On November 4, 2020, the Cyber Threat Alert Level was evaluated and is being lowered to Blue (Guarded) due to vulnerabilities in Mozilla and Cisco products and for heightened awareness of cyber activity in during the US General Election.

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

06 November 2020

In The News This Week

Russian cybercriminal sentenced to prison for $100 million botnet conspiracy

A Russian national was sentenced Oct. 30 to eight years in prison for his role in operating a sophisticated scheme to steal and traffic sensitive personal and financial information in the online criminal underground that resulted in an estimated loss of over $100 million. Aleksandr Brovko, 36, formerly of the Czech Republic, pleaded guilty in February to conspiracy to commit bank and wire fraud. According to court documents, Brovko was an active member of several elite, online forums designed for Russian-speaking cybercriminals to gather and exchange their criminal tools and services. "For over a decade, Brovko participated in a scheme to gain access to Americans' personal and financial information, causing more than $100 million in intended loss," said Acting Assistant Attorney General Brian C. Rabbitt of the Justice Department's Criminal Division. Read the full story: SecurityMag

Barbie hacked: Toymaker Mattel targeted in ransomware attack

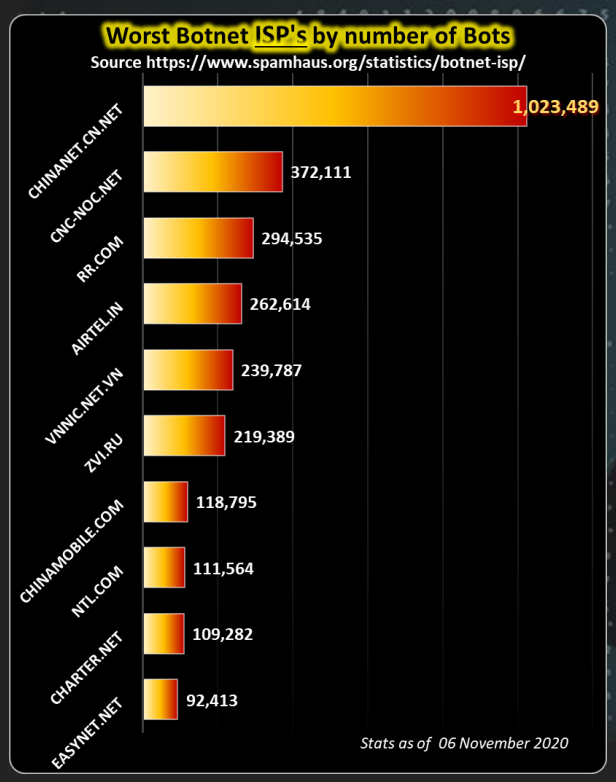
Toymaker Mattel Inc., the company behind Barbie dolls, disclosed that it was targeted in a ransomware attack, but it managed to fend it off. The ransomware attack was detected on July 28, according to a filing the company made today with the U.S. Securities and Exchange Commission. While not disclosing which sort of ransomware was involved, Mattel said it caused data on a number of systems to be encrypted. "Promptly upon detection of the attack, Mattel began enacting its response protocols and taking a series of measures to stop the attack and restore impacted systems," the filing states. "Mattel contained the attack and, although some business functions were temporarily impacted, Mattel restored its operations." The company said a forensic investigation found no evidence that any sensitive business data or retail customer, supplier, consumer or employee data had been stolen. Further, Mattel noted that there had been no material impact to its operations or finances as a result of the attack. That Mattel was able to overcome the ransomware attack is what makes this attack notable. Read the full story by Duncan Riley here: SiliconAngle

US: We've just seized $1bn in bitcoin stolen from Silk Road by 'Individual X' hacker

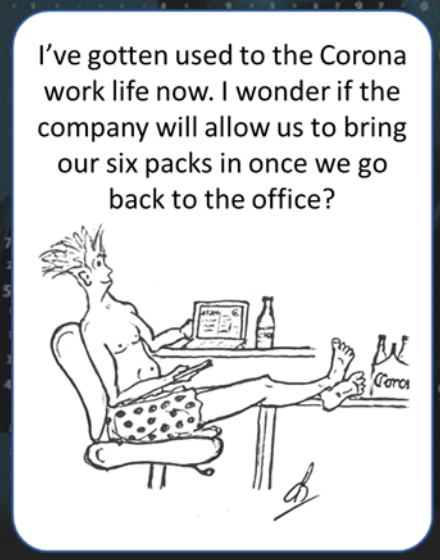
The US Justice Department says it's seized $1bn in bitcoin allegedly stolen by a hacker from Silk Road creator Ross Ulbricht before his arrest for running the dark-web market. Announcing the bitcoin seizure from the unnamed hacker, the Department of Justice revealed it is now seeking forfeiture of the illicit funds, which represent its largest haul of cryptocurrency to date. Ulbricht operated Silk Road between 2011 and October 2013, when the FBI seized the dark-web site and arrested him. He was convicted in 2015 for money laundering and distributing narcotics, and sentenced to life in prison. He lost an appeal for a new trial in 2017. Over that period, the site generated revenues of 9.5 million bitcoins and earned commissions totalling over 600,000 bitcoins. According to the complaint, earlier this year law enforcement used a bitcoin attribution company to analyze bitcoin transactions carried out by Silk Road and noticed 54 transactions around 2013 that were sent to two addresses totalling 70,411.46 bitcoins. Since the transactions weren't recorded in Silk Road's database, it was assumed the funds were stolen. In April 2013, the bulk of the funds totalling 69,471.082201 bitcoins were sent to an account referred to as '1HQ3', the first characters in the address. "Between April 2015 and November 2020, the remainder of the funds, 69,370.082201 bitcoins, remained in 1HQ3. As of November 3, 2020, 1HQ3 had a balance of 69,370.22491543 bitcoin (valued at approximately $1bn as of November 4, 2020)," the document states....
Read the full story here: ZDNet

This hacking group is using previously unknown tools to target defence contractors

Hackers used previously unknown tools in a cyber espionage campaign targeting defence and aerospace companies in a social engineering and phishing campaign which is more widely targeted than first thought. Analysis of reveals additional tactics and techniques of the campaign which has almost identical elements to Hidden Cobra – AKA The Lazarus Group – a hacking operation out of North Korea - Read more here: ZDNet



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



Quantum computers are coming. Get ready for them to change everything

In the tech world, the interest in Quantum Computing is forever rising as the technological gurus are making huge progress in harnessing the phenomenal processing power it is capable of. This goes for the cyber security world as well. CISO's are already looking for ways to counteract the potential threat when cyber criminals gets their hands on it. With Quantum technology they can potentially crack a 20 character password in 2 seconds. But lets not run ahead of ourselves, let's explore what Quantum computing is first. Below is a shortened and slightly adapted version of a recent article by ZDNet's Daphne Leprince-Ringuet, giving us a high level overview of what we can expect. (Read more here: What is Quantum Computing)

Quantum Computing Overview

Canadian grocery chain Save-On-Foods has become an unlikely pioneer, using quantum technology to improve the management of in-store logistics. In collaboration with quantum computing company D-Wave, Save-On-Foods is using a new type of computing, which is based on the downright weird behaviour of matter at the quantum level. And it's already seeing promising results. The company's engineers approached D-Wave with a logistics problem that classical computers were incapable of solving. Within two months, the concept had translated into a hybrid quantum algorithm that was running in one of the supermarket stores, reducing the computing time for some tasks from 25 hours per week down to mere seconds.

The remarkable properties of quantum computing boil down to the behaviour of qubits -- the quantum equivalent of classical bits that encode information for today's computers in strings of 0s and 1s. But contrary to bits, which can be represented by either 0 or 1, qubits can take on a state that is quantum-specific, in which they exist as 0 and 1 in parallel, or superposition. Qubits, therefore, enable quantum algorithms to run various calculations at the same time, and at exponential scale: the more qubits, the more variables can be explored, and all in parallel. Some of the largest problems, which would take classical computers tens of thousands of years to explore with single-state bits, could be harnessed by qubits in minutes.

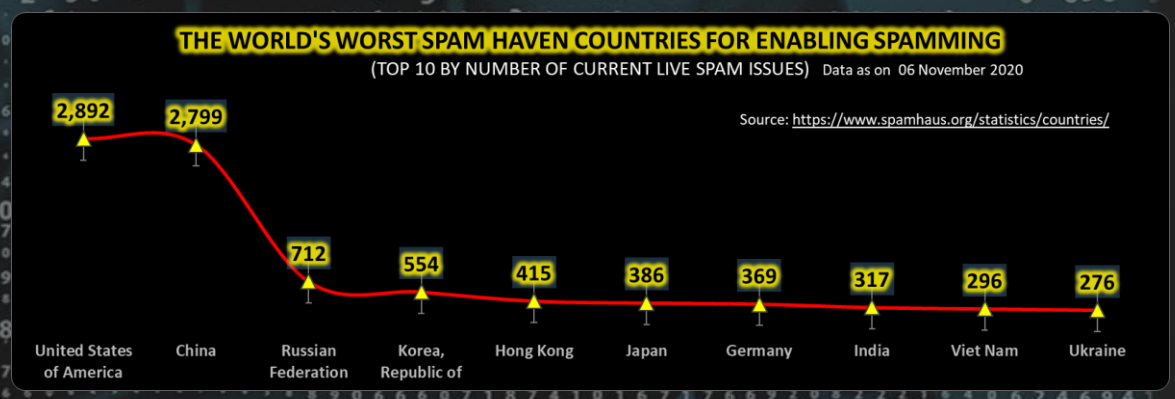
The challenge lies in building quantum computers that contain enough qubits for useful calculations to be carried out. Qubits are temperamental: they are error-prone, hard to control, and always on the verge of falling out of their quantum state. Typically, scientists have to encase quantum computers in extremely cold, large-scale refrigerators, just to make sure that qubits remain stable. That's impractical, to say the least. This is, in essence, why quantum computing is still in its infancy. Most quantum computers currently work with less than 100 qubits, and tech giants such as IBM and Google are racing to increase that number in order to build a meaningful quantum computer as early as possible. Recently, IBM ambitiously unveiled a roadmap to a million-qubit system and said that it expects a fault-tolerant quantum computer to be an achievable goal during the next ten years.

Certainly tech companies are racing to be seen as early leaders. IBM's Q Network started running in 2016 to provide developers and industry professionals with access to the company's quantum processors, the latest of which, a 65-qubit device called Hummingbird, was released on the platform last month. Recently, US multinational Honeywell took its first steps on the quantum stage, making the company's trapped-ion quantum computer available to customers over the cloud. Rigetti Computing, which has been operating since 2017, is also providing cloud-based access to a 31-qubit quantum computer.

Another approach, called quantum annealing, is especially suitable for optimisation tasks such as the logistics problems faced by Save-On-Foods. D-Wave has proven a popular choice in this field and has offered a quantum annealer over the cloud since 2010, which it has now upgraded to a 5,000-qubit-strong processor. A quantum annealing processor is much easier to control and operate than the devices that IBM, Honeywell and Rigetti are working on, which are called gate-model quantum computers. This is why D-Wave's team has already hit much higher numbers of qubits. However, quantum annealing is only suited to specific optimisation problems, and experts argue that the technology will be comparatively limited when gate-model quantum computers reach maturity.

The suppliers of quantum processing power are increasingly surrounded by third-party companies that act as intermediaries with customers. Zapata, QC Ware or 1QBit, for example, provide tools ranging from software stacks to training, to help business leaders get started with quantum experiments.

In other words, the quantum ecosystem is buzzing with activity, and is growing fast. And the exponential compute power of quantum technologies will be a game-changer in many fields. Qubits, with their unprecedented ability to solve optimisation problems, will benefit any organisation with a supply chain and distribution route, while shaking up the finance industry by maximising gains from portfolios. Quantum-infused artificial intelligence also holds huge promise, with models expected to benefit from better training on bigger datasets. Please follow the link and read the full article here: ZDNet Article



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