NEWS
# Cyber Security
Vol. 3 | Issue 9
September 2018



## Hello everyone and welcome to this month's TXDPS Cyber Newsletter.

I want to start the newsletter by reminding everyone I am still in the process of resetting the Cybersecurity Awareness Training for everyone who did the training two years ago. If you took the training in 2016, you are up for retraining. DPS policy is all new users must complete security awareness training within 30 days of being granted access to any Department information resources. The Agency also requires everyone to take cybersecurity awareness training biannually. There were approximately 9,000 people who took the training two years ago, and I am trying to space out the training so everyone is not due at the same time. I have reset approximately 6700 people between August and now. The rest of the people this pertains to should be reset at the beginning of October. Once you have received an email notifying you that your account has been reset, you will have 30 days to complete the training. You will be provided a temporary password that will have to be changed when you login to the training. After you get into the system, you will see training modules broken down into two categories. You must complete all the training modules in the Mandatory section to get credit for the training. You do not have to complete the Recommended modules but it is highly encouraged because there is good information in those modules.

This information currently only applies to those users who took the training two years ago. For people who started working at DPS less than two years ago, this does not apply until you hit your two year mark. When you are close to the two year mark, you can expect to receive an email notifying you it is time to redo your cybersecurity awareness training. You will have 30 days from when you receive that email to complete the training.


With the upcoming elections, the news has been full of talk about foreign interference with our election process. This is something we should all be concerned about, so I wanted to take a few minutes to discuss this and provide information you might find interesting and informative about the election process from the cyber point of view. As you read this month's newsletter you will see articles pertaining to the elections as well as other articles I believe you will find interesting. However, there are a few that I feel need special attention so I wanted to emphasize them here.

The first is about securing elections. Unfortunately it is impossible to 100% prevent any sort of cyber tampering on a system. Just when you think the system is completely secure, someone finds a way to compromise a computer no one else has thought about. A report from the National Academies of Sciences, Engineering, and Medicine states Internet voting should not be used at this time and only paper ballots should be used. While paper ballots are not themselves foolproof, it is believed by some they are more secure than electronic means.

Another article that should alarm everyone is about 14 million voter records being exposed online. There are 15.2 million registered voters in Texas and 14.8 million of those peoples records were found on an UNSECURED server. Apparently it is unknown who owns the server but Techcrunch says it appears the data was likely aggregated by Data Trust. Some of the more concerning information potentially leaked: voters' name, age, gender, race, phone number, voting history, and other data. Information easily used to steal a person's identity.

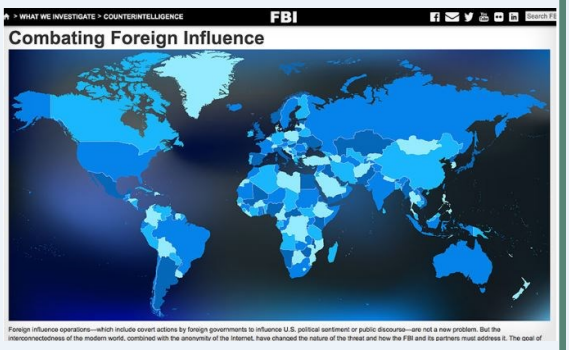
The third article I want to single out is from TheHill.com. They report a bipartisan group of lawmakers on the Senate Intelligence committee have recently raised concerns about voting systems provided by one of the largest vendors in the U.S. Their concerns stem from the vendor not agreeing to undergo independent testing on their systems to determine the security level.

The final article is about an 11-year-old who was able to hack into a voting system in 10 minutes. Don't think much needs to be said about this.

In closing, I hope you enjoy this month's newsletter and I suggest you closely read the second article on the next page.

# Election Cyber News!!

## Election Security: FBI Combats Information Operations




**(By Mathew J. Schwartz, August 31, 2018**

It's less than 10 weeks until your country's elections; do you know where your government's information warfare defenses and election security strategy are?

**See Also:** How to Combat Targeted Business Email Compromise Attacks

With the U.S. midterm election primaries already well underway, the FBI this week launched an informational website that describes the bureau's actions to counter propaganda and influence operations being run by foreign governments (see *Redoubling Efforts to Secure Midterm Election*).

> "Stymied by a lack of shared understanding of what happened, the government's sclerotic response has left the United States profoundly vulnerable to future attacks."

"Foreign influence operations - which include covert actions by foreign governments to influence U.S. political sentiment or public discourse - are not a new problem," the FBI's site notes. "But the interconnectedness of the modern world, combined with the anonymity of the internet, have changed the nature of the threat and how the FBI and its partners must address it. The goal of these foreign influence operations directed against the United States is to spread disinformation, sow discord, and, ultimately, undermine confidence in our democratic institutions and values."

Click **HERE** to read more.

## Justice Department Warns It Might Not Be Able to Prosecute Voting Machine Hackers

**(By Kim Zetter Aug 30 2018, 1:12 pm)**

**DoJ says current federal law against hacking doesn't apply to voting machines because they aren't connected to the internet; but this plus a proposed amendment could create a problem for prosecuting hacks of other computers not connected to the internet.**

After more than a decade of headlines about the vulnerability of US voting machines to hacking, it turns out the federal government says it may not be able to prosecute election hacking under the federal law that currently governs computer intrusions.

Per a Justice Department report issued in July from the Attorney General's Cyber Digital Task Force, electronic voting machines may not qualify as "protected computers" under the Computer Fraud and Abuse Act, the 1986 law that prohibits unauthorized access to protected computers and networks or access that exceeds authorization (such as an insider breach).

The report says the law generally only prohibits against hacking computers "that are connected to the Internet (or that meet other narrow criteria for protection)" and notes that voting machines generally do not meet this criteria "as they are typically kept off the Internet." Consequently, "should hacking of a voting machine occur, the government would not, in many conceivable circumstances, be able to use the CFAA to prosecute the hackers."

**NOTE: Best viewed in Firefox. Often will not display in Internet Explorer.**

Click **HERE** to read the article.

# Wayback and Google

## Archive.org's Wayback Machine is legit legal evidence, US appeals court judges rule

**(by Kieren McCarthy in San Francisco 4 Sep 2018 at 19:38)**


**Analysis** The Wayback Machine's archive of webpages is legitimate evidence that may be used in litigation, a US appeals court has decided.

The second circuit ruling [PDF] supports a similar one from the third circuit – and, taken together, the decisions could pave the way for the Internet Archive's library of webpages to be considered evidence for countless future trials.

The second circuit, based in New York, was asked over the summer to review an appeal by an Italian computer hacker in which he sought to exclude screenshots of websites run by him that tied him to a virus and botnet he was ultimately convicted over. Prosecutors had taken screenshots of his webpages from the Internet Archive and used them as trial evidence – and he wanted the files thrown out.

Fabio Gasperini argued that the presented Wayback Machine archives of his webpages were not adequately authenticated as legit and untampered, and so shouldn't have been included in his criminal trial. He cited a decision by the second circuit to argue his point, noting that in a 2009 case, the appeals court had agreed with a lower district court decision to exclude screenshots of Wayback Machine snapshots because their authenticity could not be proven.

Click **HERE** to read more.

## A Google Engineer Discovered a Vulnerability Letting Him Take Control of Keycard-Controlled Doors

**(by Tom McKay 3 Sept 2018 at 4:20 pm)**

A Google engineer discovered a vulnerability in the third-party system controlling access to doors across its campus in Sunnyvale, California, and took the opportunity to prove that he could bypass any RFID keycard-operated lock in the facility, Forbes reported on Monday.

According to Forbes, employee David Tomaschik discovered that Software House devices connected to Google's network used an unsecure, hardcoded encryption key, and launched the attack to prove the consequences that could arise:

Last summer, when Tomaschik looked at the encrypted messages the Software House devices (called iStar Ultra and IP-ACM) were sending across the Google network, he discovered they were non-random; encrypted messages should always look random if they're properly protected. He was intrigued and digging deeper discovered a "hardcoded" encryption key was used by all Software House devices. That meant he could effectively replicate the key and forge commands, such as those asking a door to unlock. Or he could simply replay legitimate unlocking commands, which had much the same effect.

Click **HERE** to read more.

# Windows / SonarSnoop

## Windows utility used by malware in new information theft campaigns

**(By Charlie Osborne for Zero Day | September 3, 2018)**

WMIC-based payloads highlight how attackers are turning to innocuous system processes to compromise Windows machines.

Researchers have uncovered a new attack chain which exploits little-known Microsoft Windows utilities and innocuous software to fly under the radar in the quest to steal data.

According to Symantec, the new malware campaign is a prime example of what the company calls "living off the land."

In other words, attackers are now turning to the resources already available on target machines -- including legitimate tools and processes -- as well as running simple scripts and shellcode in memory and performing fileless attacks.

By focusing more on homegrown software and less on introducing foreign malware into target systems, threat actors can remain undetected for longer and minimize the risk of being exposed.

A new attack chain takes this technique to heart.

Symantec noticed the campaign, which has been recently discovered, utilizes a tool found on all Microsoft Windows machines called the Windows Management Instrumentation Command-line (WMIC) utility.

Click **HERE** to read more.

## SonarSnoop attack can steal smartphone unlock patterns

**(by Catalin Cimpanu for Zero Day | September 3, 2018)**

SonarSnoop technique transforms smartphones into mini sonar systems to track a user's finger across the screen and steal phone unlock patterns.

Academics from universities in Sweden and the UK have come up with a new technique that turns a smartphone's built-in speaker and microphone into a crude sonar system to steal phone unlock patterns from Android devices.


The general idea behind this technique --named SonarSnoop-- is to use sound waves to track a user's finger position across a screen.

The technique consists of using a malicious app on the device to emit sound waves from the phone's speakers at frequencies inaudible to the human ear --between 18kHz and 20kHz.

Just like in the case of a submarine's sonar, the malicious app uses (the device's) microphones to pick up the sound waves bouncing back off nearby objects, which in this case is the user's finger(s).

Depending on the placement of speakers and microphones on a device's case, machine learning algorithms can be built to read the collected data and determine possible unlock patterns.

In a research paper published last week, academics from Lancaster University in the UK and Linköping University in Sweden detail tests of SonarSnoop on a Samsung Galaxy S4 smartphone running Android 5.0.1.

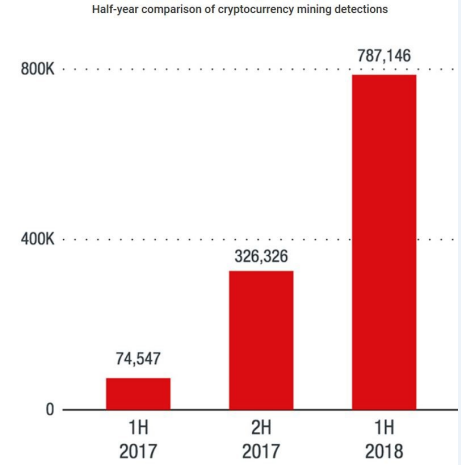
The research team says it was able to reduce the number of possible unlock patterns by 70% using data obtained with SonarSnoop.

Click **HERE** to read more.

# TTPs / Facebook

## Cybercriminals shift tools, tactics and procedures to improve infection rates

**(Help Net Security August 29, 2018)**




Trend Micro released its Midyear Security Roundup 2018, revealing that cybercriminals are moving away from attention-grabbing ransomware attacks to more covert methods intended to steal money and valuable computing resources.

Cryptojacking attempts are making the biggest impact so far this year. Trend Micro recorded a 96 percent increase in cryptocurrency mining detections in 1H 2018 compared to all of 2017, and a 956 percent increase in detections versus 1H 2017. This indicates cybercriminals are shifting away from the quick payout of ransomware in favor of the slower, behind-the-scenes approach of stealing computing power to mine digital currency.

"The recent change in the threat landscape mirrors what we've seen for years – cybercriminals will constantly shift their tools, tactics and procedures (TTPs) to improve their infection rates," said Jon Clay, director of global threat communications for Trend Micro. "Standard spray and pray ransomware attacks and data breaches had become the norm, so attackers changed their tactics to be more covert, using entry vectors not previously seen or used extensively. This means once again, business leaders must evaluate their defenses to ensure sufficient protection is in place to stop the latest and most pressing threats."

Click **HERE** to read more.

## AN UNDISCOVERED FACEBOOK BUG MADE ME THINK I WAS HACKED

**(by Louise Matsakis 08.24.18 02:55 PM)**

My legs were sticking to the vinyl back seat of a NYC cab when I received the email on a Thursday this July. I was running late to an afternoon dentist appointment, and sending messages on Facebook Messenger. Most of the conversations were for a story I was reporting about a Facebook group for sexual assault survivors, which had been overtaken by abusers.

At the time, I was messaging with one of the abusers—who was using a fake profile—hoping to find out how they weaponized the group for harassment. In the middle of our exchange, I received an email from Facebook, which said, "We wanted to let you know that your mobile number was removed from your account. Because of this, we've turned off two-factor authentication on your account to make sure you don't get locked out when using an unrecognized computer or mobile device to log in."

I hadn't removed my phone number; I immediately assumed I had been hacked, especially given the story I was reporting. Like hundreds of millions of people around the world, my Facebook account contains the record of a decade of my life. But in this case, my messages also contained stories of harassment by the same person I believed had breached my account.

The message didn't include an easy way to notify Facebook that I hadn't authorized the change, though there was a button informing me I could add a new mobile number if I wished. From the taxi, I called my editor, as well as another colleague, in an effort to contact Facebook as soon as possible.

While I paced my dentist's office and tried to explain the situation to the receptionist, my coworker reset my password from a laptop at work. She checked the "active sessions" on my account, the devices on which I was logged in. She didn't find anything amiss—my Facebook looked normal.

Click **HERE** to read more.

# More News

**Iranian hackers target 70 universities worldwide to steal research**

https://www.zdnet.com/article/iran-hackers-target-70-universities-in-14-countries/

**Hacking Pacemakers**
https://www.youtube.com/watch?v=fHW5egbktKA

(This is an old video but there are some who are starting to suspect targeted murders might be possible/happened)

**China Believes Its Cyber Capabilities Lag Behind US: Pentagon**
https://www.securityweek.com/china-believes-its-cyber-capabilities-lag-behind-us-pentagon

**Severe PHP Exploit Threatens WordPress Sites with Remote Code Execution**
https://threatpost.com/severe-php-exploit-threatens-wordpress-sites-with-remote-code-execution/136649/

**Cryptocurrency investor robbed via his cellphone account sues AT&T for $224 million over loss**
https://www.cnbc.com/2018/08/15/cryptocurrency-investor-sues-att-for-224-million-over-loss-of-digita.html

**Hackers Steal $13.5 Million Across Three Days From Indian Bank**
https://www.bleepingcomputer.com/news/security/hackers-steal-135-million-across-three-days-from-indian-bank/

**Instagram users are reporting the same bizarre hack**
https://mashable.com/2018/08/13/instagram-hack-locked-out-of-account/#3cNye3O4pqqj

**Security MadLibs: Your IoT *electrical outlet* can now pwn your *smart TV***
https://www.theregister.co.uk/2018/08/21/mcafee_flaws_smartplugs/

**Facebook removes 652 pages, groups and accounts linked to Iran, Russia**
https://www.cbsnews.com/news/facebook-pages-removed-today-linked-to-russia-iran-2018-08-21/

**Study from Vanderbilt professor finds Google tracking is even creepier than you thought**
https://www.yahoo.com/news/study-vanderbilt-professor-finds-google-tracking-even-creepier-192537593.html

# More News

**Hackers steal more than $1M from global economy in a single minute: analysis**

http://thehill.com/policy/cybersecurity/402716-security-firm-says-hackers-steal-more-than-one-million-dollars-from-the

**If you're still using a fax machine for 'security' think again**
https://www.engadget.com/2018/08/20/fax-machine-hack/?yptr=yahoo

**Animoto hack exploses personal information, location data**
https://techcrunch.com/2018/08/20/animoto-hack-exposes-personal-information-geolocation-data/?yptr=yahoo

**Skype launches end-to-end encryption for calls and texts**

https://www.engadget.com/2018/08/20/skype-private-conversations-available/?yptr=yahoo

**Microsoft uncovers more Russian hacking ahead of midterms**

https://finance.yahoo.com/news/microsoft-uncovers-more-russian-attacks-040636840.html

**Connected car data handover headache: There's no quick fix...and it's NOT just Land Rovers**

https://www.theregister.co.uk/2018/08/21/connected_car_data_handover_mess/

**Top antivirus tool nuked from macOS App Store - after it phoned browser histories to China**

https://www.theregister.co.uk/2018/09/07/adware_doctor_removed_apple/

**Your Visio smart TV might tell you if it spied on you**

https://www.engadget.com/2018/09/08/vizio-smart-tv-class-action-notice/?yptr=yahoo

**Charges against North Korea mark new phase in cyber crackdown**

http://thehill.com/policy/cybersecurity/405668-charges-against-north-korea-mark-new-phase-in-cyber-crackdown

**Trump administration weighs sanctions over Chinese hackers: report**

http://thehill.com/policy/cybersecurity/405656-trump-administration-considering-sanctions-over-chinese-hackers

# </Closing Comments>

As you can see from the newsletter there are a lot of interesting things that have happened over the last month. I provided you with 32 different articles but that is by no means all that has happened. For your own education I strongly recommend you use these articles to lead you to other cybersecurity related articles. Educating yourself about cyber related issues not only keeps DPS safer but also improves yours, your family and your friends' security. As the old saying goes, "knowledge is power." The more educated you are on a topic the better prepared you are to defend yourself.

As you are researching the topics, don't forget to email me things you find. I encourage active participation in the education process and I believe that if you find articles of value to you that others will find them of value also. Please forward articles to me so that I can incorporate them into future newsletters.

On a different topic, I came across an online game that is very simplistic but puts you in the shoes of a new Chief Information Security Officer (CISO). The online "game" is from Trend Micro and simulates challenges a new CISO faces at a local hospital when hit by Ransomware. Here is the game overview:

"In **Data Center Attack: The Game**, put yourself in the shoes of a CISO at a hospital to see if you can go back in time to prevent a data center attack from holding critical patient data hostage. You'll be prompted to make decisions that will impact your security posture. Wrong choices could result in ransomware hijacking your patient data and putting lives at risk. Right choices will show you what happens with DevOps and IT work together, will allow doctors to see patient data, and the hospital will run as expected. See if you have the knowledge it takes to stop a data center attack, and if not, learn what defenses you need to prevent one."

Remember no game can fully show you what all goes into the decisions a CISO (or anyone in Cyber or IT) has to make to protect an organization. However, I see things in this game that can help the average user not only understand the thought process behind decisions but also how THEIR actions (or inactions) can help or hinder an organizations security posture. So, if you wish to try your hand, you can find the link to the game HERE.

One final thought before you tackle this month's Cyber Challenge, all newsletters are posted on a public facing DPS website. Feel free to look at past newsletters and/or share the link with your friends. You can find the link by clicking on the General Info tab at http://www.dps.texas.gov/. In the tab you will see a link for Cyber Security Newsletter. Click the link and it will take you to a page with all of the newsletters created for the last two years.

Happy reading.

Kirk

# Cyber Challenge

**Employees Who Solved Last Month's Challenge and Notified Me**

Below are the people who emailed me with the solution to last month's challenge. The date and times listed are the

| | | |
|---|---|---|
| Deborah Wright @ 1941 on 6 Aug | Benjamin Pasmore @ 0954 on 7 Aug | Rene Hess @ 0403 on 9 Aug |
| Tracy Kingsley @ 0912 on 7 Aug | Wished not to be named @ 1117 on 7 Aug | Nirav Kumar @ 1016 on 10 Aug |
| Erich Neumann @ 0915 on 7 Aug | David Evans @ 1610 on 7 Aug | Jaelyn Edwards @ 0923 on 15 Aug 2018 |

timestamp on the email they sent with the correct answer. Congratulations to these individuals.

For those who weren't able to figure out the challenge and would like to know, email me and I'll tell you how to solve the challenge.

---

This month's challenge is another steganography and encoding challenge. You will have to find multiple hidden parts, decode them, and assemble them in order to get the quote. You will then need to determine who said the quote.. When you believe you have figured out the challenge, email me (kirk.burns@dps.texas.gov) the full quote as well as who said it. Good luck with the challenge. If you run into problems you can email me for clues.

**To get you started:**

PV VPG BGLJJO RPVYQ. YG ZTQU SVP'U RPVY.

Good Luck

Kirk