyber-threat-intelligence/threats/cryptolocker-ransomware/

Cryptolocker’s Crimewave: A Trail of Millions in Laundered Bitcoin
http://www.zdnet.com/cryptolockers-crimewave-a-trail-of-millions-in-laundered-bitcoin-7000024579/

The Florida Critical Infrastructure Protection Team

The Florida Fusion Center Network's Critical Infrastructure Protection (CIP) team consists of planners and analysts working through the network of fusion centers in Florida to prevent, deter, neutralize, and mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit Florida's critical infrastructure and key resources. Each month, *The FIPC Ledger* highlights threats and vulnerabilities within the 16 critical infrastructure sectors and explores direct impacts to Florida's public and private sector organizations.

In partnership with cyber analysts in Florida fusion centers, the CIP team works to bridge the gap between physical and cybersecurity threats and vulnerabilities. The signing of Presidential Policy Directive 21 and the Executive Order for Improving Critical Infrastructure Cyber Security brought cybersecurity to the forefront in discussions of critical infrastructure protection.

In the past, both the public and private sectors have relied exclusively on cybersecurity experts to manage the security of networks and cyber infrastructure. We now realize if we do not actively involve all members of security, both physical and cyber, we are allowing a huge vulnerability to go unchecked.

One of the primary goals of the CIP team is to enhance relationships and information sharing among private sector partners from the corporate level to the local level. The CIP team works to provide information and resources regarding common vulnerabilities and protective measures to organizations in Florida.

The Physical Side of Cyber Security

Focus: Healthcare Sector

Facilities in the healthcare sector house vast amounts of personal health information, creating an attractive target for criminals. Cyber security presents an increasingly complex risk that security managers must consider when implementing security policies, procedures, and training.

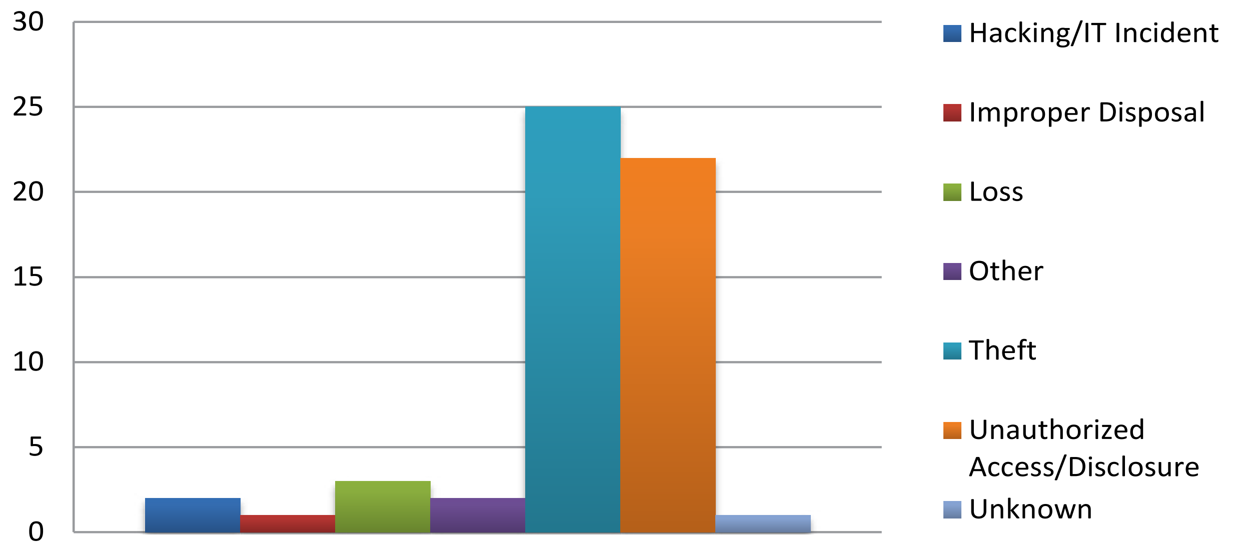
No doubt your organization has security protocols protecting your information systems. Chances are those systems are well designed and implemented. However, all security systems have in common a universal weakness in the people using the systems.

The human interface offers a dynamic and sometimes unpredictable element in information security. Sometimes it is easier to trick an employee into freely providing access to their system. Why hack what you can ask for? It is not difficult to find a used service company uniform, show up to an office with a tool belt, look official, and follow someone in. People are nice; they might even hold the door.

Theft of computer equipment, such as laptops and storage devices, is common. Laptops, due to their size and value, are particularly vulnerable; whether stolen from a facility, personal vehicle, or a hotel room. The value of the information contained on a laptop may easily outweigh the value of the laptop itself. A thief might take a laptop hoping to sell for its street value only to cost the victim business many times more in fines, lawsuits, and notification to affected clients.

Organizations in the healthcare sector are particularly vulnerable. Increased regulation due to HIPAA and the large amount of personal data residing in healthcare systems increases liability for healthcare organizations.

In October 2013 *Healthcare IT News* reported: “The Office for Civil Rights, a Department of Health and Human Services sub agency designated to investigate HIPAA breaches, has received some 80,000 complaints regarding HIPAA violations since 2003. Sixteen of those have resulted in hefty monetary penalties.”[1]



Florida Healthcare Facility PHI Breaches Affecting 500 or More Individuals March 2010 - December 2013

Source: HHS.gov

The U.S. Department of Health and Human Services listed 56 protected health information (PHI) breaches of Florida healthcare facilities affecting more than 500 individuals between March 2010 and December 2013. More than half of those breaches involved theft, loss, or improper disposal of a computer, electronic device, back-up storage, or paperwork.

Mitigating the vulnerability healthcare organizations face require close working relationships between physical security managers, policy makers, and their cybersecurity counterparts. Cyber security should be an element of an organization’s overall security and risk mitigation plan. The best network firewall available is rendered useless when an employee leaves an unencrypted thumb drive in a taxi. Likewise, the finest access control system and closed circuit camera system cannot protect against a poorly defended computer network. Information security is a team approach in any environment, particularly with such a wealth of personal information is at risk.

HealthIT.gov 10 Best Practices for the Small Health Care Environment:

- Use Strong Passwords and Change Them Regularly
- Install and Maintain Anti-Virus Software
- Use a Firewall
- Control Access to Protected Health Information
- Control Physical Access
- Limit Network Access
- Plan for the Unexpected
- Maintain Good Computer Habits
- Protect Mobile Devices
- Establish a Security Culture

www.healthit.gov/providers-professionals/cybersecurity

[1] **Unencryption at core of HIPAA breach** **http://www.healthcareitnews.com/news/unencryption-core-new-hipaa-breach**

Dispatch Highlights

This section highlights articles from the previous month's *FIPC Dispatch* 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.

Lessons Learned in Password Security 2013

http://www.net-security.org/article.php?id=1933&p=1

Summary:

- Large scale security breaches this year (as with every year) have taught us that web apps still have improvements to make.
- Two-factor authentication will continue to gain momentum as it extends security beyond a user's browser.
- The article contains four other predictions for passwords in 2014.

Analyst Note: Relying solely on passwords is increasingly less secure due to the numerous ways that hackers can harvest passwords from large-scale database breaches and deployments of malware. Many sites have started offering two-factor authentication options. Some may consider two-factor authentication bothersome, but it makes a password useless without the second factor.

Creepware - Who's Watching You?

http://www.symantec.com/connect/blogs/creepware-who-s-watching-you

Summary:

- Is a piece of tape over the webcam on your laptop overly cautious? Paranoid? Maybe not.
- Remote Access Trojans (RATs), or what we are calling "creepware," allow an attacker to have access and control of the compromised computer from a remote location.
- The article contains a video with an overview of the growing problem of creepware.

Analyst Note: Remote Access Trojans are real, particularly scary, and extremely troublesome in the hands of the wrong person. A hacker who successfully uses a remote access trojan can gain complete control of a victim machine. This blog post is a good overview of the technology, how it is being used in nefarious ways, and best practices to protect against becoming a victim.

Pre-Hacked Electronics Come Straight From China's Factories

http://www.theepochtimes.com/n3/366229-pre-hacked-electronics-come-straight-from-chinas-factories/

Summary:

- Russian customs agents found WiFi chips in several kettles and irons shipped from China.
- When plugged in the devices would search for unsecure WiFi networks and then call home.
- There is a long list of devices riddled with backdoors, infected with malware, or fitted with spying devices before leaving Chinese factories.

Analyst Note: The concept of pre "hacked" electronics is not exactly new. However, it is important to highlight the risk. This article gives a good overview of the vulnerability. In particular, it highlights the need to understand the risks associated with open WiFi networks in areas that handle sensitive information.

Help us improve *The Beacon*. Please take a moment to complete our survey.
www.surveymonkey.com/s/TheSFBeacon1

Editor
Kevin Wiggins

Design
Chris Kenworthy