NEWS
Cyber Security
Vol. 3 | Issue 3 March 2018

Trojans | IoT | uTorrent | Russians | Stats | Challenge

Hello everyone and welcome to this month's TXDPS Cyber Newsletter.

To begin this newsletter I wanted to inform everyone about an incident which happened recently. In early February an employee at a sister state agency was tricked into compromising their work computer through a Social Engineering attack. Just before 5 pm on February 9, 2018, the agency's Help Desk received a call from their employee to report having talked to an individual claiming to be tech support from cyber-security. Apparently the caller was able to convince the employee there was a virus on the computer and the caller would help remove the virus. However, to do so would require the employee to go to a website first and download some software. The caller had the employee attempt to download from two different websites, but the agency's network policies prohibited any malicious downloads. The caller was finally able to get the employee to connect to a site which had not been blocked and was able to install malicious software on the employee's computer. The employee had difficulty understanding the caller, so a second individual began speaking to the employee. The caller asked the employee several questions starting with which browser the employee used and followed up with other questions which could facilitate the attack. He even asked the employee if they watched porn on their work computer. The caller had control of the employee's computer at this time and was using the mouse to point out things on the computer. At the end of the call, the caller told the employee there was a payment due for the services. It was that last statement that made the employee think that maybe there was an issue so they contacted their Help Desk and reported what had happened.

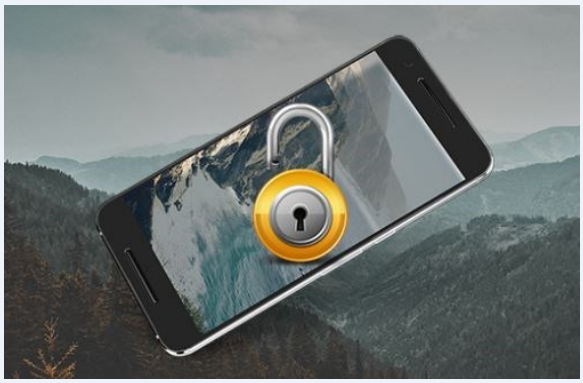
This is a classic **Social Engineering** attack. Social Engineering attacks are non-technical, easy to perform, and often the most successful types of computer attacks. These types of attacks trick a user into giving up critical information that can be used against the individual or organization. As demonstrated in the above incident, the attack can also be used to trick a user into giving up control of their computer, phone, tablet, etc. Once the user enables this compromise of the electronic device, the malicious individual will often remotely install additional software which will allow for remote control, monitoring, and unauthorized usage of the device. The above incident demonstrates the need for users to be aware and informed about cybersecurity threats. Users are the first line of defense against any attack. It doesn't matter how good an agency's IT and Cyber teams are, one simple mistake can compromise a device and allow a malicious actor to then compromise the whole agency. Put yourself in this employees place. Could you have been tricked into falling victim to this type of attack? Everyone is susceptible so vigilance at all times is a necessity.

To demonstrate just how easy this can be done, here is a video from a world renowned computer security conference where Social Engineering is one of the things demonstrated. Click **HERE** to see the video.

Here is another video from CNN Money showing another example. Click **HERE** to see the video.

Cyber News!!

Mobile banking Trojans spread confusion worldwide



Consumers around the world that use mobile banking apps are at a greater risk of being tricked by cybercriminals and falling victim to mobile banking theft. This is according to new global research from Avast, which asked almost 40,000 consumers in Spain and eleven other countries around the world to compare the authenticity of official and counterfeit banking application interfaces.

Globally, 58% of respondents identified the official mobile banking app interface as fraudulent while 36% mistook the fake interface for the real one. In Spain, the results were similar at 67% and 27% respectively, compared to 40% and 42% in the U.S.

The findings highlight the level of sophistication and accuracy applied by cybercriminals to create trusted copies designed to spy on users, collect their bank login details, and steal their money.

Researchers detected a number of mobile banking Trojans in recent months – a privacy and security threat that is on the rise. The banks targeted by cybercriminals and under the microscope in the survey include Citibank, Wells Fargo, Santander, HSBC, ING, Chase, Bank of Scotland and Sberbank.

Click **HERE** to see more.

Rock-a-byte, baby: IoT tot-monitoring camera lets miscreants watch 10,000s of kids online

More than 52,000 internet-connected Mi-Cam baby monitors are broadcasting sound and video to whoever comes looking, researchers have claimed.

These Wi-Fi gizmos, built by Chinese biz MiSafes, stream 720p video and two-way audio in real-time to apps running on parents' smartphones, via Amazon cloud servers. The application connects to an AWS-hosted backend, logs into the user's Mi-Cam account, and accesses video and audio from their linked baby monitor, which is also talking to the cloud backend.

Grownups open their app, log into their account, and keep an eye on their tykes from their Mi-Cam, essentially.

Infosec bods at SEC Consult, working with master's student Mathias Frank at the University of Applied Sciences Technikum Wien in Austria, told *The Register* on Tuesday they have found six security flaws in the product. The worst of the flaws allows miscreants to spy on video streams of kids without any kind of permission check.

Click **HERE** to see more.

More Cyber News!!

uTorrent bugs let websites control your computer and steal your downloads

Two versions of uTorrent, one of the Internet's most widely used BitTorrent apps, have easy-to-exploit vulnerabilities that allow attackers to execute code, access downloaded files, and snoop on download histories, a Google Project Zero researcher said. uTorrent developers are in the process of rolling out fixes for both the uTorrent desktop app for Windows and the newer uTorrent Web product.

The vulnerabilities, according to Project Zero, make it possible for any website a user visits to control key functions in both the uTorrent desktop app for Windows and in uTorrent Web, an alternative to desktop BitTorrent apps that uses a Web interface and is controlled by a browser. The biggest threat is posed by malicious sites that could exploit the flaw to download malicious code into the Windows startup folder, where it will be automatically run the next time the computer boots up. Any site a user visits can also access downloaded files and browse download histories.

Click **HERE** to see more.

Two Russian Nationals Sentenced to Prison for Massive Data Breach Conspiracy

Two Russian nationals were sentenced today to federal prison terms for their respective roles in a worldwide hacking and data breach scheme that targeted major corporate networks, compromised 160 million credit card numbers and resulted in hundreds of millions of dollars in losses – the largest such scheme ever prosecuted in the United States.

The sentencings were announced by New Jersey, Acting U.S. Attorney William E. Fitzpatrick, Acting Assistant Attorney General John P. Cronan of the Justice Department's Criminal Division, and Mark McKevitt, Special Agent in Charge of the U.S. Secret Service Newark Field Office.

Vladimir Drinkman, 37, of Syktyvkar and Moscow, Russia, previously pleaded guilty before U.S. District Judge Jerome B. Simandle of the District of New Jersey to one count of conspiracy to commit unauthorized access of protected computers and one count of conspiracy to commit wire fraud. He was sentenced to 144 months in prison. Dmitriy Smilianets, 34, of Moscow, previously pleaded guilty to conspiracy to commit wire fraud in a manner affecting a financial institution and was sentenced to 51 months and 21 days (in prison) time served. Both men pleaded guilty in September 2013 before Judge Simandle, who imposed the sentences today in Camden federal court.

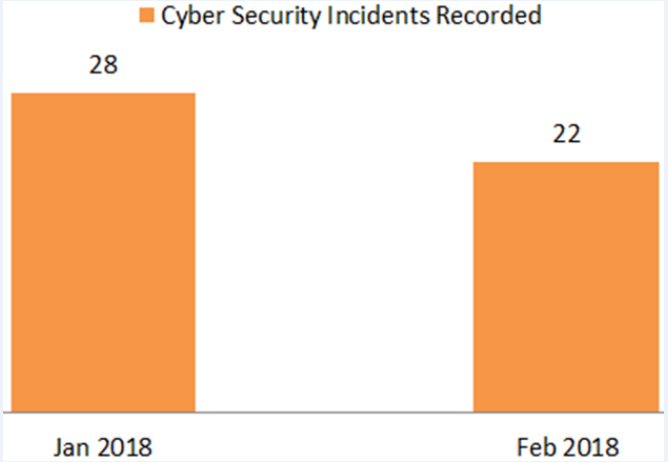
Click **HERE** to see more.

<Cyber Stats for Jan and Feb>

Email Security	January 2018	% Change	February 2018
Phishing attacks against agency	15	-53.33%	7
Emails inspected by sensors	1,700,087	-4.14%	1,629,735
Emails blocked by sensors	1,132,829	41.49%	1,602,827
DPS Custom Email Threat Signatures Created	22	-45.45%	12

Endpoint Security	January 2018	% Change	February 2018
Malware Detected	171	-23.98%	130
Malware Quarantined	171	-23.98%	130

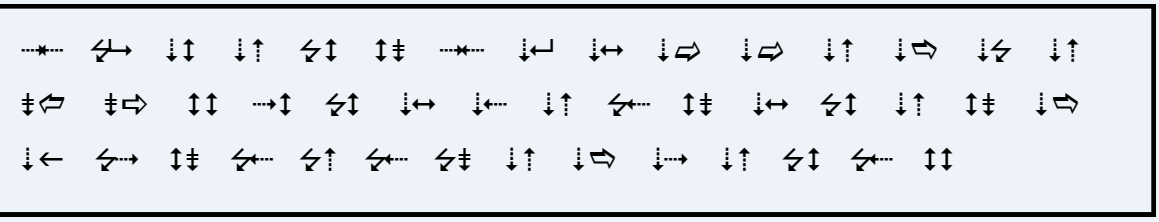
For this month's stats page, I have included various information which I feel you might find interesting. As you can see, Phishing attacks as well as malware detection and quarantines were lower last month than the month before. At the beginning of the newsletter I called the incident a Social Engineering attack. It was, but it started with a Phishing attack. We only had 7 last month but all it takes is 1 to cause huge problems. Being vigilant is a must to protect the agency.



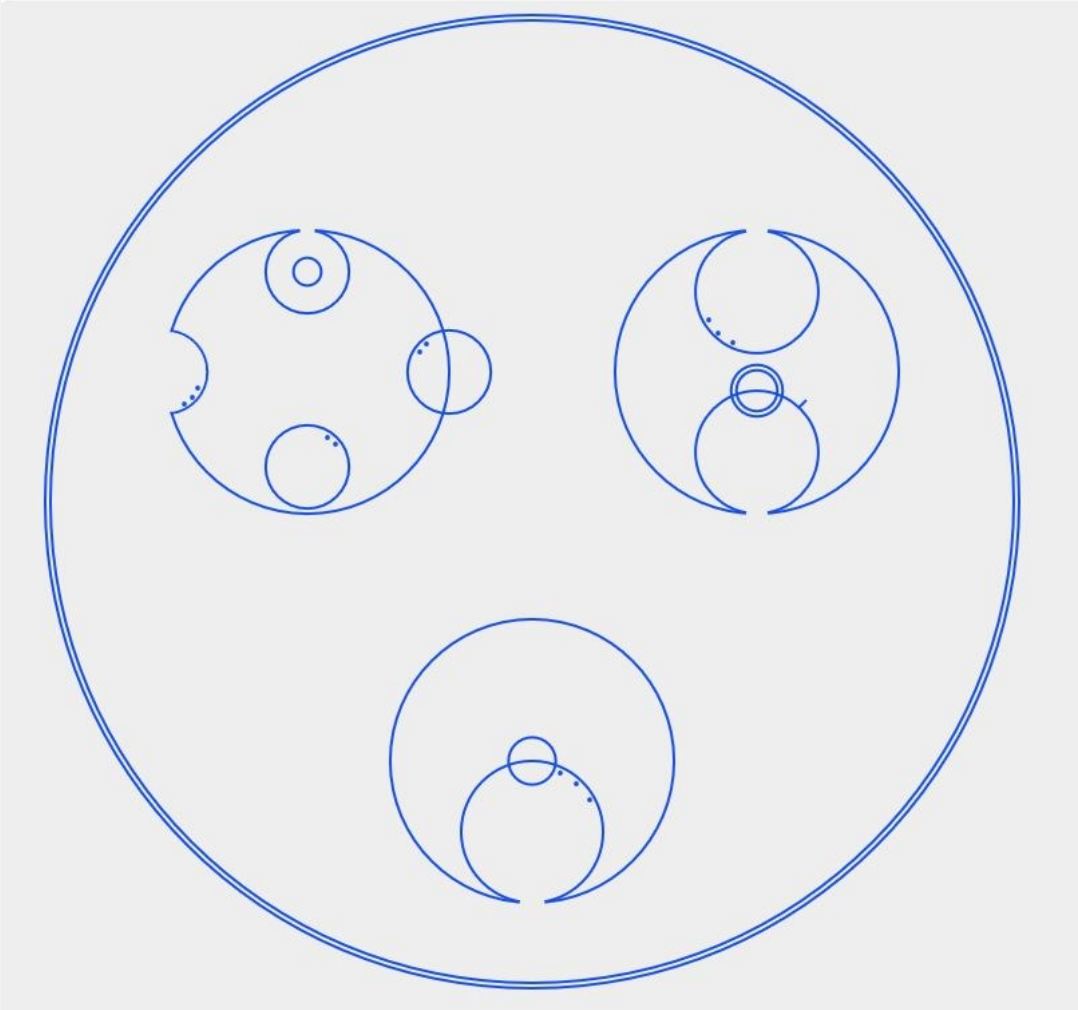
Our Cyber Security Incidents were also down from the month prior. I personally believe it is due to the continued education provided to employees. Being aware of what to look for educates everyone. This not only protects the Agency but has the added benefit of helping you keep your personal computers safe. Keep up the good work.

Please let me know if there are topics or metrics you would like to see me try to include in future newsletters. Also, if you have a cyber related story you would like to share, please do so. With your permission I might just include it in future newsletters.

Cyber Challenge



Were you able to figure out where the message was hidden in last month's newsletter?

If not, you can find it by going to the Uber security flaw compromised two-factor authentication article. You will see a space under the "To read more click HERE" sentence. If you use your mouse you will be able to highlight a hidden text similar to what you would do if you were copying and pasting in a Word document. Once you highlight the area, copy it and the paste it in Word, Notepad or similar program. If you paste the message in Notepad you will see it immediately. If you use Word you might have to highlight the text and change the color so you can read it.

This month's Cyber Challenge is actually two challenges. The easiest is at the top of this page. See if you can figure out what the message says. The second is the picture below. It is a message that might appeal to a slightly more geeky crowd but demonstrates how messages can be hidden in plain sight (steganography). Enjoy. :D