Cyber Security Newsletter

November 2016 NMCIWG

In This Issue

Other Interesting Links

- Slashdot
- Security Week
- Security Now

Contact Us

Cyber Security Site

Security Awareness Email

Introduction

For this month's newsletter I decided that I would use interesting articles from a Cyber Security newsletter I read. There are other organizations that put out Cyber Security newsletters that include very interesting articles. The articles below are from a newsletter called ***The Cyber Shield*** produced by the New Mexico Counterintelligence Working Group (NMCIWG). Information from the articles is reposted word for word from the source.

Microsoft: Beware this fake Windows BSoD from tech support Scammer's malware

ZD Net, Oct 24, 2016: Microsoft has sounded the alarm over a fake installer for its Security Essentials, which attempts to trick victims into contacting bogus help centers. Tech-support scammers have stepped up their technical game, prompting a "severe" warning from Microsoft over new Windows malware that mimics Microsoft's free Security Essentials antivirus, and then displays a fake blue screen of death, or BSoD, with an error message and a suggestion to call a 1800 number that is not a Microsoft support center. To read more click **HERE**.

Why it was so easy to hack the cameras that took down the web

C/Net, 24 Oct 2016: If you were anywhere near the internet in the US on Friday, you probably noticed a bunch of your favorite websites were down for much of the day. Now experts are saying it's all because thousands of devices -- like DVRs and web-connected cameras -- were hacked. Once the hackers had control over these devices, they manipulated them into sending an overwhelming number of requests to a company that serves up the websites for Netflix, Google, Spotify and Twitter. To read more click
HERE.

It's nearly 2017 and JPEGs, PDFs, font files can hijack your Apple Mac, iPhone, iPad

TheRegister, 24 Oct 2016: Apple has distributed a fresh round of security updates to address remote-code execution holes in iOS, macOS, Safari, and the firmware for Apple Watch and AppleTV. Miscreants who exploit these flaws can take over the vulnerable device – all a victim has to do is open a JPEG or PDF file booby-trapped with malicious code, so get patching before you're caught out. To read more click **HERE**.

IoT Devices Can Be Hacked in as Little as Three Minutes

Softpedia, 26 Oct 2016: Those apocalyptic Mr. Robot episodes are slowly becoming a reality as IoT devices are spreading not only in our homes but also across enterprise networks, providing access points into networks that often control critical services. With 6.4 billion IoT devices already online, researchers estimate that over 20 billion IoT devices will be connected to the Internet by 2020. That's why many security experts argue that now is the time to make sure that IoT security is taken seriously before it will be too late. For more details on some of the ways hackers can exploit IoT security flaws, you should take a look at ForeScout's IoT Enterprise Security Risk report (**link**). To read more click **HERE**.

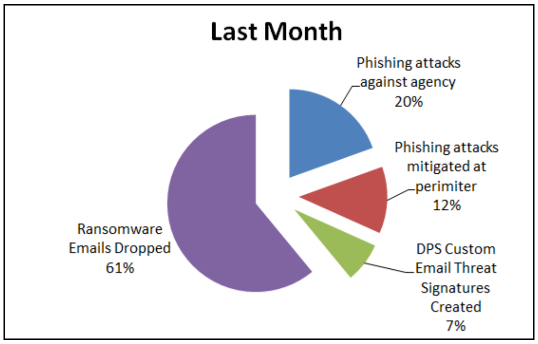
App proves Rowhammer can be exploited to root android phones

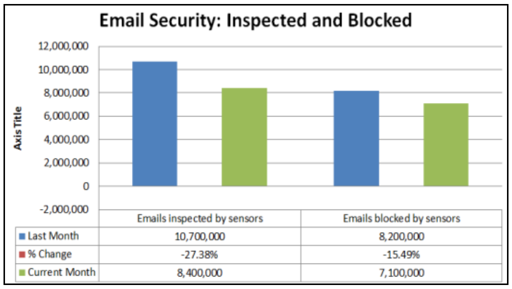
TheRegister, 24 Oct 2016: Security researchers have demonstrated how to gain root privileges from a normal Android app without relying on any software bug. The unprivileged application is able to gain full administrative permissions by exploiting the Rowhammer vulnerability present in modern RAM chips. To read more click **HERE**.

Cyber Security at work

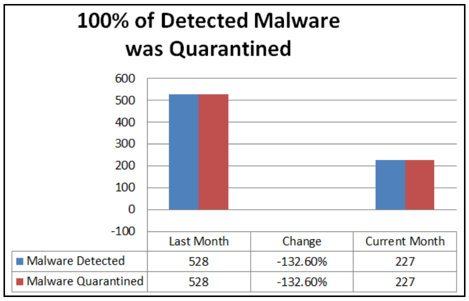
Are you curious about what kind of things Cyber Security is dealing with and protecting the agency from?

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.

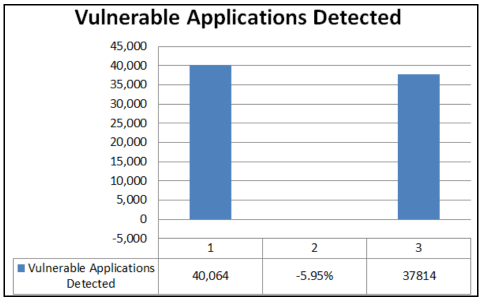




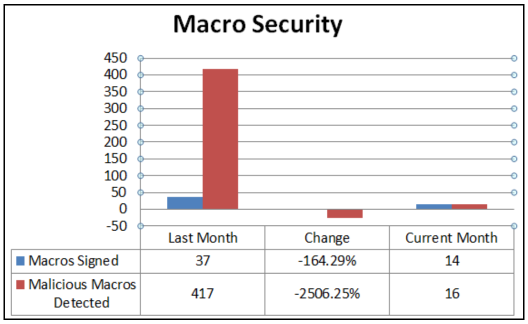
	Emails inspected by sensors	Emails blocked by sensors
🟦 Last Month	10,700,000	8,200,000
🟥 % Change	-27.38%	-15.49%
🟩 Current Month	8,400,000	7,100,000



	Last Month	Change	Current Month
🟦 Malware Detected	528	-132.60%	227
🟥 Malware Quarantined	528	-132.60%	227



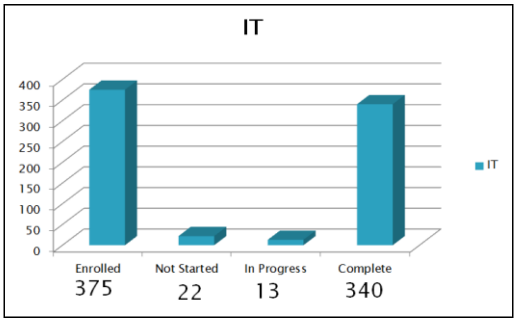
	1	2	3
🟦 Vulnerable Applications Detected	40,064	-5.95%	37814



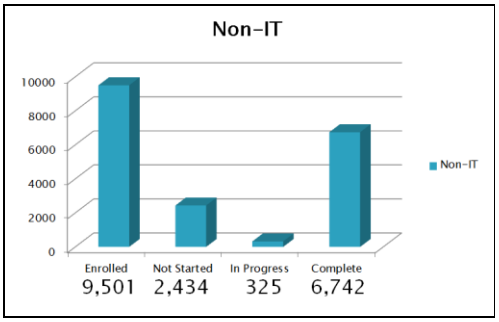
	Last Month	Change	Current Month
🟦 Macros Signed	37	-164.29%	14
🟥 Malicious Macros Detected	417	-2506.25%	16

Important Information

SANS Securing the Human Online Training: Don’t forget that everyone is required to take the SANS Securing the Human online training. Anyone with an ACID who has access to the DPS system is required to take the training. If you need assistance, you can email **GRP_Security_Awareness_Training@dps.texas.gov** and someone will be happy to assist.



IT SANS STH Training Status



Non-IT SANS STH Training Status

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 will be written and sent out by someone else on the team.

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.