NEWS
Cyber Security
Vol. 4 | Issue 1
January 2019

Welcome to the New Year and this month's TXDPS Cyber Newsletter.

Hello everyone and welcome to 2019. I hope everyone had a safe and enjoyable break over the Christmas and New Years time.

Unfortunately, starting with the beginning of the holiday season through the new year, there is always an increase in scams. This year is no exception. Recently DPS reported a new scam our Operations team found on December 11th. The information was posted on our CyberOps Twitter account and our CISO was interviewed about it by a local news agency. You can read about the scam and see the news video at this **LINK**.

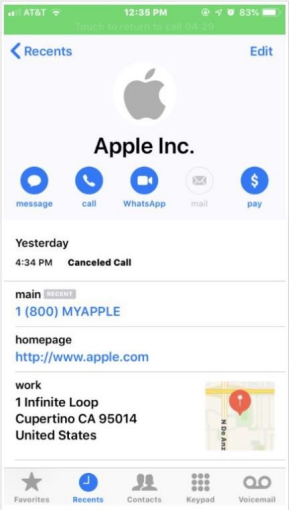
In this month's newsletter I have included several articles I feel are especially important for people to know. But to start I want to talk about a recent new **Apple Support Scam** that is going on.

While customer support scams are not new, there is a new one circulating that is successfully tricking people. KrebsonSecurity recently reported a new voice phishing (vishing) scam targeting Apple users. The scam is very sophisticated and to the average person would seem legitimate. The user receives an automated call warning of a data breach affecting Apple and the compromise of several Apple IDs. The message ends by asking the user to call 866.277.7794 to find out if their information was compromised. To add legitimacy to the scam, the call is spoofed to look like it is coming from Apple. The call displays Apple's phone number, street address and even the Apple logo (see picture below). If you were to call the number, the scam seems even more legitimate because you get an automated answering system saying your estimated wait time is about one minute thirty seconds. After about a minute wait the phone is answered and the person on the other end inquires as to the reason for your call. However, if you contact Apple through their customer support website they will verify they did not contact you.

While this scam specifically targets Apple users, that does not mean the same thing hasn't happened to Android users. There have also been scams claiming to be from service providers. It is always a good idea to be wary of phone calls from unknown numbers or those that want you to call back. Scammers are getting smarter and searching for ways to appear legitimate. A good way to identify if you are being scammed is if you are told you have to pay for their assistance. Most companies offer support for free so being requested to pay for assistance you were contacted about is normally a good indication of a scam. However, if you are unsure if the call is legitimate, look up the phone number from the company's website and call them. Or if they claim to be from your service provider, stop by a store and talk to them directly.

To find out more about this scam, click **HERE**. To read about ways to identify and avoid tech support scams, click **HERE**.

If you feel you have been a victim of this or another scam, immediately change your passwords and contact the company to let them know. They can assist you in any additional steps you should take to protect your data and safety.



Apple spoofed call looks legitimate with Apple's phone number, street address and Web address

Mac / Ransomware

A Dozen Flaws in Popular Mac Clean-Up Software Allow Local Root Access

(by **Tara Seals** | Published **January 3, 2019**)

All of the vulnerabilities arise from improper input validations.

A passel of privilege-escalation vulnerabilities in MacPaw's CleanMyMac X software would allow a local attacker to gain root access to an Apple machine in various ways.

CleanMyMac X is a cleanup application for MacOS that optimizes the drives and frees up space by scanning for unused, redundant or unnecessary files and deleting them. No fewer than a dozen flaws plague 4.0 earlier versions of the software, all of them in the package's "helper protocol."

"The application is able to scan the system and user directories, looking for unused and leftover files and applications," explained Cisco in the advisory, issued Wednesday. "The application also markets the ability to help detect and prevent viruses and malware on OS X. The software utilizes a privilege helper tool running as root to get this work done faster. This allows the application to remove and modify system files."

Click **HERE** to read the article.

Cloud Hosting Provider DataResolution.net Battling Chritmas Eve Ransomware Attack

(**KerbsonSecurity** | **2 Jan 19**)

Cloud hosting provider **Dataresolution.net** is struggling to bring its systems back online after suffering a ransomware infestation on Christmas Eve, KrebsOnSecurity has learned. The company says its systems were hit by the **Ryuk** ransomware, the same malware strain that crippled printing and delivery operations for multiple major U.S. newspapers over the weekend.

San Juan Capistrano, Calif. based **Data Resolution LLC** serves some 30,000 businesses worldwide, offering software hosting, business continuity systems, cloud computing and data center services.

The company has not yet responded to requests for comment. But according to a status update shared by Data Resolution with affected customers on Dec. 29, 2018, the attackers broke in through a compromised login account on Christmas Eve and quickly began infecting servers with the Ryuk ransomware strain.

The intrusion gave the attackers control of Data Resolution's data center domain, briefly locking the company out of its own systems. The update sent to customers states that Data Resolution shut down its network to halt the spread of the infection and to work through the process of cleaning and restoring infected systems.

Data Resolution is assuring customers that there is no indication any data was stolen, and that the purpose of the attack was to extract payment from the company in exchange for a digital key that could be used to quickly unlock access to servers seized by the ransomware.

The Ryuk ransomware strain was first detailed in an August 2018 report by security firm **CheckPoint**, which says the malware may be tied to a sophisticated North Korean hacking team known as the Lazarus Group.

Click **HERE** to read the article.

CenturyLink / Alexa

US investigating CenturyLink internet outage, 911 failures

(by **Keith Ridler** | **December 28, 2018**)

U.S. officials and at least one state said Friday that they have started investigations into a nationwide CenturyLink internet outage that has disrupted 911 service.

Federal Communications Commission Chairman Ajit Pai called the outage that began Thursday "completely unacceptable" because people who need help couldn't use the emergency number. "Its breadth and duration are particularly troubling," he said.

The commission's Public Safety and Homeland Security Bureau will investigate the cause and effect of the outage, he said.

The Monroe, Louisiana-based telecommunications giant is one of the largest in the United States. It offers communications and information technology services in dozens of states. Customers from New York to California reported outages.

CenturyLink spokeswoman Debra Peterson said the outage "is not related to hacking," but she declined further comment.

The company said on Twitter that it's working to restore service and appears to be making progress. It hasn't provided a cause for the problems.

"Where CenturyLink is the 911 service provider 911 calls are completing," the company said in a tweet.

Click **HERE** to read more.

Beware: There's a fake Amazon Alexa 'Setup' app climbing App Store charts

(by **Alex Allegro** | **Dec 27th 2018**)

There's an app currently circulating around Apple's App Store pretending to be the official set-up companion for Amazon's Alexa, and it's fooled its way to the top of the download charts. At the time of this writing, the fake app sits at #60 overall in the general "Top Free" apps section, while in an even more concerning top 10 place under the *Utilities* sections at #6.

While a handful of Reddit users have reported the app, no action has been taken from either Apple or Amazon so far.
Though the app doesn't hit you with an instant advertisement upon launch or prompt you to sign-in to Amazon, it does ask you to supply your IP address alongside the device serial number and a 'name'.
Generally, it's rather surprising to see a scam app make it past the iOS App Store review process, let alone rise so high up the charts. More than likely, the app saw success after an influx of post-Christmas Alexa owners searched the store with a query along the lines of "setup Amazon Alexa", ultimately leading it atop the charts.

The app comes way of "One World Software", who have two other questionable apps on the store as well — "Marketplace – Buy/Sell", with nearly identical colors to Facebook, and "Any Font for Instagram" for $0.99.

This isn't the first time this year we've seen a scam app fool the App Store. In September, we reported on how the the number 1 utility on the Mac App Store stole users browser history, sending it to an unknown Chinese server.

Click **HERE** to read .

IoT / Auto

IoT Report: Major Flaws in Guardzilla Cameras Allow Remote Hijack of the Security Device

(Bitddfender)

Vulnerabilities in indoor security camera allows remote compromise and device takeover

The commodification of IoT devices has paved the way to the smart home. Interconnected appliances, intelligent assistants and smart home surveillance are just some applications of the Internet of Things and customers love it.

The large number of intelligent, remotely controllable devices has opened the door not only to new opportunities. They have also unlocked new opportunities for cyber-criminals to establish a foothold into the customers' smart homes.

As a global cybersecurity solutions provider in the IoT space, Bitdefender does extensive research into vulnerabilities that affect intelligent devices and releases reports to help both customers understand risks in the connected home, as wel as drive security awareness in the vendor space.

Our latest research focuses on the Guardzilla Indoor Security Camera, an extremely affordable and popular surveillance device whose primary focus is providing physical security against break-in. While the feature set is highly appreciated by its users, the security implementation features several vulnerabilities that can be remotely exploited by ill-intended parties. We have identified several vulnerabilities that can be leveraged to totally compromise the camera, which results in a severe privacy impact on the user side.

Click **HERE** to read more.

Cyber Hacks Could Cost Auto Industry $24 Billion

(by **Security Magazine | December 17, 2018**)

Cyber hacks might cost the auto industry $24 billion within five years, according a study by Upstream Security.

The Upstream Security Global Automotive Cybersecurity Report 2019 outlines how hackers attacked -- from physical to long-range to wireless and more - - and who they targeted in the Smart Mobility space.

"With every new service or connected entity, a new attack vector is born," said Oded Yarkoni, Head of Marketing at Upstream Security. "These attacks can be triggered from anywhere placing both drivers and passengers at risk. Issues range from safety critical vehicle systems, to data center hacks on back-end servers, to identify theft in car sharing, and even privacy issues. The risk is immense. Just one cyber-hack can cost an automaker $1.1 billion, while we are seeing that the cost for the industry as a whole could reach $24 billion by 2023."

According to the report, the automotive world is becoming a Smart Mobility ecosystem, according to Yarkoni. Connected cars, autonomous vehicles, ride-sharing services and aggregated transport of all kinds are adding complexity and risk at an incredible rate. This report is the first of its kind; based on real-life incidents and provides an insight into who is at risk, how key stakeholders are protecting themselves and emerging trends for 2019.

Click **HERE** to read more.

Amazon/Baby Monitor

Amazon Sends 1,700 Alexa Voice Recordings to a Random Person

(by **Tara Seals** | December 20, 2018)

Amazon inadvertently sent 1,700 audio files containing recordings of Alexa interactions by a customer to a random person – and after a newspaper investigation exposed the snafu, characterized it as a "mishap" that came down to one employee's mistake.

In August, an Amazon customer in Germany (going by the alias "Martin Schneider" for purposes of the report) made use of his rights under the recently passed EU General Data Protection Regulation (GDPR) to ask for copies of the personal data Amazon has on file about him.

Amazon complied, sending Schneider a 100MB ZIP file which, among other things, contained about 1,700 Alexa audio files along with transcripts of Alexa voice commands. There was just one problem – Schneider doesn't use Alexa. After listening to a few of the files, they were clearly of someone else speaking, so he concluded that Amazon sent him the data in error. But Amazon didn't respond to his efforts to contact them about the problem, he said, so he contacted Heise Media's c't publication in mid-November.

The shocking part of the story is how quickly the investigative reporters were able to identify the victim. From the recordings, which cover the entire month of May 2018, they were able to determine that he has a Fire TV and an Echo box, and that he uses Alexa to control a smart home thermostat as well as his phone. A female voice speaking to Alexa indicates that he has also a female companion. They were also able to hear the man in the shower while he was issuing certain commands. There were also alarms, Spotify commands, public transport and weather inquiries.

Click **HERE** to read more.

Family on edge after man hacks Nest baby monitor, threatens to kidnap their son

(by **Kerry Justich** | December 20, 2018)

A couple in Houston thought they were taking measures to keep their family safe when they installed Wi-Fi-enabled Nest baby monitors in their home to watch over their 4-month-old son. But when an unrecognizable voice came through the system's speakers on Monday, they quickly took action to disconnect the system and the wireless network it was connected to.

According to a report from NBC affiliate KPRC in Houston, Ellen and Nathan Rigney were awoken by a beeping sound coming from the monitor and thought that it was an alarm notifying them of the presence of CO2. Suddenly, however, they heard "sexual expletives" that sounded like they were coming from their son Topper's room.

"Immediate reaction was that there's somebody in here, somebody's in my son's room! How did they get in there?!" Ellen told the station.
But things escalated when Nathan turned their bedroom light on and their own Nest camera suddenly turned on, followed by a man's voice ordering the parents to turn their light back off.

"Then [he] said, 'I'm going to kidnap your baby, I'm in your baby's room,'" Ellen continued.

Click **HERE** to read more.

More News

Iranian hackers targeted personal email accounts of US Treasury officials: report

https://thehill.com/policy/cybersecurity/421184-iranian-hackers-targeted-personal-email-accounts-of-us-treasury

The Equifax Breach Affecting Nearly Half of Americans Was 'Entirely Preventable'

https://www.nextgov.com/cybersecurity/2018/12/equifax-breach-affecting-nearly-half-americans-was-entirely-preventable/153474/

Ships infected with ransomware, USB malware, worms

https://www.zdnet.com/article/ships-infected-with-ransomware-usb-malware-worms/

U.S. Defense, Critical Infrastructure Companies Targeted in New Threat Campaign

http://www.darkreading.com/attacks-breaches/us-defense-critical-infrastructure-companies-targeted-in-new-threat-campaign/d/d-id/1333478

Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing

https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html

Cybercrooks Steal $1 Million from Save the Children Charity via BEC Attack

https://news.softpedia.com/news/cybercrooks-steal-1-million-from-save-the-children-charity-via-bec-attack-524273.shtml

Using one of the worst passwords of 2018 is a great way to get hacked

https://finance.yahoo.com/news/using-one-worst-passwords-2018-231528100.html

Some Android apps share data with Facebook, regardless of whether you have an account or not

https://www.foxnews.com/tech/some-android-apps-share-data-with-facebook-regardless-of-whether-you-have-an-account-or-not

Can't unlock an Android phone? No problem, just take a Skype call: App allows passcode bypass

https://www.theregister.co.uk/2019/01/03/android_skype_app_unlock/

Hackers spread ISIS propaganda by hijacking dormant Twitter accounts

https://www.foxnews.com/tech/hackers-spread-isis-propaganda-by-hijacking-dormant-twitter-accounts

</Closing Comments>

User Suggested:

The following articles were provided by Deborah Wright. Great articles Deborah. Thank you for sending them to me to include in the newsletter.

Criminals Use Locally Connected Devices to Attack, Loot Banks

DarkVishnya: Banks attacked through direct connection to local network

Google Accelerates Google+ Shutdown After New Bug Discovered

Securing New Devices

Microsoft, Google Use Artificial Intelligence to Fight Hackers

Start a Security To-Do List

Microsoft Digital Well-Being Tool More Broadly Available

I pledge to be Security Aware

This article was provided by previous DPS Cyber Intern. He got a good job after the internship but still keeps in contact and found this article he thought readers would enjoy.

3D-printed heads let hackers—and cops—unlock your phone

As a reminder, if you find any articles you think other readers might enjoy please send them to me. If you find them of interest, others will also.

Thank you for taking the time out of your busy schedule to read the articles in this month's newsletter. I hope you found all of them to be interesting and useful. Remember, you can only defend yourself against threats when you are knowledgeable about the threats. I realize cybersecurity is not the most liked topic, but it is important to understand the dangers you and your family face when being online and how your actions and the actions of others can affect the Agency. Knowing about cyber dangers are all part of Cybersecurity Awareness Continuation Training. Everyone in the Agency has to take Cybersecurity Awareness training every two years, but the learning does not end when the online training is over. My hope is this newsletter provides a little more up-to-date information about Cybersecurity as well as making it a little more enjoyable than watching generic training videos online. Feedback on how to improve the newsletter is always appreciated, so feel free to email me with suggestions. If possible, I will implement them in future editions.

As I mentioned above, everyone has to take the online training every two years. I send out notifications monthly to people when it is time for their retraining. If you know you are coming up on your two year mark, please be on the lookout for the email. If you are unsure, feel free to email me and I will let you know when you are due retraining.

In closing, hope you enjoyed the newsletter and good luck with the Cyber Challenge on the next page. And as always, **Do Good Cyber!**

Kirk

Cyber Challenge

Last Month's Challenge

Only three people emailed me with the correct answer to last month's challenge. Here they are:

Tracy Kingsley @ 1422 on 13 Dec 18	**Deborah Wright @ 1430 on 13 Dec 18**	**Erich Neumann @ 1526 on 13 Dec 18**

The following people decoded the QR code and provided that answer. Here they are:

Nathan Tunnell @ 1029 on 13 Dec 18	**Carla Bell @ 1400 on 13 Dec 18**	**Elizabeth Post @ 1418 on 13 Dec 18**
Kymberly Hernandez @ 1412 on 13 Dec 18	**Jimmy Ferrer @ 1431 on 13 Dec 18**	**Danny White @ 1434 on 13 Dec 18**
Michael Mchale @ 1445 on 13 Dec 18	**Anne Kirsch @ 1042 on 14 Dec 18**	

Congratulations to everyone who was able to complete any of the challenges.

Here are the steps you need to take to solve last month's challenge.

1) Decode the QR code I provided. There are several QR code readers you could use.
2) Answer the question from the QR code. The question was "Knowing my answer will help you solve this month's challenge. I am the fourth prime number. What am I?" **The answer is 7**.
3) Find the hidden message embedded in the pdf code. Open the Newsletter with a program such as Notepad or Textpad. Once you do, you will see a string of characters as the first and last lines.
4) Copy all the characters starting from the first one till where you see %PDF-1.5 and paste them into a text editor such as Notepad or Word. Next copy all the characters at the end of the document starting with the first character after %% EOF. Then paste those characters after those you pasted in the text editor.
5) Now you need to decode what you just copied. This message is encoded using a **Base64 encoding**. You can find several websites that will decode the message.
6) Once you decode the message you will get a string of characters that are encrypted using a **Caesar Cipher**.
7) Use the offset of **7** which you got from the QR code to find the challenge question you need to answer. That question is "I am a type of cyber attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. What am I known as?" The answer is **Man-in-the-Middle Attack**.

You can find next month's challenge on the next page.

Cyber Challenge

This Month's Challenge

For this month's challenge we are going to simplify them some. Below you will find some questions. The first two are simple cyber related questions. The rest are all encoded either in Binary, Hexadecimal, or Base64.

Encoding is the process of converting data into a format required for a number of information processing needs, including:

- Program compiling and execution
- Data transmission, storage and compression/decompression
- Application data processing such as file conversion

Encoding can have two meanings:

- In computer technology, encoding is the process of applying a specific code, such as letters, symbols and numbers, to data for conversion into an equivalent cipher
- In electronics, encoding refers to analog to digital conversion

While there are other types of encoding, the ones most often used with computers are binary, hexadecimal and base64. You can find out more information about each of them by clicking the links.

1) I am the art of manipulating people so they give up confidential information. The type of information varies but the individuals targeted are usually trying to trick you into giving them your passwords, bank information, access your computer to install malicious software, etc. What am I?
2) I am an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence to prove their identity. What am I?
3) SSBhbSB0aGUgZnJhdWR1bGVudCBhdHRlbXB0IHRvIG9idGFpbiBzZW5zaXRpdmUgaW5mb3JtYXRpb24gc3VjaCBhcyB1c2VybmFtZXMsIHBhc3N3b3JkcyBhbmQgY3JlZGl0IGNhcmQgZGV0YWlscyBieSBkaXNndWlzaW5nIGFzIGEgdHJ1c3R3b3J0aHkgZW50aXR5IGluIGFuIGVsZWN0cm9uaWMgY29tbXVuaWNhdGlvbi4gIFdoYXQgYW0gST8=
4) 01001001 00100000 01100001 01101101 00100000 01110011 01101111 01100110 01110100 01110111 01100001 01110010 01100101 00100000 01110100 01101000 01100001 01110100 00100000 01101001 01110011 00100000 01101001 01101110 01110100 01100101 01101110 01100100 01100101 01100100 00100000 01110100 01101111 00100000 01100100 01100001 01101101 01100001 01100111 01100101 00100000 01101111 01110010 00100000 01100100 01101001 01110011 01100001 01100010 01101100 01100101 00100000 01100011 01101111 01101101 01110000 01110101 01110100 01100101 01110010 01110011 00100000 01100001 01101110 01100100 00100000 01100011 01101111 01101101 01110000 01110101 01110100 01100101 01110010 00100000 01110011 01111001 01110011 01110100 01100101 01101101 01110011 00101110 00100000 00100000 01001001 00100000 01100011 01101111 01101101 01100101 00100000 01101001 01101110 00100000 01101101 01100001 01101110 01111001 00100000 01100110 01101111 01110010 01101101 01110011 00101110 00100000 00100000 01010111 01101000 01100001 01110100 00100000 01100001 01101101 00100000 01001001 00111111
5) 49 20 61 6d 20 61 20 74 79 70 65 20 6f 66 20 6d 61 6c 69 63 69 6f 75 73 20 73 6f 66 74 77 61 72 65 20 64 65 73 69 67 6e 65 64 20 74 6f 20 62 6c 6f 63 6b 20 61 63 63 65 73 73 20 74 6f 20 61 20 63 6f 6d 70 75 74 65 72 20 73 79 73 74 65 6d 20 75 6e 74 69 6c 20 61 20 73 75 6d 20 6f 66 20 6d 6f 6e 65 79 20 69 73 20 70 61 69 64 2e 20 20 57 68 61 74 20 61 6d 20 49 3f

Good Luck with the challenge. Make sure and email me your answers or if you need a hint to solve them.
Kirk.