Cyber Security NEWS
Vol. 5 | Issue 7
August 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, DPS has a new Cyber Security Training Officer! Please help us give a warm welcome to Eric Posadas.

Eric comes to us from Texas Parks and Wildlife where he served as a cyber security analyst. He has a little over 15 years of IT experience, all with the State of Texas spanning a few state agencies. He is looking forward to promoting cyber security awareness while engaging coworkers through customer service as the focus of his role here.

Eric finds joy in the gift of being a husband and father and is grateful for impromptu living room dance parties with his son and wife, even though he can't dance. He and his wife enjoyed live music back when attending concerts was a thing (thanks, COVID19), and they are self-proclaimed foodies. Because of this affinity for food, Eric also appreciates staying active with an outdoor fitness group and taking family walks throughout his neighborhood and nearby parks.

Eric is always open to constructive feedback and ideas so if you have any thoughts on cyber security awareness here at DPS, please feel free to share those with him. He's eager to settle in, learn the culture, and connect with each of you to continue to foster a cyber security awareness mindset you can use at the office and at home. You'll be hearing more from him soon.

International News

Chinese hackers blamed for the spread of MgBot Trojan across India, Hong Kong

(by Charlie Osborne | **July 23, 2020**)

An uptick in the spread of a new MgBot malware variant across India and Hong Kong is being laid at the feet of a suspected Chinese advanced persistent threat (APT) group.

According to Malwarebytes researchers Hossein Jazi and Jérôme Segura, the theme of phishing documents used to drop the malware, relating to tensions in Hong Kong and China, indicates that a Chinese cyberattack group -- active since 2014 -- is likely to blame.

In a blog post on Tuesday, the cybersecurity researchers said an archive file with a document masquerading as communication from the government of India was spotted on July 2.

The phishing document originally dropped a variant of Cobalt Strike, a legitimate penetration testing tool that can be abused by threat actors. However, on the same day, the template was changed to drop a loader for MgBot, a Remote Access Trojan (RAT).

On July 5, additional phishing documents laden with MgBot were found that weaponized statements from the UK Prime Minister, Boris Johnson, concerning the current political situation between China and Hong Kong.

Click **HERE** to read the article.

UK looks to new laws on spies after critical intel report

(by Danica Kirka | **July 22, 2020**)

Britain's government faced heated questions on national security Wednesday after a damning intelligence committee report on Russian meddling in the nation's politics concluded the U.K. should examine allegations of interference in the European Union referendum.

The fallout from the report from Parliament's Intelligence and Security Committee dominated the agenda on the final day in the House of Commons before the summer break, with lawmakers demanding to know whether the UK had done enough to face the threat posed by Moscow.

The report concluded that Russia sees Britain as one of its top intelligence targets, adding that Moscow's attempts to influence the U.K. are the "new normal" and successive governments have welcomed Russian oligarchs with open arms.

Russians with "very close links" to President Vladimir Putin are "well integrated into the U.K. business, political and social scene — in 'Londongrad' in particular," the report said.

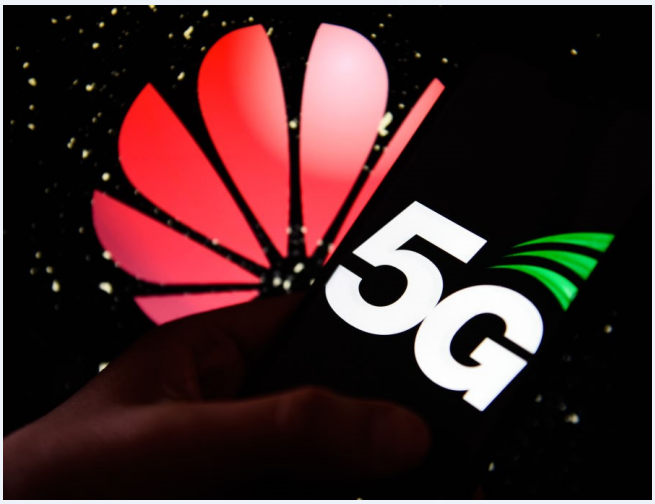
Opposition Labour Party leader Keir Starmer challenged Prime Minister Boris Johnson in the Commons, suggesting he sat on the report despite its dire warnings of the threat to national security.

Click **HERE** to read the article.

International News Cont.

French limits on Huawei 5G equipment amount to de facto ban by 2028

(by **Mathieu Rosemain, Gwénaëlle Barzic | Jul 22, 2020**)



French authorities have told telecoms operators planning to buy Huawei 5G equipment that they won't be able to renew licences for the gear once they expire, effectively phasing the Chinese firm out of mobile networks, three sources close to the matter said.

Like other countries in Europe, France is laying the ground for its next-generation 5G mobile market in the middle of a growing geopolitical storm between two global superpowers.

The United States say the company's equipment could be used by the Chinese government for espionage - a charge denied by Huawei and Beijing - and has pressed its allies to ban it.

France's cybersecurity agency ANSSI said this month it would allow operators to use equipment, including Huawei's, under licences of three to eight years. But it added it was urging telcos not currently using the Chinese company's gear to avoid switching to it.

Operators must each apply for dozens of licences for equipment to cover different parts of the country.

The sources said ANSSI had informed operators of most licence decisions for large cities. They said the bulk of authorisations for Huawei gear were for three or five years, while most of those for equipment from European rivals Ericsson (ERICb.ST) or Nokia (NOKIA.HE) received eight-year licences. ANSSI's decisions have not been made public, either by the agency or by the companies.

Click **HERE** to read more.

Indonesian businesses ramp up cybersecurity budget amid rampant attacks

(by **Eisya A. Eloksari | Jul 23, 2020**)

Indonesian companies plan to increase their cybersecurity budget this year amid the high number of cyberattacks during the pandemic, signalling a growing awareness and commitment in digital safety, a survey by a cybersecurity company shows.

US-based Palo Alto Networks stated that, based on the firm's survey in February, around 84 percent of Indonesian companies planned to raise their IT budget this year, 44 percent of which would allocate more than half of their IT budget to cybersecurity investment.

The number of companies in Indonesia committed to increasing the IT budget is higher than the ASEAN average of 73 percent.

"Almost all companies in the country have put cybersecurity as their business enabler in this digital era," said Palo Alto Networks Indonesia country manager Surung Sinamo in a press briefing on July 15. "This shows that we are moving on the right track in terms of digital safety awareness."

He went on to say that the top reasons these companies increased their budget were to tackle the growing number of sophisticated cyberattacks, upgrade their existing security framework and keep up with competitors.

Click **HERE** to read more.

National News

Twitter says hackers accessed DMs for 36 users in last week's hack

(by **Catalin Cimpanu** | **Jul 23, 2020**)

Twitter has provided another update in its investigation into its Wednesday security incident when a group of hackers breached its backend and tweeted a cryptocurrency scam on behalf of high-profile and verified accounts.

The incident became of note because hackers compromised accounts for public figures such as Barrack Obama, Joe Biden, Bill Gates, Elon Musk, Jeff Bezos, Apple, Uber, Kanye West, Kim Kardashian, Michael Bloomberg, and many others.

In light of the highly publicized incident and with all the world's eyes on its response, Twitter has been providing updates on a daily basis since the hack, as security teams sift through the logs in search of what happened and who was behind the intrusion.

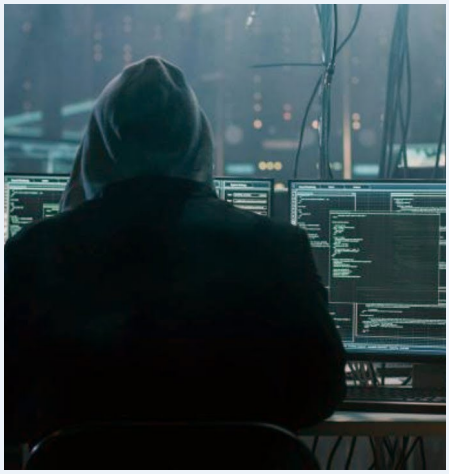
These updates have now become quite bulky and convoluted, and as a result, we'll list them below and continue to update this article as Twitter releases new evidence.

The incident took place on Wednesday, July 15, 2020. Twitter said hackers used social-engineering to gain access to Twitter employee accounts. A New York Times report that has yet to be confirmed by Twitter said that hackers breached employee Slack accounts and found credentials for the Twitter backend pinned inside a Slack channel.

Click **HERE** to read more.

Two Alleged Criminals – A Hezbollah Associated Narco-Money Launderer and a Computer Hacker - Extradited from Cyprus to the United States

(by **US DOJ** | **Jul 18, 2020**)



A Lebanese national wanted in Florida who is alleged to have conspired to engage in, and actually engaged, in the laundering of drug proceeds through the use of the black market peso exchange in support of Hezbollah's global criminal-support network and a Cypriot national who is wanted in the Northern District of Georgia and the District of Arizona for cyber intrusion and extortion, were both extradited yesterday from the Republic of Cyprus to the United States.

"These successful extraditions demonstrate the commitment of the Department of Justice to support local, state and federal law enforcement agencies throughout the United States and our strong working relationship with dedicated foreign partners who assist in apprehending foreign fugitives wherever they may be hiding," said Acting Assistant Attorney General Brian C. Rabbitt of the Justice Department's Criminal Division. "Thanks to the efforts of our law enforcement partners in Cyprus, Ghassan Diab and Joshua Polloso Epifaniou will now be held accountable in the United States for their alleged crimes."

Ghassan Diab, 37, a citizen of Lebanon, arrived in Miami yesterday after being extradited from the Republic of Cyprus. Diab is charged in the State of Florida, Circuit Court of the Eleventh Judicial Circuit in and for Miami-Dade County, with two counts of money laundering over $100,000, two counts of conspiracy to launder over $100,000, two counts of unlicensed transmission of currency over $100,000, and two counts of unlawful use of a two-way communications device to further the commission of money laundering, all felonies under Florida law.

Diab was previously identified as an alleged Hezbollah associate and charges were announced by the Miami-Dade State Attorney's Office in October 2016 as a part of the Drug Enforcement Administration (DEA) Miami Field Division's "Operation reconquista," a joint State/Federal partnership to attack money laundering which resulted in the arrest of two co-defendants.

Click **HERE** to read more.

National News Cont.

Iran-linked hackers steal sensitive data from US Navy member, researchers say

(by **Sean Lyngaas** | **Jul 16, 2020)**

Allison Wikoff has spent years tracking suspected Iranian hackers, sifting through data they've left behind and analyzing their techniques. But in May, when her colleague stumbled upon a server with 40 gigabytes of the hackers' training videos and online personas, Wikoff knew she had struck gold.

"[When] we started combing through all the data and video files we couldn't believe what we were seeing," said Wikoff, a cyber threat analyst on IBM's X-Force security team. "This discovery brought a whole new meaning to observing 'hands-on keyboard activity.'"

The nearly five hours of videos found on the server, which IBM reported publicly on Thursday, include evidence of a suspected Iranian hacker stealing data from the personal email and social media accounts of an enlisted member of the U.S. Navy and a Greek naval officer. The attacker managed to exfiltrate files on the military unit of the U.S. Navy member and their naval base, along with tax records and their personal data stored on a cloud server, according to IBM.

The research is a vivid reminder of the digital espionage that is an undercurrent of U.S-Iranian tensions in the Persian Gulf, and follows another big exposure of Iranian hacking data last year.

Click **HERE** to read more.

Decline in early cyber investments continues alongside coronavirus concerns

(by **Jeff Stone** | **Jul 22, 2020**)

Fewer face-to-face meetings between security startups and potential investors contributed to a steep decline in the number of venture capital deals since COVID-19 spread throughout the world.

Investments in early stage cybersecurity companies fell by 37.7% during the second fiscal quarter of 2020, compared to the same time period in 2019, according to a financially-focused paper published Wednesday by venture firm DataTribe.

It's a downward trend that began at the end of last year and continued into the first months of 2020 as global economies reacted to the coronavirus pandemic. Early stage investments in the overall technology sector are down by roughly 45% over the first two quarters of this year, according to DataTribe co-founder Mike Janke. Other external factors — such as uncertainty about U.S. politics, shifting monetary policy and increasingly high investment levels — also are fueling the decline in investing.

Venture deals typically close 90 days after investors strike a deal with a startup, Janke said. Initially, after the first COVID-19 infections were detected in the U.S., that 90-day lag helped create a misunderstanding that dollars were still flowing, when in fact the people involved had started to stay at home.

Click **HERE** to read more.

More News

The Fake Cisco by Dmitry Janushkevich, 15 July 2020

https://labs.f-secure.com/publications/the-fake-cisco/

Apple releases iOS and iPadOS 13.6, macOS 10.15.6, and watchOS 6.2.8

https://arstechnica.com/gadgets/2020/07/apple-updates-ios-to-13-6-with-digital-car-keys-local-news-and-more/

FYI Russia is totally hacking the West's labs in search of COVID-19 vaccine files, say UK, US, Canada cyber-spies

https://www.theregister.com/2020/07/16/russia_coronavirus_hacking/

Why the internet went haywire last week

https://www.zdnet.com/article/why-the-internet-went-haywire-last-week/

UK.gov admits it has not performed legally required data protection checks for COVID-19 tracing system

https://www.theregister.com/2020/07/20/uk_test_trace_data_protection/

Hackers Can Now Trick USB Chargers To Destroy Your Devices—This Is How It Works

https://www.forbes.com/sites/zakdoffman/2020/07/20/hackers-can-now-trick-usb-chargers-to-destroy-your-devicesthis-is-how-it-works/#591d2a045bf2

Microsoft will disable insecure TLS in Office 365 on Oct 15

https://www.bleepingcomputer.com/news/microsoft/microsoft-will-disable-insecure-tls-in-office-365-on-oct-15/

There’s a reason your inbox has more malicious spam—Emotet is back

https://arstechnica.com/information-technology/2020/07/destructive-emotet-botnet-returns-with-250k-strong-blast-of-toxic-email/

More News

Ew, that's unsanitary: SEO plugin for WordPress would run arbitrary JavaScript inputs instead of scrubbing them

https://www.theregister.com/2020/07/17/all_in_one_seo_pack_javascript_sanitisation_vuln/

MATA: Multi-platform targeted malware framework

https://securelist.com/mata-multi-platform-targeted-malware-framework/97746/

Prometei botnet and its quest for Monero

https://blog.talosintelligence.com/2020/07/prometei-botnet-and-its-quest-for-monero.html

The Cyber Threat to Sports Organisations

https://www.ncsc.gov.uk/files/Cyber-threat-to-sports-organisations.pdf

PlayStation 5 vs. Xbox Series X: What We Know So Far

https://www.pcmag.com/news/playstation-5-vs-xbox-project-scarlett-what-we-know-so-far

Bleeping Computer: Lorien Health Services discloses ransomware attack affecting nearly 50,000

https://www.bleepingcomputer.com/news/security/lorien-health-services-discloses-ransomware-attack-affecting-nearly-50-000/

Fixing the Zoom 'Vanity Clause' – Check Point and Zoom collaborate to fix Vanity URL issue

https://blog.checkpoint.com/2020/07/16/fixing-the-zoom-vanity-clause-check-point-and-zoom-collaborate-to-fix-vanity-url-issue/

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

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

APPLICATIONS	BROWSER	CODING
DIGITAL FORENSICS	DRIVER	FORGERY
MACRO	MEMORY	PROGRAM
ROUTER	SNARFING	UPDATE

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 for hints if you need help. Please email grp_cyber_security@dps.texas.gov with questions and also your answers after figuring out the challenges. We will add you to next months Newsletter!

First Challenge: What is the difference between encoding and encryption?

Second Challenge: What binary-to-text encoding scheme represents binary data in a printable ASCII string format by translating it into a radix-64 representation?

Third Challenge: Using the answer to the second challenge decode the following message:

QmUgc3VzcGljaW91cyBvZiB1bmV4cGVjdGVkIGVtYWlscy4gUGhpc2hpbmcgZW1haWxzIGFyZSBjdXJy
ZW50bHkgb25lIG9mIHRoZSBtb3N0IHByZXZhbGVudCByaXNrcyB0byB0aGUgYXZlcmFnZSB1c2VyLiB
UaGUgZ29hbCBvZiBhIHBoaXNoaW5nIGVtYWlsIGlzIHRvIGdhaW4gaW5mb3JtYXRpb24gYWJvdXQge
W91LCBzdGVhbCBtb25leSBmcm9tIHlvdSwgb3IgaW5zdGFsbCBtYWx3YXJlIG9uIHlvdXIgZGV2aWNlLi
BCZSBzdXNwaWNpb3VzIG9mIGFsbCB1bmV4cGVjdGVkIGVtYWlscy4=

SHOUT OUT! Thank you for submitting your completed challenges!

Patti Cook - License and Permit Specialist

Erich Neumann - Special Agent

Kymberly Hernandez - Program Supervisor

Faye Krueger - Admin. Asst. III

Gary Gregg - Technical Services Manager

Haven Cain - LPS III

Jared Crouse - Team Lead - IT

E. "René" Hess - System Analysis

Jana Connor - License and Permit Specialist

Irma Irizarry - Human Resources Operations

Aleandra Keenan - DNA Evidence Technician

Linda Prosperie - GIS Analyst

Lyman Campbell - Compliance Review Investigator

Cassie Snyder - Lubbock DLD

Cindy Gillam - Communications Supervisor

Margaret Westling - License and Permit Specialist II

Jessica Alvidrez - LPS II

Frank Hooton - Texas Rangers

Shelli Turner - Lead License & Permit Analyst V

Lisa Schiff - IT Finance & Resource Planning

Peggy Gillum - Cyber

</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 September. 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.**