The Cyber Threat Alert Level as evaluated by CIS remains at Blue (Guarded)

Covid-19 Global Stats

Date	Confirmed Cases	Total Deaths
23 July	193,326,750	4,150,247

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

23 July 2021

In The News This Week

Cyber attack disrupts major South African port operations

A cyber attack has disrupted container operations at the South African port of Cape Town, an email seen by Reuters on Thursday said. Durban, the busiest shipping terminal in sub-Saharan Africa, was also affected, three sources with direct knowledge of the matter told Reuters. Cape Town Harbour Carriers Association said in an email to members, seen by Reuters: "Please note that the port operating systems have been cyber-attacked and there will be no movement of cargo until the system is restored." Transnet's official website was down on Thursday showing an error message. Transnet, which operates major South African ports, including Durban and Cape Town, and a huge railway network that transports minerals and other commodities for export, confirmed its IT applications were experiencing disruptions and it was identifying the cause. Read the story here: ITNews

Saudi Aramco Confirms Data Leak After Reported Cyber Ransom Attack

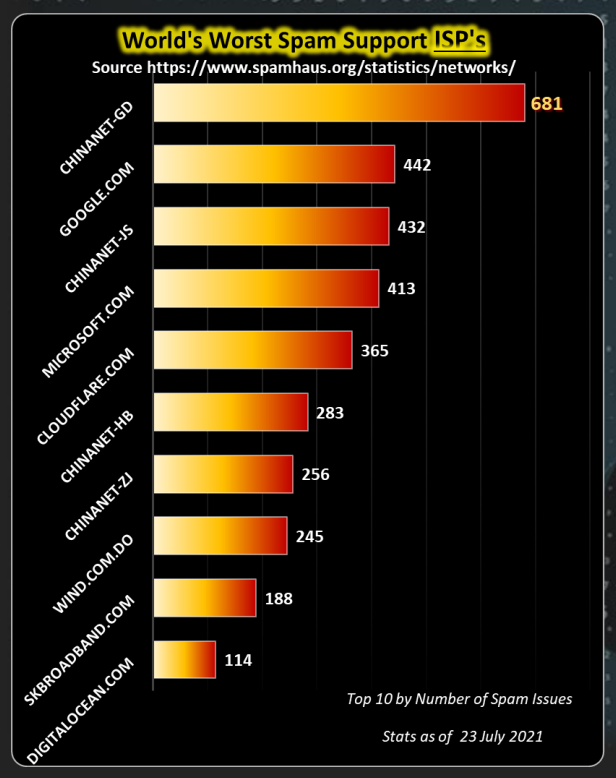
Saudi Aramco confirmed that some company files were leaked after hackers reportedly demanded a $50 million ransom from the world's most-valuable oil producer. "Aramco recently became aware of the indirect release of a limited amount of company data which was held by third-party contractors," the Middle Eastern oil major said Wednesday in an email. "We confirm that the release of data was not due to a breach of our systems, has no impact on our operations, and the company continues to maintain a robust cybersecurity posture." The Associated Press reported earlier that 1 terabyte of Saudi Arabian Oil Co. data had been held by an extortionist, citing a web page it had accessed on the darknet. The state-owned driller was offered the chance to have the data deleted for $50 million in cryptocurrency, the AP said. Read the full story here: Bloomberg

British man arrested in connection with Twitter mega-hack

Police in Spain have arrested a British man in connection with what many consider the worst hack in Twitter's history. In July 2020, the Twitter accounts of public figures and well-known organisations were compromised, allowing malicious hackers to post tweets to millions of unsuspecting followers. Compromised accounts included those of then-Presidential candidate Joe Biden, Bill Gates, Elon Musk, and Jeff Bezos, as well as the corporate Twitter identities of Apple, Uber, and Coinbase. As we described at the time, the accounts were hijacked to publish a cryptocurrency scam that read "*I am giving back to my community due to Covid-19! All Bitcoin sent to my address below will be sent back doubled. If you send $1,000 I will send back $2,000! Only doing this for the next 30 minutes! Enjoy*". The scale of the attack suggested that the malicious hackers had somehow managed to compromise Twitter's internal systems to gain access to so many accounts that would normally be expected to be protected by strong passwords and multi-factor authentication. The authorities quickly identified Graham Ivan Clark, of Tampa, Florida as having gained access to Twitter's internal support tools through what the social network described as a "phone spear phishing attack" against a small number of its employees. Clark, who was 17 years old at the time of the attack, is said to have managed to dupe unsuspecting Twitter users out of $117,000 worth of Bitcoin through the scam. He was ultimately sentenced to three years in a juvenile detention facility. But the authorities have said for some time that they do not believe that Clark was the only person involved with the attack. On Wednesday, 21 July, the US Department of Justice announced the arrest in Estepona, Spain of 22-year-old Joseph O'Connor, a British citizen. O'Connor's name is one that is not unknown to cybercrime investigators. After the Twitter hack, cybersecurity blogger Brian Krebs alleged that Joseph O'Connor was the true identity of "PlugWalkJoe", a hacker who was thought to have been involved in SIM-swapping attacks to compromise accounts. ….
Read the rest of the story by Graham Cluley here: tripwire

Ransomware gang breached CNA's network via fake browser update

Leading US insurance company CNA Financial has provided a glimpse into how Phoenix CryptoLocker operators breached its network, stole data, and deployed ransomware payloads in a ransomware attack that hit its network in March 2021. As revealed by the US insurer, the attackers first breached an employee's workstation on March 5 using a fake and malicious browser update delivered via a legitimate website…
Read the full story here: Bleeping Computer



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

Bulletproof Your Enterprise Cybersecurity

Rakesh Soni of CPO Magazine wrote an interesting article this week giving some pointers on how organisations can attempt to bulletproof their environments against so-called State-Sponsored attacks. It raises the awareness of certain things that can and needs to be done to minimize the risk of being attacked or how to weather the storm once attacked. The word "bulletproof" is probably a bit strong as we see how some of the largest and most secure organisations (like Pfizer), who acted like superheroes and deemed themselves impenetrable, got breached. I can see how these organisations, who probably implemented most of the controls mentioned by Soni, thought they were bulletproof but sadly they weren't. The good thing, however, these controls will undoubtedly help to minimise the risk and to enhance the overall security posture of the organisation. Below then is an extract of the controls mentioned by Soni.

Zero trust security – The pressing need

Today's digital era has made it difficult for enterprises to differentiate what's inside or outside their network, significantly when cloud and on-premise assets are quickly distorting. Moreover, many organizations aren't even aware that they've allowed unauthorized professionals to bypass their lines of defences when they switched to cloud or even hybrid models.
The reason is- they didn't understand the overall security mechanism of the newly-adopted architecture.
Here's where zero-trust security comes into play. This smart mechanism ensures no trust is provided to any user or device, whether inside or outside the enterprise's network. Furthermore, permission is offered at every stage through robust identity verification and access management processes. With SASE (Secure Access Service Edge) coupled with zero-trust strategies in place, an organization can ensure the maximum level of security as the company's assets/resources can't be accessed regardless of the network architecture. This is what enterprises need at the earliest in an era where cybercriminals are quickly side-stepping different authentication layers.

Passwordless authentication and authorization

Most of the security breaches result from compromised credentials, which can be fatal for an organization.
Whether it's phishing, malware attacks, or password spraying, attackers continuously explore new ways to steal passwords to access organizations' sensitive information.
Once these attackers gain access to passwords, they quickly bypass the authentication barriers, and in most cases, these kinds of attacks don't come to the enterprise's notice until months.
Passwordless authentication and authorization can be a game-changer in overcoming these issues as it paves the path for a secure login without the hassle of securing user passwords.
Moreover, the passwordless login options are easier to use and implement, reinforcing the overall defense system against unauthorized access to sensitive information related to consumers and the enterprise.
Hence, there's not a single reason for enterprises relying on old-school credential management mechanisms not to switch to passwordless authentication.

Getting privacy compliant (GDPR, CCPA, POPIA, etc)

For those who aren't aware of privacy compliance laws- it states how organizations (regardless of their domain) meet regulatory & legal requirements for collecting, processing, and maintaining consumers' personal information.
These privacy laws and regulations protect customers in different countries by ensuring consumer data is being handled appropriately.
Privacy compliances, including the EU's GDPR and California's CCPA, have pushed enterprises to implement new stringent policies, reviews, and enhance focus to get better at detecting a breach continuously.
Also, getting these policies in place helps organizations improve the overall defense system and reinforce breach identification to minimize the loss at the earliest, especially in a state-sponsored attack.
So, how could a business get compliant with these regulatory compliances?
Well, businesses can leverage a consumer identity and access management solution that offers compliance to ensure consumer data isn't compromised, and businesses can quickly safeguard their sensitive information.

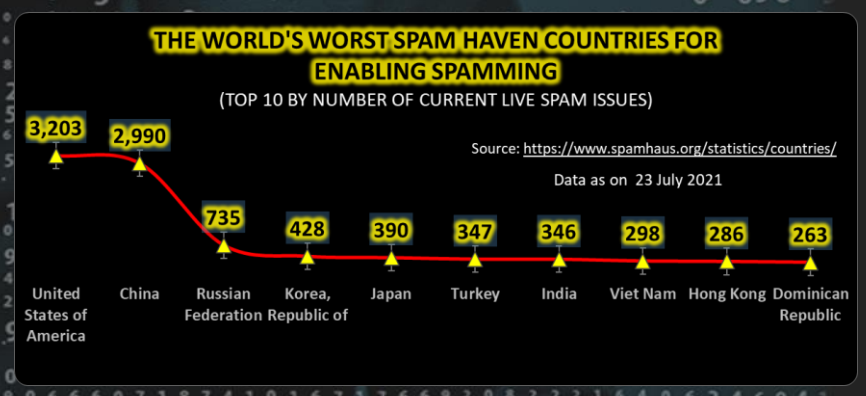
Enhancing security awareness

As per stats, the primary cause of data exposures is a human error such as weak internal cyber-security, which results in record vulnerability. Training employees regarding the latest trends in cybersecurity could be quite fruitful for a business as it may prevent any unauthorized access, whether through phishing attacks or social engineering practices.
It's important for businesses to frequently organize cybersecurity training as attackers continue to explore new ways to exploit user identities to sneak into an enterprise's network.
But the biggest question is- does it affect the overall defense mechanism against state-sponsored attacks?
Yes, undoubtedly!
The unintentional insider threat to a network by means of phishing techniques by state rivals continues to hinder the most informed defense systems just because of the negligence of an employee. Hence, enterprises can lower the risk by regularly training and testing their employees regarding awareness and cyber hygiene.

Please read the full article and other stories here: CPO Magazine

Other Interesting News and Cyber Security bits:

- Preventing the Next Cybersecurity Attack with Effective Cloud Security Audits
- Apple Issues Urgent iPhone Updates – Update Now
- 2022 Toyota Land Cruiser Buyers Banned From Reselling It Due To Security Concerns



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