On July 22, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Cisco and Apple products.

Threat Level's explained

- **GREEN or LOW** indicates a low risk.
- **BLUE or GUARDED** indicates a general risk of increased hacking, virus, or other malicious activity.
- **YELLOW or ELEVATED** indicates a significant risk due to increased hacking, virus, or other malicious activity that compromises systems or diminishes service.
- **ORANGE or HIGH** indicates a high risk of increased hacking, virus, or other malicious cyber activity that targets or compromises core infrastructure, causes multiple service outages, causes multiple system compromises, or compromises critical infrastructure.
- **RED or SEVERE** indicates a severe risk of hacking, virus, or other malicious activity resulting in widespread outages and/or significantly destructive compromises to systems with no known remedy or debilitates one or more critical infrastructure sectors.

WEEKLY IT SECURITY BULLETIN

24 July 2020

In The News This Week

Garmin services and production go down after ransomware attack

Smartwatch and wearables maker Garmin has shut down several of its services on July 23 to deal with a ransomware attack that has encrypted its internal network and some production systems. The company is currently planning a multi-day maintenance window to deal with the attack's aftermath, which includes shutting down its official website, the Garmin Connect user data-syncing service, Garmin's aviation database services, and even some production lines in Asia. In messages shared on its website and Twitter, Garmin said the same outage also impacted its call centers, leaving the company in the situation of being unable to answer calls, emails, and online chats sent by users. The incident didn't go unnoticed and has caused lots of headaches for the company's customers, most of which rely on the Garmin Connect service to sync data about runs and bike rides to Garmin's servers, all of which went down on Thursday 23 July 2020. Read the full story here: ZDNet Article

Hackers using pirated software to spread new cryptomining Mac malware

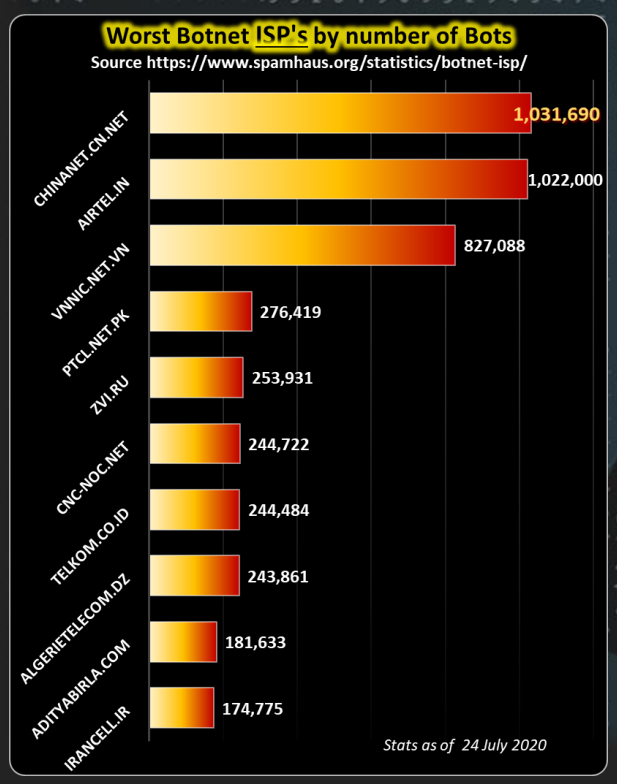
If you download pirated content from torrent platforms, you can be a victim of this Mac malware. - There is a new variant of cryptomining malware that is specifically targeting Apple's Mac devices and those users who prefer downloading pirated software from torrent platforms. Dubbed Bird Miner by researchers; this cryptocurrency mining malware is actually a strain of malicious code with a very interesting twist – This Mac malware emulates Linux or Mac to run. Initially, the malware was discovered as OSX.BirdMiner in a pirated Ableton Live 10 software installer, which is basically software used commonly to create music. Later on, researchers detected it in other files and Reddit users report that in the past four months or maybe longer than that they have observed the similar type of Mac malware distributed via the VST Crack website. According to the details shared by Malwarebytes earlier, the first thing that Bird Miner does to keep itself hidden from the user's detection is by checking for Activity Monitor. If this system tool isn't running and the CPU usage is lower than 85%, this Mac malware runs the open source Qemu OS virtual box that loads and runs a wide range of OS image files including .img, .iso, or .dmg. In fact, Qemu loads Tiny Core Linux custom versions as two .dmg images prior to launching the Xmrig cryptomining tool.
Read the full article here: HackRead

Hackers Can Now Trick USB Chargers To Destroy Your Devices—This Is How It Works

Not all cyber attacks focus on data theft. Sometimes the intent is "to achieve destruction of the physical world through digital means," Chinese tech giant Tencent warns. The company's researchers have just disclosed a serious new vulnerability in many of the mass-market fast chargers now used around the world. When you connect your device to a fast charger with a USB cable, there is a negotiation between the two, establishing the most powerful charge the device can safely handle. This negotiation is managed between the firmware on the device and the firmware on the charger, and assumes both will play nicely with one another. But Tencent's researchers have now proven that a compromised charger can override this negotiation, pushing more power down the cable than the device can safely handle, likely destroying the device and potentially even setting it on fire.
Read more here: Forbes *(Thank you to my good friend Yazan Shapsugh who pointed me to this story. Also see related article about "Juice Jacking" & USBHarpoons in the January 17th Edition of this bulletin)*

Cybersecurity at risk after hackers try to sabotage Premier League transfer deal

Professional sports organisations have been urged to tighten their cybersecurity after it was revealed hackers attempted to sabotage a Premier League transfer deal. The National Cyber Security Centre (NCSC) said the email address of a Premier League club's managing director had been hacked during a transfer negotiation and only intervention from the bank prevented the club losing around £1m.
Read the full story here: TheGuardian



For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov

Crypto Currency (Bitcoin) Scams

In a conversation this week, the topic of crypto currency scams and fraud came up and I thought it would be a good topic to cover. However, this is one area that I'm not very knowledgeable about, so I've put my Google boots on and traversed through the vast online jungle to see what people wrote about it. I came across a good article by Anne Sraders of the investment magazine TheStreet, looking at the top 7 scams. Below is an adapted and shortened version of the article, but I urge you to visit their web page for the full article and many other interesting facts including investment news on cannabis ☺.

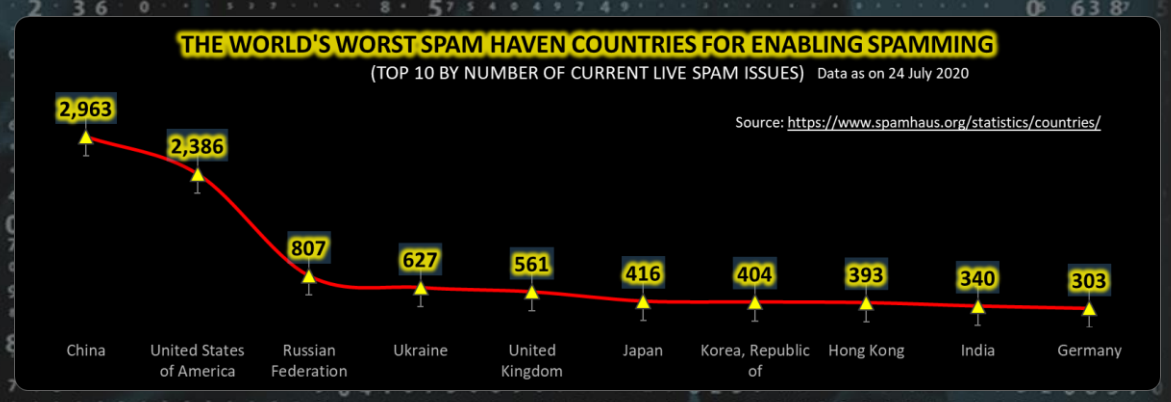
Bitcoin, the possible Pandora's Box of the currency world - has never been short of controversy. Whether it be aiding the black market or scamming users out of millions, bitcoin is no stranger to the front page. Still, the jury is out on the legality and usefulness of bitcoin - leaving it in a proverbial grey area. However, there have been several infamous bitcoin scams, and you need to know about them. Listed below are the top 7 bitcoin scams according to Anne.

What Is a Bitcoin Scam? - For most cases, it may be pretty obvious what a scam is - but with bitcoin, and cryptocurrency in general, things become murkier. Bitcoin itself is an unregulated form of currency that essentially is a mere number that is only given value because of an agreement. It's basically like a moneybag with a lock on it - the code of which is given to the recipient of the bitcoin (an analogy drawn by Forbes in 2017). Bitcoin scams have been famously criminal and public in nature. With no bank as a middleman in exchange, things become more complicated; so hackers and con men have had a heyday.

Top 7 Bitcoin Scams

There have been nearly countless bitcoin scams, but these frauds make the list of the top 7 worst bitcoin scams to date.

1. Malware Scams - Malware has long been the hallmark of many online scams. But with cryptocurrency, it poses an increased threat. Recently, a tech support site, Bleeping Computer, issued a warning about cryptocurrency-targeting malware. "This type of malware, called CryptoCurrency Clipboard Hijackers, works by monitoring the Windows clipboard for cryptocurrency addresses, and if one is detected, will swap it out with an address that they control," wrote Lawrence Abrahams of Bleeping Computer. The malware, CryptoCurrency Clipboard Hijackers (which reportedly manages 2.3 million bitcoin addresses) switches addresses used to transfer cryptocoins with ones the malware controls - thus transferring the coins to the scammers instead.
2. Fake Bitcoin Exchanges – BitKRX - Surely one of the easiest ways to scam investors is to pose as an affiliate branch of a respectable and legitimate organization. Well, that's exactly what scammers in the bitcoin field are doing. South Korean scam BitKRX presented itself as a place to exchange and trade bitcoin, but was ultimately fraudulent. The fake exchange took on part of the name of the real Korean Exchange (KRX), and scammed people out of their money by posing as a respectable and legitimate cryptocurrency exchange. The scam was exposed in 2017.
3. Ponzi Scheme – MiningMax - "Ponzi bitcoin scam" has got to be the worst combination of words imaginable for financial gurus. Several organizations have scammed people out of millions with Ponzi schemes using bitcoins, including South Korean website MiningMax. The site, which was not registered with the U.S. Securities and Exchange Commission, promised to provide investors with daily ROI's in exchange for an original investment and commission from getting others to invest (basically, a Ponzi scheme). Apparently, the site was asking people to invest $3,200 for daily ROI's over two years, and a $200 referral commission.
4. Fake Bitcoin Scam - My Big Coin - A classic (but no less dubious) scam involving bitcoin and cryptocurrency is simply, well, fake currency. One such arbiter of this faux bitcoin was My Big Coin. Essentially, the site sold fake bitcoin. Plain and simple. In early 2018, My Big Coin, a cryptocurrency scam that lured investors into sinking an alleged $6 million, was sued by the U.S. Commodity Futures Trading Commission.
5. ICO Scam - Bitcoin Savings and Trust and Centra Tech - Still other scammers have used ICO's - initial coin offerings - to dupe users out of their money. Along with the rise in blockchain-backed companies, fake ICOs became popular as a way to back these new companies. However, given the unregulated nature of bitcoin itself, the door has been wide open for fraud. Most ICO frauds have taken place through getting investors to invest in or through fake ICO websites using faulty wallets, or by posing as real cryptocurrency-based companies. Notably, $32 million Centra Tech garnered celebrity support (most famously from DJ Khaled), but was exposed for ICO fraud back in April of 2018, according to Fortune. The company was sued for misleading investors and lying about products, among other fraudulent activities.
6. Bitcoin Gold Scam - mybtgwallet.com - Nothing catches the eye of the naïve quite like the promise of gold - bitcoin gold, of course. That is exactly what mybtgwallet.com did to unsuspecting bitcoin investors. According to CNN, the bitcoin gold (BTG) wallet duped investors out of $3.2 million in 2017 by promising to allow them to claim their bitcoin gold. The website allegedly used links on a legitimate website (Bitcoin Gold) to get investors to share their private keys or seeds with the scam. Before the scam was done, the website managers (slash scammers) was able to get their hands on $107,000 worth of bitcoin gold, $72,000 of litecoin, $30,000 of ethereum, and $3 million of bitcoin, according to CNN.
7. Pump and Dump Scam - A pump-and-dump scam is especially dangerous in the internet space. The basic idea is that investors hype up (or "pump up") a certain bitcoin - that is usually an alternative coin that is very cheap but high risk - via investor's websites, blogs, or even Reddit, according to The Daily Dot. Once the scammers pump up a certain bitcoin enough, skyrocketing its value, they cash out and "dump" their bitcoin onto the naïve investors who bought into the bitcoin thinking it was the next big thing.



Author: Chris Bester (CISA,CISM)
chris.bester@yahoo.com