On October 5, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded). On October 4, the MS-ISAC released an advisory for multiple vulnerabilities in Google Android OS, the most severe of which could allow for arbitrary code execution.
CIS Security Advisories

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
07 October 2022

In The News This Week

Lloyd's of London Detects Suspicious Network Activity

Lloyd's of London is probing a possible cybersecurity incident that led it to yank some systems offline. - A spokesperson for the massive U.K. insurance and reinsurance market said unusual network activity provoked an overnight scramble to secure systems. "We are currently evaluating the best options for reconnecting these systems as we continue to investigate the issue," the spokesperson told Information Security Media Group. "We are working with specialist partners and a dedicated team and we continue to keep market participants and relevant parties updated," the spokesperson added.
Details are scarce at the moment, including whether the incident is malicious or involves ransomware and who may have instigated the incident. The market has been active in applying international sanctions against the Kremlin by denying marine insurance for Russia oil experts, the Financial Times reported earlier this year. "Lloyd's supports and remains focused on the delivery of a global sanctions regime against the Russian state," a spokesperson told Reuters....
Read the rest of the story by Akshaya Asokan here: Bank Info Security

Ferrari Suffers Document Leak Days After Announcing Cybersecurity Partnership

Automaker Ferrari confirmed the leak of some internal documents but didn't say how it happened. On Monday, RansomEXX, a ransomware-as-a-service operator, claimed to have breached Ferrari, though the company said it is investigating how the leak occurred. Italy's Red Hot Cyber reported that internal documents, including repair manuals, datasheets, etc., sizing up to 6.99 gigabytes, were leaked. RansomEXX has added Ferrari, whose racing division Scuderia Ferrari partnered with Bitdefender last week, to its list of victims. "If the claims from the ransomware gang are true, this once again highlights that criminals are constantly on the lookout for new victims to target, and they will often hit a company in retaliation to something it has done or said," Jordan Schroeder, managing CISO at Barrier Networks, told Spiceworks.)...
Read the full story by Sumeet Wadhwani here: Spiceworks

The astronomical costs of an asset disposal program gone wrong

As Morgan Stanley Smith Barney has learned, an information technology asset disposal program can protect a company against the potential catastrophe of data leaks from gear you're getting rid of. - Every entity should have an information technology asset disposal (ITAD) program as part of its information security process and procedure. Indeed, every time an IT asset is purchased, the eventual disposal of that asset should already be defined within an ITAD. When one doesn't exist, data becomes exposed, compromises occur, and in many cases, fines are levied. Such was the case with Morgan Stanley Smith Barney (MSSB), which continues to feel the repercussions of their ITAD's failure over the past several years, which has now resulted in $155 million USD in fines and penalties. On September 20, 2022, the Securities and Exchange Commission (SEC) reached a settlement agreement in which MSSB paid a $35 million USD penalty for the improper disposal of devices containing MSSB customer persona identifying information (PII). In October 2020, a consent order was issued by the Office of the Comptroller of Currency in which MSSB agreed to pay a penalty of $60 million. This was followed in January 2022 with the settlement of a class-action lawsuit in which MSSB agreed to pay an equal amount to victims of the ITAD failure and the resultant exposure of data.. Read the story by Christopher Burgess here: CSO

Former Uber Security Chief Found Guilty of Data Breach Coverup

A U.S. federal court jury has found former Uber Chief Security Officer Joseph Sullivan guilty of not disclosing a 2016 breach of customer and driver records to regulators and attempting to cover up the incident. Sullivan has been convicted on two counts: One for obstructing justice by not reporting the incident and another for misprision. He faces a maximum of five years in prison for the obstruction charge, and a maximum of three years for the latter. "Technology companies in the Northern District of California collect and store vast amounts of data from users," U.S. Attorney Stephanie M. Hinds said in a press statement. "We expect those companies to protect that data and to alert customers and appropriate authorities when such data is stolen by hackers. Sullivan affirmatively worked to hide the data breach from the Federal Trade Commission and took steps to prevent the hackers from being caught."... Read the full story by Ravie Lakshmanan: The Hacker News

The FBI says it caught an ex-NSA employee trying to sell top-secret intelligence documents

The NSA, as a rule, wants to employ people who are good at spying. But according to the FBI, one former employee tried to turn the tables on the agency and was caught in the act. Per details released by the Department of Justice this week, a Colorado resident was arrested Wednesday and charged with attempting to transmit classified information to a representative of a foreign government. The press release says that Jareh Sebastian Dalke, 30, was employed by the NSA from June 6th to July 1st, 2022. Between August and September 2022, feds say that he used an encrypted email account to transmit portions of three classified documents to an individual who he believed to be working for a foreign government. In fact, that individual was an FBI agent who lured Dalke into a sting operation that eventually led to his capture....
Read the full story by Corin Faife here: The Verge

Lets talk about digital hoarding

Digital hoarding is a topic that came up a few times in conversations I had recently, and as we've seen in the news lately can become a security risk where forgotten data can expose personally identifiable information (PII) if not disposed of properly. Since digital storage became cheaper in the late eighties to early nineties than conventional paper-based information storage, the amount of data created and stored on a daily basis is mind-boggling. Just as an example, more than 100 Billion WhatsApp messages are sent daily, some with photos or other documents. Telegram messages amount to more than 15 Billion and Facebook Messenger more than 7 Billion. That is apart from the billions of photos saved and corporate data, all are digitally stored somewhere!
The problem, however, is much broader than a security risk as Chris Merriman highlighted in a recent Computer Weekly post, which I want to share with you today. Below then is an extract from the article.

Carbon copies: How to stop data retention from killing the planet

Our society has a serious digital hoarding problem, which is coming at a cost to the environment. But what can be done to address it? - There's a hidden environmental cost to the age of data that few of us ever think about – and it is time that changed. While the average content management system may be full of business intelligence data with the potential to revolutionise how an enterprise operates, it accounts for just a fraction of the petabytes of data being stored every day. A report from IDC cited by The Conversation estimates that by 2025, society will be storing 175ZB (zettabytes) of data – an exponential explosion from the 59ZB total in 2020. To put it in perspective, that's enough to fill nearly 1.5 trillion mobile phones.

And the truth is the way data is stored has turned businesses and consumers into a race of hoarders, logging everything, just in case it is needed again one day – most of which is never going to be accessed again.
But for better or worse, it has to be stored somewhere, and regardless of the greenest credentials of your stakeholders, it comes at a cost. A single plain text email produces around 4g of CO2. Add pictures and it's more like 50g. That's not insignificant – and yet it's an environmental impact that is rarely talked about.

A heated debate - Computer hardware, like most electronic equipment, creates heat. Lots of it. And one of the great ironies of that is that heat is extremely detrimental to the chips and diodes, meaning it has to be cooled down. As a result, even the smallest of server rooms requires cooling equipment to bring the temperature below the ambient temperature of an empty room. In effect, we're using twice the electricity, twice the energy and twice the carbon, just to maintain the status quo.

So what can be done about it? It is a question that has been plaguing the IT industry for years, and the lack of a definitive answer often makes it easier to just turn on another air-conditioning unit and look the other way. But that's causing even more harm. So what are the alternatives?

Storing less data appears to be an obvious answer, but it would be almost impossible to implement, because who decides what parameters are worth recording and what are not? The BBC learned this the hard way when it trashed much of its TV archive during the 1970s and 1980s, assuming that it would be no use. Then came the VCR, the DVD player and, of course, streaming. Ask any Doctor Who fan and they will grimace at the number of early episodes of the long-running Sci-Fi series that have been lost, perhaps forever, because of a lack of foresight.
So, that's the case to justify digital hoarding. But it all has to be stored somewhere, and those facilities have to be environmentally controlled.

Deep freeze data - Not all information necessarily has to be instantly accessible. Offline storage still has a valid place in the online world. Take CERN, for example, the home of the Large Hadron Collider. Much of the data it has generated over the past 50 years through myriad experiments is still kept on spools of tape, and is only available if requested by, say, a university. It can take between 30 minutes and two hours to make that cold storage data available – but it is there. Of course, in another great irony, this shining beacon would be better served if all that data was digitised and could be cross-referenced – but at least, as it is, it has a much lower carbon footprint.

There's an even colder type of storage – the GitHub Arctic Vault.... It's not designed to be accessed, but rather to act as a disaster recovery plan for the end of the world. But it raises the question – does our data really need to be online?

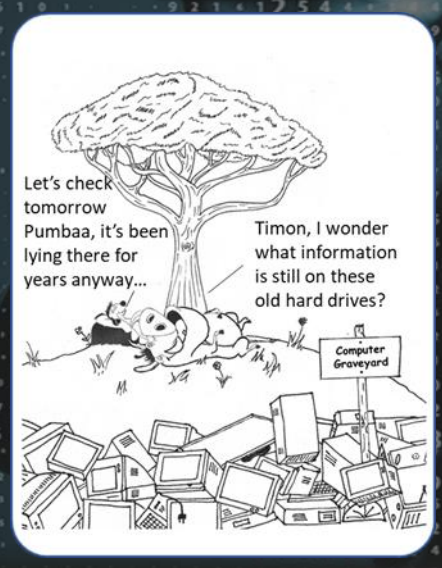
Another increasingly popular way of keeping computer equipment cool is with water – gallons of recirculated liquid is cooled and sent through tubes to pass over heat-generating hardware, reducing the need for cooling the whole environment. The downside is that such systems are extremely difficult to retrofit. ... Many companies are already investigating more radical solutions that are both greener and, ultimately, cheaper. Microsoft launched Project Natick in 2018 as an experiment, which saw two datacentres submerged 117ft under the Pacific Ocean.

Acres of space - Nasa has just begun to send its first unmanned test missions back to the moon, as part of Project Artemis... With temperatures on the dark side of the moon capable of plunging to a rather chilly -230°C, and Nokia already contracted to provide a lunar 4G service, it does give rise to the question of whether datacentres on the moon could be a future possibility... The downside of this would be latency for now.

Solutions in training - It's also worth considering that, in the right circumstances, all this heat could be a good thing. Rather than wasting it, if the excess temperatures can be harnessed, it could be used as a cheap source of heat for homes and businesses. At a disused London Underground station in Islington, the Bunhill 2 Energy Centre harnesses all the waste heat produced by the Northern Line and converts it to heating for local office buildings and an entire housing estate... If it can be done for waste transport heat, there's no reason why the same couldn't be done for waste-spewing datacentres.

As much as it would be wonderful to be able to conclude by saying that we've solved all the problems caused by the wastage and environmental impact caused by our obsession with data, all of these ideas have drawbacks. Some are practical... Some are financial... What's important is that there are possibilities – lots of them – that would make our dirty data a bit cleaner, and maybe even have a positive effect on the environment. What's required is a collective will by the industry to take these ideas forward and to make the revolution part of the solution, rather than part of the problem... Read the full article here

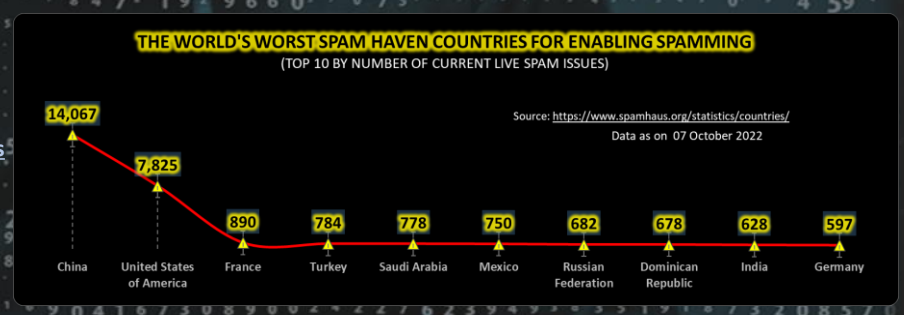
For Reporting Cyber Crime in the USA go to (IC3) , in SA go to Cybercrime, in the UK go to ActionFraud



Other Interesting News and Cyber Security bits:

- Reshaping the Threat Landscape: Deepfake Cyberattacks Are Here
- A Jane Austen quote encoded in plastic molecules demonstrates the potential for a new kind of data storage
- SANS Daily Network Security Podcast (Storm cast)

flightradar24 LIVE AIR TRAFFIC Track any Aeroplane in flight globally
Marine Traffic Track any Sailing Vessel globally
SatelliteXplorer Track satellites in orbit



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