Vol. 4 | Issue 4

Cyber Security NEWS

April 2019

Welcome to the TXDPS Cyber Newsletter

Hello everyone and welcome to this month's cybersecurity newsletter. I hope you find this month's newsletter articles relevant and interesting. While all the articles should be relevant for most people, I suggest those of you who have an iPhone pay special attention to the second article on page four. If you haven't updated your phone recently I think you will agree you need to do so immediately. And for those of you in the Dallas area, you should probably read the article on page 6 about the hacked tornado sirens.

Since we are still in Tax Season, I wanted to remind everyone about the tax scams I have mentioned in the last two newsletters. If you haven't done so, I would encourage you to visit the websites below to make yourself familiar with the most current tax scams.

IRS website Tax Scams / Consumer Alerts

IRS website IRS Urges Public to Stay Alert for Scam Phone Calls

TurboTax website Beware of IRS Phone Scams

YouTube video published Jul 24, 2018 Two IRS scammers arrested in Arizona

Federal Trade Commission IRS Imposter Scams

The IRS warns taxpayers, businesses and tax professionals to be alert for a continuing surge of fake emails, text messages, websites and social media attempts to steal personal information. While these attacks are always occurring, as you might expect, they increase during tax season and identity theft is a major problem for individuals.

"Taxpayers should be on constant guard for these phishing schemes, which can be tricky and cleverly designed to look like it's the IRS," said IRS Commissioner Chuck Rettig. "Watch out for emails and other scams posing as the IRS, promising a big refund or personally threatening people. Don't open attachments and click on links in emails. Don't fall victim to phishing or other common scams."

The IRS also urges taxpayers to learn how to protect themselves by reviewing safety tips prepared by the Security Summit, a collaborative effort between the IRS, state revenue departments and the private-sector tax community.

To learn more about new variations on phishing schemes, schemes aimed at tax pros, payroll offices, human resources personnel, and how to report phishing attempts, click **HERE**.

Good luck and hopefully you will not have to give extra money to the IRS this year.

Dating Scheme / Asus

Two Men Found Guilty in International Cyber-Fraud Scheme Involving Online Dating and Business Email Compromises

(The United States Department of Justice Press Release Number 19-259)

A citizen of Nigeria residing in Atlanta, and a citizen of Mexico residing in California, were convicted Wednesday after a seven-day trial in the U.S. District Court for the Western District of Tennessee on charges related to the part each played in an international cyber fraud scheme.

Olufolajimi Abegunde, 31, of Atlanta, Georgia, and Javier Luis Ramos-Alonso, 29, of Seaside, California, participated in a criminal organization in which members "spoofed" emails and created fake profiles on dating websites in order to fool victims into sending money to bogus bank accounts under the control of members of the conspiracy. The proceeds would be laundered and subsequently wired out of the United States to destinations including West Africa.

Abegunde, who received an MBA from Texas A&M University in College Station, Texas, engaged in black-market currency exchanges over the life of the conspiracy. Purporting to hold himself out as a legitimate businessman, the proof at trial showed that Abegunde claimed association with a business entity that was not yet operational in late 2017, so for his primary source of income he relied on his off -the-book currency exchanges. Through this network, Abegeunde played a key role, along with Ramos-Alonso, in laundering fraud funds from an Oct. 3, 2016, business email compromise (BEC) of a land title company located in Bellingham, Washington. The proceeds of another BEC perpetrated in July 2016 upon a real estate company in Memphis, Tennessee, also moved through parts of the same criminal organization.

Click **HERE** to read the article.

Asus: Yo dawg, we hear a million of you got pwned by a software update. So we got you an update for the update

(by **Shaun Nichols** on **26 Mar 2019 @ 18:45**)

Asus has released an update for its software update utility to rid about a million of its notebooks of a spyware-laden software update pushed to victims by its software update system.

And breathe in.

The Taiwanese PC giant on Tuesday published a fresh clean version of Live Update, which is a tool that keeps firmware driver and BIOS software up to date, and is bundled with Asus computers. Users should download and install it. Between June and November of last year, during a cyber-espionage campaign dubbed ShadowHammer, someone broke into Asus's software update servers, and hid a backdoor in a copy of Live Update.

When about a million Asus laptops checked in automatically for software updates, they downloaded from Asus's systems the dodgy copy of Live Update, which was cryptographically signed using Asus's security certificate, and had the same file length as a previous legit version, so everything looked above board, and then installed it. In effect, these machines were inadvertently fetching spyware over the internet from Asus's servers, and running it. The compromised utility was designed to snoop on roughly 600 targets, identified by network MAC addresses hardcoded in the binary. Thus hundreds of thousands of Asus notebooks got a dormant backdoor in a compromised download of Live Update, and a few hundred were actively spied on.

The hijacked utility was discovered in January by Kaspersky Lab, and came to light this week. You can use this online tool to check if your machine was actively hijacked, based on your MAC address

Click **HERE** to read the article.

Office Depot / Spyware Leak

Office Depot, OfficeMax, Support.com cough up $35m after charging folks millions in 'fake' malware cleanup fees

(by **Thomas Claburn** on **27 Mar 2019 @ 23:54**)

Tech support outfits settle out of court after allegations of bogus infection symptoms to extract repair charges

Office Depot and Support.com have coughed up $35m after they were accused of lying to people that their PCs were infected with malware in order to charge them cleanup fees.

On Wednesday, the pair of businesses settled a lawsuit brought against them by the US Federal Trade Commission, which alleged staff at the tech duo falsely claimed software nasties were lingering on customers' computers to make a fast buck.

The lawsuit, filed in southern Florida, claimed the two companies, including Office Depot subsidiary OfficeMax, from 2009 until November 2016 misrepresented the state of consumers' computers by using a sales tool designed to convince people to pay for diagnostic and repair services.

"In numerous instances throughout this time period, Defendants used the PC Health Check Program to report to Office Depot Companies customers that the scan had found or identified 'Malware Symptoms' when it had not done so," the complaint stated. "Additionally, in numerous instances, the PC Health Check Program falsely reported to consumers that the program had found 'infections' on the consumer's computer."

Click **HERE** to read more.

Hosting Provider Finally Takes Down Spyware Leak of Thousands of Photos and Phone Calls

(by **Lorenzo Franceschi-Bicchierai** on **Mar 26, 2019 @ 3:32pm**)

After Motherboard reported that a consumer spyware vendor left a lot of incredibly sensitive and private data online, the company's hosting provider took it down.

A company that sells cellphone spyware to consumers left 95,000 images and more than 25,000 audio recordings on a server accessible to anyone on the internet for weeks. The sensitive data was so easy to access, that Motherboard couldn't even name the spyware company in its report without risking more people finding and abusing that data.

But now, after Motherboard reported the breach, the company that was hosting the database took the whole spyware company's site down.

"Codero has taken action on this matter and the mentioned URL should no longer be accessible," Jason Ackley, the vice president of operations and network engineering at Codero, told Motherboard.

Earlier this year, security researcher and student Cian Heasley found the server, which belonged to Mobiispy, one of many companies that sell spyware to parents and employers to monitor their children and employees. In many cases, these type of spyware apps are used by abusive partners, as several Motherboard articles reported over the last couple of years.

For weeks, Motherboard tried to reach John Nguyen, the owner of Mobiispy.com. But he did not respond to multiple emails to a Gmail address that was used to register the domain, as well as the official Mobiispy contact address.

Click **HERE** to read .

LinkedIn / iOS 12.2

LinkedIn is becoming China's go-to platform for recruiting foreign spies

(by **Jeff Stone** on **Mar 26, 2019)**

Buried in the 41-page felony complaint charging a former U.S. intelligence operative of spying for the Chinese, FBI investigators declare that the suspect, Ron Rockwell Hansen, had been printing information from his colleagues' LinkedIn pages.

Hansen, a former Defense Intelligence Agency case officer who pleaded guilty on March 15 to attempted espionage against the U.S. took information from the professional networking site related to several former and current DIA case officers before a 2015 trip to China.

The complaint does not state how that information was used, if at all, but it's enough to raise the notion Hansen may have been passing LinkedIn data to Chinese handlers in addition to other secrete DIA materials files.

"I solicited from an intelligence case officer working for the Defense Intelligence Agency national defense information that I knew Chinese Intelligence services would find valuable, and I agreed to act as a conduit to sell that information the Chinese" in exchange for hundreds of thousands of dollars, Hansen said as part of his plea deal.

Click **HERE** to read more.

iOS 12.2 fixes bug that granted apps hidden access to the microphone

(by **Catalin Cimpanu** on **March 26, 2019 @ 09:19 GMT**)

Apple fixes 51 iOS security bugs, including a whopping 13 WebKit code execution flaws.

Apple released yesterday iOS version 12.2 that, like never before, includes fixes for a considerable number of security-related issues, including some that are downright disturbing.

In total, the company fixed 51 security flaws. Probably the scariest security bug, at first glance, is CVE-2019-8566, a vulnerability in Apple's ReplayKit. Used by various iOS apps, this is a component for recording and streaming audio and video feeds from a device.

Apple said a bug that existed in this component would have allowed malicious applications to access microphones without indication to the user, and surreptitiously record or stream nearby conversations.

"An API issue existed in the handling of microphone data. This issue was addressed with improved validation," Apple said.

CODE EXECUTION VIA SMS LINKS

Another major issue fixed in this release is the one affecting iOS GeoServices, the component responsible for working with geo-location data.

Click **HERE** to read more.

Prisons / Tesla

Federal bills would let state prisons jam cellphone signals

(by **Meg Kinnard** on **March 28, 2019**)

Federal legislation proposed Thursday would give state prison officials the ability they have long sought to jam the signals of cellphones smuggled to inmates within their walls.

U.S. Sen. Tom Cotton of Arkansas and U.S. Rep. David Kustoff of Tennessee introduced companion bills in both chambers, The Associated Press has learned.

The legislation could help provide a solution to a problem prison officials have said represents the top security threat to their institutions. Corrections chiefs across the country have long argued for the ability to jam the signals, saying the phones 0 smuggled into their institutions by the thousands, by visitors, errant employees, and even delivered by drone - are dangerous because inmates use them to carry out crimes and plot violence both inside and outside prison.

But the Federal Communications Commission, which regulates the nation's airwaves, has said a decades-old prohibition on interrupting signals at state-level institutions prevents the agency from permitting jamming on that level. Wireless industry groups have said they worry signal-blocking technologies could thwart legal calls.

Prison officials, including South Carolina Corrections Director Bryan Stirling, have pushed for the ability to jam signals, saying it's the best way to combat the dangerous devices. In 2017, Stirling testified at an FCC hearing in Washington alongside Robert Johnson, a former South Carolina corrections officer nearly killed in 2010 in a hit orchestrated by an inmate using an illegal phone.

Click **HERE** to read more.

Tesla cars keep more data than you think, including this video of a crash that totaled a Model 3

(by **Kate Fazzini** and **Lora Kolodny** on **29 March 2019 @ 4:33 PM ET**)

- Crashed Tesla vehicles, sold at junk yards and auctions, contain deeply personal and unencrypted data including info from drivers' paired mobile devices, and video showing what happened just before the accident.
- Security researcher GreenTheOnly extracted unencrypted video, phonebooks, calendar items and other data from Model S, Model X and Model 3 vehicles purchased for testing and research at slavage.
- Hackers who test or modify the systems in their own Tesla vehicles are flagged internally, ensuring that they are not among the first to receive over-the-air software updates first.

If you crash your Tesla, when it goes to the junk yard, it could carry a bunch of your history with it.

That's because the computers on Tesla vehicles keep everything that drivers have voluntarily stored on their cars, plus tons of other information generated by the vehicles including video, location and navigational data showing exactly what happened leading up to a crash, according to tow security researchers.

One researcher, who calls himself GreenTheOnly, describes himself as a "white hat hacker" and a Tesla enthusiast who drives a Model X. He has extracted this kind of data from the computers in a salvaged Tesla Model S, Model X and two Model 3 vehicles, while also making tens of thousands of dollars cashing in on Tesla bug bounties in recent years. He agreed to speak and share data and video with CNBC on the condition of pseudonymity, citing privacy concerns.

Click **HERE** to read more.

More News

Android Apps with Over 700,000 Installs Use New Trick to Escape Full Removal

https://news.softpedia.com/news/android-apps-with-over-700-000-installs-use-new-trick-to-escape-full-removal-525233.shtml

Google: Chrome zero-day was used together with a Windows 7 zero-day

https://www.zdnet.com/article/google-chrome-zero-day-was-used-together-with-a-windows-7-zero-day/

Avoid Taking the Bait of W-2 Phishing Schemes

https://www.natlawreview.com/article/avoid-taking-bait-w-2-phishing-schemes

New "Final Warning" Sextortion Emails State Adult Sites Infected You

https://www.bleepingcomputer.com/news/security/new-final-warning-sextortion-emails-state-adult-sites-infected-you/

BEWARE—New 'Creative' Phishing Attack You Really Should Pay Attention To

https://thehackernews.com/2019/03/ios-mobile-phishing-attack.html

Medical IoT Devices with Outdated Operating Systems Exposed to Hacking

https://www.bleepingcomputer.com/news/security/medical-iot-devices-with-outdated-operating-systems-exposed-to-hacking/

Airline e-ticket systms' vulnerabilities could compromise PII to hackers

https://www.biometricupdate.com/201903/airline-e-ticket-systems-vulnerabilities-could-compromise-pii-to-hackers

2 South Carolina Men Sentenced in Darknet Mail Bomb Case

https://darkwebnews.com/law-enforcement/two-south-carolina-men-sentenced-in-darknet-mail-bomb-case/

Hacked tornado sirens taken offline in two Texas cities ahead of major storm

https://www.zdnet.com/article/hacked-tornado-sirens-taken-offline-in-two-texas-cities-ahead-of-major-storm/

Hundreds of Thousands of Medtronic Defibrillators Could Be Vulnerable to Hacking Due to Flaw

https://gizmodo.com/hundreds-of-thousands-of-medtronic-defibrillators-could-1833481773

Researchers Create Fake Profiles on 24 Health Apps and Learn Most Are Sharing Your Data

https://gizmodo.com/researchers-create-fake-profiles-on-24-health-apps-and-1833474535

More News

Man pleads guilty to swatting attack that led to death of Kansas man

https://arstechnica.com/tech-policy/2018/11/man-pleads-guilty-to-swatting-attack-that-lead-to-death-of-kansas-man/

Toyota Security Breach Exposes Personal Info of 3.1 Million Clients

https://www.bleepingcomputer.com/news/security/toyota-security-breach-exposes-personal-info-of-31-million-clients/

AirPower officially misses 2018 deadline, Apple silent on its status

https://9to5mac.com/2019/01/01/airpower-officially-misses-2018-deadline/

Former Facebook exec: 'Zuckerberg is sitting on more data about what people want to do online than anyone else in the world'

https://www.cnbc.com/2019/03/27/facebook-former-security-chief-alex-stamos-on-zuckerberg-privacy.html

Internal Documents Show Apple Is Capable of Implementing Right to Repair Legislation

https://motherboard.vice.com/en_us/article/d3mqna/internal-documents-show-apple-is-capable-of-implementing-right-to-repair-legislation

Microsoft takes control of 99 domains operated by Iranian state hackers

https://www.zdnet.com/article/microsoft-takes-control-of-99-domains-operated-by-iranian-state-hackers/

Senators demand to know why election vendors still sell voting machines with 'known vulnerabilities'

https://techcrunch.com/2019/03/27/senators-security-voting-machines/

GITAI Partners With JAXA to Send Telepresence Robots to Space

https://spectrum.ieee.org/automaton/robotics/space-robots/gitai-partners-with-jaxa-to-send-telepresence-robots-to-space

Democrats introduce Save the Internet Act to restore net neutrality

https://www.cnet.com/news/democrats-introduce-save-the-internet-act-to-restore-net-neutrality/

Top dark web marketplace will shut down next month

https://www.zdnet.com/article/top-dark-web-marketplace-will-shut-down-next-month/

RESEARCHERS BULT AN 'ONLINE LIE DETECTOR' HONESTLY, THAT COULD BE A PROBLEM

https://www.wired.com/story/online-lie-detector-test-machine-learning/

Reader Suggested Articles

As you can see below, we again had several reader suggested articles this month. I encourage you to read all of them, but I want to highlight a couple of the articles I think most readers will benefit from reading.

The last two articles from Deborah Wright will probably be of interest to most people. The next to the last is an article about how Google Photos Flaw Allowed Hackers to Track Users. And the last article is about the dangers of just throwing old tech away. Old computers, hard drives, flash drives, tablets, phones, TVs, etc have lots of data on Personally Identifiable Information (PII) about you. This article discusses how to safely dispose of unwanted technology.

The article Bruce Whitaker submitted should **DEFINITELY** be read. It is about a strand of specialty malware designed to infect ecommerce sites and skim credit card information.

And for those of you who are MAC users, if you have not taken my advice and installed Sophos on your computer you might want to read the article Doc Petty submitted. It is a Microsoft anti-virus solution for Macs. And if you are one of those Mac users who believed the commercials about Macs not catching viruses…….email me so I can educate you on how incorrect that belief is.

Deborah Wright:

- https://www.zdnet.com/article/microsoft-windows-10-can-now-automatically-uninstall-buggy-updates/
- https://www.forbes.com/sites/kateoflahertyuk/2019/03/10/citrix-data-breach-heres-what-to-do-next/#d1d210b14763
- https://www.cisecurity.org/white-papers/security-primer-trickbot/
- https://blog.mozilla.org/blog/2019/03/12/introducing-firefox-send-providing-free-file-transfers-while-keeping-your-personal-information-private/
- https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS/Overview
- https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS/FIPS_Mode_-_an_explanation
- Code 42 Website
- https://blog.talosintelligence.com/2019/03/ipv6-unmasking-via-upnp.html
- https://www.securityweek.com/google-photos-flaw-allowed-hackers-track-users
- https://blog.rapid7.com/2019/03/19/buy-one-device-get-data-free-private-information-remains-on-donated-devices/

Bruce Whitaker

- https://arstechnica.com/information-technology/2019/03/a-new-rash-of-highly-covert-card-skimming-malware-infects-ecommerce-sites/

Stephen "Doc" Petty

- https://techcommunity.microsoft.com/t5/Windows-Defender-ATP/Announcing-Microsoft-Defender-ATP-for-Mac/ba-p/378010

Cyber Challenge

Last Month's Challenge

Here are the people who completed last month's challenges:

Faye Krueger @ 1358 on 7 March	Michael Mchale @ 1434 on 7 March	Erich Neumann @ 1437 on 7 March
Jared Crouse @ 1440 on 7 March	Betty Newman @ 1558 on 7 March	Russell Cooper @ 0816 on 8 March
Jimmy Ferrer @ 1259 on 8 March	Daniel Martinez @ 1445 on 8 March	James Taylor @ 1440 on 11 March
Colin Jowry @ 1001 on 14 March		

Below are the people who got 2 of the 3 challenges correct.

Norman McLeod	Stephen "Doc" Petty	

Last month's cyber challenge was to pick the phishing site from two choices. One was a legitimate site while the other was an actual phishing site. This challenge shows just how vigilant you must be to keep from falling victim to a phishing scam. Malicious people are constantly finding ways to trick unsuspecting people and stealing their information, money, identities, etc from these types of sites. So here are the answers to last month's challenge:

1) The picture on the **RIGHT** is the phishing site. This one was very difficult to tell. About the only way to be sure which was the real site was to go to the website and look. But even then you had to pay close attention to the icons at the bottom of the page.
2) The picture on the **LEFT** is the phishing site. Best way to be sure is to go to the website. But one thing that should have given it away was the "Login with Other Mail" button. Why would Microsoft allow you to log into their email site with a different email address?
3) The picture on the **LEFT** is the phishing site. Again, the best way to be sure is to go to the actual website and look. The giveaway to me on this one is the greyed out icons at the bottom of the page.

So how do people fall victim to these types of sites? Normally its from clicking on links in emails they receive. Clicking links in emails is often a very BAD idea. But people get in a hurry and often get nervous when they receive an email saying their account is about to be locked out and they need to login to verify to keep it open. Or some other type of scare tactic. People often click on the conveniently placed link that takes them to a false site. They then put in their information without even stopping to think if this might be a scam. I suggest always be vigilant and a little paranoid when putting in any information online. Never click on a link in an email. Always open a web browser and go to the legitimate site and then verify if what the email said is actually correct.

For those of you who didn't attempt or were unable to complete last month's challenges, I encourage you to look at the pictures again and see if you can understand what I described above. If you need assistance, email me.

This month's challenge is on the next page. Remember, if you have difficulties solving the challenges you can always email me for hints.

Cyber Challenge

This Month's Challenge

This month's Cyber Challenge is a combination challenge. I have hidden three (3) Cryptograms in the newsletter. I am using a technique knows as Steganography to hide the messages. Once you find the Cryptograms you will need to solve them then email me the answers.

Some of you might be asking "What is a Cryptogram?" The answer is that cryptograms are text written in code. It is not encryption because there is no key needed to convert the code into something readable. If you do not recognize the term, you might recognize it by another name; a Caesar cipher. Caesar ciphers have been around for a long time. The process is simple, you take a message and change each letter to another letter in the alphabet thus making the original message illegible. While this might seem to be a very difficult code to figure out, it is actually very easy. Ciphers like this can be broken using simple pattern recognition, frequency analysis and a general knowledge of grammar and vocabulary. Because of this, simple-substitution ciphers are inadequate for providing confidentiality of information but can be fun to play with.

Some of you might also be asking "What is Steganography?" The answer to that is steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data. The word steganography is derived from the Greek words steganos (meaning hidden or covered) and the Greek root graph (meaning to write). Most often steganography is used to hide files or messages inside pictures, videos, and audio files. But there are other ways to employ steganography as you will see with this challenge. Steganography dates back to at least the 5th century BC and is one of the oldest methods of concealing secret information. According to the classical author Herodotus, it was first used by the tyrant Histiaeus, who shaved the head of a servant before tattooing a message on his scalp. This obviously had some flaws as in only being able to happen once, but it apparently was very successful after the servant's hair grew back. The use of steganography has obviously changed since the 5th century BC and while there are several legitimate uses for steganography, criminals and terrorist organizations have used them in several different ways. One of the most interesting cases I have heard about is how al-Qaeda hid secret documents in a porn video in 2012. To find our more about this incident, click **HERE**.

Good luck with this month's challenge. If you get stuck, feel free to email me and ask for hints.

</Closing Comments>

Thank you for taking the time out of your day to read the 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. 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.

I covered a wide range of cyber topics in this month's newsletter. Topics ranging from prosecution of people for cyber scams to hardware and ecommerce sites being infected with malware to LinkedIn being used to recruit spies to other more personal cyber dangers to you. Hopefully you will take the time to read and research more on these topics and others you come across in your research. If you do not understand something you read, feel free to reach out to me and ask questions. I am more than willing to assist you in understanding these or other cyber security topics. Some of them can get very confusing and it helps to have a person you can contact to ask for clarification.

A final reminder about taxes. It is still the season and there are lots of IRS scams out there. Be careful and vigilant so you do not fall victim. Be very wary of emails you receive claiming to be from the IRS. If you did not view the links, I strongly encourage you to look at the IRS scam links on the first page.

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

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

In closing, hope you enjoyed the newsletter and good luck with the Cyber Challenges. And as always, **THANK YOU FOR YOUR CYBER VIGILANCE.**

Kirk