NEWS
Cyber Security
Vol. 3 | Issue 7 July 2018

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

Before we get to the interesting articles I found for this month's newsletter, I want to spend a couple of minutes talking about the upcoming online cybersecurity re-training. If you were a DPS full-time employee two years ago, you are more than likely due for re-training. For those employees, you can expect to receive an email about the training sometime between August and October. When you receive the email it will show it is coming from me but will also have the red banner notifying you the email is coming from a non-DPS email address. Please do not delete the email because it is a legitimate email and not spam. The training is required by TAC 202 as well as Agency policy for ALL employees. Per the General Manual, you will have thirty (30) days to complete the assigned training. If you do not complete it in that time you will receive an email reminder and have an additional week to complete before your supervisor is notified that you need to complete the training. If you have any questions, feel free to email or call me.

A couple of days ago, one of our Operations Security Analyst told me they have received several tickets in the past couple of weeks regarding spoofing of DPS emails being sent to retirees. He suggested it might be a good idea to talk about this in the newsletter. As our analyst pointed out, just because you have retired from DPS does not mean you will not still be a target.

So, what is spoofing? Except under special circumstances, spoofing is when an entity impersonates another device or user on a network in an attempt to do something malicious such as attack a network, steal data, spread malware, bypass access controls, etc. While not the only way to spoof, most people encounter this via email. There are legitimate uses of spoofing, such as our online security training, but most are often malicious. It is very easy to spoof an email or phone call so it looks like it came from a specific person or organization. This is one of the tricks used in a phishing attack to convince people it is safe to click on hyperlinks in the email or open the attached documents. Unfortunately there is nothing we can do to prevent it. Anyone can pretend to be someone you know in an email. So be warry of clicking on or opening anything that comes via email. If you do not know it was supposed to be coming to you, best to verify even if it seems to be coming from someone you know. If it appears to be coming from a corporation, such as your bank, call them to verify before clicking on the link. A little bit of paranoia is not a bad thing when trying to stay safe online.

To find out more about spoofing checkout these links:

Email Spoofing

Phone Spoofing Video

Another Phone Spoofing Video

Cyber News!!

Novel transmitter protects wireless devices from hackers

(From EurekAlert!, 7 June 2018) Device uses ultrafast 'frequency hopping' and data encryption to protect signals from being intercepted and jammed.

Today, more than 8 billion devices are connected around the world, forming an "internet of things" that includes medical devices, wearables, vehicles, and smart household and city technologies. By 2020, experts estimate that number will rise to more than 20 billion, all uploading and sharing data online.

But those devices are vulnerable to hacker attacks that locate, intercept, and overwrite the data, jamming signals and generally wreaking havoc. One method to protect the data is called "frequency hopping," which sends each data packet, containing thousands of individual bits, on a random, unique radio frequency (RF) channel, so hackers can't pin down any given packet. Hopping large packets, however, is just slow enough that hackers can still pull off an attack.

Now MIT researchers have developed a novel transmitter that frequency hops each individual 1 or 0 bit of a data packet, every microsecond, which is fast enough to thwart even the quickest hackers.

The transmitter leverages frequency-agile devices called bulk acoustic wave (BAM) resonators and rapidly switches between a wide range of RF channels, sending information for a data bit with each hop. In addition, the researchers incorporated a channel generator that, each microsecond, selects the random channel to send each bit. On top of that, the researchers developed a wireless protocol—different from the protocol used today—to support the ultrafast frequency hopping.

Click **HERE** to read more.

IRS' Rush to Secure Exposed Taxpayer Data Left It Vulnerable Again

(**By Joseph Marks, June 25, 2018**) Personal information about more than 350,000 taxpayers was compromised in 2015. Three years later, it's still not secure.

In its rush to respond to a 2015 crisis that allowed scammers to access the personal information of more than 350,000 taxpayers, the Internal Revenue Service skipped required security plan updates and risk assessments.

That haste may have left the already compromised taxpayer data vulnerable for years to come, according to an audit released Thursday.

The 2015 crisis was spawned by weaknesses in the identity verification process for the IRS; "Get Transcript" feature.

Because the verification process wasn't rigorous enough, scammers were able to use taxpayers' personal information gathered from other sources including data breaches, to get copies of their tax records and all the personal information they contained.

The fraudsters could then use that data to file phony tax returns and steal refunds or for other nefarious purposes.

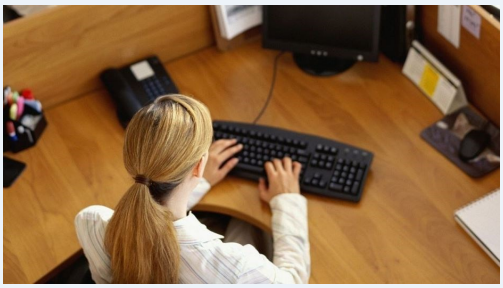
Click **HERE** to read more.

More Cyber News!!

How telework fuels the insider threat

(**By Justin Lynch, 25 Jun 2018**) Executives and business owners believe that working out of the office is a security risk.

An overwhelming majority of American business leaders believe that the risk of a data breach is higher when employees work remotely, a grave warning that comes on the heels of intelligence secrets being stolen from home computers.



According to a June 20 study by Shred-it, 86 percent of corporate executives and 60 percent of small business owners believe that the risk of a data breach increases when employees work out of the office.

"Employees working remotely can expose businesses to both physical and digital breaches, so it is important to have policies and safeguards in place," the report said.

The report found that 69 percent of corporate executives and 71 percent of small business owners attribute data breaches to employees through accidental error and human loss. Business and government leaders have ramped up their focus on the "insider threat," or belief that employees are the biggest risk to a company's information security.

Click **HERE** to read more.

"WannaCrypt" ransomware scam demands payment in advance!

(**By Paul Ducklin, 22 June 2018**) What's worse than ransomware that scrambles all your files and demands money for the key to unlock them and get them back?

Well, WannaCry certainly added a new dimension to the ransomware danger, because it combined the data-scrambling process with self-spreading computer virus code.

As a result, WannaCry could worm its way through your network automatically, potentially leaving you with hundreds or even thousands of scrambled computers in a single attack, even if only one user opened a booby-trapped attachment or downloaded a file from a poisoned website.

The crooks behind the SamSam ransomware have also latched onto a rather different approach: instead of trying to reach thousands or tens of thousands of victims around the world with a hard-hitting spam campaign, and squeezing each of them for hundreds or thousands of dollars each, the SamSammers seem to attack one organization at a time.

Indeed, the SamSammers generally keep their hand hidden until they have broken into the network and figured out, using similar techniques to penetration testers, a list of computers they know they can encrypt all at the same time.

Click **HERE** to read more.

More Cyber News!!

Malicious App Infects 60,000 Android Devices—But Still Saves Their Batteries

(**By Lindsey O'Donnell, 22 June 2018**) A battery-saving app that also allows attackers to snatch text messages and read sensitive log data has been downloaded by more than 60,000 Android devices so far.

But what's unique about the attack, according to the researchers at RiskIQ who discovered it, is that it holds true to its advertising: It actually does monitor devices' battery status, even killing unwanted background processes.

"Although the app these scam pages send users to does its advertised function, it also has a nasty secret—it infects victims' devices and comes with a side of information-stealing and ad-clicking," Yonathan Klijnsma, threat researcher at RiskIQ, said in a post on Thursday.

Klijnsma told Threatpost that after a complaint was filed for take-down, the app, called "Advanced Battery Saver," has been taken down by Google Play.

Google did not respond to a request for comment from Threatpost.

Click **HERE** to read more.

Windows 10 update broken Google Chrome? Microsoft releases new fix

(**By Nick Heath, June 27, 2018**) The latest round of patches for Windows 10 resolves recent issues with Google's popular browser.

If you've been struggling to get Chrome to work on Windows 10 then help may be at hand.

Microsoft's latest round of patches for the OS resolves an issue that was stopping Chrome from working on some Windows 10 devices.

The fix should resolve issues with all versions of Chrome following build 67.0.3396.79, which was released in early June.

It is not the first time that Windows 10 has clashed with the popular Google browser. After Microsoft introduced a bundle of new features to Windows 10 with the April 2018 Update, a number of users complained about frozen screens and other issues.

These latest patches for Windows 10, bundled under the update KB4284848, are for machines that have applied the April 2018 Update and are running build 1803.

Click **HERE** to read more.

More Cyber News!!

Facebook tests lasers that shoot high-speed internet through the sky

(**By Gordon Gottsegen, June 28, 2018**) How can Facebook expand past its 2.2 billion monthly active users? Perhaps by bringing the internet to more places.

Facebook has tested one method that users plane-mounted lasers that can shoot a high-speed internet connection through the sky, according to February 2018 paper seen by Business Insider. With the lasers, the company was able to create a wireless link between the plane and a ground station 9 km (5.6 miles) away. Facebook confirmed these details to CNET.

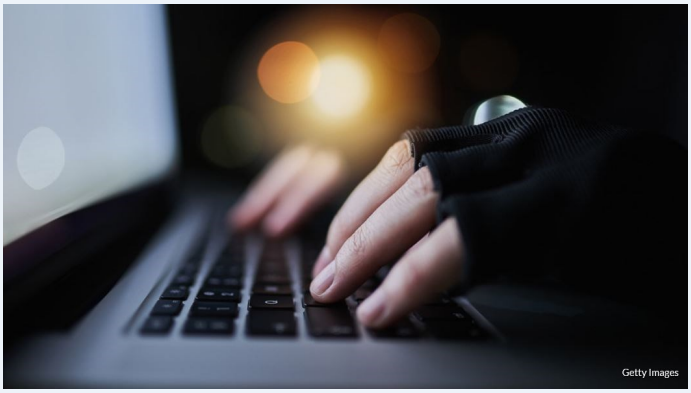
Although experimental, this shows one way to send high-speed internet to remote locations. How fast is this internet? According to Facebook, it was able to create a 10-gigabit-per-second bidirectional optical link.

Click **HERE** to read more.

A new data breach may have exposed personal information of almost every American adult

(**By Mike Murphy, June 28, 2018**) A little-known Florida company may have exposed the personal data of nearly every American adult, according to a new report.

Wired reported Wednesday that Exactis, a Palm Coast, Fla.-based marketing and data-aggregation company, had exposed a database containing almost 2 terabytes of data, containing nearly 340 million individual records, on a public server. That included records of 230 million consumers and 110 million businesses.



"It seems like this is a database with pretty much every U.S. citizen in it," security researcher Vinny Troia, who discovered the breach earlier this month, told Wired. "I don't know where the data is coming from, but it's one of the most comprehensive collections I've ever seen," he said.

While the database apparently does not include credit-card numbers or Social Security numbers, it does include phone numbers, email and postal addresses as well as more than 400 personal characteristics, such as whether a person is a smoker, if they own a dog or cat, their religion and a multitude of personal interests. Even though no financial information was included, the breadth of personal data could make it possible to profile individuals or help scammers steal identities.

Troia told Wired that he was easily able to access the database on the internet, and in theory, plenty of other people could have too. He said he warned Exactis and the FBI about the vulnerability, and the data is no longer publicly accessible.

Click **HERE** to read more.

More News

Yattaze, an APT that has been around for many years, is selling a new malware called "Kardon Loader."

https://asert.arbornetworks.com/kardon-loader-looks-for-beta-testers/

FREDI, a brand of baby monitors, may be open to attack and could be hacked by a malicious actor to ultimately take over the camera.

https://www.sec-consult.com/en/blog/2018/06/true-story-the-case-of-a-hacked-baby-monitor-gwelltimes-p2p-cloud/

A new malware in the FormBook family that utilizes four different malicious documents in a phishing campaign.

https://blog.talosintelligence.com/2018/06/my-little-formbook.html

How rampant are cyberattacks in Texas? Fort Worth defends about 15,000 threats daily

https://www.star-telegram.com/news/local/community/fort-worth/article198030174.html#storylink=cpy

Symantec has an online tool that will determine whether your router is infected with VPNFilter malware.

http://www.symantec.com/filtercheck/

The 6 Worst Insider Attacks of 2018 – So Far

https://www.darkreading.com/the-6-worst-insider-attacks-of-2018---so-far/d/d-id/1332183

US 'Most Vulnerable in the World' to Cyber Attacks

https://www.fifthdomain.com/critical-infrastructure/2018/07/02/us-most-vulnerable-in-the-world-to-cyberattacks/

<Cyber Stats for May and June>

	May 2018	% Change	June 2018
Phishing attacks against agency	9	-44.44%	5
Emails blocked by sensors	901,390	-0.39%	897,853
DPS Custom Email Threat Signatures Created	9	-88.89%	1

As you can see from this month's stats, phishing attacks against the agency have again decreased from the previous month. Emails blocked by sensors has decreased as well but still remain very high.

There is an old adage I learned long ago: "There are lies, there are bigger lies, and then there are statistics." While it is possible to derive almost anything you want from statistics, I think everyone can agree these stats show our Operations team is working hard to protect the agency from threats. Even though they are working very hard, they still need your assistance. You can assist them by submitting any email you believe is spam or a phishing attempt to spam@dps.texas.gov. One of our analyst will evaluate the email and take the appropriate action. No matter how hard the Ops section works, scammers and phishers are working just as hard to bypass defenses. This means that sometimes malicious emails make it through. Remember that all users are the first line of defense in protecting the agency. So that means like it or not, you are part of the Cybersecurity team also. :)

Another statistic I want to let everyone know about is our online cybersecurity awareness training status. Because of people being hired and others leaving the Agency, we will never be at 100%. However, we currently have 97.6% of all full-time DPS employees (9857 employees) complete with basic cybersecurity awareness training. And I will continue to push to get as close to 100% as possible.

As mentioned earlier in the newsletter, most of the agency is coming up on mandatory cybersecurity awareness re-training. If you took the training two years ago, you are one of the people I'm talking about. To minimize nearly 8000 employees from trying to do the training at the same time, I am going to start to space people out. You can expect to receive notification about the re-training starting next month. So please be looking for the email and try to knock out the training as soon as possible.

Unfortunately, we have not done as good a job identifying contractors and having them take the training. In the near future we will be pushing to correct this. Some of the people who manage contractors have already done this, if you have not, please email me a list of all contractors who work in your area along with their ACID so I can get them entered for training. If you have already sent me a list, please send me an updated one.

Thank you for your assistance in this.

Kirk

Remember, you are part of the cyber team and **it isn't paranoia if they really are out to get you**.

Cyber Challenge

Employees Who Reported Solving Last Month's Challenge

Several people emailed me with the correct answer to last month's challenge. I had 22 people out of almost 10,000 in the agency solve and reply. Below is the list of people in order of when they solved and emailed me.

Special Agent Erich Neumann on 6 June
Deborah Wright on 6 June
Adrian Garza on 7 June
Lindsey Bynum on 7 June
Steven Campbell on 7 June
Nirav Kumar on 7 June
Christine Hay on 7 June
Lane Tippett on 7 June
Rebecca Shane on 7 June
Tracy Kingsley on 7 June
Ester Herrera on 7 June
Alika Valdez on 7 June
Tracy Keller on 8 June
Joseph Deutschendorf on 8 June
Jaelyn Edwards on 8 June
Mercedez-Faye Wallace-Morrison on 8 June
Virginia Healer on 8 June
Rene Hess on 9 June
Benjamin Pasmore on 11 June
Renne Weise on 11 June
Lisa Stuart on 14 June
Sylvia Gonzalez on 18 June

The answer to last month's challenge is "Trust but verify. Hope for the best but plan for the worst. Hackers can see and hear everything."

For this month's challenge it will incorporate several different challenges that have been highlighted in past newsletters. As a refresher, you can look at previous newsletters the DPS website at this **link**. The page is public facing so feel free to share it with friends outside of DPS.

This is a four (4) part challenge. First you will have to FIND the challenge. As a hint…….steganography. After you find the message, you will have to decode it (maybe twice) before you can come up with the answer. Once you have the answer, email me the answer so you can be recognized in the next newsletter. Good luck with the challenge. If you get stuck you can always email me and ask for a hint. :)