Cyber Security NEWS
Vol. 5 | Issue 5 May/June 2020

TXDPS Cyber Security Newsletter

Texas Department of Public Safety Cyber Security welcomes you to this month's Cybersecurity Newsletter. To start off this issue I will provide an overview on how some cyber-attacks work. This overview will help you understand the different types of attacks. Understanding this information will leave you better prepared to defend against them. Cyber-attacks can be either un-targeted or targeted.

During an un-targeted attack, malicious actors will attempt to reach out to many devices or users. Actors are basically casting a large net in hopes of exploiting unsuspecting users, devices or services. To accomplish this they use tactics that take advantage of how expansive the internet is. These are some of the tactics that are used:

Phishing – Is the sending of bulk amounts of emails in an attempt to get people to give up sensitive information (passwords) or to click on malicious links.

Watering hole attack – Attackers will either set up a malicious website or compromise a legitimate website to exploit users. One example was the NotPetya ransomware incident which was spread through comprised M.E.Doc accounting software servers. M.E.Doc was legitimate software that was used throughout Ukraine and other parts of the world. It is estimated that the damages from NotPetya were around $10 billion dollars. If you would like to know more about NotPetya please visit HERE.

Ransomware – Can include distributing hard disk encrypting extortion malware

Scanning – Is the scanning of various parts of the internet for vulnerabilities

For targeted attacks, specific users or business entities are picked because attackers are after targeted information. An attacker could have also been paid to target a specific individual or business entity. Targeted attacks can be more severe compared to non-targeted attacks because malicious actors have customized their attacks for specific systems, processes or personnel. Targeted attacks can include:

Spear- Phishing – Is the sending of specifically tailored emails to targeted personnel. The emails could contain an attachment with malware or a link that directs users to download malware.

Activating a botnet – A botnet is a network of internet connected devices that can be used to perform a Distributed Denial of Service (DDos). A DDoS attack can overwhelm information systems and bring down business services.

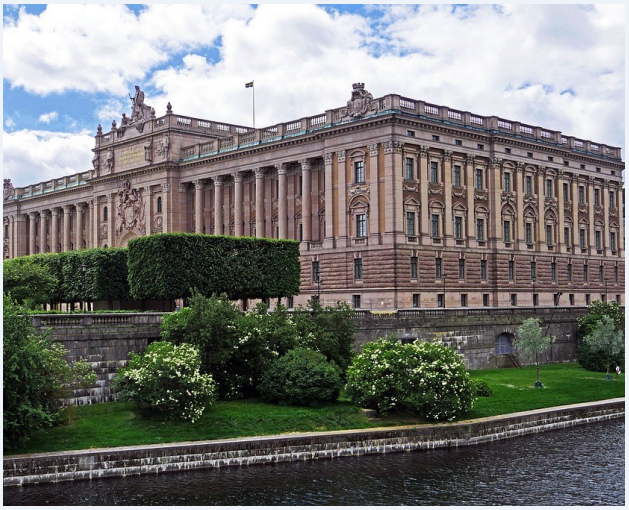
Corrupting the supply chain – In this attack software and equipment is targeted prior to delivery to a business entity.

Being aware and understanding the different ways an attacker can target you and our organization leaves us better prepared for the eventuality of an attack. I hope you enjoyed reading about the different attacks and continue to be cyber vigilant. For more information please visit HERE.

International News

German intelligence agencies warn of Russian hacking threats to critical infrastructure

(by Sean Lyngaas | **May 26, 2020**)



A Kremlin-linked hacking group has continued its long-running efforts to target German companies in the energy, water and power sectors, according to a confidential German government advisory obtained by CyberScoop.

Investigators earlier this year uncovered evidence of the hackers' "longstanding compromises" at unnamed German companies, according to the memo that German intelligence and security agencies sent last week to operators of critical infrastructure.

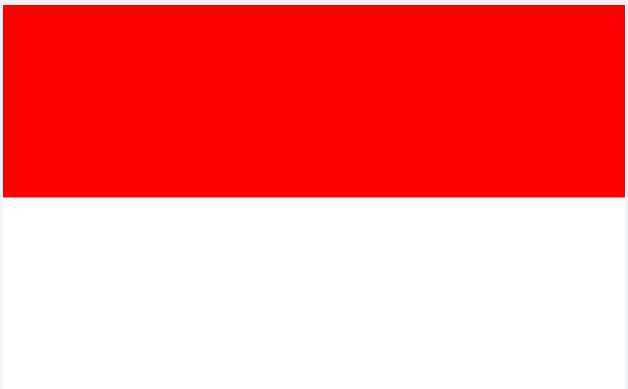
The hacking group — dubbed Berserk Bear and suspected by some industry analysts of operating on behalf of Russia's FSB intelligence agency — has been using the supply chain to access the German companies' IT systems, said the alert from the BSI, BND, and BfV federal agencies.

"The attackers' goal is to use publicly available but also specially written malware to permanently anchor themselves in the IT network…steal information or even gain access to productive systems [OT networks]," the advisory said. There was no evidence of a disruptive attack on any company's industrial networks, German authorities said. The agencies did not respond to a request for comment.

Click **HERE** to read the article.

Indonesia probes breach of data on more than two million voters

(by Stanley Widianto and Fanny Potkin | **May 22, 2020**)



JAKARTA (Reuters) - Indonesia's election commission is investigating the release of 2.3 million voters' private information on a hacker website along with a threat to release of the data of about 200 million people, the agency said on Friday.

The electoral data from the world's fourth most-populous nation was posted anonymously on the hacking forum raidforums on Wednesday and analysts said it could be used for identity theft and fraud.

The General Election Commission (KPU) confirmed the authenticity of the data, such as home addresses and national identification numbers, and said it was working to determine the source. It confirmed some of the data dated back to 2013.

"The KPU has been working since last night to look into that," Viryan Aziz, one of its commissioners, told Reuters.

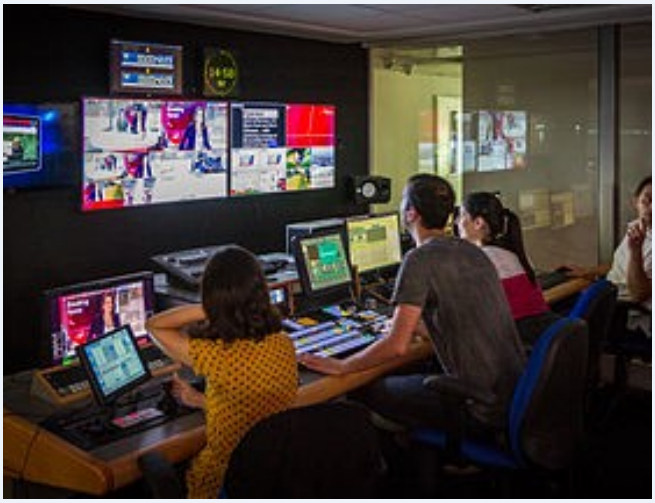
He denied the leak had originated from the commission's servers, saying the same data had been shared with political parties and presidential candidates, in line with the law.

Click **HERE** to read the article.

International News Cont.

Iranian Cyberattack Aimed to Raise Chlorine Level in Israeli Water, Report Says

(by **Haaretz** | **Jun 01, 2020**)



An Iranian cyberattack in April on Israel's water systems aimed to raise chlorine levels in drinking water, the Financial Times reported on Sunday, quoting an unnamed intellience official from a Western country.

The attack, first reported by Israeli daily Yedioth Ahronoth in early May, had been noticed after water pumps started malfunctioning. According to the report, it had focused "on operational systems and mechanisms for adding chlorine to wells."

According to the Financial Times report, the attack, if successful, could have left tens of thousands without water, including farmers, and, at worst, hundreds of people could have fallen seriously ill.

The Financial Times' Western intelligence source said the attack had been "more sophisticated than they [Israel] initially thought." “It was close to successful, and it’s not fully clear why it didn’t succeed,” the source added.

An Iranian source which the Financial Times identified as a regime insider said Tehran was not behind the events. “Iran cannot politically afford to try to poison Israeli civilians," the source said, adding that “our suspicion is that Israelis want more money from the U.S. and made up the whole thing.”

Click **HERE** to read more.

Cyberattack hits internal IT systems of key player in British power market

(by **Sean Lyngaas** | **May 14, 2020**)

Elexon, a company that facilitates transactions on the British electricity market, said Thursday that a cyberattack had hit its internal computers, cutting off email access for employees.

The company grappled with the digital attack throughout Thursday, tweeting that it had identified the “root cause” of the incident.

“The attack is to our internal IT systems and Elexon’s laptops only,” the company said. It was unclear who was responsible for the cyberattack.

The attack didn’t affect the external IT systems that the company uses to track trading between producers and suppliers of electricity, Elexon said. The company manages transactions worth some $2 billion a year, resolving the difference between what electricity generators and suppliers say they will produce or use and what they actually do.

A spokesperson for National Grid ESO — Britain’s national electricity system operator — said the organization was investigating the incident, calling it a “cyber intrusion on Elexon’s internal IT systems.”

Click **HERE** to read more.

National News

Minnesota State Computers Withstand Cyberattacks

(by **Dave Orrick** | **Jun 01, 2020**)

Minnesota is fending off cyber-attacks aimed at crippling the state's computer systems, officials announced Sunday afternoon.

Officials haven't explicitly said that the attacks are connected to attempts to foment civil unrest as law enforcement and the National Guard mount an unprecedented mobilization to tamp down unprecedented violence over the past several days following the death of George Floyd, a black man who died Monday after a white police officer knelt on his neck. But the inference is there to be made.

Here's a statement from Tarek Tomes, the state's chief information officer and commissioner of MNIT, the state's information technology agency:

"MNIT's Security Operations Center is defending against distributed denial-of-service (DDOS) cyber-attacks aimed at overloading state information systems and networks to tip them offline. Keeping our communications systems secure during times of crisis is critical to protecting the Minnesotans that we serve, and we work to meet the challenging and evolving threat to those systems every day. At this time, these attacks have not successfully disrupted the state services that Minnesotans depend upon, and MNIT is working in close coordination with partners at the Department of Public Safety and with the federal government to share intelligence and stay proactive on cyber threats."

Click **HERE** to read more.

Microsoft warns about attacks with the PonyFinal ransomware

(by **Catalin Cimpanu** | **May 27, 2020**)

Microsoft's security team has issued an advisory today warning organizations around the globe to deploy protections against a new strain of ransomware that has been in the wild over the past two months.

"PonyFinal is a Java-based ransomware that is deployed in human-operated ransomware attacks," Microsoft said in a series of tweets published today.

Human-operated ransomware is a subsection of the ransomware category. In human-operated ransomware attacks, hackers breach corporate networks and deploy the ransomware themselves.

This is in opposition to classic ransomware attacks that have been seen in the past, such as ransomware distributed via email spam or exploit kits, where the infection process relies on tricking the users in launching the payload.

Click **HERE** to read more.

National News Cont.

Russian hackers are exploiting bug that gives control of US servers

(by **Dan Goodin** | **May 28, 2020)**

A Russian hacking group tied to power-grid attacks in Ukraine, the world's most destructive data wiper worm, and other nefarious Kremlin operations is exploiting a vulnerability that allows it to take control of computers operated by the US government and its partners.

In an advisory published on Thursday, the US National Security Agency said that the Sandworm group was actively exploiting a vulnerability in Exim, an open source mail transfer agent, or MTA, for Unix-based operating systems. Tracked as CVE-2019-10149, the critical bug makes it possible for an unauthenticated remote attacker to send specially crafted emails that execute commands with root privileges. With that, the attacker can install programs of their choosing, modify data, and create new accounts.

A patch CVE-2019-10149 has been available since last June. The attacks have been active since at least August.

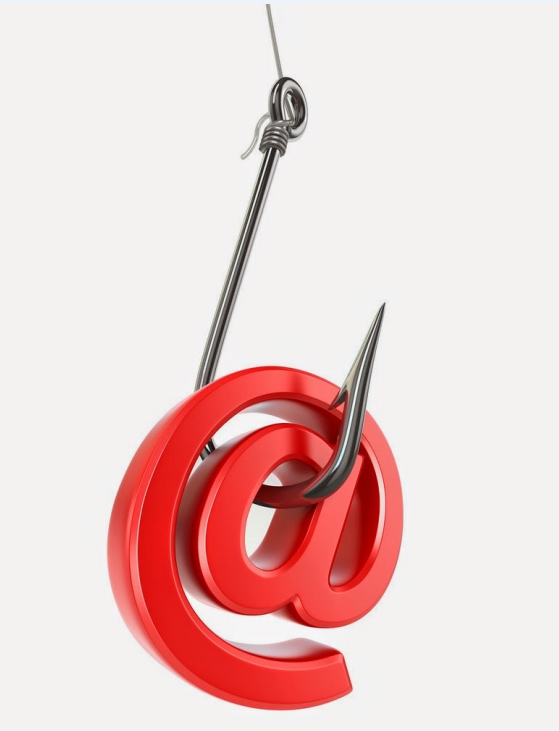
Click **HERE** to read more.

Frankenstein's phishing using Google Cloud Storage

(by **David Murphy** | **Jan. 28, 2020**)

Phishing e-mail messages and/or web pages are often unusual in one way or another from the technical standpoint – some are surprisingly sophisticated, while others are incredibly simple, and sometimes they are a very strange mix of the two. The latter was the case with an e-mail, which our company e-mail gateway caught last week – some aspects of it appeared to be professionally done, but others screamed that the author was a "beginner" at best.

The message appeared to come from info[@]orlonvalves[.]com and passed both SPF and DKIM checks. Contrary to popular belief, it is not that unusual to see a phishing e-mail from an SPF-enabled domain[1,2]. Phishing message with a valid DKIM signature, on the other hand, is something, which is usually seen in connection with a compromised e-mail server. Although it is possible that this was the case in this instance as well, I'm not completely sure about that. The reason is that the domain in question was registered about half a year back using Namecheap, neither it nor any existing subdomain appears to be hosting any content and no company of corresponding name seems to exist. In contrast, a company named Orion Valves, which uses the domain orionvalves[.]com, does exist and although we may only speculate on whether the domain was intended to be used for phishing, since the substitution of characters (i.e. "l" for "i") in lookalike domain names is a common tactic for phishers, I wouldn't be surprised if this effect was what the domain holder was actually going for.



Click **HERE** to read more.

More News

Forget BYOD, this is BYOVM: Ransomware tries to evade antivirus by hiding in a virtual machine on infected systems

https://www.theregister.co.uk/2020/05/22/byovm_ransomware_in_virtualbox/

Threatpost: 70 Percent of Mobile, Desktop Apps Contain Open-Source Bugs

https://threatpost.com/70-of-apps-open-source-bugs/156040/

It wasn't just a few credit cards: Entire travel itineraries were stolen by hackers, Easyjet now tells victims

https://www.theregister.co.uk/2020/05/22/easyjet_hack_victim_notification/

House leaders agree to vote on amendment restricting surveillance of internet browsing

https://www.politico.com/news/2020/05/22/fisa-amendment-house-leaders-274968

eBay port scans visitors' computers for remote access programs

https://www.bleepingcomputer.com/news/security/ebay-port-scans-visitors-computers-for-remote-access-programs/

Hackers leak credit card info from Costa Rica's state bank

https://www.bleepingcomputer.com/news/security/hackers-leak-credit-card-info-from-costa-ricas-state-bank/

Japan investigates potential leak of prototype missile data in Mitsubishi hack

https://www.zdnet.com/article/japan-investigates-potential-leak-of-prototype-missile-design-in-mitsubishi-hack/

Snake ransomware leaks patient data from Fresenius Medical Care

https://www.bleepingcomputer.com/news/security/snake-ransomware-leaks-patient-data-from-fresenius-medical-care/

Spike of Scans for Port 62234

https://isc.sans.edu/forums/diary/What+is+up+on+Port+62234/26144/

More News

New virtual cyber school gives teens chance to try out as cyber security agents from home

https://www.gov.uk/government/news/new-virtual-cyber-school-gives-teens-chance-to-try-out-as-cyber-security-agents-from-home

Ransomware mentioned in 1,000+ SEC filings over the past year

https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/

Security experts warn: Don't let contact-tracing app lead to surveillance

https://www.zdnet.com/article/security-experts-warn-dont-let-contact-tracing-app-lead-to-surveillance/

In trying times like these, it's reassuring to know you can still get pwned five different ways by Adobe Illustrator files

https://www.theregister.co.uk/2020/04/30/adobe_illustrator_patches/

Detect & Prevent Cyber Attackers from Exploiting Web Servers via Web Shell Malware

https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/2159419/detect-prevent-cyber-attackers-from-exploiting-web-servers-via-web-shell-malware/

The Legacy of Women in American Cryptology: Part 1

https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/2103832/the-legacy-of-women-in-american-cryptology-part-1/

Microsoft Warns of Malware Hidden in Pirated Film Files

https://www.darkreading.com/threat-intelligence/microsoft-warns-of-malware-hidden-in-pirated-film-files/d/d-id/1337688

Bugs in WordPress plugins for online courses let students cheat

https://www.bleepingcomputer.com/news/security/bugs-in-wordpress-plugins-for-online-courses-let-students-cheat/

Cyber Challenge

Word Search

Definitions of Cyber

Please use a drawling utensil and email (GRP_Cyber_Ops@dps.texas.gov) a screenshot of the completed version!

Cyber Word Search

V	H	I	W	Y	S	F	J	A	I	E	N	C	R	Y	P	T	I	O	N
C	J	V	Z	B	G	Y	A	W	W	B	Q	V	L	L	G	Q	G	D	C
F	U	B	R	I	G	X	F	J	A	I	X	E	X	P	L	O	I	T	C
U	H	J	G	M	L	X	K	T	G	X	E	C	R	U	G	I	I	S	K
B	A	D	H	H	B	O	O	R	V	Y	A	Z	W	P	U	Y	S	Y	J
S	K	T	R	R	J	I	R	R	N	E	K	M	I	C	D	M	Q	C	Q
G	Y	F	K	A	U	F	H	Z	Y	W	X	G	L	T	E	Q	L	M	X
R	D	Y	X	O	B	D	N	A	S	R	G	K	Y	A	I	H	W	A	F
D	C	F	K	G	J	B	K	S	N	S	N	S	C	E	O	O	Q	W	D
I	J	Q	D	Q	I	L	D	Q	Z	P	I	V	M	R	H	S	X	P	B
I	N	R	X	Q	F	C	H	P	K	R	K	N	S	H	S	U	I	Q	R
Y	W	T	S	G	Y	P	T	Y	N	W	C	E	Z	T	L	Y	F	L	E
J	L	F	E	J	D	U	S	P	G	O	A	T	X	V	E	I	T	K	A
M	V	U	J	G	E	N	V	K	T	J	J	R	R	G	R	I	S	H	C
J	G	N	P	K	R	S	H	N	K	E	K	O	Y	E	Y	E	R	S	H
Z	B	I	G	X	U	I	H	C	V	U	C	J	W	U	E	K	V	A	X
E	G	A	V	P	W	E	T	N	D	R	I	A	Q	W	E	L	V	H	Q
Z	H	M	L	M	O	M	E	Y	K	K	L	N	V	G	U	K	O	L	Q
N	I	O	R	R	X	R	X	O	N	L	C	K	O	F	H	L	T	L	F
M	Z	D	Q	O	S	F	R	G	R	N	P	C	Z	I	P	U	H	T	L

BREACH	DOMAIN	ENCRYPTION
FIREWALL	EXPLOIT	CLICKJACKING
INTEGRITY	THREAT	SANDBOX
HASH	TROJAN HORSE	VPN (Virtual Private Network)

Cyber Challenge

Cryptography

This Month's Challenges

For this month's challenges, We have two challenge questions. We will begin with an easy question. Good luck & remember you can always email me (Jonathan.Espinosa@dps.texas.gov) for hints if you need help. Please email me your answers after figuring out the challenges and I will add you to next months Newsletter!

SHOUT OUT! for submitting your completed Word Find!

- Cynthia Burr, Compliance and Enforcement Service
- Jackie Halsted, Texas Highway Patrol, District 5B

First Challenge:

What cryptographic cipher is named after a famous Roman Emperor?

Second Challenge

Use the answer for the first challenge to help decipher the following text:

Fbehu Vhfxulwb Wlsv

Nhhs vriwzduh xs wr gdwh.
Eh dzduh ri vxvslflrxv hpdlov dqg skrqh fdoov.
Eh fduhixo zkhq folfnlqj rq olqnv iurp dq xqnqrzq vrxufh.
Gr qrw ohdyh ghylfhv xqdwwhqghg
Lqvwdoo dqwl-yluxv surwhfwlrq
Edfn xs brxu gdwd

.

</Closing Comments>

We realize your time is valuable, but education should never end and being aware of cyber issues/dangers are key to protecting not only yourself but the agency. We hope you have enjoyed reading this newsletter and it has given you things to think about.

To close this month's newsletter I want to provide (10) best practices for cybersecurity.

1. Clicking without Thinking Is Reckless
2. Stick to your own devices
3. Be aware of your surroundings
4. Keep track of your digital footprint
5. Keep up with Updates
6. Connect Securely
7. Secure Your Mobile Device
8. Beware Social Engineering
9. Back Up Your Data
10. You're not immune

The link to an explanation of what these practices mean can be found HERE.

Closing out this newsletter, I want to thank our readers and let me know if you would like anything to be added for July. Feel free to email me at Jonathan.Espinosa@dps.texas.gov or call at (512)-424-2329. Our team needs to keep all of DPS up to date with the latest cyber-security trends. Continuing to learn of the latest technologies is an important way to reduce risk and potential breaches to not only DPS but also your personal lives. Thank you for reading this edition of the newsletter.

We hope you enjoyed the newsletter. Please pass it on to others you know so we can spread the knowledge. The better educated everyone is, the safer everyone will be in regard to cyber security. You can see previous issues of the newsletter at this public facing TXDPS website:

http://www.dps.texas.gov/InformationTechnology/Cyber/index.htm

Good luck with the Cyber Challenges. Again, If you have suggestions on how the newsletter could be improved, please let me know.

Stay Safe,

Jonathan

And as always, **THANK YOU FOR YOUR CYBER VIGILANCE.**