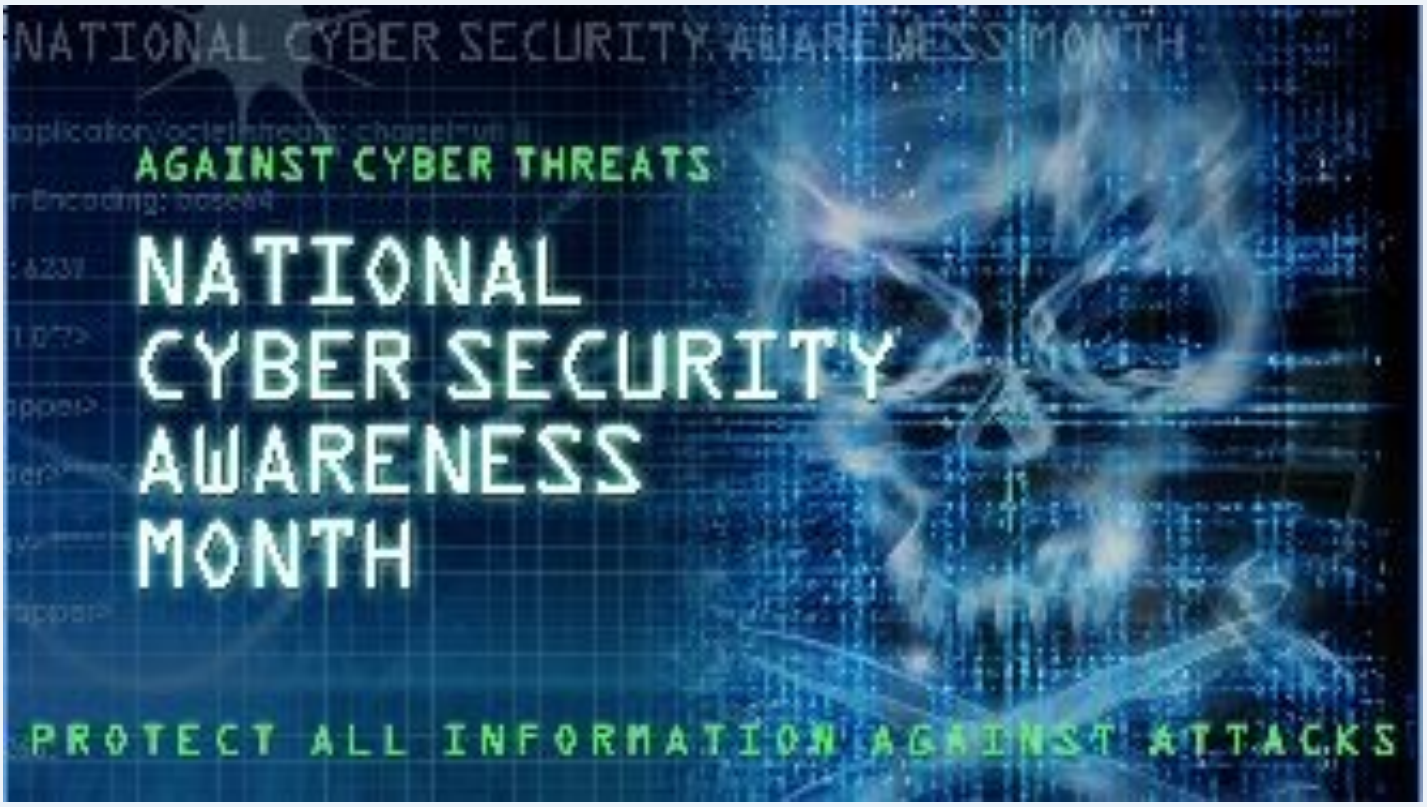
Vol. 3 | Issue 10

Cyber Security NEWS

October 2018

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



Hello everyone and welcome to this month's DPS Cybersecurity Newsletter. To start the newsletter, I want to spend a couple of seconds talking about the recent Cybersecurity Awareness retraining. For those people who took the training two years ago, you should have received a retraining notification by now. If you know you took the training two years ago but do not remember seeing an email, please contact me to get a new email sent to you. If you know someone in your work area who should have received an email, please have them contact me. Supervisors are currently being notified about people who have not completed the training in the allotted time. Please be proactive and complete the training so they don't have to be contacted.

The majority of DPS employees have had their training reset, but each month there will be new people reset as they come up on their two year retraining requirement. So every month I will be sending out retraining notifications for those who require retraining. If you know you are close to the two year retraining time, please be on the lookout for an email.

Now on to the newsletter. For those who are not aware, October is **Cybersecurity Awareness Month**. It is also the month of my favorite holiday….Halloween. In that theme, I have found articles I believe are not only relevant but should also be scary to everyone. The articles are not only relevant towards issues here at DPS, but I believe most of them are also relevant to people's personal life. Hopefully you will agree and enjoy this month's newsletter.

Phantom Secure/China

Phantom Secure CEO pleads guilty to providing drug cartels with encrypted phones

(by Charlie Osborne for Zero Day | October 4, 2018)

The chief executive of Phantom Secure, a phone service designed to keep criminal activity away from the eyes of law enforcement, has pled guilty to his role in the operation of the network.

Vincent Ramos, the CEO of Vancouver-based Phantom Secure, was taken into custody in California following efforts by the FBI, Australian Federal Police (AFP), and Canadian police to track down the operators of the network.

As part of a plea agreement, Ramos admitted to "leading a criminal enterprise that facilitated the transnational importation and distribution of narcotics through the sale and service of encrypted communications devices," US prosecutors said this week.

The guilty plea follows the indictment of Ramos and three others in connection to Phantom Secure in March.

The Phantom Secure network was built upon customized BlackBerry handsets. These devices were given custom software which enhanced the encryption of each device via PGP, as well as offered secure email communications.

According to US prosecutors, Ramos and Phantom Secure technicians maintained servers used by the network in Panama and Hong Kong, and virtual proxies were established to disguise their locations.

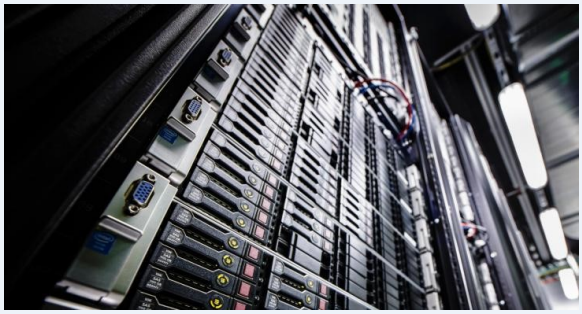
Click **HERE** to read the article.

China reportedly infiltrated Apple and other US companies using 'spy' chips on servers

(by Jon Russel | October, 4 2018)

Ready for information about what may be one of the largest corporate espionage programs from a nation-state? The Chinese government managed to gain access to the servers of more than 30 U.S. companies, including Apple, according to an explosive report from Bloomberg published today.

Bloomberg reports that U.S-based server motherboard specialist Supermicro was compromised in China where government-affiliated groups are alleged to have infiltrated its supply chain to attach tiny chips, some merely the size of a pencil tip, to motherboards which ended up in servers deployed in the U.S.



The goal, Bloomberg said, was to gain an entry point within company systems to potentially grab IP or confidential information. While the micro-servers themselves were limited in terms of direct capabilities, they represented a "stealth doorway" that could allow China-based operatives to remotely alter how a device functioned to potentially access information.

Once aware of the program, the U.S. government spied on the spies behind the chips but, according to Bloomberg, no consumer data is known to have been stolen through the attacks. Even still, this episode represents one of the most striking espionage programs from the Chinese government to date.

The story reports that the chips were discovered and reported to the FBI by Amazon, which found them during due diligence ahead of its 2015 acquisition of Elemental Systems, a company that held a range of U.S. government contracts, and Apple, which is said to have deployed up to 7,000 Supermicro servers at peak. Bloomberg reported that Amazon removed them all within a one-month period. Apple did indeed cut ties with Supermicro back in 2016, but it denied a claim from The Information which reported at the time that it was based on a security issue.

Click **HERE** to read the article.

Cyberattack/Apps

The 6 most popular cyberattack methods hackers use to attack your business

(by Alison DeNisco Rayome | October 3, 2018)

Cyberattacks show no sign of slowing down this year, according to a Wednesday report from Positive Technologies. Q2 2018 saw a 47% increase in cyberattacks over Q2 2017, with targeted attacks outnumbering mass campaigns as cybercriminals grow more sophisticated. Most cases involved targeted attacks on companies and their clients, as well as cryptocurrency exchanges, the report found.

Data theft is driving an increasing number of attacks, with many criminals seeking personal data (30%), credentials (22%), and payment card information (15%). To steal this data, hackers are compromising online platforms, including e-commerce websites, online ticketing systems, and hotel booking sites, according to the report.

Attackers targeted cryptocurrency platforms twice as often in Q2 2018 as the year before, the report found: In May and June, a number of attacks affected Verge, Monacoin, Bitcoin Gold, ZenCash, Litecoin Cash, and others, with attackers stealing more than $100 million total from these platforms.

"Cyberattacks in Q2 victimized 765 million ordinary users to the tune of tens of millions of dollars," Leigh-Anne Galloway, cybersecurity resilience lead at Positive Technologies, said in a press release. "Today, you can never be sure that criminals don't have your credit card number from one source or another. Even when you buy a brand-new smartphone in a store, you can still end up getting pre-installed malware."

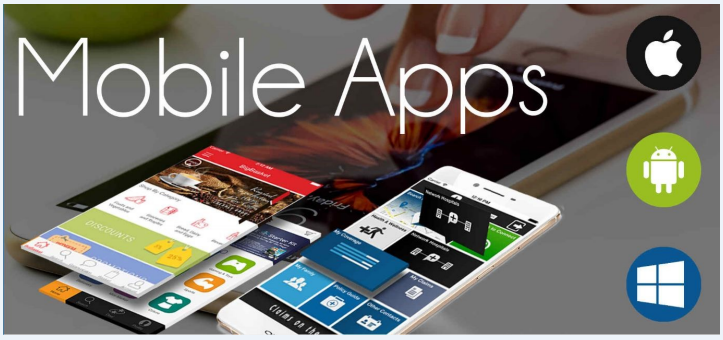
Click **HERE** to read more.

How 85% of mobile apps violate security standards

(by Alison DeNisco Rayome | October 4, 2018, 6:27 AM PST)

Cybercriminals are increasingly targeting mobile apps for attacks, due in part to lax security standards, according to a Thursday report from WhiteHat Security. The majority of mobile apps—85%—violate one or more of the Open Web Application Security Project (OWASP) Mobile Top 10, meaning they contain at least one common security vulnerability that can be exploited, the report found.

Half of the 15,000 applications analyzed in the report violated the OWASP standard for insecure data storage—the most common risk found. This means they may include data leakage in local files and system logs, client-side injection, and weak server-side controls. Android apps had a higher rate of violations in this area than iOS apps, the report found: 52% of Android apps included the world writable executable vulnerability, which could put data at risk—especially concerning for businesses, as GDPR is now in effect.



Close to half of all mobile apps tested also violated the OWASP standard for insecure communication, leaving those apps vulnerable to man-in-the-middle attacks. Some 30% of iOS apps still use insecure HTTP (compared to HTTPs), and more than 50% of iOS apps do not use the recommended Application Transport Security (ATS) method for secure encrypted communications, the report found.

On the other side of the spectrum, apps fared the best in authentication and authorization practices, according to the report. Very few mobile apps tested had CVSS-scored vulnerabilities, the report found, meaning developers are better at implementing access control and protection in mobile apps.

Click **HERE** to read more.

Routers/Phishing

Study Finds 83 Percent of Home Routers are Vulnerable to Attacks

(by Segiu Gatlan | Sep 27, 2018 09:25 GMT)

A study published by The American Consumer Institute found that out of a sample of 186 home routers, 83% of them were exposed to security attacks because of known vulnerabilities in their firmware.

The study, which used Insignary's Clarity to scan for and detect potential vulnerabilities in the routers' firmware, discovered that every sample router was vulnerable to an average of 172 exploits, with a total of 32,003 vulnerabilities found for the 186 routers sampled.


Router under attack

What's even more worrying is that out of all the security risks found to affect the examined routers, 28% of them had critical and high-risk vulnerabilities, with an average of 36 high risk and 12 critical attack vectors.

This is important to mention since critical and high-risk security flaws are a lot easier to be exploited and also come with a significant increase in the level of damage when compared to low and medium ranked weaknesses.

As detailed in the research (.PDF), all detected vulnerabilities had a CVE identifier in MITRE's public database, and some of the analyzed routers had more than one component exploitable using the same CVE identification number.

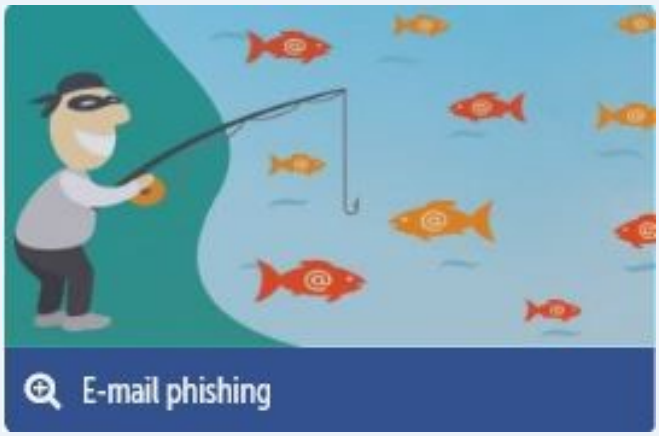
Click **HERE** to read more.

New Phishing Campaign Targets US Employees' Online Payrolls

(by Sergiu Gatlan | Sep 28, 2018 16:06 GMT)

The US Federal Bureau of Investigation (FBI) in collaboration with the Internet Crime Complaint Center (IC3) issued a public service announcement detailing a new phishing campaign targeting the online payrolls of US employees.

"The IC3 has received complaints reporting cybercriminals are targeting the online payroll accounts of employees in a variety of industries," says the report. "Institutions most affected are education, healthcare, and commercial airway transportation. "


E-mail phishing

According to multiple complaints received by IC3, threat actors are using social engineering techniques to gather information on employees to be able to devise custom phishing e-mails which ask for login credentials.

After the crooks get their hands on an employee's credentials, they go straight into their online payroll account and change the bank account information to redirect funds to their own.

The bad actors behind the phishing scheme are quite astute at what they're doing since they also take great care to disable any future direct deposit alerts reaching the victim's e-mail or phone.

Click **HERE** to read more.

3-Party Apps/Facebook

Third-Party Apps Using Facebook Login Also Affected by Latest Hacking Incident

(by Sergiu Gatlan | Oct 1, 2018 14:32 GMT)

Until now, there was no mention of other applications or platforms being affected by the Facebook chain of vulnerabilities which allowed attackers to compromise 50 million accounts.

Facebook logo

However, Guy Rosen, Facebook's VP of Product Management, did speak about third-party apps which use the Facebook login feature as being affected according to a public September 28 press call transcript (PDF).

Attackers who exploited a bug in the "View As" profile feature which helps users see their profile as other users would see them, were able to steal 50 million Facebook access tokens. Facebook also said that 40 million more accounts which have used the "View As" feature during the last year would be reset.

The security issue in the "View As" feature was introduced via a video uploading code change from July 2017 and Facebook found the bug on Tuesday, September 25, publicly announcing the issue on September 28.

As Rosen told the press in a press call, the Irish Data Protection Commission was notified about the breach to comply with Facebook's GDPR (General Data Protection Regulation) obligations.

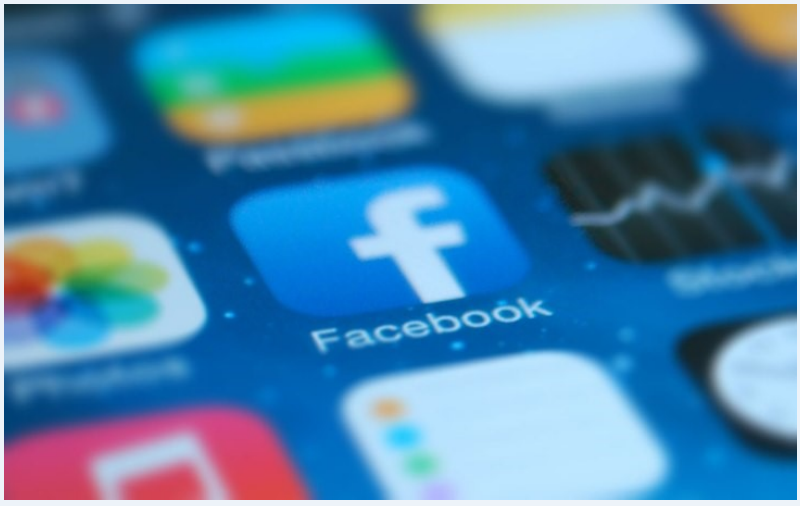
Click **HERE** to read more.

Yes Facebook is using your 2FA phone number to target you with ads

(by Natasha Lomas)

Facebook has confirmed it does in fact use phone numbers that users provided it for security purposes to also target them with ads.

Specifically a phone number handed over for two factor authentication (2FA) - a security technique that adds a second layer of authentication to help keep accounts secure.



Facebook's confession follows a story Gizmodo ran a story yesterday, related to research work carried out by academics at two U.S. universities who ran a study in which they say they were able to demonstrate the company uses pieces of personal information that individuals did not explicitly provide it to, nonetheless, target them with ads.

While it's been - if not clear, then at least *evident* - for a number of years that Facebook uses contact details of individuals who never personally provided their information for ad targeting purposes (harvesting people's personal data by other means, such as other users' mobile phone contact books which the Facebook app uploads), the revelation that numbers provided by Facebook by users in good faith, for the purposes of 2FA, are also, in its view, fair game for ads has not been so explicitly 'fessed up to before.

Some months ago Facebook did say that users who were getting spammed with Facebook notifications to the number they provided for 2FA was a bug. "The last thing we want is for people to avoid helpful security features because they fear they will receive unrelated notifications," Facebook then-CSO Alex Stamos wrote in a blog post at the time.

Click **HERE** to read more.

More News

Android password managers vulnerable to phishing apps

https://nakedsecurity.sophos.com/2018/09/28/mobile-password-managers-vulnerable-to-phishing-apps/

Hackers Report Cites 'Staggering' Vulnerabilities in U.S. Voting Systems
https://www.nextgov.com/cybersecurity/2018/09/hackers-report-cites-staggering-vulnerabilities-us-voting-systems/151637/

Mattis predicts DoD will one day offer cyber protection to private sector
https://www.nextgov.com/cybersecurity/2018/09/hackers-report-cites-staggering-vulnerabilities-us-voting-systems/151637/

Hackers are finding creative ways to target connected medical devices
https://www.helpnetsecurity.com/2018/09/28/target-connected-medical-devices/

Instagram is testing the ability to share your precise location history with Facebook
https://www.theverge.com/2018/10/5/17940364/instagram-location-sharing-data-sharing-facebook-test

Facebook bug prevented users from deleting their accounts
https://venturebeat.com/2018/10/04/facebook-bug-prevented-users-from-deleting-their-accounts/

Police Use Fitbit Data to Charge 90-Year-Old Man in Stepdaughter's Killing
https://www.nytimes.com/2018/10/03/us/fitbit-murder-arrest.html

Fully driverless @aymo taxis are due out this year, alarming critics
https://arstechnica.com/cars/2018/10/waymo-wont-have-to-prove-its-driverless-taxis-are-safe-before-2018-launch/

Remote Access System Hacking Is No. 1 Patient Safety Risk
https://healthitsecurity.com/news/remote-access-system-hacking-is-no.-1-patient-safety-risk

Hackers selling Facebook logins on the dark web for $2
https://nypost.com/2018/10/01/hackers-are-selling-facebook-logins-on-the-dark-web-for-2/

More News

That sign telling you how fast you're driving may be spying on you

https://qz.com/1400791/that-road-sign-telling-you-how-fast-youre-driving-may-be-part-of-a-us-government-surveillance-network/

Feds Force Suspect To Unlock An Apple iPhone X With Their Face

https://www.forbes.com/sites/thomasbrewster/2018/09/30/feds-force-suspect-to-unlock-apple-iphone-x-with-their-face/#174207ad1259

FBI solves mystery surrounding 15-year-old Fruitfly Mac malware

https://www.zdnet.com/article/fbi-solves-mystery-surrounding-15-year-old-fruitfly-mac-malware/

Social engineering attacks skyrocket more than 500 percent

https://www.fifthdomain.com/industry/2018/09/26/social-engineering-attacks-skyrocket-more-than-500-percent/

Boffins bypass password protection with pilfering by phony programs

https://www.theregister.co.uk/2018/09/26/password_manager_theft/

Kids as young as 7 are finding ingenious ways around Apple's screen time controls

https://finance.yahoo.com/news/kids-young-7-finding-ingenious-101635503.html

How a malicious USB could lead to a years-long cryptomining infection on your PC

https://www.techrepublic.com/article/how-a-malicious-usb-could-lead-to-a-years-long-cryptomining-infection-on-your-pc/

With USB-C, even plugging in can set you up to be hacked

https://gcn.com/articles/2018/09/24/usbc-vulnerabilities.aspx?admgarea=TC_SecCybersSec

Phone Phishing Level Ups: Smart Slaves to Digital Wizardry

http://www.ehackingnews.com/2018/10/phone-phishing-level-ups-smart-slaves.html

'Desperate' North Korea turns to bank hacking sprees to rake in much-needed dosh

https://www.theregister.co.uk/2018/10/03/north_korea_tcash/

</Closing Comments>

User Suggested:

I want to thank a reader in our CJIS department who suggested the following websites for readers:

Security Tip (ST18-004) from US-CERT

This website talks about malicious code and then gives examples from US-CERT how you protect yourself against them. It also talks about what you should know about antivirus software as well as how to recover if you become a victim of malicious code. The article is a good read and gives lots of useful information.

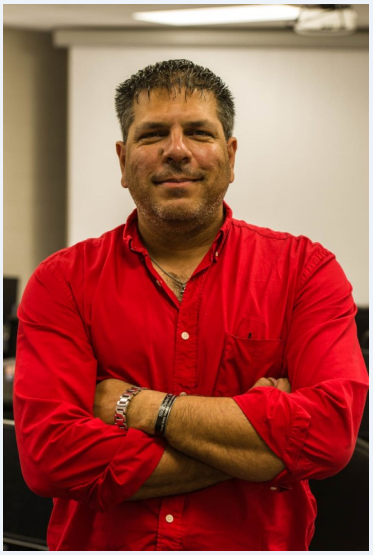
Click **HERE** to read the article.

Red Team vs. Blue Team Which Are You?

The best offense is a good defense, which is why cybersecurity has two teams - the red team (offense) and the blue team (defense). Each side requires a very particular set of skills, and the two balance each other out to protect an organization. Whether you're trying to decide which way to take your career or you want to confirm that you've picked the right side, take our quiz to see if your skills align better with the red team or blue team.

To take the quiz, click **HERE**.

Hopefully you found this Cybersecurity Newsletter informative and useful. Remember it is the Halloween season and there will be children Trick-or-Treating on Halloween as well as possibly running around for Halloween parties all month. Please be watchful for the little ghouls, goblins, princesses, etc. Also remember people will be attending parties and not everyone is wise enough to have a designated driver or other safe way home. So be careful as we enter the holiday season so you can keep yourself and your family safe.



As a reminder, all newsletters are posted on a public facing DPS website. Feel free to look at past newsletters and/or share the link with your friends. You can find the link by clicking on the General Info tab at http://www.dps.texas.gov/. In the tab you will see a link for Cyber Security Newsletter. Click the link and it will take you to a page with all of the newsletters created for the last two years.

For those of you brave enough to try, enjoy this month's Cyber Challenges found on the next page. Good Luck

Happy Cybersecurity Awareness Month and Happy Halloween.

Kirk

Cyber Challenge

Employees Who Solved Last Month's Challenge and Notified Me

Below are the people who emailed me with the solution to last month's challenge. The date and times listed are the timestamp on the email they sent with the correct answer. Congratulations to these individuals.

David Evans @ 1056 on 18 Sept	Jennifer Taylor @ 1840 on 18 Sept	Tracy Kingsley @ 0954 on 19 Sept
Erich Neumann @ 1240 on 18 Sept	Deborah Wright @ 1937 on 18 Sept	Jimmy Ferrer @ 1042 on 19 Sept
Nirav Kumar @ 1412 on 18 Sept	Gustavo Reina @ 0819 on 19 Sept	Rene Hess @ 0232 on 20 Sept

For those who weren't able to figure out the challenge and would like to know, email me and I'll tell you how to solve the challenge.

For this month's challenge I am giving three challenges. There will be one for beginners, a more advanced challenge, and then the third one is a much more difficult assignment. Please email me with what you are able to solve.

First Challenge:

I am a ransomware program that reportedly makes my creators $300,000 a month and no one is sure who created me. I have been in the news recently affecting a major US city as well as other locations. What is my name?

Second Challenge:

U21nIDUgYmN6Z3ZxZ2JydmFzYyBsdmZic2FiZ3EgZ3BndmMgZ2Rsb25jZ2cgcW1ucm9oIHdub29uazogMSkgVmdm
b2F0ZyBjbnIgZnZnIGZ5IGZzc3ZmYnNhcGcgc2Z2aWdzLiBZZ3BndiBzbWF5ZSAiQXMga255J3MgbWZsbGd5IHNuI
GRnLiIgMikgTHZmYnNhYmcgaW5uaCBsZnFxa252aCBkZnlmaWdkZ3lzLiAzKSBZZ3BndiBvZ2ZwZyBjbnJ2IGhnc
GFiZ3Egcnlmc3NneWhnaC4gNCkgRm9rZmNxIHpnIGJmdmd3cm8ga21neSBib2FiZWF5aSBueSBmc3NmYm1kZ3lzc
SBudiBvYXllcSBheSBnZGZhby4gNSkgUWd5cWFzYXBnIHp2bmtxYXlpLCBxcmJtIGZxIHpmeWVheWkgbnYgcW1
ubGxheWksIHFtbnJvaCBueW9jIHpnIGhueWcgbnkgZiBoZ3BhYmcgc21mcyB6Z29ueWlxIHNuIGNuciwgZnloIG55IG
YgeWdza252ZSBjbnIgc3ZycXMu

Third Challenge:

The final challenge is a Steganography challenge that is much more difficult than the previous ones I have provided.

GOOD LUCK with the challenges.

Kirk