NEWS
Cyber Security
Vol. 3 | Issue 6 June 2018

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

This month I want to start off with an article I found that I believe several of you might find interesting. Especially other Star Wars geeks like me. Here is the article:

Rogue One—the best cybersecurity videotraining

(Kaspersky.com 4 May 2018) Last year we analyzed an incident depicted in *Star Wars: Episode IV*. However, we got the feeling even back then that the security failures that led to the destruction of the Death Star were only the tip of the iceberg. The Empire's problems with information systems security are clearly of a more galactic nature. Fortunately, researchers from Lucasfilm conducted a thorough investigation of the events preceding this incident and published it under the name *Rogue One: A Star Wars Story*. Here's what this video document revealed.

Security begins with HR

Rogue One begins with the Imperial Military's head of innovative projects, Orson Krennic, and a team of HR specialists headhunting top developer Galen Erso to work on the Death Star superweapon project. What do we know about Erso? First, he previously worked on the project before tendering his resignation. Second, he's in no hurry to return. But Imperial HR makes him an offer that he can't refuse, and back he goes. Later, it hits Krennic that Erso was an industrial spy, the source of the leaked plans.

Such an employee should never have been allowed to work with sensitive information—or hired at all—something the HR team should have picked up on at the recruitment stage. But they failed to identify the risks. Some timely security awareness training would have helped them spot the red flags during the screening process.

Top-secret lab on Eadu

Galen Erso is taken to a kyber crystal processing plant on the planet Eadu. This is essentially a Gulag-style "experimental design bureau," where he is coerced into working on a top-secret military project. As we said, entrusting him with a secret project is stupid. But having him work there with no supervision is doubly stupid. Erso implants a vulnerability in the Death Start.

To read more, and I strongly suggest you do, click **HERE**.

Cyber News!!

An FBI agent mapped out the countries capable of unleashing a crippling cyber attack on the US

(Business Insider, 4 Jun 2018: provided by NMCIWG) Business Insider spoke to Aristedes Mahairas, a special agent in charge of the New York FBI's Special Operations/Cyber Division, about the cybersecurity landscape in America. He said the US is always alive to threats from cyber criminals, cyber terrorists, and renegade hacktivists, but nation states are at the "very top" of the threat list. Mahairas said there has been a "significant increase in state-sponsored computer intrusions" over the past 12 years as it has become a potent way of unsettling an adversary alongside traditional espionage. Here's a breakdown of the four nations, and the different threats they pose to the US:

1. Russia: "Russia remains the most sophisticated and technically capable. They are really good at hiding the digital breadcrumbs that lead back to them," Mahairas said. The FBI agent pointed to the Yahoo hack, which compromised 1 billion accounts in the biggest data breach in history. Mahairas highlighted a different kind of cyber attack: Influence operations. This resulted in Russia interfering in the 2016 US presidential election, and the indictment in February of 13 Russians affiliated with St Petersberg troll farm the Internet Research Agency. "Cyber is a vector and some of the nation states have realised that this vector can be used as a capability to weaponized the information that has been stolen as a result of hacks," Mahairas said. "The goal is to erode the population's confidence, not only in its institutions, its values, its leaders, and most importantly in its ability to find the truth. The objective is to undermine the target by magnifying any number of existing issues that currently divide people in order to create discord and aggravate tensions." "These influence operations are not new, but there is an observed increase in their scalability due to... modern social media."

2. China: Up until recently, China launched extremely noisy cyber attacks. "China used to be loud in and around your network, almost like the drunk burglar who's banging on your door and breaking windows to get in," Mahairas said. But after the US charged five Chinese military officials for computer hacking and economic espionage in 2014, the country has switched up its tactics. "Today, they operate in a more patient and methodical manner, akin to death by a thousand cuts," Mahairas continued. A notable attack the former counterterrorism agent pointed to was the one on Lockheed Martin, when Chinese military officers stole US state secrets on fighter planes, including the F-35 jet. In a series of attacks codenamed "Byzantine Hades", they carried out the attack and the economic impact was estimated to be around $100 million.

3. Iran: Mahairas said there has been a "noticeable uptick in activity" from Iranian hackers in recent years, as they become more sophisticated and targeted in their attacks on the US. This was evidenced last year when Iranian hacker Behzad Mesri attacked American broadcaster HBO. Although Mesri appeared to be acting alone, Mahairas said the FBI is increasingly concerned about the "blended threat" from some countries. This is when they work with criminal contract hackers to "do their dirty work."

4. North Korea: North Korea remains a significant cyber threat to the US, despite a thawing in diplomatic relations in recent months. Mahairas said the health of diplomacy between two common enemies has very little to do with how nation states conduct cyber activity. "Diplomacy isn't going to impact their ability or desire to continue in this activity," the FBI agent explained. "What they're looking for is information, access, and advantage. Whether it's in the cyber universe or not, those are the objectives."

Ultimately, Mahairas said cybercriminals are not fussy about their targets: "These nation state actors, they're not targeting just the US. Anyone is fair game. What they do is generally the same, I don't think any one nation state brings more specific threat."

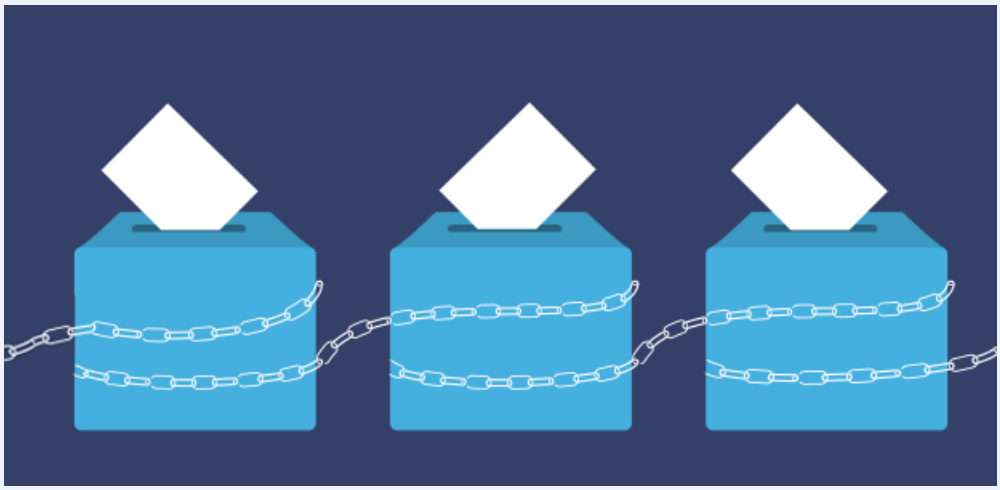
To find out more, click **HERE**.

More Cyber News!!

Cyber threats to the midterm elections

(GCN.com 1 Jun 2018) After the 2016 election, it took cybersecurity analysts months to pin down where the threats to elections systems where coming from. This year, even without no single national race, threats continue to multiply.

The United States' vast array of locally controlled election systems faces attacks to voter registration, election websites, voting machines and the election management systems that aggregate voting data. A new report from FireEye outlines likely attack methods and offers suggestions for securing this year's midterm elections.



In 2016, voter registration databases were hacked in Pennsylvania, Ohio, Rhode Island, Delaware and Washington, giving malicious actors the ability to change or delete voter information. Voter registration systems are vulnerable to spearphishing and distributed denial of service attacks, the report warned. And unpatched or poorly maintained websites allow malicious actors to change or block key information on state websites that voters need to get to their polling places.

Click **HERE** to read more.

Canadian who helped Yahoo email hackers gets five years in prison

(Reuters 29 May 2018) A Canadian accused of helping Russian intelligence agents break into email accounts as part of a massive 2014 data breach at yahoo was sentenced to five years in prison on Tuesday and ordered to pay a $250,000 fine.

Karim Baratov, who pleaded guilty in November 2017 in San Francisco, was sentenced by U.S. District Judge Vince Chhabria, a spokesman for the U.S. Attorney's Office said.

Baratov, a Canadian citizen born in Kazakhstan, was arrested in Canada in March 2017 at the request of U.S. prosecutors. He later waived his right to fight a request for his extradition to the United States.

Lawyers for Baratov in a court filing had urged a sentence of 45 months in prison, while prosecutors had sought 94 months.

"This case is about a young man, younger than most of the defendants in hacking cases throughout this country, who hacked emails, one at a time, for $100 a hack, " the defense lawyers wrote in a May 19 court filing.

Click **HERE** to read more.

More Cyber News!!

Android bug causes text messages to show up in Google Search; here's how to fix it

(By Brandon Vigliarolo, 30 May 2018 and posted on techrepublic.com) Android users searching for very specific things found their text messaged in Google Search results instead. Are business users at risk of having data compromised?

An unusual Android bug found by a Reddit user is causing a lot of people to scratch their heads. When typing "the1975..com" (note the extra dot) the poster found all of his recent text messages displayed through Google instead of the content he was searching for.

Other Reddit users chimed in saying that they were getting the same results, with some even experiencing it when they performed a search for "Vizela viagens" (a travel agency in one Reddit user's home town), and the glitch also appeared with variant spellings too.

Reddit users with a wide variety of Android devices said they were affected as well. Particularly interesting is one comment stating that if you type "my text messages" into the search bar you receive the same result. What this means for how Google may be caching text message is unknown.

Click **HERE** to read more.

Does your BMW need a security patch?

(By John E Dunn for Sophos.com, 25 May 2018) If you're a BMW owner, prepare to patch! Chinese researchers have found 14 security vulnerabilities affecting many models.

The ranges affected (some as far back as 2012) are the BMW I Series, X Series, 3 Series, 4 Series and 7 Series, with a total of seven rated serious enough to be assigned CVE numbers.

The vulnerabilities are in the Telematics Control Unit (TCU), the Central Gateway Module, and Head Unit, across a range of interfaces including via GSM, BMW Remote Service, BMW ConnectedDrive, Remote Diagnosis, NGTP, Bluetooth, and the USB/OBD-II interfaces.

Some require local access (e.g. via USB) to exploit but six included the Bluetooth flaw were accessible remotely, making them the most serious.

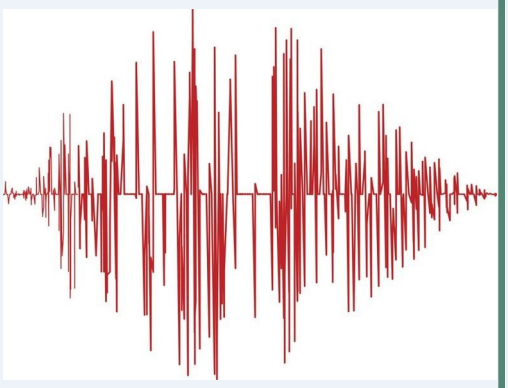
Click **HERE** to read more.

More Cyber News!!

Certain sounds played on laptops can cause system crashes and disrupt hard drives

(By James Sanders, May 30, 2018 for techrepublic.com) Researchers were capable of causing Windows 10 to crash by playing sounds via a web browser, making remote execution a possibility.

Researchers at the University of Michigan and Zhejiang University have found that specialized sounds played in speakers found in laptop and small form factor (SFF) computers can be co-opted to cause damage to traditional hard disk drives, according to a recent paper. While the risk is not limited to the aforementioned devices—speakers placed near drives have the same effect—this would imply that attackers have physical access to a given device.



The researchers found that audible sound can cause the drive head mechanics to "vibrate outside of operational bounds" while "ultrasonic sound causes false positives in the shock sensor, which is designed to prevent a head crash," the paper noted. This effect has been demonstrated in hard drives from all three major vendors—Seagate, Western Digital, and Toshiba—and tests have resulted in drives becoming unresponsive (until the system is rebooted) on both Windows and Linux, as well as causing intermittent freezing and computer system crashes on Windows.

Click **HERE** to read more.

How hackers can exploit devices used at home

(By Olivia Beavers, 05/28/18 for thehill.com) As Americans increasingly fill their homes with smart technology, the risk of hackers exploiting their devices is growing.

Experts say the expanding ecosystem of internet-connected devices such as smart thermostats, home security systems and electric door locks are increasingly susceptible to hackers, including those trying to leverage voice-command devices.

This risk is further compounded if an individual stores sensitive data on certain internet-connected products, like a credit card number or mailing address, which a hacker may be able to gain access to through other connected devices.

One incident that drew particular attention this week highlighted some of the privacy fears surrounding voice-controlled devices and how they can operate seemingly independently of their owners' intentions.

A woman in Portland, Ore., said her Amazon Echo recorded a private conversation she had with her husband and then sent an audio file of the recording to someone in the couple's contact list.

An Amazon spokesperson explained that the device had misinterpreted a series of words in a background conversation as commands, leading the Echo in question to send the recording.

While the incident—described as extremely rare—did not apparently involve an active third-party, it added to renewed scrutiny over how voice-controlled devices can operate outside their owners' intent and how they might be exploited by hackers.

Click **HERE** to read more.

Reader Suggestions

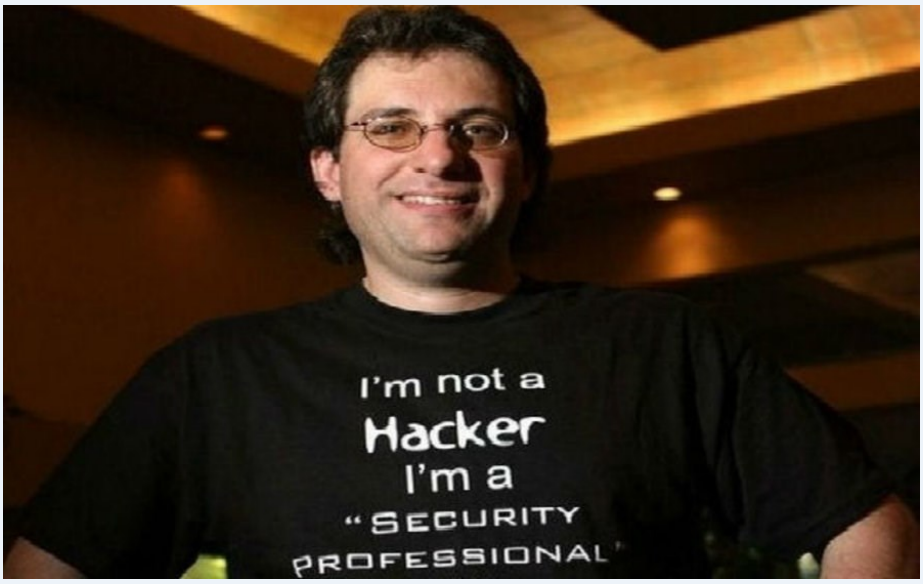
This month's article is again provided by the CJIS team. They want to remind everyone to

"Stop, Look, Think before you click the link"

Two-factor authentication hackable

Two-factor authentication may not be the panacea of security access to online accounts that many believe it is as KnowBe4's Kevin Mitnick shows how easily this defensive measure can be spoofed.

Mitnick, KnowBe4's chief hacking officer, has put together a video showing how a phishing email containing a bit of code capable of swiping login information placed into a login box can be stolen to totally compromise a person's account and eliminate the level of protection normally afforded by two-factor authentication. The core of the attack comes in a phishing email, in this case, one purportedly sent by LinkedIn, to a member indicating someone is trying to connect with them on that social network.



Mitnick points out that at a brief glance the email looks legitimate, but upon closer scrutiny, the return address is not correct. So, if the target falls for the fake email and clicks the "interested" button the malware is downloaded onto the victim's computer. At this point, the person is taken to the real LinkedIn site where login information is required to complete the connection process, including having the site send an access code to the account holder's phone. However, in the background, the malware has grabbed the email and password associated with the account, along with the session cookie.

This cookie then can be used by the attacker to access the account directly, thus avoiding the 2FA part of the sign in.

To see the article and view the associated video, click **HERE**.

If you see any cyber related articles you believe others could benefit from, please send them to me. I would like to have several articles provided by different departments. Anything cyber related such as social engineering, steganography, encryption, IoT, vulnerabilities, recent hacks, ransomware, aircraft hacks, car hacks, critical infrastructure hacks, etc. Anything you see that you find interesting and is cyber related will work. Email them to me at kirk.burns@dps.texas.gov.

<Cyber Stats for Apr and May>

	April 2018	% Change	May 2018
Phishing attacks against agency	20	-55.00%	9
Emails blocked by sensors	125,700	617.10%	901,390
DPS Custom Email Threat Signatures Created	19	-52.63%	9

As you can see from this month's stats, phishing attacks against the agency have decreased from the previous month. However, the number of emails blocked by our defensive systems have significantly risen. Thankfully this has not too badly increased the workload for our Operations team and hopefully has not caused any business delays for anyone.

As a reminder, phishing is a type of social engineering attack designed to obtain sensitive information such as usernames, passwords, credit card information, etc. for malicious reasons. It is one of the oldest types of cyberattacks and dates back to the 1990s. Phishing is accomplished by sending emails purported to be from reputable well known companies in order to trick people into revealing personal information. If it helps you to understand the concept, think of this as a weaponized email intended to do you harm.

Phishing emails come in many forms, but are all malicious. The most dangerous ones come from malicious entities (individuals, groups, and/or countries) that have researched you, or the agency. These entities structure the phishing emails to look like emails you are use to seeing from vendors, your bank, stores you shop at, utility companies you use, etc. The intent is to make you click without stopping to think if this is legitimate or not.

I recently read the 2018 Cyberthreat Defense Report from the CyberEdge Group. One of the things that stood out to me was that in 2016, 40% of spam emails (which most phishing emails could classify as spam) contained Ransomware. The other thing that stood out to me was that out of the 1,100 IT security professionals surveyed from 15 countries and 19 different industries, it was found that "low security awareness among employees" was the greatest danger to organizational security. While it is slow in happening, it has been recognized by industry that the best way to defend against cyber attacks is to not only invest in the equipment and personnel needed, but to also educate users. You may not realize it, but everyone (including you) is part of the cybersecurity team. Everyone has to do their part to keep the organization secure. IT and Cyber can do everything perfectly, but all it takes is one user to disregard security procedures to compromise the whole network. A well educated employee goes a long way in preventing a cyber attack.

For further information I recommend you check out these links:

How a cyber attack works and how to prevent it | 15 real-world phishing examples | Phishing Attacks | What is Phishing?

Video on why people fall victim | Video on Intro to Phishing Email Hacking Attacks | Phishing as a Science

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

Cyber Challenge

IMPORTANT INFO

Before we get to this month's cyber challenge, I would like to take a few minutes to notify everyone about our new Internet facing link to the Cybersecurity Newsletter. Our IT Web team created a page which contains all previous newsletters and linked it to the main DPS page. You can find the link under the General Info tab at www.dps.texas.gov. Feel free to tell your friends about it and go back and read previous newsletters.

I would also like to remind everyone that you are required to complete the online Cybersecurity training. Most of the agency has completed it but there are people who still need to. If that is you, it is an Agency requirement so please complete the training. Also, some of you are coming up on the two year recurrency training. Look for notifications to start to be sent out in the next few months. Once you get the notification you will have 30 days to complete to stay in compliance with the General Manual.

Now on to the Cyber Challenge. For this month's challenge I am providing everyone with a cryptogram to decode. This is similar to challenges presented months ago. Feel free to review older newsletters for more information. :)

Some of you might be asking "What is a Cryptogram?" The answer is that cryptograms are text written in code. It isn't encryption because there is no key needed to convert the code into something readable. If you don't recognize the term, you might recognize it by another name; a Caesar cipher. Caesar ciphers have been around for a long time. The process is simple, you take a message and change each letter to another letter in the alphabet thus making the original message illegible. While this might seem to be a very difficult code to figure out, it is actually very easy. Ciphers like this can be broken using simple pattern recognition, frequency analysis and a general knowledge of grammar and vocabulary. Because of this, simple-substitution ciphers are inadequate for providing confidentiality of information but can be fun to play with.

So, for this month's challenge I am providing you with a phrase I want you to try to decode. If you do, please email me and let me know so I can recognize you in next month's newsletter. Good luck with the challenge. Here it is:

PCVIP DVP EGCZQN. UYHG QYC PUG DGIP DVP HSXF QYC PUG OYCIP. UXRWGCI RXF IGG XFK UGXC GEGCNPUZFL.

Again, good luck with the challenge. If you complete it, make sure and email me to let me know what you decoded.

Kirk