Cyber Security NEWS
Vol. 4 | Issue 7
July 2019

Welcome to the TXDPS Cyber Newsletter

Hello everyone and welcome to this month's DPS cybersecurity newsletter. If you are a new reader, welcome. If you are a regular reader, thank you for reading the newsletter and finding it interesting enough to view new issues. For those new readers, inside you will find several articles about various cybersecurity issues. Hopefully you find them as interesting and informative as I have. You will also find cybersecurity related challenges at the end of the newsletter. Please try to solve them. Doing so should be just as informative as the articles I have provided.

At the beginning of each newsletter I like to start with some sort of relevant public type announcement or information. For this newsletter I want to talk about a subset of phishing that is occurring more and more frequently. In case you are unaware of what phishing is, it is a form of fraud where an attacker masquerades as a reputable entity or person in email or other form of communication. Malicious links or attachments are often part of a phishing attempt and almost all of them attempt to scare you into taking some sort of immediate foolish action.

The subset of phishing I want to talk about today is known as sextortion. Most readers have probably heard of this or might even have received one of these phishing attempts. Sextortion phishing is the practice of extorting money from someone by threatening to reveal evidence of their sexual activity. The emails are often very explicit and attempt to scare the reader into believing some sort of compromising sexual act they were involved with has been recorded. The intent is to get you to pay money to keep the act secret. While it is possible for someone to remotely record you through your webcam without your knowledge, I have not heard of a sextortion case where this has actually happened.

For those who might not have ever seen one of these emails, here is an excerpt of one:

> ^^ is your password. You don't know me and you're thinking why you received this email, right?
>
> I placed malware on the porn website and guess what, you visited this web site to have fun (you know what I mean). While you were watching the video, your web browser acted as an RDP (Remote Desktop) and a keylogger which provided me access to your display screen and webcam.
>
> Right after that, my software gathered all your contacts from your Messenger, Facebook account, and email account. What exactly did I do? I made a split-screen video. First part recorded the video you were viewing (you've got a fine taste haha), and next part recorded your webcam *(Yep! It's you doing nasty things!)*.
>
> **What should you do?**
>
> Well, I believe, $1400 is a fair price for our little secret. You'll make the payment via Bitcoin to the below address (if you don't know this, search "how to buy bitcoin" in Google).

For most people this would be offensive and laughable at the same time. Because these emails often contain information that can allow an organization to block all incoming sextortion emails so people never see them. However, nothing blocks them from your personal email. And link with any phishing email, clicking on any links is a very dangerous thing to do. Please see my closing comments on the last page for more important things to know about sextortion emails.

Georgia / Florida

RANSOMWARE HITS GEORGIA COURTS AS MUNICIPAL ATTACKS SPREAD

(by **LILY HAY NEWMAN** on **07.01.19** at **07:49 PM**)

RANSOMWARE HAS NO shortage of cautionary tales and wakeup calls from the past decade. But for local governments, this past year has been a particularly brutal reminder of the threat. Following a 2018 attack that paralyzed the City of Atlanta for weeks, more than half a dozen cities and public services across the country have fallen to ransomware so far in 2019, on a near-monthly basis; the Administrative Office of the Georgia Courts became the latest victim on Saturday, when an attack knocked its systems offline.

The string of attacks on municipalities may seem like a new pattern. But it's unclear how many of them, if any, were perpetrated by the same actors. And law enforcement officials emphasize that the spate of attacks actually fits into a broader, ever-growing trend of ransomware attacks that spans numerous industry sectors.

"We are seeing an increase in targeted ransomware attacks; however, we do not have enough data to indicate one industry or sector is being targeted more than another," the FBI told WIRED in a statement. "Cyber criminals are opportunistic. They will monetize any network to the fullest extent."

Incident responders agree with this assessment and note that attackers will capitalize on any technique that sees some success, to infect as many targets as possible and maximize the possibility of return.

"There's definitely an increase or uptick in the amount of ransomware campaigns that we're seeing out there, but it's not specific to municipalities or state or federal organizations, it's just pretty much across the board in every industry vertical," says David Kennedy, CEP of the penetration testing and incident response consultancy TrustedSec. "We're working seven consecutive ransomware attacks right now—a couple of manufacturing, a couple of credit unions, and one local type of government incident."

Click **HERE** to read the article.

Florida city fires IT employee after paying ransom demand last week

(by **Catalin Cimpanu** for **Zero Day | July 1, 2019**)

At least one head rolls after second Florida city pays gigantic ransom demand to ransomware gang.

Officials from Lake City, Florida, have fired an IT employee last week after the city was forced to approve a gigantic ransomware payment of nearly $500,000 last Monday.

The employee, whose name was not released, was fired on Friday, according to local media reports, who cited the Lake City mayor.

The city's IT manager is also planning to revamp the town's entire IT department to prevent a similar incident from happening in the future.

AFTERMATH OF THE "TRIPLE THREAT" ATTACK

Lake City's IT network was infected with malware on June 10. The city described the incident as a "triple threat."

In reality, an employee opened a document they received via email, which infected the city's network with the Emotet Trojan, which later downloaded the TrickBot Trojan, and later, the Ryuk ransomware.

The latter spread to the city's entire IT network and encrypted files. Hackers eventually demanded a ransom to let the city regain access to its systems.

The city's leadership approved a ransom payment last Monday, which was paid the next day, on Tuesday. The city's IT staff started decrypting files on the same day.

Click **HERE** to read the article.

Microsoft / Yandex

Microsoft to Require Multi-Factor Authentication for Cloud Solution Providers

(by **KrebsonSecurity** on **28 Jun 19**)

It might be difficult to fathom how this isn't already mandatory, but **Microsoft Corp.** says it will soon force all Cloud Solution Providers (CSPs) that help companies manage their **Office365** accounts to use multi-factor authentication. The move comes amid a noticeable uptick in phishing and malware attacks targeting CSP employees and contractors.

When an organization buys Office 365 licenses from a reseller partner, the partner is granted administrative privileges in order to help the organization set up the tenant and establish the initial administrator account. Microsoft says customers can remove that administrative access if they don't want or need the partner to have access after the initial setup.

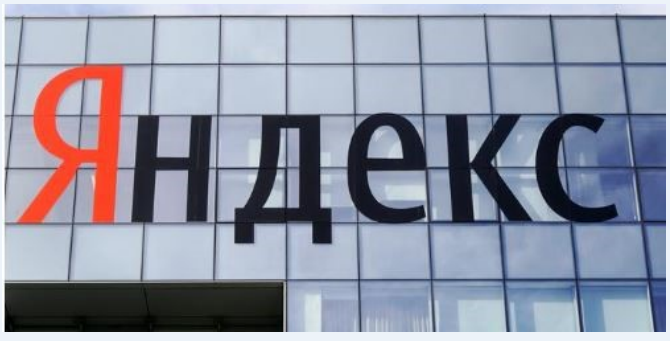
But many companies partner with a CSP simply to gain more favorable pricing on software licenses—not necessarily to have someone help manage their Azure/O365 systems. And those entities are more likely to be unaware that just by virtue of that partnership they are giving someone at their CSP (or perhaps even outside contractors working for the CSP) full access to all of their organization's email and files stored in the cloud.

This is exactly what happened with a company whos email systems were rifled through by intruders who broke into PCM Inc., the world's sixth-largest CSP. The firm had partnered with PCM because doing so was far cheaper than simply purchasing licenses directly from Microsoft, but its security team was unaware that a PCM employee or contractor maintained full access to all of their employees' email and documents in Office 265.

Click **HERE** to read more.

Exclusive: Western intelligence hacked 'Russia's Google' Yandex to spy on accounts—sources

(by **Christopher Bing, Jack Stubbs, Joseph Menn** on **June 27, 2019**)



WASHINGTON/LONDON/SAN FRANCISCO (Reuters) - Hackers working for Western intelligence agencies broke into Russian internet search company Yandex in late 2018, deploying a rare type of malware in an attempt to spy on user accounts, four people with knowledge of the matter told Reuters.

The malware, called Regin, is known to be used by the "Five Eyes" intelligence-sharing alliance of the United States, Britain, Australia, New Zealand and Canada, the sources said. Intelligence agencies in those countries declined to comment.

Western cyberattacks against Russia are seldom acknowledged or spoken about in public. It could not be determined which of the five countries was behind the attack on Yandex, said sources in Russia and elsewhere, three of whom had direct knowledge of the hack. The breach took place between October and November 2018.

Yandex spokesman Ilya Grabovsky acknowledged the incident in a statement to Reuters, but declined to provide further details.

"This particular attack was detected at a very early stage by the Yandex security team. It was fully neutralized before any damage was done," he said. "Yandex security team's response ensured that no user data was compromised by the attack."

The company, widely known as "Russia's Google" for its array of online services from internet search to email and taxi reservations, says it has more than 108 million monthly users in Russia. It also operates in Belarus, Kazakhstan and Turkey.

Click **HERE** to read more.

Insulin Pumps / Dridex

Cybersecurity Risk Prompts Recall of Medtronic Insulin Pumps

(by **Amanda Pedersen** on **June 28, 2019)**

Medtronic cannot update the MiniMed 208 and Paradigm insulin pump models to address the potential cybersecurity risks so FDA says patients should replace these pumps with models that are better equipped to protect them from hacking.

At least 4,000 U.S. patients who are using Medtronic MiniMed insulin pumps are vulnerable to potential hacking. The company is working with distributors to identify additional patients who may be using the pumps that are now being recalled due to potential cybersecurity risks, according to an FDA notice issued Friday.

The agency said it is concerned that, due to cybersecurity vulnerabilities identified in the device, a hacker could potentially connect wirelessly to a nearby MiniMed insulin pump and change the pump's settings. This could allow a person to over deliver insulin to the patient, leading to low blood sugar, or to stop insulin delivery, leading to high blood sugar and a buildup of acids in the blood.

FDA said it is not currently aware of any confirmed reports of patient harm related to these risks, but because the company cannot update the MiniMed 508 and MiniMed Paradigm pump models to address the vulnerabilities, the devices are being recalled. The agency said patients using these models should replace the devices with models that are better equipped to protect them from hacking. Medtronic is providing patients with alternative insulin pumps that have enhanced built-in cybersecurity capabilities.

Click **HERE** to read more.

New variant of Dridex Trojan fools antivirus solutions

(by **Ryan Stewart** on **July 1, 2019**)

- This new variant uses a whitelisting technique in order to evade mitigation from antivirus software.
- It is believed that the attack campaign related to this variant also uses a new command and control infrastructure.

Security researchers have recently identified an ongoing attack campaign distributing a new variant of the Dridex Trojan. Discovered by malware researcher Brad Duncan, this variant reportedly goes undetected under many of the popular antivirus solutions. Security firm eSentire, which conducted an extensive analysis of this unique variant, suggests that the new infrastructure used for the malware is expected to change over time.

Dridex is one of the fastest evolving malware which has seen advanced features being incorporated in its structure at frequent intervals.

Worth noting

- The malware is customarily distributed through spam emails containing malicious Word documents. These documents make use of macros for downloading the trojan.
- The macro script uses an application whitelisted bypass technique to avoid mitigation done through Windows Script Host.
- If the macro is successfully executed, it connects to the ssl-pert[.]com to download server.exe, which is the Dridex installer.
- Samples analyzed by Duncan and eSentire contained malicious JavaScript code embedded in an XSL template. This script actually downloads and executes the Dridex installer.
- According to eSentire, only 16 antivirus solutions detected the new variant of Dridex.

Click **HERE** to read more.

‘Retro’ / ZipaMicro

US wants to isolate power grids with ‘retro’ technology to limit cyber-attacks

(by **Catalin Cimpanu** on **July 2, 2019**)

The US is very close to improving power grid security by mandating the use of “retro” (analog, manual) technologies on US power grids as a defensive measure against foreign cyberattacks that could bring down power distribution as a result.

The idea is to use “retro” technology to isolate the grid’s most important control systems, to limit the reach of a catastrophic outage.

“Specifically, it will examine ways to replace automated systems with low-tech redundancies, like manual procedures controlled by human operators,” said US Senators Angus King (I-Maine) and Jim Risch (R-Idaho), who introduced the bill on the Senate floor in 2016.

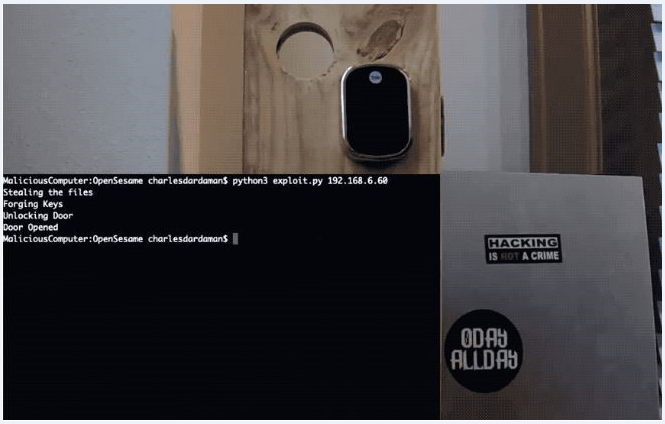
“This approach seeks to thwart even the most sophisticated cyber-adversaries who, if they are intent on accessing he grid, would have to actually physically touch the equipment, thereby making cyber-attacks much more difficult,” they said in a press releast last week, after the bill, named the Securing Energy Infrastucture Act (SEIA) passed the Senate floor.

The bill now needs approval from the US House of Representatives, where SEIA had been introduced as part of the National Defense Authorization Act for Fiscal Year 2020.

Click **HERE** to read more.

Security flaws in a popular smart home hub let hackers unlock front doors

(by **Zack Whittaker**)



When is a smart home not so smart? When it can be hacked.

That’s exactly what security researchers Chase Dardaman and Jason Wheeler did with one of the Zipato smart hubs. In new research published Tuesday and shared with TechCrunch, Dardaman and Wheeler found three security flaws which, when chained together, could be abused to open a front door with a smart lock.

Smart home technology has come under increasing scrutiny in the past year. Although convenient to some, security experts have long warned that adding an internet connection to a device increases the attack surface, making the devices less secure than their traditional counterparts. The smart home hubs that control a home’s smart devices, like water meters and even the front door lock, can be abused to allow landlords entry to a tenant’s home whenever they like.

In January, security expert Lesley Carhart wrote about her landlord’s decision to install smart locks—forcing her to look for a new home. Other renters and tenants have faced similar pressure from their landlords and even sued to retain the right to use a physical key.

Dardaman and Wheeler began looking into the ZipaMicro, a popular smart home hub developed by Croatian firm Zipato, some month’s ago, but only released their findings once the flaws had been fixed.

The researchers found they could extract the hub’s private SSH key for “root” - the user account with the highest level of access - from the memory card on the device. Anyone with the private key could access a device without needing a password, said Wheeler.

They later discovered that the private SSH key was hardcoded in every hub sold to customers - putting at risk every home with the same hub installed.

Click **HERE** to read more.

More News

Unprotected database belonging to MedicareSupplement.com exposed almost 5 million user records

https://cyware.com/news/unprotected-database-belonging-to-medicaresupplementcom-exposed-almost-5-million-user-records-5aec44db

Personalized medicine software vulnerability uncovered by Sandia researchers

https://phys.org/news/2019-07-personalized-medicine-software-vulnerability-uncovered.html

Hackers are repeatedly targeting Navy contractors

https://www.fifthdomain.com/industry/2019/06/27/hackers-are-repeatedly-targeting-navy-contractors/

HOW HACKERS TURN MICROSOFT EXCEL'S OWN FEATURES AGAINST IT

https://www.wired.com/story/microsoft-excel-hacking-power-query-macros/

Potent Firefox 0-day used to install undetected backdoors on Macs

https://arstechnica.com/information-technology/2019/06/potent-firefox-0day-used-to-install-undetected-backdoors-on-macs/

Trump officials weigh encryption crackdown

https://www.politico.com/story/2019/06/27/trump-officials-weigh-encryption-crackdown-1385306

Deconstructing Apple Card: A Hacker's Perspective

https://www.cisomag.com/deconstructing-apple-card-a-hackers-perspective/

Facebook Removes Accounts Used to Infect Thousands With Malware

https://threatpost.com/facebook-malware-laced-links/146149/

Breach at Cloud Solution Provider PCM Inc.

https://krebsonsecurity.com/2019/06/breach-at-cloud-solution-provider-pcm-inc/

Microsoft warns about Astaroth malware campaign

https://www.zdnet.com/article/microsoft-warns-about-astaroth-malware-campaign/

More than 1,000 Android apps harvest data even after you deny permissions

https://www.cnet.com/news/more-than-1000-android-apps-harvest-your-data-even-after-you-deny-permissions/

FBI, ICE find state driver's license photos are a gold mine for facial-recognition searches

https://www.stripes.com/news/us/fbi-ice-find-state-driver-s-license-photos-are-a-gold-mine-for-facial-recognition-searches-1.589314

More News

They Paid Nearly a Half Million in Ransom. Where's the Data?

https://www.news18.com/news/world/lake-city-they-paid-nearly-a-half-million-in-ransom-wheres-the-data-2220743.html

Windows 10 Hit Repeatedly By Serious New Vulnerability

https://www.forbes.com/sites/gordonkelly/2019/06/08/microsoft-windows-10-upgrade-update-security-problem-warning-cost-windows-10-home/#568e35bd6dd4

Microsoft Issues Warning For 50M Windows 10 Users

https://www.forbes.com/sites/gordonkelly/2019/07/06/microsoft-windows-10-upgrade-vpn-warning-upgrade-windows/#2bef338d53d5

UChicago and Google Sued in Federal Class Action Suit for Data Sharing

https://www.chicagomaroon.com/article/2019/6/27/uchicago-google-sued-federal-class-action-suit-dat/

U. of C. Medicine, Google hope to use patterns in patient records to predict health

http://www.chicagotribune.com/business/ct-google-university-chicago-partnership-0518-biz-20170517-story.html

What if All Your Slack Chats Were Leaked?

https://www.nytimes.com/2019/07/01/opinion/slack-chat-hackers-encryption.html

Google still keeps a list of everything you ever bought using Gmail, even if you delete all your emails

https://www.cnbc.com/2019/07/05/google-gmail-purchase-history-cant-be-deleted.html

British Airways fined $229 million under GDPR for data breach tied to Magecart

https://www.cyberscoop.com/british-airways-gdpr-fine-magecart/

Popular genetic-mapping software potentially exposed patients' data

https://www.cyberscoop.com/burrows-wheeler-aligner-genetic-mapping-sandia-patch/

A zombie game with 50,000 Play Store downloads was pulling sensitive data from Gmail

https://www.cyberscoop.com/scary-granny-zomby-android-credential-stealing-wandera/

A bug in Wi-Fi 'extenders' could give a hacker full control over the devices

https://www.cyberscoop.com/wi-fi-extenders-remote-code-ibm-xforce/

Reader Suggested Articles

Below are readers suggestions for this month. They are very interesting articles so hopefully you will find them as interesting as I did.

From Jeff Vogelpohl:

- https://www.geek.com/news/sound-of-keystrokes-reveals-passwords-560821/
- https://medium.com/@billatnapier/wi-fi-signals-can-reveal-your-password-bd5ac176410b
- https://www.youtube.com/watch?v=2OjzI9m7W10

From Deborah Wright:

- https://arstechnica.com/tech-policy/2019/06/minnesota-cop-awarded-585000-after-colleagues-snooped-on-her-dmv-data/
- https://threatpost.com/feds-hackers-mission-control-data-nasa-jpl/145842/

From Erich Neumann:

- https://www.securityweek.com/telcos-pwned-multi-wave-attacks-stealing-obscene-amount-data-providers
- https://www.engadget.com/2019/06/28/cell-phone-hack-is-ruining-lives-identity-theft/

From Stephen "Doc" Petty:

- https://thehackernews.com/2019/06/microsoft-onedrive-personal-vault.html
- https://cloud.cio.gov/strategy/
- https://www.cio.gov/assets/files/Application-Rationalization-Playbook.pdf

From Lane Helms:

- https://gizmodo.com/hacker-used-raspberry-pi-to-steal-sensitive-nasa-docs-1835802380

Podcast suggestion from Kayla Richardson:

- Darknet Diaries Podcast (or look for it in your favorite Podcast Aggregator)

Podcast are a great way to learn about new developments or concepts in any field. For Cybersecurity and other computer topics I would suggest looking into **Security Now from Steve Gibson**. That is what I listen to. You might also want to check out **Cyberwire**.

Cyber Challenge

Last Month's Challenge

Last month's challenge was to answer 6 questions saved as QR codess. The people who completed all six of the challenge are listed below

Steven Campbell @ 1022 on 12 June	David Evans @ 1122 on 12 June	Deborah Wright @ 1403 on 12 June
Erich Neumann @ 1543 on 12 June	Gabriel Huber @ 1411 on 13 June	Walker Pyle @ 1634 on 13 June
Rene Hess @ 1259 on 14 June		

The following people were able to complete 4 of the 6 challenges

Robin Lovelace @ 1545 on 12 June

Josef Lopez @ 1709 on 12 June

And Jeff Vogelpohl was able to complete 2 of the 6 challenges on 17 June. For those of you who were unable to complete the challenge, remember you can always email me for assistance.

Here are the questions and answers for last month's challenges:

1) We are a hacking group suspected of being backed by the GRU (Russian military intelligence agency) and are famous for interfering with European election results. We use spear phishing and zero-day vulnerabilities and mostly target web-based email services. Who are we? **Fancy Bear**

2) I am a company who designed a television ad in 2017 to intentionally set off Alexa, Google Homes and Android phones. The ad would play a Wikipedia entry for our product. What company am I? **Burger King**

3) I am a television series that started my 21st season by causing viewers' Alexa to add items to their shopping cart and set an alarm for 7 am. During the episode I also caused some peoples' Alexa to talk to their Google Home unit and setup a never-ending loop of profanity. What series am I? **South Park**

4) I am a victim of the first known successful cyberattack on a country's power grid. What country am I and when did the first attack occur? **Ukraine and 23 December 2015**

5) I am the country who is thought to have pulled off the first successful cyberattack on another country's critical infrastructure. What country am I? **I was looking for Russia in relation to the attack in question #4. However, it can be argued that Stuxnet in 2005 was the first successful cyberattack on a nations critical infrastructure. For those who don't know what Stuxnet was, I suggest you go to this link: https://en.wikipedia.org/wiki/Stuxnet**

6) My Latitude and Longitude is 30.328176, -97.723650. What is at this location? **I was looking for the DPS Museum but apparently due to proximity error inherent with GPS, not everyone got the same answer. So as long as you mentioned that it was a DPS building I accepted the answer.**

Cyber Challenge

For those of you who don't know what a QR code is, it is a machine-readable code consisting of an array of typically black and white squares. It is most often used for storing URLs or other information and can be read by a camera on a smartphone with a QR code reader program installed. However, as the challenge showed, it is possible to hide other information besides a URL. Because other than URLs can be stored in a QR code, it is possible for malware to infect your phone and have information stolen directly from it by scanning a QR code. All a malicious actor has to do is encode the malicious payload or web address into a QR code format, print the code on some adhesive paper and affix it over a legitimate QR code. Or the code can just be emailed to you. Since the QR encoding is not human readable, the victim who scans the code would have no idea they are scanning a malicious link until it is too late.

How do you protect yourself from a malicious QR code? Caution is the best way. I suggest you do not scan random QR codes. Phishing emails can easily include a QR code and since most email scanners do not read any emailed QR code the average user will assume the code is safe to scan. Be careful about scanning codes you find on buildings or anywhere someone might have placed a malicious code. Another way to protect yourself is to download a QR scanner that will inspect the scanned code and display it to you before going to the website or activating the code. Norton Snap is a QR code reader that is available for both iPhone and Android. After the QR code is scanned the program scans the content against a database of known malicious links prior to showing you the link. The program then lets you decide if you wish to visit the link or not. To read more about how a QR code can be weaponized, you can find more information in these links:

https://www.lifewire.com/how-to-protect-yourself-from-malicious-qr-codes-2487772

https://resources.infosecinstitute.com/security-attacks-via-malicious-qr-codes/#gref

https://www.welivesecurity.com/2018/03/28/scanning-qr-codes-ios-11s/

To read about other QR code readers similar to Norton Snap, click on this weblink:

https://www.topappslike.com/norton-snap-qr-code-reader/

Cyber Challenge

This Month's Challenge

This month's challenges are going to be a little more straight forward. Instead of encoding or hiding the questions, I'm going to provide them in plain English. I believe finding the answers to the questions might be challenging, but I think most readers might enjoy a break from the normal challenges I provide.

The intent of this challenge is to make you acquainted with some famous hackers and some of their exploits. Some of these people are still alive and working on interesting projects. I encourage you to find out more about these people as you are searching for their names. I have provided the pseudonym of all of the people so I am looking for the actual name of the person described. As normal, email me at **kirk.burns@dps.texas.gov** with your answers or if you need hints.

---

1) I am know as '**the homeless hacker**' because I used coffee shops, libraries and internet cafes as my base. Most of my activities involved breaking into computer networks and then reporting on their vulnerabilities to the companies that owned them. Who am I?

2) I am known as "**Mafiaboy**". When I was 15-years-old I discovered how to take over networks of university computers and used their combined resources to perform a Distributed Denial of Service (DDoS) attack on Dell, eBay, CNN and Amazon. Who am I?

3) At the age of 17 I hacked into the Petnagon's computer network known as ARPANET. Seven years later I hacked a radio station contest and ensured I was the 102nd caller. I won a brand new Porsche, a vacation, and $20,000. I used the Alias **Dark Dante**. Who am I?

4) I am best known as **Mudge**. I was the most prominent member of the hacking group L0pht and a longtime member of the hacking group the Cult of the Dead Cow. I was a pioneer in buffer overflow work and was the original author of the password cracking software L0phCrack. Who am I?

5) I am a virus writer from Belgium known for a long-standing dispute with the security firm Sophos because of a comment about the gender of virus writers made by Graham Cluley, a Sophos employee. I wrote the viruses Quis, Coconut and YahaSux (also known as Sahay). I also wrote the virus Sharp (also known as "Sharpei") which is credited as being the first virus written in C#. I'm best known as **Gigabyte**. Who am I?

Cyber Challenge

This Month's Challenge Continued

6) I am a German hacker who's death was ruled a suicide. However, peers of mine from the Chaos Computer Club and others believe I was murdered because my research and activities in the areas of Pay TV cracking and voice scrambling might have upset intelligence agencies and organized crime operations. I presented the first public implementation of a telephone with built-in voice encryption. I was known by the pseudonym '**Tron**'. Who am I?

7) I am an American Cyber Security Research and White Hat Hacker. I am a founding member of the hacker security think tank L0pht Heavy Industries and was one of the seven members who testified before the U.S. Senate committee on Governmental Affairs in 1999 about government and homeland computer security. I made the statement my group could "take down the internet within 30 minutes." I am known as **Space Rogue**. Who am I?

8) I am a hacker known as **MinorThreat** or **mthreat**. I am also a software developer and was the first employee and lead software architect for indeed.com. In 1995 I was sentenced to 70 months in the Federal Correctional Institute in Bastrop for money laundering and banned from the Internet; thus becoming the first person to be banned from the Internet even though I was not tried and did not plead guilty to any computer crimes. Who am I?

9) I am a hacker known as **geohot**. I developed limera1n, a jailbreak tool, and bootrom which allowed people to unlock iPhones to be used on other wireless carriers. This was contract to AT&T and Apple's intentions. I also reverse engineered the PlayStation 3 and was sued by Sony. I am currently working on my vehicle automation machine learning company comma.ai. Who am I?

10) I am a hacker known as **Sabu**. I am the co-founder of the hacking group LulzSec and was facing a 124 year prison sentence so I became an informant for the FBI. I spent over ten months helping the FBI identify and build cases against other hackers in LulzSec and other related groups. My help enabled the arrest of 5 other hackers associated with Anonymous, LulzSec and antisec. The FBI tried to use me to build a case against Tron, but they were unsuccessful. Who am I?

</Closing Comments>

Thank you for taking the time out of your day to read this newsletter. As always, I hope you found this month's newsletter informative, interesting, and useful. Remember, you can only defend against threats when you are knowledgeable about them. And protecting the Agency and yourself does not end when you leave work. I realize cybersecurity is not the most liked topic, but it is important to understand the dangers you and your family face when online and how your actions and the actions of others can affect the Agency and your personal life.

At the beginning of the newsletter I talked about sextortion phishing attempts. I ran out of room but thankfully I have room on the last page to continue educating you about sextortion emails.

As I said earlier, the people who send these types of phishing emails do so in the attempt to scare you into believing you have been recorded doing something you would not want made public and are willing to pay to keep it secret. While most businesses have been able to block these emails on their network, that has caused the bad guys to develop a new tactic. To bypass automated blocking of phishing emails, the bad guys have started to draft their messages and then save them as a picture. They then embed the picture in the email and send. Because email scanning technology cannot scan text in a picture, these emails cannot be blocked. By using a picture, phishers are able to get these emails past email filters and into the hands of people who they believe might be willing to pay the extortion.

So by now you might be asking what can you do to protect yourself from sextortion emails and/or other phishing emails? Unfortunately there isn't much you can do to prevent receiving these types of emails, especially to your personal email accounts. The best defense you have, as with anything cybersecurity related, is knowledge. If you are aware of a danger and are vigilant you can keep yourself safe. And as with all forms of phishing attempts, I suggest you do NOT click on any links or open any attachments. Doing so is only going to potentially expose you to malicious software and identity theft. For phishing emails received at DPS you should forward the original email to spam@dps.texas.gov. If you are a reader who does not work for DPS, I suggest you contact your cybersecurity or IT departments and notify them of the email. For phishing emails to your personal email, I suggest you just delete the email.

In closing I want to thank you for taking the time to read this newsletter. I hope you find it interesting and informative.

Kirk

As a reminder, feel free to share this and previous newsletters with friends and family. The better educated everyone is on cyber issues the safer everyone is. You can see previous issues of the newsletter at this public facing DPS website:

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

Again, I hope you enjoyed the newsletter and good luck with the Cyber Challenges. If you have suggestions on how the newsletter could be improved, please let me know.

And as always,

THANK YOU FOR YOUR CYBER VIGILANCE.