Cyber Security Newsletter

December 2016

Cyber Security Articles

In This Issue

Other Interesting Links

- Slashdot
- Security Week
- Security Now

Contact Us

Cyber Security Site

Security Awareness Email

Introduction

Last month's newsletter was a different format from previous newsletters. Several people gave positive responses to that format, so I decided to do the same thing this month. Below you will see several articles that I feel most people will find interesting. Hopefully everyone will find the articles informative and interesting.

Malicious images on Facebook lead to Locky Ransomware

CSO, 21 Nov 2016: Researchers have discovered an attack that uses Facebook Messenger to spread Locky, a family of malware that has quickly become a favorite among criminals. The Ransomware is delivered via a downloader, which is able to bypass whitelisting on Facebook by pretending to be an image file. The attack was discovered on Sunday by malware researcher Bart Blaze, and confirmed later in the day by Peter Kruse, another researcher that specializes in internet-based crime and malware. The attack leverages a downloader called Nemucod, which is delivered via Facebook Messenger as a .svg file. The usage of SVG (Scalable Vector Graphics) files, is important. SVG is XML-based, meaning a criminal can embed any type of content they want – such as JavaScript. In this case, JavaScript is exactly what the attackers embedded. If accessed, the malicious image will direct the victim to a website that appears to be YouTube in design only, as it's hosted on a completely different URL.

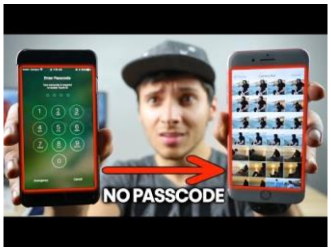
To read more click **HERE**.

Five Dollar Raspberry Pi-Based Hacking Device Can Break into Any Computer in Seconds

Softpedia, 17 Nov 2016: Passwords, iris scanning, and fingerprint protection, are all here to help protect a computer from unauthorized access, but all of these have been rendered useless by a device that costs only $5 to build. Samy Kamkar has shown in a video [**https://youtu.be/Aatp5gCskvk**] that it takes only a $5 Raspberry Pi Zero computer and free software to bypass protection on a computer using backdoor that's installed through USB. The hacking device is called PoisonTap and can emulate an Internet over USB connection that tricks the computer into believing that it's connected via the Ethernet.

To read more click **HERE**.

iOS Flaw Allows Anyone to Bypass iPhone Passcode and access photos and Messages



Softpedia, 16 Nov 2016: A new security flaw discovered in iOS allows pretty much anyone with access to your phone to bypass the passcode protection (it doesn't even matter if you configured Touch ID or not) and look at your photos or read the existing messages. Discovered by EverythingApplePro and iDeviceHelps, this glitch uses Siri to break into the device, and all it takes is a few simple steps. What's more important to know is that the same flaw exists on iOS 8 and newer, including 10.2 beta 3, but Apple is very likely to patch it in the next beta now that it has gone public

To read more click **HERE**.

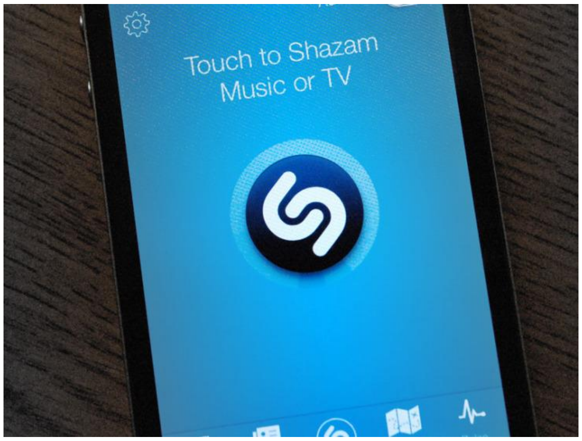
Ransomware Piggybacking on Free Software Downloads

Graham Cluley, 15 Nov 2016: A ransomware sample is piggybacking off of free software downloaded from the internet to encrypt the files of unsuspecting users. A researcher by the name of slipstream/RoL discovered the ransomware, which goes by the name "Karma." Other ransomware samples have masqueraded as Pokémon Go apps or IT security software solutions in the past. They've done so to disguise themselves so that they trick users into thinking they're benign programs. Karma is no different, which is why it's donned the mask of a Windows optimization program known as Windows-TuneUp. All that remains is for the ransomware to catch users off-guard. It does this by bundling its fake Windows-TuneUp program with other downloadable software available on the web.

To read more click **HERE**.

Shazam for Mac Keeps the Microphone on Even After Users Manually Turn It Off

Softpedia, 16 Nov 2016: Shazam has become quite a popular app for those who want to find the name of a song in a second, but it turns out that Mac users are getting some extra features that they didn't necessarily ask for. Mac security expert Patrick Wardle has discovered that Shazam keeps the microphone enabled even after the user manually turns it off, which is undoubtedly worrying for users aiming for uncompromised privacy. The company, however, claims that the simple fact that the microphone stays on is a feature and not a bug, pointing out that the app needs to do that because, otherwise, it would take longer to load and users could miss a song they want to scan.



To read more click **HERE**.

DPS Cyber Security Assists Local High School Students in Preparing for National Youth Cyber Defense Competition

Earlier this fall, several DPS Cyber Security analysts teamed up with the Liberal Arts and Science Academy (LASA) here in Austin to work with students as part of the Cyber Patriot program. Cyber Patriot is a National Youth Cyber Education Program established in 2009 that strives to inspire students toward careers in cyber security or other science, technology, engineering, and mathematics (STEM) disciplines.

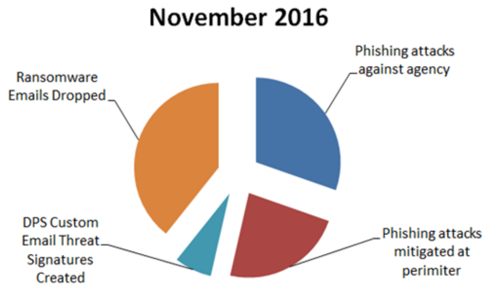
DPS Cyber Security analysts visit the LASA campus three times a week during their lunch hour to work with the high school students (mostly sophomores and juniors). The students are formed into two teams of six and are currently learning about advanced system hardening techniques and networking. Each Cyber Patriot team across the country trains to compete in the National Youth Cyber Defense Competition, which began its early rounds in November. In each round, teams are tasked with finding cyber security vulnerabilities and hardening a system while also keeping other computer functions and services (such as email) working over a six hour period. Teams can progress to the state level and even the National Finals that take place in Baltimore, MD in the spring, where they can earn national recognition and scholarship money.

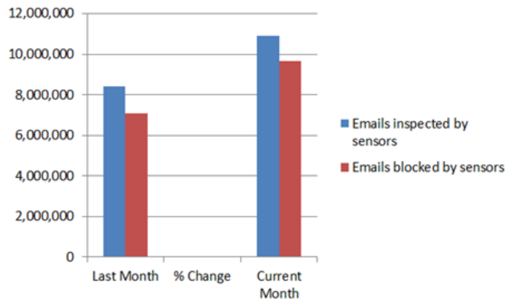
The LASA Cyber Patriot team recently competed in the first qualifying round of the competition. One team placed 175th and the other team placed 446th out of 2,000 teams nationwide. That means one of the teams placed in the top 10% in the country! The second qualifying round will be held in mid-December and offer a chance for the teams to move on to the State round in January. DPS Cyber Security is proud to be a part of introducing these students to an exciting and vital career!

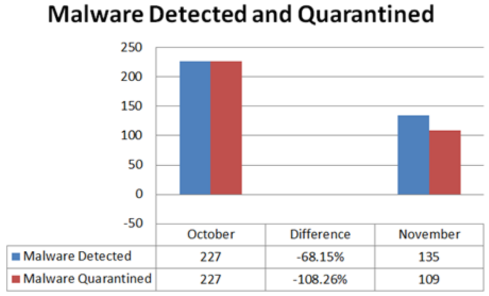
Cyber Security at work

Are you curious about what kind of things Cyber Security is dealing with and protecting the agency from?

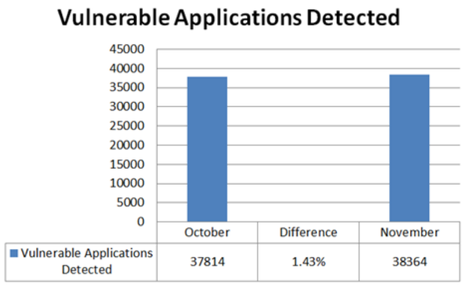
Here is some graphical information on some of the more important things we are able to release regarding what was handled within the last month.



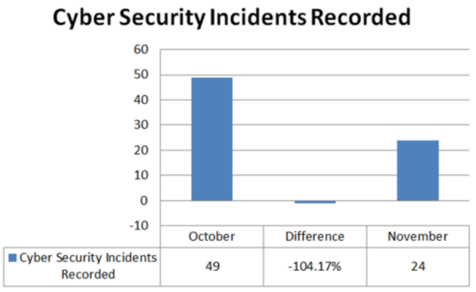




	October	Difference	November
🟦 Malware Detected	227	-68.15%	135
🟥 Malware Quarantined	227	-108.26%	109



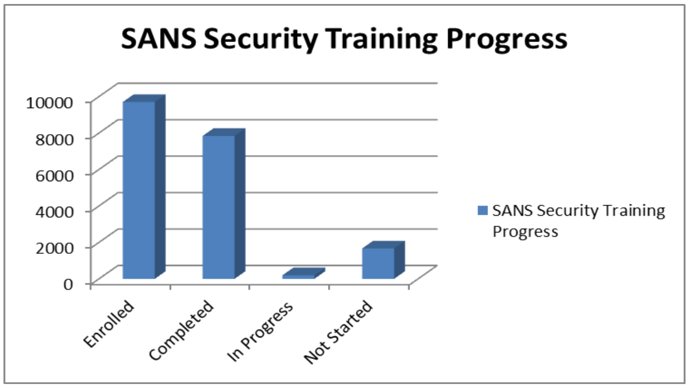
	October	Difference	November
🟦 Vulnerable Applications Detected	37814	1.43%	38364



	October	Difference	November
🟦 Cyber Security Incidents Recorded	49	-104.17%	24

Important Information

SANS Securing the Human Online Training: As a reminder, this is yearly training that everyone who has access to the DPS network must take. If you have not taken the training in the last couple of months, you need to email **GRP_Security_Awareness_Training@dps.texas.gov** and someone will be happy to assist. Those that have already completed the training can expect to see a reminder they need to take the training again in about a year.



Cyber Security Awareness Training Officer: For those who don't know, I am also a pilot in the Texas Army National Guard. I am currently scheduled to be deployed to the Middle East after the first of the year. Others on the Cyber Security team will be taking over my duties while I am gone. January's newsletter, and all other newsletters until I get back, will be written and sent out by someone else on the team. I am confident that you will find those newsletters just as informative as mine have been.

For More Information

For information, tutorials and contact information about this month's topics, you can click the links on the side of the newsletter. For other Cyber Security news, please visit the Cyber Security website. Remember that security is a shared responsibility and,

"**Do Good Cyber.**"

Cyber Security Training Officer

Kirk Burns is the Cyber Security Training Officer for DPS. He has a BS in Criminal Justice, a BS in Computer Science, and an MS in Digital Forensics. He is a Computer Science professor for Sam Houston State University with over 16 years of IT experience. Kirk serves as a member of the Texas Army National Guard and holds a current CISSP certification.

If you have further questions about this month's topic or any other security issue, do not hesitate to contact him. He is happy to assist. You can contact him via email at kirk.burns@dps.texas.gov, on his work phone at 512.424.5183 or on his work cell at 512.466.3151.