NEWS
Cyber Security
Vol. 3 | Issue 8 August 2018

Routers/Iran | Cyberwar/Apps | LifeLock/Gas | Spray/Russia | Links | Stats | Challenge

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

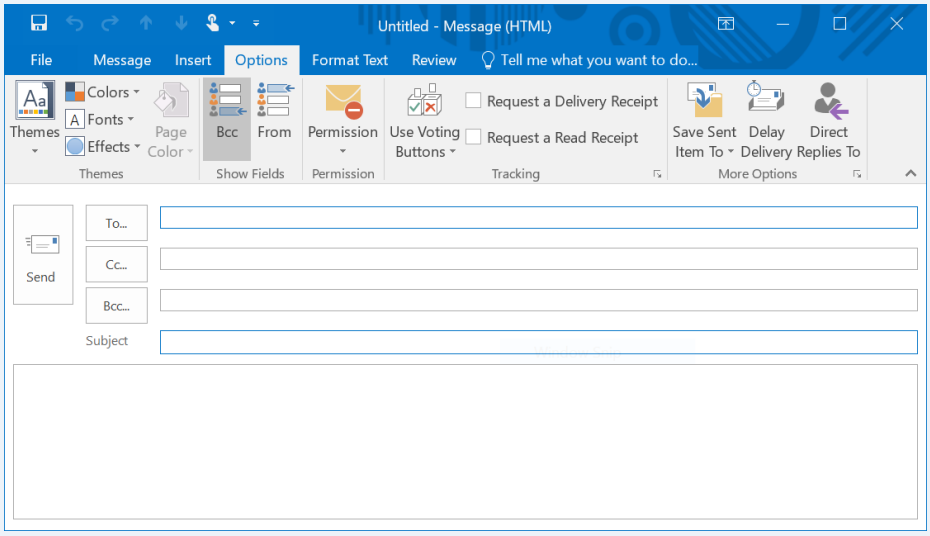
I want to start off by reminding everyone that the cybersecurity online re-training started this month. Roughly 4500 people should have received a reset of their online security training on 1 August 2018, with the bulk, but not all, of the resets being troopers and drivers license personnel. Next month there will be almost as many people reset with the remaining of those needing training being reset in October. If you know you are due for re-training, please do NOT login to your account till after you receive the reset. I have to prep accounts for reset and most people will see modules that show uncompleted and others that show completed. If you complete any of the modules before the rest, they will be required to be redone after I reset your account.

Consider a Blind Carbon Copy

It was recently observed users sometimes send emails outside the Agency which have a large number of email recipients. While this is not really a security risk, it could be a business or privacy risk. Blind Carbon Copy is a perfect way to send to everyone while still protecting their email addresses.

What is blind carbon copy and why is it important? Blind carbon copy, also referred to as Bcc, is a way of sending an email to multiple people without them knowing who else is receiving the message. It is especially useful when sending bulk email messages because it would not reveal all the other recipients and would prevent the dreaded mistake of a recipient replying to all.

If the Bcc field is not available when creating a new message, it can be enabled by clicking the "Options" tab and then the "Bcc" button within the "Show Fields" section.



If you want more information about how to use Outlook or other Microsoft Office products, I would suggest you search on YouTube. **HERE** is a link for Outlook 2010 on YouTube. You can also learn more about other Office products for free at **Cybrary**. The site is free but will require you to register. Once you do, click on "Courses" and you can search for LOTS of different types of computer training.

Cyber News!!

Dasan and D-Link routers targeted by apparent botnet in new wave of exploit attacks

(By Bradley Barth, 23 July 2018) An apparent botnet comprised of more than 3,000 separate source IPs generated a large, sudden spike in exploit attacks on July 19, targeting D-Link 2750B and certain Dasan GPON (Gigabit Passive Optical Network) small and home office routers.

The operation may have been an attempt to compromise routers so they could be leveraged to launch distributed denial of service attacks, distribute malicious content or spy on browsing activity, suggests the eSentire Threat Intelligence team, which authored a corresponding blog post and threat advisory after observed the incident while monitoring its customers.

Reportedly, the attackers sought to capitalize on a pair of vulnerabilities that collectively can result in remote code execution, and for which there is only an unofficial patch available. The vulnerabilities — CVE-2018-10561, an authentication bypass flaw and CVE-2018-10562, a command injection bug — were discovered and publicly disclosed in May 2018, and have since been used in various campaigns. Dasan routers using ZIND-GPON-25xx firmware, some Dasan H650 series GPON routers, and D-Link DSL-2750B routers with firmware 1.01 to 1.03 are prone to the exploits.

Click **HERE** to read more.

Iran cyber activity on the rise with Leafminer, OilRig leading the way

(**By Doug Olenick, July 25, 2018**) Iran has once again found itself in the crosshairs of cybersecurity researchers with Palo Alto Networks Unit 42, Symantec and German intelligence all pointing accusatory fingers at Tehran over several recently revealed cyber campaigns.

Unit 42 researchers have singled out the well-known OilRig group (aka PT34, Helix Kitten) for launching multiple attacks between May and June 2018. Unit 42 said the activity involved three waves of attacks, all using a single spear phishing email designed to look as if it came from a Middle Eastern government agency.

"Based on our telemetry, we have high confidence the email account used to launch this attack was compromised by the OilRig group, likely via credential theft," Unit 42 wrote. Palo Alto Networks has previously connected OilRig to Iran.

In this case, the attackers went after an unnamed technology services provider and a separate government entity, also not named. OilRig executed a high-level of obfuscation, making it appear as if the malicious email came from the same country that was being attacked, but Unit 42 has determined the attack originated from another country, most likely using stolen credentials.

The attack involved delivering the QUADAGENT PowerShell backdoor, a tool that is also attributed to OilRig by FireEye and ClearSky Cyber Security, Unit 42 said.

The attackers behind the spear phishing campaign put in a great deal of effort to find their target's email address, as the email addresses were not easily discoverable via common search engines. To the researchers, this indicated the targets were likely part of a previously collected target list, or possibly known associates of the compromised account used to sent the attack emails.

Click **HERE** to read more.

More Cyber News!!

Cyberwar: What happens when a nation-state cyber attack kills?

(**By Danny Palmer, 24 July 2018**) A cyber attack that kills someone is getting ever more likely. What happens then is a big — and scary — question.

The increasing sophistication and power of state-backed cyber attacks has led some experts to fear that, sooner or later, by design or by accident, one of these incidents will result in somebody getting killed.

It might sound far-fetched, but a former head of the UK's intelligence agency has already warned about the physical threat posed by cyber attacks and the potential damage they could do.

"Nation-states are getting more sophisticated and they're getting more brazen. They're getting less worried about being caught and being named — and of course that's a feature of geopolitics." said Robert Hannigan, who served as director general of GCHQ from 2014 to 2017.

"The problem is the risk of miscalculation is huge," he said, speaking at a security conference in London last month. "If you start to tamper with industrial control systems, if you start to tamper with health systems and networks, it feels like it's only a matter of time before somebody gets hurt and somebody is ultimately killed.

Click **HERE** to read more.

How Apps Could Be Sneaking Malware Onto Your Phone

(**By Caitlin Fairchild, 23 July 2018**) Some malware comes right through the front door.

Have you noticed your Android device has been slower and riddled with annoying pop-ups lately? You might have contracted malware that made its way onto your phone through the Google Play Store.

In a report, technical support site BleepingComputer details a growing trend in mobile malware that involves the use of a tool known as a "dropper" which hides code within an app.

While contained within an app, droppers are benign, making it hard for Google to detect them in the Play Store with its standard security tests. Once they're on your device, however, droppers will attack with malware in multiple stages over time. This makes them similar to Trojan horses. Sometimes hackers will include an additional aspect of mischief, like adding a timer to space out malware deployments.

"It is quite difficult to detect dropper apps," security researcher Gaetan van Diemen told BleepingComputer. "As you can imagine, threat actors will put a lot of energy in keeping those apps undetected."

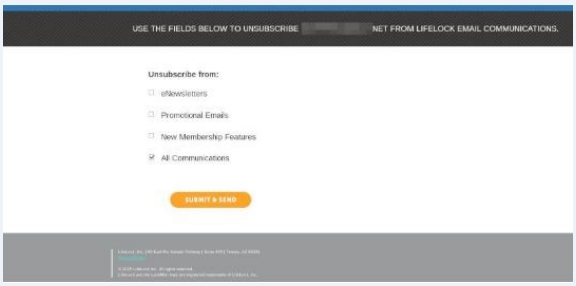
Until Google gets a handle on the situation, there are a few ways to stay safe. Security experts recommend you keep the operating system on your phone updated and be very wary about which apps you download from the app store and in general maintain good cyber hygiene.

Click **HERE** to read the article.

More Cyber News!!

LifeLock ID theft protection leak could have aided identity thieves

(**By Mariella Moon, 26 July 2018**) LifeLock's identity theft protection service suffered from a security flaw that put users' identities in jeopardy. The event forced its parent company, Symantec, to pull its website down to fix the issue after it was notified by KerbsOnSecurity. According to Krebs, Atlanta-based security researcher Nathan Reese discovered the vulnerability through a newsletter email he received from the service. Upon clicking "unsubscribe," a page that clearly showed his subscriber key popped up. That allowed Reese to write a script that sequences numbers, which was able to pull keys and their corresponding email addresses from the service.



Reese said: "If I were a bad guy, I would definitely target [the firm's] customers with a phishing attack because I know two things about them. That they're a LifeLock customer and that I have those customers' email addresses. That's a pretty sharp spear for my spear phishing right there. Plus, I definitely think the target market of LifeLock is someone who is easily spooked by the specter of cybercrime."

Click **HERE** to read more.

Hackers steal 600 gallons of fuel from a US gas station

(**From E Hacking News, 9 June, 2018**) We have read about credit card skimmers at ATMs or gas stations but how would someone hack into fuel pumps to steal gas? From recent hacks and data breach incidents, it seems the hackers have changed their targets. Apparently, cybercriminals have got their hands on a high-tech electronic device that allows them to steal gasoline from fuel pumps without getting caught. These hackers hacked a US gas station to pilfer 600 gallons of gas worth $1,800 and did so brazenly in the middle of the day.

The Detroit police department is looking for two men suspected in the larceny of fuel from a Marathon Oil Service Station in the 17800 block of W. Seven Mile on the city's west side.

The Marathon gas station suffered this attack around 1pm on June 23, 2018, when two men reached the pump for fuel. Reportedly, they took control of the pump at the gas station through a remote device, thus preventing the hack from being blocked by the clerk present at the station from his system.

Click **HERE** to read more.

To read more about dangers at the gas pump, click **HERE**.

More Cyber News!!

Spray you, spray me: defending against password spraying attacks (British Article)

(**By Andy P., 15 May 2018**) One common way that online accounts are breached is through *password spraying*, whereby lists of a small number of common passwords are used to brute force large numbers of accounts. These attacks are successful because for any given large set of users there will likely be some who are using very common passwords, and these attacks can slip under the radar of protective monitoring which only look at each account in isolation.

To understand how much of a problem this is, the NCSC recently conducted a research study which allowed participating organisations to assess how vulnerable they would be to a password spraying attack. The PowerShell script we used to collect data is still available to download for your own use if needed, but since the study is now over we can't provide support. From the study we found:

- 75% of the participants' organisations had accounts with passwords that featured in the top 1,000 passwords
- 87% had accounts with passwords that featured in the top 10,000

Click **HERE** to read more.

Russian DragonFly hackers accessed electrical utilities control rooms in lengthy campaign

(**By Teri Robinson, July 24, 2018**) The Russian DragonFly APT, which last year broke into air-gapped networks run by U.S. electric utilities in a likely ongoing campaign that victimized hundreds, accessed the providers' control rooms where they could have caused blackouts and other damage.

The group, which also goes by Energetic Bear, used phishing and waterhole attacks to gain access to supplier networks, nick credentials and then access the utilities, the Wall Street Journal cited Department of Homeland Security (DHS) as confirming.

"Hackers, including state-sponsored Russian hackers, exploit the weakest link in the security chain—the people. This was noted in great detail in the Mueller Investigation's indictments against 12 Russian nationals on July 13 where they spearfished unsuspecting users to steal passwords to gain access to the Clinton Campaign and DNC systems," said Michael Magrath, director, global regulations and standards at OneSpan, Inc. "Do we really expect Russian hackers to exclude critical infrastructure?"

His colleague, David P. Vergara, head of security product marketing OneSpan, agreed. This is "big game hunting" for cybercriminals. The motivation may pivot between political and monetization, but the impact to the target is the same, terror through vulnerability and exposure," he said. "It's not difficult to extrapolate the outcome when an entire power grid goes offline during peak hours and the attack follows the weakest link, unsophisticated utility vendors or third parties."

The hackers were "very successful" in penetrating "completely through to the utility control rooms where they had the ability to disrupt power flows," said Provin Kothari, CEO of CipherCloud.

Click **HERE** to read more.

More News

Riverside police lost access to crime-fighting tool in cyber attack

https://www.mydaytondailynews.com/news/local/riverside-police-lost-access-crime-fighting-tool-cyber-attack/eaFIb0FunQ88rRNXng5lGP/

Some vote-counting computers came with a critical flaw that could have let hackers access them

https://www.businessinsider.com/election-systems-and-software-admits-shipping-vote-systems-with-key-flaw-2018-7?elqTrackId=95b34eedfb6f4e539728d64de97df53c&elq=3e0e25a282194ffd918f0f988b2ec79e&elqaid=16391&elqat=1&elqCampaignId=12090

The Worst Cybersecurity Breaches of 2018 So Far

https://www.wired.com/story/2018-worst-hacks-so-far/

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

Thermanator Attack Steals Passwords by Reading Thermal Residue on Keyboards

https://www.bleepingcomputer.com/news/security/thermanator-attack-steals-passwords-by-reading-thermal-residue-on-keyboards/

China brings Star Wars to life with 'laser AK-47' that can set fire to targets a kilometer away

https://www.scmp.com/news/china/diplomacy-defence/article/2153310/china-brings-star-wars-life-laser-ak-47-could-set-fire

Tomorrow's Quantum Computers are Already Threatening Today's Data

https://www.defenseone.com/threats/2018/07/future-quantum-computers-already-threatening-todays-data/149557/

More News

Cybercriminals take the day off to watch the World Cup

https://www.scmagazine.com/cybercriminals-take-the-day-off-to-watch-the-world-cup/article/780398/

Sextorion Scam Uses Recipient's Hacked Passwords

https://krebsonsecurity.com/2018/07/sextortion-scam-uses-recipients-hacked-passwords/

Researchers Mount Successful GPS Spoofing Attack Against Road Navigation Systems

https://www.bleepingcomputer.com/news/security/researchers-mount-successful-gps-spoofing-attack-against-road-navigation-systems/

Senators Ask FTC to Investigate Smart TVs for Invading Users' Privacy

https://www.bleepingcomputer.com/news/technology/senators-ask-ftc-to-investigate-smart-tvs-for-invading-users-privacy/

The 10 airports where your phone is most likely to get hacked

https://www.techrepublic.com/article/the-10-airports-where-your-phone-is-most-likely-to-get-hacked/

Flaws in Diqee 360 Smart Vacuums Let Hackers Spy on Their Owners

https://www.bleepingcomputer.com/news/security/flaws-in-diqee-360-smart-vacuums-let-hackers-spy-on-their-owners/

New Gmail features pose cyber threat

http://www.ehackingnews.com/2018/07/new-gmail-features-pose-cyber-threat.html

Bluetooth security: Flaw could allow nearby attacker to grab your private data

https://www.zdnet.com/article/bluetooth-security-flaw-could-allow-nearby-attacker-to-grab-your-private-data/

From the Readers

Earlier this month a friend of mine in our Aviation Division received the email below. He thought it was very funny and so do I. Figured I would include it in this newsletter for others to appreciate just how ludicrous the scare tactic was. The more offensive and sensitive parts of the email have been redacted.

Subject: Fwd: Compromising material ID Ip9xQBzj!!!

When you were [redacted] your device screen when you called on [redacted] Internet resource your notebook get malicious software as a result vulnerability the Internet browser. The malware registers all the operations at your device and among other things it is informed about coockie of the sites which you run over. And the primary advantage of this malware is that it could switch web cam and download all the Contacts from yours mail. Well I own access to yours out box and social media service. So I have viral and snap [redacted]. If you don't want that content to bring out and to be dispatched to all your friends family I suggest you the succeeding decision. You must deliver dispatch to mine Bitcoin address [redacted] 400 $ in BTC. After obtaining of cash I am going to destroy sensitive information about you and you should never again heard about me. In other circumstances if I don't get th is cash within 24 hours after reading that letter I gonna deliver [redacted] evidence on you to your loved ones and collaborates and as well through social media platforms for overall estimation of your activity. P.S. My English isn't far from good because its not my native language nevertheless you can to understand what I mean. Can you be so kind and and don't give an answer to this letter I shall never login to it again.

This was obviously a scare tactic to try to convince people to send money to prevent a non-existent, potentially embarrassing video and other material from being sent out. But, this does bring up some things to think about. It is possible to turn on a webcam and microphone without the person sitting in front of the computer knowing they are being recorded. This means it is possible for someone to see whatever your webcam can see and your microphone can hear.

As a suggestion, if you have a built-in webcam you might want to cover it when not needed. You can buy sliding webcam blockers or just put a piece of tape over the camera. If you go the tape route, I suggest you use Painter's Tape. It will stick to the camera but should not leave a residue.

That will easily and cheaply protect you from being videoed, but not from having anything said around your computer from being recorded. That is a little more complicated, especially if you have a built-in mic like most laptops do. There are things you can do to protect yourself but most are not quick to undo if you need to use your mic. The cheapest tactic to protect you, which is not very realistic, is to never talk about anything confidential around your computer, tablet, etc. If you have questions or suggestions on what you can do to protect against this, feel free to email them to me.

This article was provided by a reader in the CJIS department. Interesting article about how a group was able to setup a fake site to compromise a package in a PDF editor app for the purpose of compromising machines to deploy cryptocurrency miners on them. She has not wanted to be recognized in previous submissions but I want to thank her for this submission.

Microsoft Discovers Supply Chain Attack at Unnamed Maker of PDF Software

<Cyber Stats>

I am not including this month's cyber stats but they might return next month. If you look back at the previous months' newsletter stats, I think everyone will agree they show Texas DPS Cyber Security Operations is working hard to protect the agency from threats. And even though they are working very hard, they still need your assistance. Users are the first line of defense and you can assist them by submitting any email you believe is spam or a phishing attempt to spam@dps.texas.gov. One of our analysts will evaluate the email and take the appropriate action.

No matter how hard the Texas DPS Cyber Security Operations works, scammers, phishers, and other malicious entities 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 Cyber Security team also. :)

As I stated at the beginning of the newsletter, I have reset the online training for several people in the agency. Please check your Spam and Deleted folders if you do not see an email from me notifying you to take the training. If you do not see an email, it is probably because you are not on this month's list for retraining; you will likely be on next months or October's re-training list. Another option would be to contact me and I will let you know if you should have received an email or not.

Remember that once you are notified of the re-training that you have 30 days to complete. You do not have to complete all of the modules at one time but if you did it would take you roughly an hour to an hour and a half to complete. Again, contact me if you have any questions or problems with the training.

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

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

Lane Tippett @ 1238 on 6 July	Joseph Kimbler @ 1509 on 6 July	Ryan Strand @ 1636 on 11 July
Nathan Gilbert @ 1305 on 6 July	Cynthia Burr @ 1554 on 6 July	Rene Hess @ 1130 on 13 July
Tracy Kingsley @ 1333 on 6 July	Joseph Deutschendorf @ 1628 on 6 July	David Evans @ 0534 on 15 July
Devin Mathews @ 1333 on 6 July	Elizabeth Tuten @ 1927 on 6 July	Mercedez-Faye A Wallace-Morrison @ 0914 on 18 July
Nirav Kumar @ 1335 on 6 July	Christopher Martin @ 1935 on 6 July	Jaelyn Edwards @1330 on 25 July
Erich Neumann @ 1338 on 6 July	Steven Campbell @ 1134 on 9 July	Jose Razo @ 0859 on 27 July
Ben Pasmore @ 1411 on 6 July	Stephen "Doc" Petty @ 1303 on 11 July	

For those who weren't able to complete the challenge, the first thing you had to do was find the hidden message on top of the picture on the first page. That message then needed to be converted to text which provided you with a cryptogram. Once that cryptogram was decoded you got this message: ***"I am a form of social engineering. I can be thought of as a real-world Trojan horse that uses physical media and relies on the curiosity of the victim. What am I?"*** The correct answer to the question is: **Baiting**. Again, congratulations to everyone who completed the challenge.

Since several people were able to solve the last challenge so quickly, I've upped the difficulty level for this month. I have again used a form of Steganography to hide a message in this month's newsletter. Like last month, there are multiple phases to solve the challenge. When you find all the parts to the hidden message, piece them together and begin to solve the puzzle. Email me at kirk.burns@dps.texas.gov when you solve the challenge OR if you are stuck and need a hint.

Good luck. I think this challenge will take people a little longer to accomplish.

Kirk