Vol. 4 | Issue 9

Cyber Security NEWS

September 2019

Page 2 | Page 3 | Page 4 | Page 5 | News | Challenge | Closing

Welcome to the TXDPS Cyber Newsletter

Hello everyone and welcome to this month's DPS Cybersecurity Newsletter. If you are a new reader, welcome. I hope you find the information provided relevant and useful. If you are a regular reader, thank you for continuing to read the newsletter and I encourage you to forward it on to anyone you know who needs some cyber education.

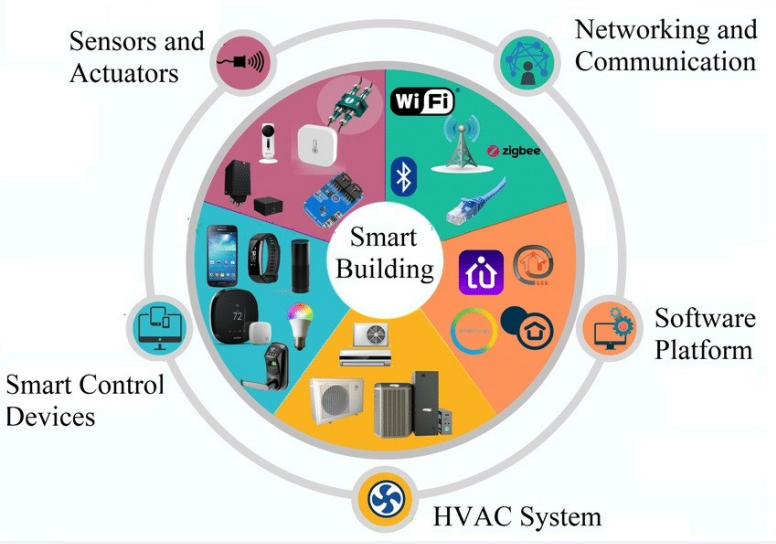
Before you read the articles I selected for this month's newsletter, I want to take a few minutes to talk about an article a reader sent me. Robert Merrifield sent an article about *How smart buildings are the latest threat vector for cyberattacks* by Macy Bayern on August 27, 2019. I have talked about and provided articles about similar things in previous newsletters. This article talks about how there is a rise in cyberattacks on smart buildings. This is because of the explosion of Internet of Things (IoT) devices, which are what make up smart buildings. Digitizing buildings is a major trend with everyone wanting to modernize and have the latest cool technology. But if security is not thought about during the devices creation, and often manufactures of these devices do not, then any network that device is connected to is in danger of being compromised. Here is the link to the article:

https://www.techrepublic.com/article/how-smart-buildings-are-the-latest-threat-vector-for-cyberattacks/

Here are some statistics about IoT devices that will probably shock you and should probably scare you.

- Every second there is approximately 127 devices connected to the Internet.
- There are expected to be more than 21 billion IoT devices by 2025.
- By 2020 it is believed that 90% of all automobiles will be connected to the Internet.
- Companies are expected to invest approximately $15 Trillion in IoT devices by 2025.

With this type of growth, is it any surprise cyber criminals are focusing their efforts on attacking IoT devices? Most manufacturers have said they are providing functionality but are not concerned with security. They believe that to be the concern of the end user and not their problem. However, as IoT devices are being regularly compromised, manufacturers have been forced to start to consider security in their products. There have been cases of ransomware attacks on IoT devices, IoT devices being compromised and used to attack networks, cars being hacked and controlled, trans-Atlantic/Pacific ships being hacked and controlled, possible assassinations via biomedical devices, etc.



As you read this month's newsletter I hope you will keep in mind how technology can improve our lives. But you should also keep in mind how technology can harm us. If we do not think about how the technology can be misused, someone else will. And it is very likely those people will have no qualms in stealing your identity, money, information, or even harming you.

Newb / Ransomware

Newb admits he ran Satori botnet that turned thousands of hacked devices into a 100Gbps+ DDoS-for-hire cannon

(by **Shawn Nichols** | **5 Sep 2019 @ 00:47**)

The script kiddie at the center of the Satori botnet case has pleaded guilty.

Kenneth Schuchman, 21, of Vancouver in Washington state, this week admitted to aiding and abetting computer hacking in an Alaskan federal district court. In exchange for only having to confess to a single criminal count, and increasing his chances of a reduced sentence, Schuchman admitted he ran the destructive Satori Internet-of-Things botnets.

From July 2017 to late 2018, Schuchman, along with co-conspirators referred to by prosecutors as "Vamp" and "Drake," built and maintained networks of hijacked devices: these internet-connected gadgets would be infected and controlled by the gang's Satori malware, which was derived from the leaked Mirai source code. Schuchman, who is said to have gone by the handle "Neus-Zeta," admitted to taking the lead in acquiring exploits to commandeer vulnerable machines and add to them the botnets, while "Drake" apparently wrote the code for the malware, and "Vamp" handled the money.

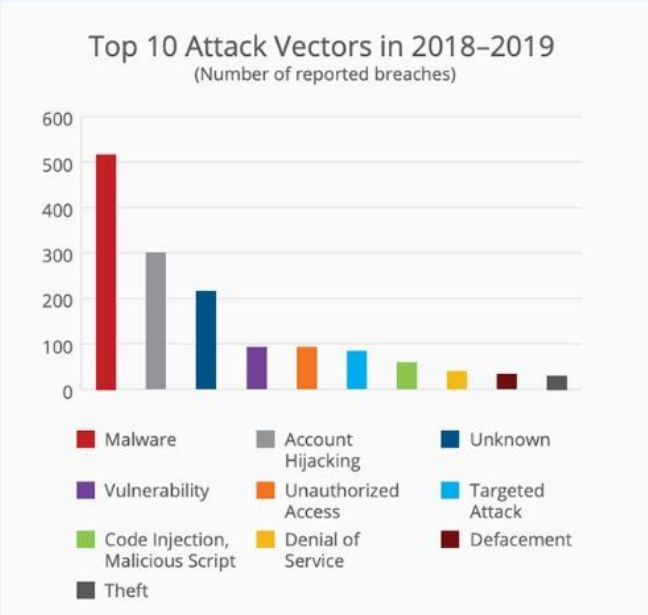
The money, you ask? Yes, the crew would launch distributed denial-of-service (DDoS) attacks from their armies of malware-infected gear for cash: you could hire them to smash your rivals and other victims offline by overwhelming systems with internet traffic from the Satori-controlled botnets.

"All three individuals and other currently uncharged co-conspirators took an active role in aiding and abetting the criminal development and deployment of DDoS botnets during this period for the purpose of hijacking victim devices and targeting victims with DDoS attacks," Schuchman's plea deal paperwork reads.

Click **HERE** to read the article.

New ransomware grows 118% as cybercriminals adopt fresh tactics and code innovations

(by **Help Net Security** | **August 29, 2019**)



McAfee Labs saw an average of 504 new threats per minute in Q1 2019, and a resurgence of ransomware along with changes in campaign execution and code. More than 2.2 billion stolen account credentials were made available on the cybercriminal underground over the course of the quarter. Sixty-eight percent of targeted attacks utilized spear-phishing for initial access, 77% relied upon user actions for campaign execution.

"The impact of these threats is very real," said Raj Samani, McAfee fellow and chief scientist. "It's important to recognize that the numbers, highlighting increases or decreases of certain types of attacks, only tell a fraction of the story. Every infection is another business dealing with outages, or a consumer facing major fraud. We must not forget for every cyberattack, there is a human cost."

Ransomware resurgence features new campaign tactics

McAfee Advanced Threat Research (ATR) observed innovations in ransomware campaigns, with shifts in initial access vectors, campaign management and technical innovations in the code.

While spear phishing remained popular, ransomware attacks increasingly targeted exposed remote access points, such as Remote Desktop Protocol (RDP); these credentials can be cracked through a brute-force attack or bought on the cybercriminal underground. RDP credentials can be used to gain admin privileges, granting full rights to distribute and execute malware on corporate networks.

Click **HERE** to read the article.

Data Breaches / DOE

Cost of data breaches to surpass $5 trillion in 2024

(by **Help Net Security** | **August 28, 2019**)

A new report from Juniper Research found that the cost of data breaches will rise from $3 trillion each year to over $5 trillion in 2024, an average annual growth of 11%.

This will primarily be driven by increasing fines for data breaches as regulation tightens, as well as a greater proportion of business lost as enterprises become more dependent on the digital realm.

The research noted that while the cost per breach will steadily rise in the future, the levels of data disclosed will make headlines but not impact breach costs directly, as most fines and lost business are not directly related to breach sizes.

Cybercrime is increasingly sophisticated; the report anticipates that cybercriminals will use AI which will learn the behavior of security systems in a similar way to how cybersecurity firms currently employ the technology to detect abnormal behavior.

Click **HERE** to read more.

'Cyber event' disrupted U.S. grid networks—DOE

(by **Blake Sobczak** | **April 30, 2019**)

A "cyber event" interrupted grid operations in parts of the western United States last month, according to a cryptic report posted by the Department of Energy.

The March 5 incident lasted from 9 a.m. until nearly 7 p.m. but didn't lead to a power outage, based on a brief summary of the electric disturbance report filed by the victim utility.

If remote hackers interfered with grid networks in California, Utah and Wyoming, as the DOE filing suggests, the event would be unprecedented. A cyberattack is not known to have ever disrupted the flow of electricity anywhere in the United States, though Russian hackers briefly cut off power to parts of Ukraine in 2015 and again in 2016.

DOE uses a broad definition of "cyber event," describing it as any disruption to an electrical system or grid communication network "caused by unauthorized access" to hardware, software or data. That leaves open the possibility that a utility employee or trespasser, rather than a remote hacker, triggered the March 5 event.

In January 2018, for instance, Michigan utility Consumers Energy filed the same type of DOE notice when an employee in training accidentally caused a blackout for about 15,000 people (Energywire, March 8, 2018).

"There was no malicious intent" in that case, a spokeswoman said at the time, and Consumers Energy brought the lights back on within a few hours.

U.S. utilities are required to notify DOE within one hour of any successful cyberattack on their systems. Power companies that fail to file an OE-417 electric disturbance report can be fined up to $2,500 per day, although DOE has never issued civil or criminal penalties related to the form. The document is supposed to include a high-level overview of the incident, whether it be a hurricane-related outage or a physical attack on the facility. A second, more closely guarded portion of the form contains a detailed summary of actions taken to resolve the incident and "preliminary results from any investigations," per DOE guidelines.

Click **HERE** to read more.

XKCD / YouTube

XKCD forum breach exposes details from over 560,000 user accounts

(by **Amrita Khalid | 09.03.19)**

Hackers breached the forum of the popular webcomic.

XKCD, the sarcastic webcomic revered by science and tech geeks, is now the butt of someone else's joke. Hackers breached the forum of the 14-year old site, stealing over 560,000 usernames, emails, IP addresses and hashed passwords. Security researcher Troy Hunt, who owns the data breach website Have I Been Pwned, alerted the site's administrators over the weekend. Hunt was originally tipped off about the breach by white hat hacker Adam Davies.

XKCD promptly took down its forum, and posted a short message warning users to change their passwords -- as well as any similar passwords for other accounts. "The xkcd forums are currently offline. We've been alerted that portions of the PHPBB user table from our forums showed up in a leaked data collection. The data includes usernames, email addresses, salted, hashed passwords, and in some cases an IP address from the time of registration. We've taken the forums offline until we can go over them and make sure they're secure. If you're an echochamber.me/xkcd forums user, you should immediately change your password for any other accounts on which you used the same or similar password," wrote XKCD.

Click **HERE** to read more.

YouTube promised to halt comments on kids videos already. It hasn't

(by **Joan E. Solsman | September 9, 2019 5:00 AM PDT**)

A pedophilia scandal compelled YouTube to vow to suspend comments on videos with kids age 13 and younger. Six months later, comments are still easy to find.

YouTube is about to reposition how its massive online video service treats clips for children. Following a record $170 million penalty, announced Wednesday, for violating kids' data privacy, Google's YouTube pledged to disable comments, notifications and personalized ads on all videos directed to children. And its machine learning will police YouTube's sprawling catalog to keep kids videos in line, the company said.

One problem: YouTube's machine learning was supposed to be suspending comments on videos featuring young minors already. It hasn't.

Comment-enabled videos prominently depicting young kids are still easy to find on YouTube. A single YouTube search for one kids-focused subject -- "pretend play" -- returned more than 100 videos with comments enabled, all prominently featuring infants, preschoolers and other children young enough to still have their baby teeth.

After CNET contacted YouTube with a list of these videos, comments were disabled on nearly half of them.

"We invest significantly in the teams and technologies that allow us to provide minors and families the best protection possible," YouTube spokeswoman Ivy Choi said. "We've suspended comments on hundreds of millions of videos featuring minors in risky situations and implemented a classifier that helps us remove two times the number of violative comments. We continue to disable comments on hundreds of thousands of videos a day and improve our classifiers."

YouTube is the world's biggest online video source, with 2 billion monthly users -- so big, in fact, it's the world's top source for kids videos too. Kids content is one of its most-watched categories, but YouTube has come under fire for a range of scandals involving children. That $170 million penalty addressed the data YouTube collects on kids without parents' consent. But YouTube has also faced scandals involving videos of child abuse and exploitation and nightmarish content in its YouTube Kids app, pitched as a kid-safe zone.

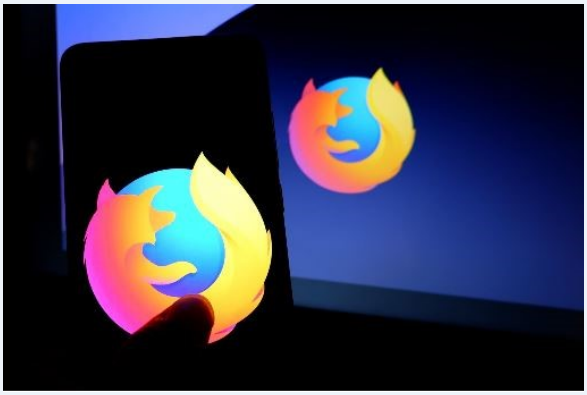
Click **HERE** to read more.

Firefox / Biohackers

Firefox will encrypt web domain name requests by default

(by **Jon Fingas** | **09.07.19**)

You can expect to see DNS over HTTPS by the end of September.



Mozilla's Firefox privacy protections will soon include one of the most basic tasks for any web browser: fielding the domain name requests that help you visit websites. The developer will make DNS over encrypted HTTPS the default for the US starting in late September, locking down more of your web browsing without requiring an explicit toggle like before. Your online habits should be that much more private and secure, with fewer chances for DNS hijacking and activity monitoring.

Not every request will use HTTPS. Mozilla is relying on a "fallback" method that will revert to your operating system's default DNS if ther's either a specific need for them (such as some parental controls and enterprise configurations) or an outright lookup failure. This should respect the choices of users and IT managers who need the feature turned off, Mozilla said. The team is watching out for potential abuses, though, and will "revisit" its approach if attackers use a canary domain to disable the technology.

Click **HERE** to read more.

Biohackers chase Johnny Mnemonic with 'Pegleg' implanted hard drive

(by **Seth Rosenblatt** | **August 12, 2019**)

In a small house nestled among the oak trees here, a four-hour drive west of the Black Hat and DefCon cybersecurity and hacker conferences taking place in Las Vegas and high enough into the hills above town that Google Maps can't accurately find it, biohackers took one small but important step toward the science fiction dystopia depicted in William Gibson's *Johnny Mnemonic*.

Biohackers immediately after implanting Michael Laufer's Pegleg networked drive in his upper right thigh: Jeff Tibbetts, Zack Shannon, Nick Titus, and seated, Laufer. *Photo by Seth Rosenblatt/The Parallax*.

In that 1981 short story (and in a critically panned 1995 Keanu Reeves blockbuster of the same name), Gibson imagines a near future in which technology has developed to the point where humans can erase their memories and replace them with data and files that they can't access themselves. In a futuristic, dirty, cluttered world plagues by Yakuza mobsters, people are paid to use their bodies to courier information.

The Four Thieves Vinegar biohacking collective has not figured out how to precisely mimic the memory data transfer scenario Gibson conjured, but it has built a device to enable people to store and transfer data wirelessly in their bodies.

Using off-the-shelf parts and focused efforts, the biohacking group has designed and built a networked hard drive, coated in a biosafe resin, to be subcutaneously implanted in the human body. It's powered by an external battery that connects to the device via an induction coil, and its storage capacity is limited only by the size of the microSD card it contains. Michael Laufer, who founded Four Thieves Vinegar, calls it the Pegleg.

In the small hours of August 8, in an operating room within the small house, two patients received the second version of the Pegleg implant, which Laufer says is the world's first subcutaneous networked drive.

Click **HERE** to read more.

More News

Supermicro server boards can be remotely hijacked

https://www.theregister.co.uk/2019/09/03/supermicro_server_flaw/

Soldiers may 'wear' unhackable computers into combat

https://www.foxnews.com/tech/soldiers-may-wear-unhackable-computers-into-combat

The Dangers in Smart Cities

https://www.nextgov.com/ideas/2019/09/dangers-smart-cities/159617/

Microsoft, Hewlett Foundation preparing to launch nonprofit that calls out cyberattacks

https://www.cyberscoop.com/microsoft-cyber-peace-institute-hewlitt-foundation-brad-smith/

Cyber Command's biggest VirusTotal upload looks to expose North Korean-linked malware

https://www.cyberscoop.com/cyber-command-virus-total-north-korean-malware/

Symantec finds that a 'new' Chinese hacking group has actually been around for a decade

https://www.cyberscoop.com/thrip-lotus-blossom-symantec-china/

'Indiscriminate' iOS hacking was relatively limited, Apple says. Try telling that to the Uighur population

https://www.cyberscoop.com/apple-indiscriminate-hacking-ios-uighur/

Apple's $1 million bug bounty makes a lot more sense after that iOS hacking spree

https://www.cyberscoop.com/ios-bug-bounty-apple-hack-china-zerodium/

As NSA expands election security task force, Director Paul Nakasone talks lessons learned

https://www.cyberscoop.com/us-election-security-2020-nsa/

Accused Capital One hacker pleads not guilty to all charges

https://www.cyberscoop.com/capital-one-hacker-not-guilty-paige-thompson/

Good news Flash lovers! Microsoft won't be disabling it by default (so long as you use IE or old Edge)

https://www.theregister.co.uk/2019/09/03/microsoft_flash/

Major Security Flaw Found in Google Chrome, Patch Must Be Installed ASAP

https://news.softpedia.com/news/major-security-flaw-found-in-google-chrome-patch-must-be-installed-asap-527229.shtml

More News

Hackers are actively trying to steal passwords from two widely used VPNs

https://arstechnica.com/information-technology/2019/08/hackers-are-actively-trying-to-steal-passwords-from-two-widely-used-vpns/

Mysterious iOS Attack Changes Everything We Know About iPhone Hacking

https://www.wired.com/story/ios-attack-watering-hole-project-zero/

The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks

https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks

How to See if Police Are Using Ring Doorbells to Monitor Your Neighborhood

https://lifehacker.com/how-to-see-if-police-are-using-ring-doorbells-to-monito-1837797394

Apple apoligises for allowing workers to listen to Siri recordings

https://www.theguardian.com/technology/2019/aug/29/apple-apologises-listen-siri-recordings

Twitter disables SMS-to-tweet feature after its CEO got hacked last week

https://www.zdnet.com/article/twitter-disables-sms-to-tweet-feature-after-its-ceo-got-hacked-last-week/

$5.3M Ransomware Demand: Massachusetts City Says No Thanks

https://threatpost.com/ransomware-demand-massachusetts-city-no-thanks/148034/

NSA Cyber Chief Wants to Share Digital Threats Early and Often

https://www.nextgov.com/cybersecurity/2019/09/nsa-cyber-chief-wants-share-digital-threats-early-and-often/159673/

This Site Shows the Security Risks of Your Smart Devices

https://www.nextgov.com/cybersecurity/2019/09/site-shows-security-risks-your-smart-devices/159655/

Author of multiple IoT botnets pleads guilty

https://www.zdnet.com/article/author-of-multiple-iot-botnets-pleads-guilty/

National Guard looks to help states help with ransomware response

https://fcw.com/articles/2019/08/28/national-guard-states-cyber.aspx?admgarea=TC_Security

Google is working on a fix for malicious Calendar spam

https://www.engadget.com/2019/09/03/google-calendar-fix-malicious-spam/

Cyber Challenge

Last Month's Challenge

Congratulations to everyone who everyone who was able to solve last month's challenges. I provided six questions which I thought were interesting and were intended to educate while being fun to solve. Three of the questions were in the form of a picture that you had to decode what was shown to get the question. The pictures are what is known as Baudot. Baudot code, or International Teleprinter Code, was invented by Emile Baudot in 1870. It is a binary code which uses crosses and dots. It was used for teleprinter messages instead of the morse code system.

For those who were stumped and couldn't solve the picture challenges, I encourage you to go back and try them again. You can use these websites to understand how Baudot codes are created and then figure out how to decode the pictures I provided:

https://v2.cryptii.com/select/ita2

https://cs.stanford.edu/people/eroberts/courses/soco/projects/2008-09/colossus/baudot.html

https://codegolf.stackexchange.com/questions/94056/telegraphy-golf-decode-baudot-code

If these websites don't help, remember that when looking for information Google is your friend. There are several other sites that might help you understand the code.

Before I provide you with the questions and answers from last month's challenges, I first want to acknowledge and congratulate those readers who emailed me with their answers. I'm sure there are more who completed but didn't email me their answers. If you fall into that category, please email me your answers so I can acknowledge you in the next month's newsletter. If you would rather not have your name listed, just let me know in your email that you do not want your name published. I will keep it anonymous and only you and I will know. :)

Here are the people who emailed me their answers for the challenges:

	Completed all 6 Challenges	
Rene Hess @ 0204 on 14 Aug	Erich Neumann @ 1010 on 14 Aug	Faye Krueger @ 1011 on 14 Aug
Jordan Hancock @ 1240 on 14 Aug	David Evans @ 1300 on 14 Aug	Jim Bussell @ 2045 on 14 Aug
Rebekah Lloyd @ 1101 on 19 Aug	Jacqueline Halsted @ 0958 on 28 Aug	Jaysen Gonzales @ 1636 on 28 Aug
	Completed 3 of the 6 Challenges	
Amanda Dunn @ 1149 on 13 Aug	Joanna Morgan @ 1240 on 14 Aug	Lynni Ward @ 0808 on 15 Aug
	Completed 2 of the 6 Challenges	
Anne Kirsch @ 1007 on 14 Aug		

The challenges are not limited to only those here at TXDPS. This newsletter has a very wide readership and readers are always forwarding to others people around the United States. Any reader who wishes to try the challenges are welcome. And if you are not a DPS employee and wish to be put on the newsletter direct mailing list, please email me and let me know.

Cyber Challenge

Last Month's Challenge Answers

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

1) While not what would be considered a computer by today's standards, I was designed between 1847 and 1849 but was not built till 1991 when the London Science Museum built me. I am driven by a crank handle and contain cogs, gears and levers. I accurately calculated and printed tables of polynomials that were used for astronomy and ballistics. What am I?

ANSWER: Babbage's Difference Engine

2) In 1971 I made history by creating a program that is widely accepted as the first ever computer WORM. The worm bounced between computers and was not malicious. The worm displayed "I'm the creeper: catch me if you can." on affected computers. Who am I?

ANSWER: Bob Thomas

3) In 2002, President George W. Bush filed a bill to create this department. The department took on the responsibilities for IT infrastructure and eventually created a division specifically for cybersecurity. What is the Department?

ANSWER: Department of Homeland Security

4) I am the Creeper worm and infected a type of computer on the ARPANET in 1971. What is the type of computer I infected?

ANSWER: DEC PDP-10

5) I was the first completely electronic computer created by Tommy Flowers and his team at the Post Office Research Station in 1944. What was my name?

ANSWER: Colossus

6) I am a computer that was completed in 1946. I had 17,468 valves, 7,200 diodes, 1,500 relays, 70,000 resistors, and 10,000 capacitors all held together by about five million hand-soldered joints. I weighed 27 tonnes, measured 2.6m x 0.9m x 26m and consumed 150kW of electricity. What was my name?

ANSWER: Eniac

Cyber Challenge

This Month's Challenge

This month I decided to be straightforward with the challenges. Below are 10 questions that the answers are cybersecurity terms. Make sure and email me your answers so I can recognize your cybersecurity knowledge in next month's newsletter. If you get stuck on a question, email me and ask for hints. Good luck with the questions.

1. I am a bundle of programs that is designed to bombard users with advertisements. The main aim behind it is to redirect the user's search requests to advertising websites and collect marketing data. What am I?
2. I am a specific type of malware designed to infect several Internet connected devices such as PCs, mobiles, servers and IoT devices. I am often referred to as a small robot. What type of malware am I?
3. While I am a vast network of websites and portals that are not categorized by search engines, I am a smaller section where lots of illegal activities occur. What am I?
4. I am a non-malicious surprise embedded in a program or media which is entertaining and accessible to anyone. I am often found in video games and even in movies. I am an intentional joke intended to be amusing to everyone who finds me. What am I?
5. I am a fraudulent Wi-Fi hotspot or access point that appears to be legitimate but is setup to eavesdrop on wireless communications. I am the wireless equivalent of a phishing scam. What am I?
6. I am the measure of difficulty an attacker has to guess in order to crack the average password using a system. The lower I am the easier it is to guess a password. The higher I am the more difficult it is to guess a password. What am I?
7. I am a thing that is designed to record everything you do on your computer, phone, tablet, etc. I record every interaction and can either send that data on my own to a remote location or wait to have it requested. I can be either software or hardware. What am I?
8. I am a sort of Phishing which has become a major threat to all e-commerce websites. I redirect a user to a fake site which appears to be a genuine one. A user enters all their credentials into the duplicate site considering it to be a legitimate site. What type of Phishing attempt am I?
9. I am a term used to describe a new hacker/cracker. I do not have enough knowledge or skill to write my own exploits and often have to idea how the exploit works. I use scripts developed by other hackers to cause the mischief I create. I am called what?
10. I am an industry best practice and the best protection an organization has to recover from ransomware. Ransomware can happen no matter how vigilant an organization is. However, if I have been done and tested, an organization is often able to recover very quickly with little to no cost to the organization. What am I?

</Closing Comments>

As always, thank you for taking the time to read the newsletter. I 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. I hope you have enjoyed reading this newsletter and it has given you things to think about. Personally I found the Bio-hackers one of the most interesting articles. Feel free to email me and let me know what your favorite article was.

To close out the newsletter I want to make sure that all TXDPS employees are aware of some changes in the Cyber-security department. Recently we underwent a reorganization in our Risk team which we believe will be beneficial to the Agency. Previously our Risk team was somewhat siloed. We had two people who performed all risk assess-ments for the agency, two people who managed the Agency Security Plan, one person who did all the technical writing and one person (me) who was responsible for all cyber awareness training. While this structure worked, it was not the most user friendly for the various Agency departments. With the reorganization each department now has a direct representative in cybersecurity. This should provide cybersecurity a greater understanding of each divi-sions needs as well as provide a central point of contact departments can reach out to with questions. If you have questions about the reorganization you can email me, Miguel Scott or Jeremy Wilson and one of us will be happy to answer your questions. Below are the Cybersecurity Risk employees along with the divisions they are responsible for:

Miguel Scott / Risk and Vulnerability Manager			
Risk Team	**Divisions Responsible For**	**Risk Team**	**Divisions Responsible For**
Noemi Nieto	DLD/CAO	Diep Phan	LES/OIG
Kirk Burns	THP/AOD/HSC/IOD/EPB	Ean Meacham	ICT/OGC/RGR
Lane Helms	CID/RSD/ETR	Rebecca Maguire	ITD/FIN/HR

Again, thank you for taking the time to read the newsletter. Please pass it on to others you know so we can spread the knowledge.

Kirk

The better educated everyone is on cyber issues the safer everyone is. You can see previous issues of the newsletter at this public facing TXDPS 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.