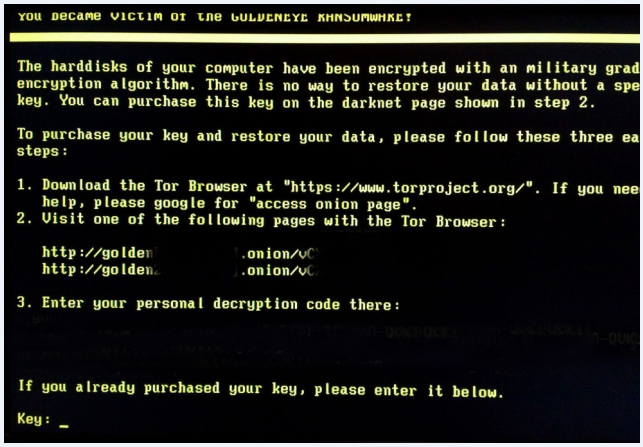
Cyber Security NEWS
Vol. 5 | Issue 6 July 2020

TXDPS Cyber Security Newsletter

The Texas Department of Public Safety Cyber Security welcomes you to this month's Cybersecurity Newsletter. Before diving into this month's issue, we'd like to take a moment to provide a general overview of ransomware: what it is, why it is important to understand, and how to protect against this very real threat.

For example, during Summer 2019, 22 Texas municipalities were compromised with Sodinokibi/REvil ransomware. During that breach, hackers were able to comprise municipal Information Technology (IT) networks by leveraging third party software. The software was being used to remotely manage the network.[1]

Ransomware is a term used to describe malicious software that is used to extort victims into payment. Payment is usually required to be in cryptocurrency, credit cards or untraceable gift cards. This form of "digital extortion" can be grouped into two different strands and further divided by the systems they are tailored to. The two different forms of ransomware either encrypt, obfuscate, and deny access to files, or restrict access and lock users out of systems.[2] An example of this can be seen in the following screenshot of the Goldeneye ransomware.



There are different ways that ransomware can make it to workstations. One of them is through email phishing and spam. Users will receive messages that include either a malicious attachment or a link to a malicious or compromised website. Another way ransomware can infect systems is by using an exploit kit. Exploit kits take advantage of unpatched vulnerabilities in systems or software. Once ransomware infects a system it will block user access to the hard drive or begin encrypting all files located on the system. Mathematically, it is impossible to decrypt files without having the malicious actor's key.[3]

Due to the seriousness of ransomware, it is important to keep your computer updated and patched. Ensure you verify email senders and use caution when opening email attachments. It is also important to keep an eye out for attached files that are compressed (.tar, .zip, .tgz, .tz, .rar, etc.). Being aware of threats leaves us better prepared for the eventuality of an attack. I hope you enjoyed reading about ransomware and continue to be cyber vigilant. For more information please visit CISA.

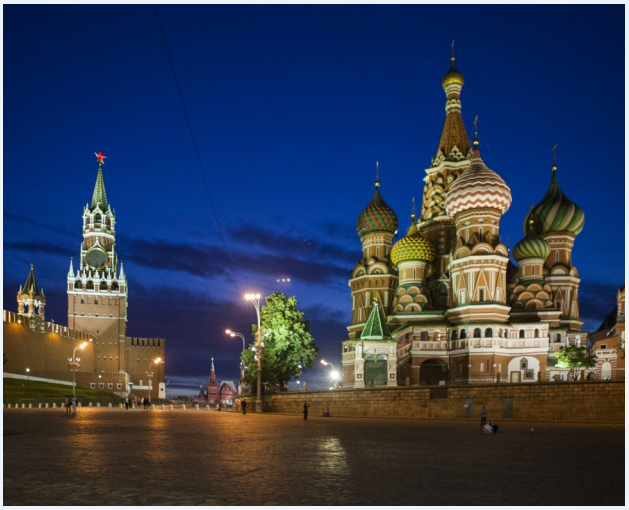
Footnotes

[1] https://www.zdnet.com/article/no-municipality-paid-ransoms-in-coordinated-ransomware-attack-that-hit-texas/
[2] "Ransomware by Allan Liska and Timothy Gallo (O'Reilly). Copyright 2017 Allan Liska and Timothy Gallo, 978-1-491-96788-1."
[3] https://www.crowdstrike.com/epp-101/what-is-ransomware/

International News

Russian hacker group Evil Corp targets US workers at home

(by BBC | **June 26, 2020**)



A Russian hacking group is launching ransomware attacks against a number of US companies, targeting employees who are working from home due to Covid-19. Evil Corp hackers have tried to access at least 31 organisations' networks in order to cripple systems and demand millions of dollars in ransom. The group's two alleged leaders were indicted by the US Justice Department in December 2019.

There are concerns that US voting systems could also be targeted. Last year, US authorities filed charges against Evil Corp's alleged leaders Maksim Yakubets and Igor Turashev, accusing them of using malware to steal millions of dollars from groups including schools and religious organisations in over 40 countries. Officials announced a $5m reward for information leading to their arrest, which they said was the largest amount ever offered for a cyber criminal. Both men are still at large.

The threat comes as the majority of Americans have been working from home due to the coronavirus pandemic - 62% according to a Gallup poll. The US presidential election is also just months away, and federal and local officials have been working to put measures in place to protect voter records as well as manage safe voting practices amid the pandemic.

Click **HERE** to read the article.

Australia says state-based actor is behind surge of sophisticated cyberattacks

(by Bradley Barth | **June 22, 2020**)

Australian Prime Minister Scott Morrison warned late last week that a sophisticated, state-sponsored cyber actor has been attacking the country's government and corporate institutions, as well as critical infrastructure operators, with increasing regularity.

Morrison did not name-and-shame the specific country that is responsible for the alleged attacks. But inside sources told Reuters that China is the culprit, noting similarities between the recent attacks and past malicious activities that were also attributed to Beijing and were aimed at Australia's national parliament and three largest political parties. A Chinese Foreign Ministry spokesman on Friday reportedly denied China was involved.

"Based on advice provided to the Government by our cyber experts, the Australian Cyber Security Centre (ACSC), Australian organizations are currently being targeted by a sophisticated state-based cyber actor," reads an official statement issued by the offices of the Prime Minister, Minister for Home Affairs and Minister for Defense. "This activity is targeting Australian organizations across a range of sectors, including all levels of government, industry, political organizations, education, health, essential service providers, and operators of other critical infrastructure."

Click **HERE** to read the article.

International News Cont.

Morocco used NSO's spyware to snoop on journalist, Amnesty says

(by **Tova Cohen | Jun 22, 2020**)

Technology developed by Israeli cyber security company NSO Group was used by the Moroccan government to spy on journalist Omar Radi, a critic of Morocco's human rights record, Amnesty International said on Monday. The organization found that Radi's phone was subjected to several attacks using a "sophisticated new technique" that silently installed NSO's Pegasus spyware.

"The attacks occurred over a period when Radi was being repeatedly harassed by the Moroccan authorities, with one attack taking place just days after NSO pledged to stop its products being used in human rights abuses and continued until at least January 2020," Amnesty said. If NSO won't stop its technology from being used in such incidents, "then it should be banned from selling it to governments who are likely to use it for human rights abuses," said Danna Ingleton, deputy director of Amnesty Tech.

Several messages left with Moroccan government spokesperson Said Amzazi and human rights minister Mustapha Ramid were not immediately returned.

Click **HERE** to read more.

Cyberbunker 2.0: Analysis of the Remnants of a Bullet Proof Hosting Provider

(by **Karim Lalji and Johannes Ullrich | Jun 23, 2020**)

"Cyberbunker" refers to a criminal group that operated a "bulletproof" hosting facility out of an actual military bunker. "Bullet Proof" hosting usually refers to hosting locations in countries with little or corrupt law enforcement, making shutting down criminal activity difficult. Cyberbunker, which is also known as "ZYZtm" and "Calibour", was a bit different in that it actually operated out of a bulletproof bunker. In September of last year, German police raided this actual Cybebunker and arrested several suspects. At the time, Brian Krebs had a great writeup of the history of Cyberbunker [1].

According to the press release by State Central Cybercrime Office of the Attorney General over 2 petabytes of data were seized including servers, mobile phones, hard drives, laptops, external storage and documents. One of the sites, C3B3ROB, seized by the state criminal police listed over 6000 darknet sites linked to fraudulent bitcoin lotteries, darknet marketplaces for narcotics (with millions of Euros in net transactions for Marijuana, Hashish, MDMA, Ecstasy), weapons, counterfeit money, stolen credit cards, murder orders, and child sexual abuse images [2].

Click **HERE** to read more.

National News

Millions of documents from >200 US police agencies published in "BlueLeaks" trove

(by **Dan Goodin** | **Jun 22, 2020**)

Millions of law enforcement documents—some showing pictures of suspects, bank account numbers, and other sensitive information—have been published on a website that holds itself out as an alternative to WikiLeaks, according to security news website KrebsOnSecurity.

DDOSecrets, short for Distributed Denial of Secrets, published what it said were millions of documents stolen from more than 200 law enforcement groups around the country. Reporter Brian Krebs, citing the organization National Fusion Center Association (NFCA), confirmed the validity of the leaked data. DDOSecrets said the documents spanned at least a decade, although some of the dates in documents suggested a timespan twice as long.

Dates on the most recent documents were from earlier this month, suggesting the hack that first exposed the documents happened in the last three weeks. The documents, which were titled "BlueLeaks," were published on Friday, the date of this year's Juneteenth holiday celebrating the emancipation of enslaved African Americans in the Confederacy. BlueLeaks had special significance in the aftermath of a Minneapolis police officer suffocating a handcuffed Black man to death when the officer placed his knee on the man's neck for 8 minutes and 45 seconds.

Click **HERE** to read more.

Hacker arrested for stealing, selling PII of 65K hospital employees

(by **Sergiu Gatlan** | **June 20, 2020**)

29-year-old Michigan man Justin Sean Johnson was arrested earlier this week for allegedly being behind the 2014 hack of the health care provider and insurer University of Pittsburgh Medical Center (UPMC), stealing the PII and W-2 information of over 65,000 employees, and selling it on the dark web. Pittsburgh-based UPMC is Pennsylvania's largest healthcare provider with over 90,000 employees, integrating 40 hospitals and 700 doctors' offices and outpatient sites.

Johnson, aka "TDS" and "DS", was charged in a forty-three count indictment with conspiracy, wire fraud, and aggravated identity theft. "Justin Johnson stands accused of stealing the names, Social Security numbers, addresses and salary information of every employee of Pennsylvania's largest health care system," U.S. Attorney Brady said in a press release.

"After his hack, Johnson then sold UPMC employees' PII to buyers around the world on dark web marketplaces, who in turn engaged in a massive campaign of further scams and theft."

According to the indictment, Johnson purportedly initially infiltrated UPMC's HR database network around December 1, 2013, by hacking the company's Oracle PeopleSoft human resource management system. On the same day, he ran a test query on the HR database which resulted into the PII of roughly 23,500 UPMC employees being accessed. Between January 21 and February 14, 2014, he supposedly continued remotely accessing the HR database multiple times per day to steal the PII of tens of thousands of other UPMC employees.

Click **HERE** to read more.

National News Cont.

Former DIA Analyst Sentenced for Leaking Classified Information to Journalists

(by **DOJ** | **Jun 18, 2020)**

A former employee of the Defense Intelligence Agency (DIA) was sentenced today to 30 months in prison for leaking classified information to two journalists in 2018 and 2019. "Frese repeatedly passed classified information to a reporter, sometimes in response to her requests, all for personal gain," said Assistant Attorney General for National Security John C. Demers. "When this information was published, it was shared with all of our nation's adversaries, creating a risk of exceptionally grave harm to the security of this country. His conviction and sentence demonstrate the Department's commitment to the investigation and prosecution of such betrayals by clearance holders as part of our mandate to protect our citizens and defend the national security of the United States."

"The American people expect those entrusted with our nation's most sensitive secrets to keep those secrets safe. Mr. Frese did just the opposite," said Assistant Director Alan E. Kohler Jr. of the FBI's Counterintelligence Division. "The FBI is committed to protecting the national security interests of the United States and will vigorously pursue investigations into current and former clearance holders who leak classified information."

Click **HERE** to read more.

Cyberattackers raising stakes in financial sector, security experts tell House subcommittee

(by **Larry Jaffee** | **Jun 17, 2020**)

Cyberattacks on the U.S. financial sector amid COVID-19 rose 238 percent over the first five months of 2020, VMware/Carbon Black told Congress during a House Subcommittee on National Security, International Development and Monetary Policy virtual hearing Tuesday. Four NGOs brought to the attention of the lawmakers of how attackers are raising the stakes with fraudulent schemes and the need for public and private sector vigilance during testimony for the nearly two -hour session entitled "Cybercriminals and Fraudsters: How Bad Actors Are Exploiting the Financial System During the COVID-19 Pandemic."

In his opening statement, subcommittee Chairman Emanuel Cleaver, D-Mo., cited a 148 percent spike in cyberattacks in March when compared to February, and that the financial sector in that period received a 38 percent increase in ransomware attacks. Cleaver cited cybersecurity complaints to the FBI's Internet Crime Complaint Center quadrupled in the past four months from 1,000 daily before the pandemic to as many as 4,000 incidents in a day. Ninety percent of the financial sector's employees are working from home, making exploitation even more probable due to vulnerabilities without the parameter defenses found in a corporate environment, noted Tom Kellermann, VMWare head of cybersecurity strategy.

Click **HERE** to read more.

More News

Ransomware operators lurk on your network after their attack

https://www.bleepingcomputer.com/news/security/ransomware-operators-lurk-on-your-network-after-their-attack/

Multiple “CIA failures” led to theft of agency’s top-secret hacking tools

https://arstechnica.com/information-technology/2020/06/theft-of-top-secret-cia-hacking-tools-was-result-of-woefully-lax-security/

T-Mobile's outage yesterday was so big that even Ajit Pai is mad

https://arstechnica.com/tech-policy/2020/06/t-mobiles-outage-yesterday-was-so-big-that-even-ajit-pai-is-mad/

Netgear moves to plug vulnerability in routers after researchers find zero-day

https://www.cyberscoop.com/netgear-remote-code-execution-grimm-zdi/

AWS said it mitigated a 2.3 Tbps DDoS attack, the largest ever

https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/

Honda resumes production at plants hit by suspected cyber attack

https://www.reuters.com/article/honda-cyber/honda-resumes-production-at-plants-hit-by-suspected-cyber-attack-idUSL4N2DP14K

Enter the RAT.

https://thecyberwire.com/podcasts/research-saturday/141/notes

The Golden Tax Department and the Emergence of GoldenSpy Malware

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-golden-tax-department-and-the-emergence-of-goldenspy-malware/

More News

Hackers break into the Ethiopian government sites and leave a message about “the Nile”

https://www.eg24.news/2020/06/hackers-break-into-the-ethiopian-government-sites-and-leave-a-message-about-the-nile.html

Secondary Infektion

https://secondaryinfektion.org/downloads/secondary-infektion-report.pdf

U.S. Supreme Court to Weigh in on Computer Fraud and Abuse Act (CFAA) for the First Time

https://www.jdsupra.com/legalnews/u-s-supreme-court-to-weigh-in-on-39718/

Zoom says free users will get end-to-end encryption after all

https://www.theverge.com/2020/6/17/21294355/zoom-security-end-to-end-encryptoin-beta-release-july-2020-new-feature

New Android Spyware ActionSpy Revealed via Phishing Attacks from Earth Empusa

https://blog.trendmicro.com/trendlabs-security-intelligence/new-android-spyware-actionspy-revealed-via-phishing-attacks-from-earth-empusa/

Drupal fixes three vulnerabilities, including one RCE

https://www.helpnetsecurity.com/2020/06/19/cve-2020-13663/

Italian company exposed on Clearnet earned up to $ 500,000 helping cybercriminals to deliver malware using cloud drives.

https://research.checkpoint.com/2020/guloader-cloudeye/

Kasada Raises $10 Million in Series B Funding to Fuel Rapid U.S. Expansion and Enhance Its Web Traffic Integrity Solution

https://www.prnewswire.com/news-releases/kasada-raises-10-million-in-series-b-funding-to-fuel-rapid-us-expansion-and-enhance-its-web-traffic-integrity-solution-301077573.html

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

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

BLACKLIST	BUG	DECRYPT
HACTIVISM	KEYLOGGER	PATCH
RESTORE	SPOOFING	VISHING
WHITELIST	WHITEHAT	ZOMBIE

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 and Challenge!

Aja Alvarez, Human Resources Employee Services
Alejandra Aguilar, Program Supervisor V
Brenda Deats, THP-CVE
Cassie Snyder, Lubbock DLD
Catherine E. Mustoe, Crime Lab
Dannie Rogers, DLD
DiAnn N. Shaw, Intelligence & Counterterrorism Division
Erich Neumann CFCE, Special Agent
Estela Navejas, Crime Lab
Faye Krueger, Motor Carrier Bureau
Gary Gregg, Technical Services Manager
Jared Crouse, Texas Rangers
Jeanine C. Hudson, Legal Operations
Karyn Duty, IOD
Kim Stevens, Assistant Manager
Kymberly Hernandez, Program Supervisor V
Linda Prosperie, TXMAP Team
Mark Inabinet, Crime Analyst
Melissa Clair, HR Specialist
Melissa Vega, CID
Mike Dayton, Toxicology Technician
Mike McHale, Trooper, Texas Highway Patrol
Miriam Marshall, CID
Paul Lancaster, IOD
Peggy Gillum, Law Enforcement Services, Cyber Security
Robin Neathery, Finance Division
Sarah Siedelmann, LPS II
SSG Brynja Burns, Texas Rangers
Stephanie Erlewine, Business Intel Statistician
Stephen "Doc" Petty, CISSP, SSCP, CJIS ISO – Texas, Law Enforcement Support
Susan Rowe, License and Permit Specialist
Tiffany Stacey, License and Permit Specialist
Tracy Kingsley, LESD
Vikki Graves, District 2A - Houston, THP

First Challenge:

Who published a type of polyalphabetic cipher called an autokey cipher in 1586?

Second Challenge

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

Xsab ueq M yw zs cvvzfyt zsrvshegvr mejfntqgrv?

Yklgxr eeh qltkz crym kuqcykis.

Fsm uexxdwt avxy pjyka srg acmt iaxvvjyg ewfvmom ghqvvwtps.

Whiq ihiop nxkedsmmfxv adbn gnykmpy. Bm oeuc jn utrrzrh pmiap dxoiilziext, pvmf jush akrqiiw zzu bzmqo twa oasn, tbctquyoemte auie eueakzqhroa gvr gfqqceakig jdtkw bv QMQ qitww.

Nizx eshv gisdovsp lrawxqnxzso danw.

Zhvdne izezp tpnlwvv. Ma guy nvv yoduzw akiopkv bv esu ln meelp da ritmkmnltm, lvb xj dkvvjp xip eusmo'w gmmmgmdedj bg usqxvkzmak klf devviu hdzkggpp. Hp yob uplgf wt eac cmovs qf xki zugmy.

Mejpcm ggyuwztl. Orig cpfrawpi minuvziu eczub jifiib icoiiwfnuzaxb xczkegw rre fp bg hdxz wt vnrjsnhazw xhgcvouhij.

Modtidp droqbmeyj wpqtesvh, jdzkanpcw, byd meelp aqrxrvj. Ofpp bzip yklgxrh ks spdcui pegqimbyj rfewwjo wvvnlmp.

</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 August. 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.

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