On September 2, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded). The MS-ISAC is aware of high levels of exploit activity targeting out-of-date web servers, as well as attempts to gain access through password brute force attempts against login prompts on web pages. Organizations and users are advised to apply all vendor security patches.

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
04 September 2020

In The News This Week

CenturyLink outage led to a 3.5% drop in global web traffic

US internet service provider CenturyLink has suffered a major technical outage on Sunday after a misconfiguration in one of its data centres created havoc all over the internet. Due to the technical nature of the outage, involving both firewall and BGP routing, the error spread outward from CenturyLink's network and also impacted other internet service providers, ending up causing connectivity problems for many more other companies. The list of tech giants who had services go down today because of the CenturyLink outage includes big names like Amazon, Twitter, Microsoft (Xbox Live), EA, Blizzard, Steam, Discord, Reddit, Hulu, Duo Security, Imperva, NameCheap, OpenDNS, and many more. Cloudflare, which was also severely impacted today, said CenturyLink's outward-propagating issue led to a 3.5% drop in global internet traffic, which would make this one of the **biggest internet outages ever recorded**. Root cause is said to be a misconfigured Flowspec rule.
Read the full story here: ZDNet Article

US DoJ Wish To Seize 280 Cryptocurrency Accounts Used By Hackers!

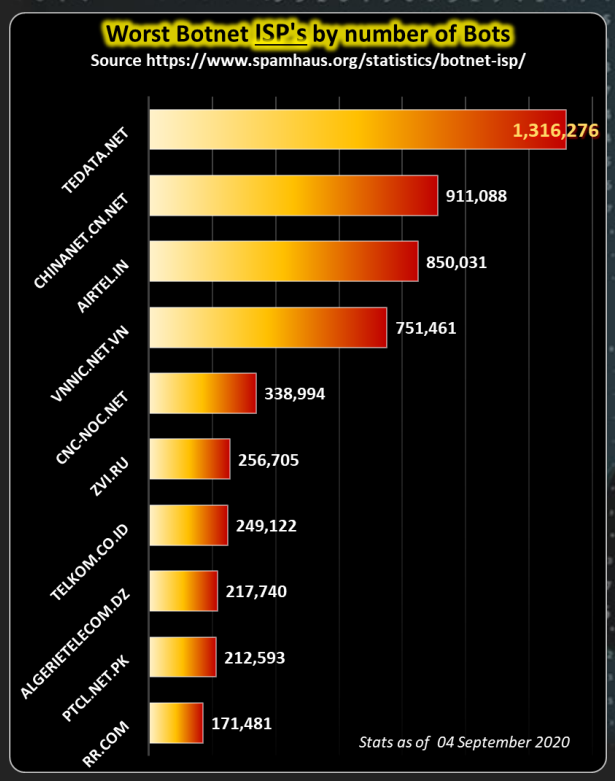
The North Korean saga continues - The US Govt. aims to gain control of 280 illegal cryptocurrency accounts that it says were used by N. Korean state-sponsored attackers in their efforts to hack cryptocurrency exchanges & channel 100s of millions in stolen money through a Chinese money-laundering network. The US Department of Justice (DoJ) filed a civil forfeiture complaint against N. Korea on Thurs. as part of a bigger effort to close down that it explained were state-sponsored cyber-attacks on currency exchanges by hackers. The charge details 2 specific attacks against virtual currency exchanges in 2019 allegedly carried out by N. Korean hackers. The US DoJ also claims threat players in China were involved & helped launder over $250m stolen from more than 12 exchanges. "Today's action publicly exposes the ongoing connections between N. Korea's cyber-hacking program & a Chinese cryptocurrency money-laundering network," Acting US Assistant Attorney General Brian Rabbitt of the DoJ's Criminal Division commented in a press statement. Read the full story here: CyberNewsGroup

Apple Approved Malware Hits macOS 'For The First Time'

MacOS is thought of as more secure than Microsoft's Windows, but the amount of malware targeting Apple's operating system is growing. Apple has taken steps to mitigate malware on macOS through a process called notarization—but even this can be bypassed by new and improved adware, a security researcher has discovered. The adware campaign uses notarized malware, meaning it was scanned and "approved" by Apple and will run on Catalina and BigSur, security researcher Patrick Wardle has found. "As far as I know, this is the first time hackers have been able to abuse Apple's new notarization," Wardle told Kate O'Flaherty at Forbes. Read the full article by Kate O'Flaherty here: Forbes *(Thanks to My good friend Yazan Shapsugh who pointed me to this story)*

Warner Music discloses months-long web skimming incident

On Thursday, Music recording powerhouse Warner Music Group has disclosed a security incident that involved some of the company's online stores. Called "web skimming" or "**magecart,**" this type of attack happens when hackers take control over a website and insert malicious code that logs customer details entered inside payment forms. In a data breach notification letter filed today with the Office of the Attorney General in the state of California, Warner Music said it suffered one such attack earlier this year. Between April 25 and August 5, Warner Music said hackers compromised "a number of US-based e-commerce" that were "hosted and supported by an external service provider. "Any personal information you entered into one or more of the affected website(s) between April 25, 2020 and August 5, 2020 after placing an item in your shopping cart was potentially acquired by the unauthorized third party," the company said. "This could have included your name, email address, telephone number, billing address, shipping address, and payment card details (card number, CVC/CVV and expiration date)." Payments made through PayPal were not impacted, Warner Music added. Read the full story here: ZDNet Article



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

Blockchain, what is it and how does it work?

If you dabble in the relatively new realm of crypto currencies, you are presented with a myriad of terminologies , names and ellipses of some sort that can be a bit confusing for both the novice and experienced trader. These include anything from, "Mining", "Genesis Block", "Laddering", "Hot Wallet", "Cold Storage, "Hash Rate", and the list goes on. Today I want to explore "Blockchain", what it is, how it works and some notes on privacy. In my research, I came across a few sources that attempt to explain blockchain in a digestible format, but I found the explanation in an article on Investopedia to be a simple but descriptive piece that most of us can handle. Following is an extract of the article but please visit the page to get a complete view Investopedia. Also check out the article in Blockgeeks and the other sources listed here: Mobidea, Deloitte, Blockgeeks

What is Blockchain?

If this technology is so complex, why call it "blockchain?" At its most basic level, blockchain is literally just a chain of blocks, but not in the traditional sense of those words. When we say the words "block" and "chain" in this context, we are actually talking about digital information (the "block") stored in a public database (the "chain").
"Blocks" on the blockchain are made up of digital pieces of information. Specifically, they have three parts:

1. Blocks store information about transactions like the date, time, and dollar amount of your most recent purchase from Amazon. (NOTE: This Amazon example is for illustrative purchases; Amazon retail does not work on a blockchain principle as of this writing)
2. Blocks store information about who is participating in transactions. A block for your splurge purchase from Amazon would record your name along with Amazon.com, Inc. (AMZN). Instead of using your actual name, your purchase is recorded without any identifying information using a unique "digital signature," sort of like a username.
3. Blocks store information that distinguishes them from other blocks. Much like you and I have names to distinguish us from one another, each block stores a unique code called a "hash" that allows us to tell it apart from every other block. Hashes are cryptographic codes created by special algorithms. Let's say you made your splurge purchase on Amazon, but while it's in transit, you decide you just can't resist and need a second one. Even though the details of your new transaction would look nearly identical to your earlier purchase, we can still tell the blocks apart because of their unique codes.

While the block in the example above is being used to store a single purchase from Amazon, the reality is a little different. A single block on the Bitcoin blockchain can actually store around 1 MB of data. Depending on the size of the transactions, that means a single block can house a few thousand transactions under one roof.

How Blockchain works

When a block stores new data it is added to the blockchain. Blockchain, as its name suggests, consists of multiple blocks strung together. In order for a block to be added to the blockchain, however, four things must happen:

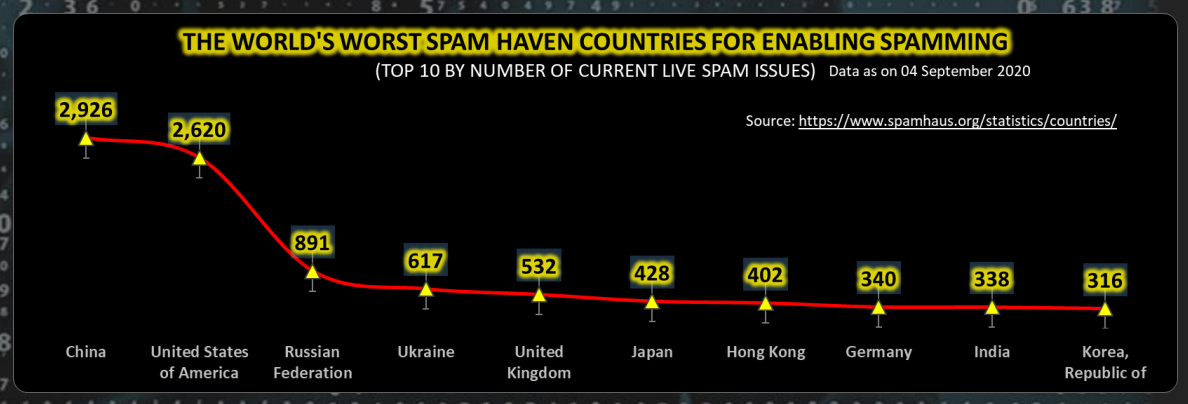
1. A transaction must occur. Let's continue with the example of your impulsive Amazon purchase. After hastily clicking through multiple checkout prompt, you go against your better judgment and make a purchase. As we discussed above, in many cases a block will group together potentially thousands of transactions, so your Amazon purchase will be packaged in the block along with other users' transaction information as well.
2. That transaction must be verified. After making that purchase, your transaction must be verified. With other public records of information, like the Securities Exchange Commission, Wikipedia, or your local library, there's someone in charge of vetting new data entries. With blockchain, however, that job is left up to a network of computers. When you make your purchase from Amazon, that network of computers rushes to check that your transaction happened in the way you said it did. That is, they confirm the details of the purchase, including the transaction's time, dollar amount, and participants. (More on how this happens in a second.)
3. That transaction must be stored in a block. After your transaction has been verified as accurate, it gets the green light. The transaction's dollar amount, your digital signature, and Amazon's digital signature are all stored in a block. There, the transaction.
4. That block must be given a hash. Not unlike an angel earning its wings, once all of a block's transactions have been verified, it must be given a unique, identifying code called a hash. The block is also given the hash of the most recent block added to the blockchain. Once hashed, the block can be added to the blockchain.

When that new block is added to the blockchain, it becomes publicly available for anyone to view—even you. If you take a look at Bitcoin's blockchain, you will see that you have access to transaction data, along with information about when ("Time"), where ("Height"), and by who ("Relayed By") the block was added to the blockchain.

Is Blockchain Private?

Anyone can view the contents of the blockchain, but users can also opt to connect their computers to the blockchain network as nodes. In doing so, their computer receives a copy of the blockchain that is updated automatically whenever a new block is added, sort of like a Facebook News Feed that gives a live update whenever a new status is posted. Each computer in the blockchain network has its own copy of the blockchain, which means that there are thousands, or in the case of Bitcoin, millions of copies of the same blockchain. Although each copy of the blockchain is identical, spreading that information across a network of computers makes the information more difficult to manipulate. With blockchain, there isn't a single, definitive account of events that can be manipulated. Instead, a hacker would need to manipulate every copy of the blockchain on the network. This is what is meant by blockchain being a "distributed" ledger.

That is all I have space for in this week's bulletin but please read the full article to learn more about how it is secured, encryption methods, and how a user group called "Bitfury" was able to manipulate some aspects of the "Blockchain" - Investopedia



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