On January 19, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Zoho and Oracle products.
CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
21 Jan	343,323,364	5,593,646

Deaths this week: 54,225

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
21 January 2022

In The News This Week

Beijing Olympics App Flaws Allow Man-in-the-Middle Attacks

Attackers can access audio and files uploaded to the MY2022 mobile app required for use by all winter games attendees – including personal health details. The mobile app that all attendees and athletes of the upcoming Beijing Winter Olympics must use to manage communications and documentation at the event has a "devastating" flaw in the way it encrypts data that can allow for man-in-the-middle attacks that access sensitive user information, researchers have found. MY2022 is an app mandated for use by all attendees – including members of the press and athletes – of the 2022 Olympic Games in Beijing. The problem is, it poses a significant security risk because the encryption used to protect users' voice audio and file transfers "can be trivially sidestepped" due to two vulnerabilities in how it handles data transport, according to a blog post from Citizen Lab posted online Tuesday. Read the rest of the story by Elizabeth Moltalbano here: ThreatPost

FBI warning: Crooks are using fake QR codes to steal your passwords and money

As businesses turned to QR codes for contactless payments during the pandemic, scammers seized on the trend to steal cash and financial credentials.- QR codes are useful shortcuts to online resources via a phone's camera, but scammers are now tampering with them to direct victims to phishing pages and cryptocurrency scams. QR or 'Quick Response' codes have been connecting scanners to real-world objects since the 1990s, but got widely adopted during the pandemic as businesses moved to contactless communication and payments via QR codes on restaurant menus, parking meters and other public spaces. But scammers are now targeting the QR code's increased familiarity by tampering with the pixelated barcodes and redirecting victims to sites that steal logins and financial information, according to an FBI alert... Read the rest of the article by Liam Tung here : ZDNet

Nigerian Police Arrest 11 Individuals in BEC Crackdown

Police in Nigeria, with the help of Interpol, have arrested 11 individuals in the country for their alleged involvement in **B**usiness **E**mail **C**ompromise (BEC) scams associated with more than 50,000 targets worldwide. Six of those arrested were identified as members of SilverTerrier, a known BEC gang that is thought to have harmed thousands of companies globally and has successfully evaded prosecution for more than five years.
A laptop belonging to one of the 11 alleged BEC operatives contained some 800,000 user names and credentials belonging to potential victim organizations. Another arrested individual was found to have been monitoring conversations between 16 companies and their customers, as well as attempting to divert money to SilverTerrier accounts when transactions between them were about to be made, Interpol said Wednesday.
Read the story by Jai Vijayan here: Darkreading

Red Cross cyberattack sees data of thousands at-risk people stolen

A supply chain attack has resulted in the data of more than half a million "highly vulnerable people" stolen from Red Cross systems. A contractor for the Swiss-based International Committee of the Red Cross (ICRC) fell victim to a cyberattack recently, with unknown malicious actors making away with sensitive data on more than 515,000 individuals. And not just any individuals - people who got separated from their families through conflict, migration, or natural disasters, missing persons and their families, as well as people in detention. The data that was stolen came from at least 60 Red Cross and Red Crescent "national societies", comprising of information on staff, volunteers, first respondents, as well as those affected by various tragedies.
Read the rest of the article here: TechRadar & BBC

Poland raises cybersecurity terror threat after Ukraine cyber attack

WARSAW, Jan 18 (Reuters) - Poland on Tuesday raised its nationwide cybersecurity terror threat in the wake of a cyber attack on Ukraine last week, adding that the new alert level was preventative. Last week, Ukraine was hit by a cyber attack that warned Ukrainians to "be afraid and expect the worst" as the country braces for a possible new military offensive from neighbouring Russia. Ukrainian officials say the attack hit around 70 internet sites of government bodies including the security and defence council, the cabinet of ministers and several ministries..
Read the rest of the article here: Reuters

Blockchain explained in layman's terms

If you are dabbling in the cryptocurrency scene, you would have heard or read about all the concerns around cyber security and how the whole thing is designed to keep everything above board. In among the noise, you would have come across the term "Blockchain" which is really the main building block making cryptocurrency transactions possible. It is essentially a system in which a record of transactions made in bitcoin or another cryptocurrency is maintained across a multitude of computers that are linked in a peer-to-peer network. The aim today is then to try and give a layman's view of what a blockchain is and how the underlying technology works to secure transactions in cryptocurrencies like Bitcoin, Ethereum, Tether, Litecoin, and so on.
While doing my research on the subject, I found a short and simple explanation written by Rob Hibbard in the Level Up Coding publication a while back that I'll share below.

"Often blockchain technology is explained in technical terms that sound foreign to most people, leaving most them feeling more confused than when they started. Instead, this article will focus on how to explain blockchain to someone who does not have an IT background.

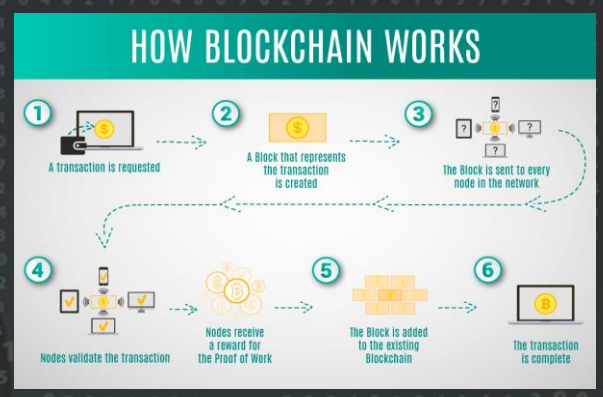
At its core, the blockchain can be thought of as a shared database populated with entries that have been verified and encrypted. In other words, the blockchain is a shared transaction log with a non-editable history and built-in security. The simplest comparison is to an accounting record book. Each "block" is really just a "line item" in the shared record book. Every time a new block is added to the chain, a new line item is added to the book. The book can contain all kinds of information, not just financial transactions.
The "shared" component refers to the fact that the record book isn't stored in one central location. Instead, thousands of copies are stored all around the world in home computers and business servers. This is why the blockchain is often described as "decentralized" or distributed. Even though thousands of copies of the record book are stored all over the world, that does not necessarily mean that anyone with a copy of the record book can read the information inside. Blockchains like Hyperledger are developed with enterprise needs in mind and include built-in securities features that can be set up to only share the information with certain people.

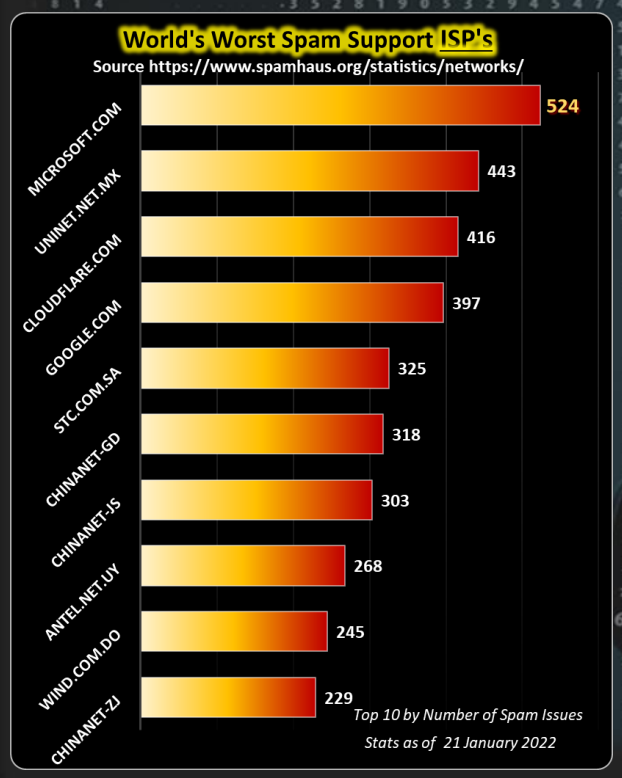
Before a line item can be added to the record book, the transaction information has to be confirmed by multiple computers who have a copy of the record history. The computers make sure every detail of the transaction is authorized and legitimate before agreeing (or disagreeing) on approval to add the line item to the record book. Once the record is added, it cannot be changed. The line item has to perfectly match in every copy of the record book. This verification process is why blockchain's history cannot be edited. If anyone attempts to modify a record, it will be rejected since the entire network has proof that the entry is invalid.
The verification process can be compared to paying your friend, Sam, with hundreds of friends circled around you. Everyone watched you hand the money to Sam and, if asked, would all agree that the money has been handed over. They could also confirm other details of the transaction, such as the amount paid, location, and time.

This is only a high-level explanation of blockchain technology, and you likely still have lots of questions. However, you should now understand the basics of how blockchain technology works and have the foundation required to work towards an even stronger understanding."

MLSDev provides this simple schematic on their site to give you a visual representation of how a cryptocurrency transaction traverse through the blockchain and how it is validated. You will also see where in the chain rewards are offered and where the concept of crypto mining comes in.
As described by PCMag, "Crypto mining or Bitcoin Mining is the process by which new units of digital currency are made, or "minted," and introduced into the market."
Crypto mining is a costly affair that needs lots of processing resources, and as you know, in the cybersecurity world, we are constantly battling with criminals taking over private or company machines to create Botnets to do their crypto mining for them.

Resources: Investopedia, CoinMarketCap, MLSDev, Level Up, PCMag, Darktrace, Kaspersky, PWC

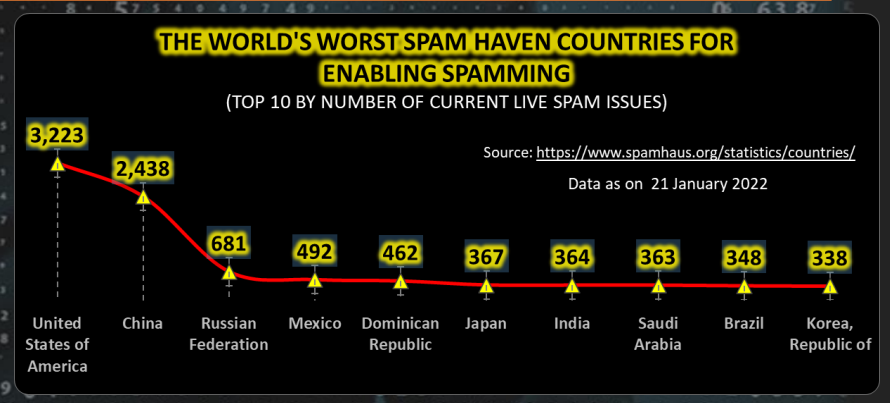




For Reporting Cyber Crime in the USA go to the Internet Crime Complaint Center (IC3)

Other Interesting News and Cyber Security bits:

- Intel orders ASML system for well over $340 million in quest for chipmaking edge
- Here's What Scientists Know About the Tonga Volcano Eruption
- Beijing 2022 Olympic Schedule
- SANS Daily Network Security Podcast (Stormcast)



AUTHOR: CHRIS BESTER (CISA,CISM)
chris.bester@yahoo.com