

On July 20, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Oracle and Google products. **CIS Security Advisories**

Covid-19 Global Statistics		
Date	Confirmed Cases	Total Deaths
22 Jul 22	572,836,962	6,398,503
Deaths this week: 15,884		

Threat Level's explained

GREEN or LOW indicates a low risk.

Cloud Computing In Simple Terms

- 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.
- 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.

For us who have been in the cyber & technology world for most of our lives, we sometimes forget that the terms and terminology used in our

daily conversations are not always that well understood by those in other walks of life. The fact of our modern life, however, is that since the advent of the smartphone and Internet of Things, most of society is pulled into the technology world whether they like it or not. With that also comes the exposure to the criminal threats that the connected world brings, and in recent conversation security of data in the cloud came up. I was then asked what it really means to have 'data in the cloud', "where is this so-called 'data in the cloud' kept?" So, today I'll share an extract of a recent post by Steve Ranger of <u>ZDNet</u>, attempting to explain the cloud computing concept in simple terms.

WEEKLY IT SECURITY BULLETIN 22 July 2022

In The News This Week Critical flaws in GPS tracker enable "disastrous" and "life-threatening" hacks

China-based Micodus has yet to patch critical vulnerabilities in MV720 GPS tracker. - A security firm and the US government are advising the public to immediately stop using a popular GPS tracking device or to at least minimize exposure to it, citing a host of vulnerabilities that make it possible for hackets to remotely disable cars while they removing, track location histories, disarm alarms, and cut off fuel. An assessment from security firm BitSight found six vulnerabilities in the Micodus MV720, a GPS tracker that sells for about \$20 and is widely available. (<u>CISA Advisory</u>) The researchers who performed the assessment believe the same critical vulnerabilities are present in other Micodus tracker models. The China-based manufacturer says 1.5 million of its tracking devices are deployed across 420,000 customers. BitSight found the device in use in 169 countries, with customers including governments, militaries, law enforcement agencies, and aerospace, shipping, and manufacturing compar nica & Sec Read the full story by Dan Goodin here: ARS Tee

UK cybersecurity chiefs back plan to scan phones for child abuse images

Tech companies should move ahead with controversial technology that scans for child abuse imagery on users' phones, the technical heads of GCHQ and the UK's National Cybersecurity Centre have said. So-called "client-side scanning" would involve service providers such as Facebook of Apple building software that monitors communications for suspicious activity without needing to share the contents of messages with a centralised server. Ian Levy, the NCSC's technical director, and Crispin Robinson, the technical director of cryptanalysis – codebreaking – at GCHQ, said the technology could protect children and privacy at the same time. "We've found no reason why client-side scanning techniques cannot be implemented safely in many of the situations one will encounter," they wrote in a discussion paper published on Thursday, which the pair said ent policy"... Read the full story by Alex Hern here:

Sensitive Roblox data stolen in yet another cyber attack

A sizable amount of Roblox internal documents have been hacked and leaked by cyber criminals after the game's owners did not pay a ransom to keep the data from being exposed. - Whilst there are many positive changes happening in the gaming stratosphere such as state-of-the-art hardware delivering big titles like God of War Ragnarok and Call of Duty: Modern Warfare 2, there are sadly always dark sides to the industry. Cybercrime has become one of the most prominent examples of this, with ransomware/extortion becoming a popular means to a quick buck for hackers. Roblox has become the latest victim of this unfortunate practice and its makers have commented on the matter. Like Minecraft, Roblox is a simple content creation game aimed at a much younger target audience who revel in the many ways the game can be enjoyed. Like Bandai Namco, CD Projekt Red, EA, and countless others though, even the Roblox Corporation are susceptible to these calculated cyber attacks. Read the full article by Andrew Highton here - D

New Air-Gap Attack Uses SATA Cable as an Antenna to Transfer Radio Signals

logy Attachment (SATA) or Serial np over air-gaps takes advantage of Serial Ad ATA cables as a communication medium, adding to a long list of electromagnetic, magnetic, electric, optical, and acoustic methods already demonstrated to plunder data. "Although air-gap computers have no wireless connectivity, we show that attackers can use the SATA cable as a wireless antenna to transfer radio signals at the 6GHz frequency band," Dr. Mordechai Guri, the head of R&D in the Cyber Security Research Center in the Ben Gurion University of the Negev in Israel, wrote in a paper published last week. The technique, dubbed **SATAn**, takes advantage of the prevalence of the computer bus interface, making it "highly available to attackers in a wide range of computer systems and IT environments." Put simply, the goal is to use the SATA cable as a covert channel to emanate electromagnetic signals and transfer a brief amount of sensitive information from highly secured, air-gapped computers wirelessly to a nearby receiver more than 1m away. An <u>air-gapped network</u> is one that's physically isolated from any other networks in order to increase its security. Air-gapping is seen as an essential mechanism to safeguard high-value systems that are of huge interest to espionage-motivated threat actors. est of the post by

ID Cards, Home Addresses of Nigerians Exposed in Huge Alleged Government Security Failure

A new report from the cyber-security team of online resource supplier Website Planet indicates that a huge alleged security fault at Nigerian government healthcare organisation PLASCHEMA (Plateau State Contributory Health Care Management Agency) has exposed over 45GBs of personal data, over 75,000 files, from an estimated 37,000 people. The massive oversight, according to Website Planet's team, has left information such as ID cards – including full names, dates of birth, occupations, blood groups and even personal addresses, parents' full names and registration details – birth certificates, personal photographs, identification for government officials and more, in the open online with no ction... Read the rest of the article by Luis Mo

Albanian government services suffer 'massive' cyber attack

The government of Albania has been forced to shut down its online services after suffering "a synchronised criminal attack from abroad'. -Albanians were unable to use scores of government services on Monday as a cyber attack caused the main servers of the National Agency for Information Society to go down only a few months after shifting most public sector services to an online portal. "Albania is under a massive cybernetic attack that has never happened before. This criminal cyber-attack was synchronised... from outside Albania," the Council of Ministers said in a press release. The "wide and complex" attack began on Friday and targeted government infrastructure and other public online services and rendered them functionless, the government added.. Read the story by Beatriz Valero de Urquía here: Eng



For Reporting Cyber Crime in the USA go to (IC3), in SA go , in the UK go to to 9 2 1 4 1 2 5 4

Other Interesting News and Cyber Security bits: -Cyber Warfare Future is What the ...!!, It '<u>Machine on Machine'</u> With China, Says Biden feels like someone has taken over The 5 best electric cars: Plus, the cheapest EV • control of my car!!

149

- available (ISC)2 offers free cyber • security certifications to one million people Meteoroid hit has caused - 💠
 - ignificant uncorrectable damage to James Webb
 - Space Telescope SANS Daily Network • Security Podcast (Storm



(TOP 10 BY NUMBER OF CURRENT LIVE SPAM ISSUES)



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

That is all that I have space for in this post, please read the rest of the article here as Steve expands on the benefits, advantages and disadvantages of cloud computing. Resources: ZDNet, BOX, AWS, AT&T, Goog 1 8 51 3 52 6 5 7

What is cloud computing, in simple terms? Cloud computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet ("the cloud") to offer faster innovation, flexible resources, and economies of scale.

How does cloud computing work? - Rather than owning their own computing infrastructure or data centres, companies can rent access to anything from applications to storage from a cloud service provider. One benefit of using cloud-computing services is that firms can avoid the upfront cost and complexity of owning and maintaining their own IT infrastructure, and instead simply pay for what they use, when they use it. In turn, providers of cloud-computing services can benefit from significant economies of scale by delivering the same services to a wide

What cloud-computing services are available? - Cloud-computing services cover a vast range of options now, from the basics of storage, networking and processing power, through to natural language processing and artificial intelligence as well as standard office applications. Pretty much any service that doesn't require you to be physically close to the computer hardware that you are using can now be delivered via the cloud – even quantum computing.

What are examples of cloud computing? - Cloud computing underpins a vast number of services. That includes consumer services like Gmail or the cloud backup of the photos on your smartphone, though to the services that allow large enterprises to host all their data and run all of their applications in the cloud. For example, Netflix relies on cloud-computing services to run its video-streaming service and its other business systems, too. Cloud computing is becoming the default option for many apps: software vendors are increasingly offering their applications as services over the internet rather than standalone products as they try to switch to a subscription model. However, there are potential downsides to cloud computing, in that it can also introduce new costs and new risks for companies using it.

Why is it called cloud computing? - A fundamental concept behind cloud computing is that the location of the service, and many of the details such as the hardware or operating system on which it is running, are largely irrelevant to the user. It's with this in mind that the metaphor of the cloud was borrowed from old telecoms network schematics, in which the public telephone network (and later the internet) was often represented as a cloud to denote that the location didn't matter – it was just a cloud of stuff. This is an over-simplification of course; for many customers, location of their services and data remains a key issue.

What is the history of cloud computing? - Cloud computing as a term has been around since the early 2000s, but the concept of computing as a service has been around for much, much longer – as far back as the 1960s, when computer bureaus would allow companies to rent time on a mainframe, rather than have to buy one themselves. These 'time-sharing' services were largely overtaken by the rise of the PC, which made owning a computer much more affordable, and then in turn by the rise of corporate data centres where companies would store vast amounts of data. But the concept of renting access to computing power has resurfaced again and again – in the application service providers, utility computing, and grid computing of the late 1990s and early 2000s. This was followed by cloud computing, which really took hold with the emergence of software as a service and hyperscale cloud-computing providers such as Amazon Web Services.

What are the core elements of cloud computing? - Cloud computing can be broken down into a number of different constituent elements, focusing on different parts of the technology stack and different use cases. Let's take a look at some of the best known in a bit more detail.

What is Infrastructure as a Service? - Infrastructure as a Service (laas) refers to the fundamental building blocks of computing that can be rented: physical or virtual servers, storage and networking. This is attractive to companies that want to build applications from the very ground up and want to control nearly all the elements themselves, but it does require firms to have the technical skills to be able to

What is Software as a Service? - Software as a Service (SaaS) is the delivery of applications as a service, probably the version of cloud computing that most people are used to on a day-to-day basis. The underlying hardware and operating system is irrelevant to the end user, who will access the service via a web browser or app; it is often bought on a per-seat or per-user basis. SaaS is the largest chunk of cloud spending simply because the variety of applications delivered via SaaS is huge, from CRM such as Salesforce, through to Microsoft's Office 365".

database management, operating systems, and development tools.

orchestrate services at that level.

t is Platform as a Service? - Platform as a Service (PaaS) is the next layer up – as well as the underlying storage, networking, and virtual ers, this layer also includes the tools and software that developers need to build applications on top, which could include middleware,

What is multi-cloud computing? - While the big cloud vendors would be very happy to provide all the computing needs of their enterprise customers, increasingly businesses are looking to spread the load across a number of suppliers. All of this has lead to the rise of multi-cloud. Part of this approach is to avoid being locked in to just one vendor (which can lead to the sort of high costs and inflexibility that the cloud is often claimed to avoid), and part of it is to find the best mix of technologies across the industry. That means being able to connect and integrate cloud services from multiple vendors is going to be a new and increasing challenge for business.