On October 27, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Oracle, Mozilla, and Google products.
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
28 October 2022

In The News This Week

US govt warns of Daixin Team targeting health orgs with ransomware
CISA, the FBI, and the Department of Health and Human Services (HHS) warned that a cybercrime group known as Daixin Team is actively targeting the U.S. Healthcare and Public Health (HPH) sector in ransomware attacks. The federal agencies also shared indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) in a joint advisory issued today to help security professionals detect and block attacks using this ransomware strain. "The Daixin Team is a ransomware and data extortion group that has targeted the HPH Sector with ransomware and data extortion operations since at least June 2022," the advisory revealed. Since June, Daixin Team attackers have been linked to multiple health sector ransomware incidents where they've encrypted systems used for many healthcare services, including electronic health records storage, diagnostics, imaging services, and intranet services. They're also known for stealing patient health information (PHI) and personal identifiable information (PII) and using it for double extortion to pressure victims into paying ransoms under the threat of releasing the stolen information online. Read the rest of the story by Sergiu Gatlan here: Bleeping Computer

Australia - Optus and Medibank hacks prompt government to increase fines for massive data breaches to a minimum of $50 million - The financial penalty imposed on companies engaged in serious or repeated privacy breaches will be increased to at least $50 million. The current penalty is $2.2 million, and the federal government believes that is insufficient given massive cyber-attacks on Optus and Medibank Private in recent weeks. Attorney-General Mark Dreyfus will fast-track amendments to the Privacy Act when federal parliament returns next week "When Australians are asked to hand over their personal data, they have a right to expect it will be protected," Mr. Dreyfus said. "Unfortunately, significant privacy breaches in recent weeks have shown existing safeguards are inadequate. "It's not enough for a penalty for a major data breach to be seen as the cost of doing business." The proposed legislation would see the fine for "serious or repeated privacy breaches" increased to either $50 million, three times the value of the benefit obtained through misuse of data, or 30 per cent of a company's adjusted turnover in the relevant period.
The fine would be whichever value is the highest.. Read the full story by Henry Belot here: ABC News

Japan, Australia upgrade security pact against China threat
Japan and Australia on Saturday signed a new bilateral security agreement covering military, intelligence and cybersecurity cooperation to counter the deteriorating security outlook driven by China's increasing assertiveness. The upgrade of the Joint Declaration on Security Cooperation, a pact first signed in 2007 when China's rise was less concerning, was the major outcome of Japanese Prime Minister Fumio Kishida's meeting with his Australian counterpart Anthony Albanese in the west coast city of Perth. It builds on a reciprocal access agreement that Kishida inked in January with then-Australian Prime Minister Scott Morrison that removes obstacles to holding joint military exercises in either country. That is the first such agreement Japan has struck with any country other than the United States. Japan announced Saturday that its Self-Defense Forces will train and take part in exercises with the Australian military in northern Australia for the first time under the agreement..
Read the story here: CNBC News

Hacker who made £130,000 selling stolen Ed Sheeran songs online jailed
A hacker who stole unreleased songs from Ed Sheeran and sold them on the dark web has been sentenced to 18 months in prison. - Adrian Kwiatkowski, 23, illegally accessed the cloud-based accounts of dozens of top musicians, including Frank Ocean, Post Malone and Kanye West. He would then steal unreleased material from these artists and trade their songs online in exchange for cryptocurrency. City of London Police, who investigated the case, believe Kwiatkowski had made over £131,000 pounds from selling the illegally-obtained tunes. 'Kwiatkowski had complete disregard for the musicians' creativity and hard work producing original songs and the subsequent loss of earnings,' said Joanne Jakymec of the Crown Prosecution Service. She added: 'He selfishly stole their music to make money for himself.' Read the story by Tom Sanders here: Metro

How China plots to use anti-satellite nuclear weapons to blast spacecraft out of orbit... and cripple Elon Musk's Starlink - CHINA is planning to use anti-satellite nuclear weapons to blast a spacecraft out of orbit and cripple Elon Musk's Starlink. - The Northwest Institute of Nuclear Technology, a Xian-based research institute, claims to have developed a model to evaluate the performance of nuclear anti-satellite weapons.... It comes after Chinese defense scientists said the nation needs to be able to protect itself from SpaceX's Starlink satellites if they pose a threat to national security.
In a paper published in Modern Defense Technology, officials called for the development of a defense system that would be able to disable or destroy Starlink satellites and feature a surveillance tool that can track and monitor them. Ren Yuanzhen, a researcher with the Beijing Institute of Tracking and Telecommunications, led the study alongside several senior scientists in China's defense industry. Read the full story by Aliki Kraterou here: The Sun

Hidden Social Media Cyber-Risks

Social media apps has come a long way since the first chat rooms saw the light in the late seventies to early eighties in the form of MUD servers and the infamous IRC chat rooms. Although it was originally just meant to be an online bulletin board, IRC chat rooms soon became a headache for corporates. Suddenly there was a poorly controlled platform where anyone can voice his or her opinion or share sensitive information not meant for public consumption. Immature corporate policies at the time did not particularly cover the use of these chat rooms and had to be amended on the fly. These chat rooms were the humble beginnings of the social media platforms as we know it today, but the risks since then has grown exponentially in our modern interconnected world. Most of us are using a social media app in one way or another, whether it is Facebook, Twitter, Strava or a lesser-known app, it means we are all exposed to the risks that comes along with it. Ericka Chickowski posted an article this week in DarkReading highlighting some of these risks and I would like to share some of them in the post today.

Biometric Attack Fodder
A new study out by TrendMicro details how sharing high-resolution photos and videos can pose a long-term threat to individuals (and enterprise executives), namely by providing cannon fodder for hacking biometric protections. "Unfortunately, by sharing personal media content in high resolution, we also unintentionally expose sensitive biometric patterns," the report explains, detailing that a high-definition video or image can provide facial, eye, or fingerprint details that could potentially be used to *fool* facial recognition or fingerprint scanners. Similarly, audio could be exposed that could manipulate voice-recognition biometrics. "One of the problems with biometric data is that, unlike a password, once it is exposed, it is nearly impossible to change. How can we get a new iris pattern or fingerprint?" the report explains. "These are lifelong 'passwords,' and once exposed to the public, an attacker can use them five or even 10 years from now."

Deepfake Material
In the same vein of video and audio being mined for biometrics, an endless slew of social content from corporate executives could also be used to build convincing voice cloning and deepfake videos. Social content-fueled deepfakes can be used to power a range of different cybercriminal ends; cybercriminals can scrape content from platforms and doctor it. With cheap and free AI tools that can be used to build this synthetic content more available than ever, the FBI says it expects malicious actors of all types to increasingly leverage deepfakes in their attacks. In a report last year, the FBI warned that cybercriminals and foreign governments are going to be leaning on deepfakes to bolster their capabilities.
"We anticipate malicious cyber-actors will use these techniques broadly across their cyber operations — likely as an extension of existing spearphishing and social engineering campaigns, but with more severe and widespread impact due to the sophistication level of the synthetic media used," the FBI wrote.

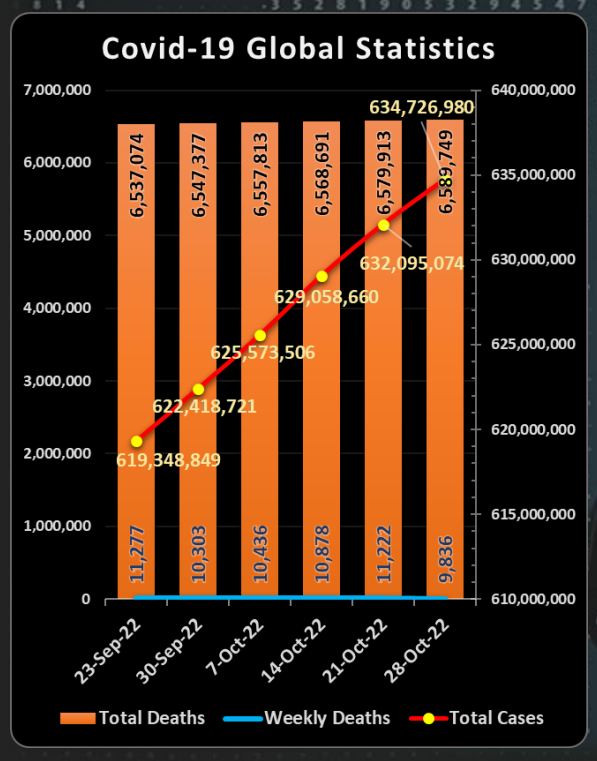
Social Media Account Takeover
According to analysis released by the Identity Theft Resource Center (ITRC) last month, social media account takeovers have skyrocketed in the past year, increasing by more than 1,000%. Attackers are going after any social account they can hijack, but corporate accounts are particularly juicy, as they can be used in lucrative frauds or to embarrass the brand. For example, just last week the cryptocurrency exchange Gate.io had its Twitter account taken over by scammers, who used the opportunity to promote a phishing scheme. And even big brands have fallen prey to social media account takeovers. *Another* example, several years ago, McDonald's Twitter account was taken over by activists who pushed out a political tweet attacking President Donald Trump. Even Twitter itself has been famously breached for such outcomes.

So Many LinkedIn Hiring Scams
With so much recruiting and hiring activity occurring on and around the LinkedIn platform, it should come as little surprise to cybersecurity veterans that the bad guys are sniffing around for a way to exploit this activity. This summer the FBI Internet Crime Complaint Center (IC3) warned of increased movement by criminals who are gaming the online interview process for remote-work positions. The fraudsters are using a combination of deepfake videos, stolen personally identifiable information (PII) and other tactics to impersonate applicants. The motivations behind the attacks are still hazy, but some security experts speculate that this could be a future avenue for attackers to place themselves as trusted insiders within an organization in order to carry out sophisticated scams and spying.

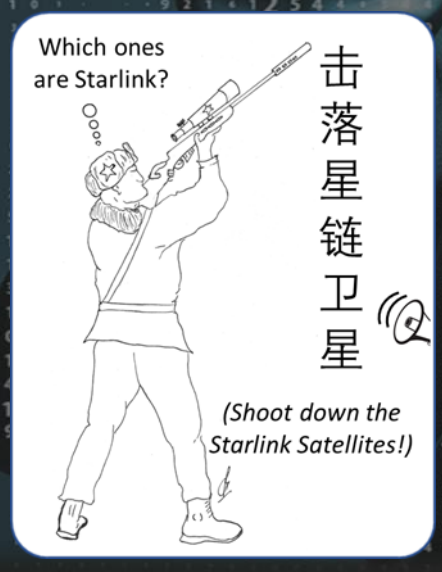
Espionage & Reconnaissance
The volume and depth of personal and business information that people share on social media make social networks a fruitful hunting ground for anyone actively or passively doing reconnaissance. This includes a mix of foreign state actors, corporate spies, and everyday fraudsters hoping to boost their social engineering ploys. They can learn a lot about high-profile executives or corporate activities just based on what companies publicly share on their profiles, including who they regularly do business with, their travel habits, and who they interact with most within their organization. Spies can do even more damage if they connect with their targets through fake profiles. A recent warning from the UK government says that spies are using malicious profiles on "an industrial scale" to pump well-placed professionals for information.

Please visit the DarkReading site to read the full article

Resources: Techwalla, Computerworld, Wikipedia, Social Media Week



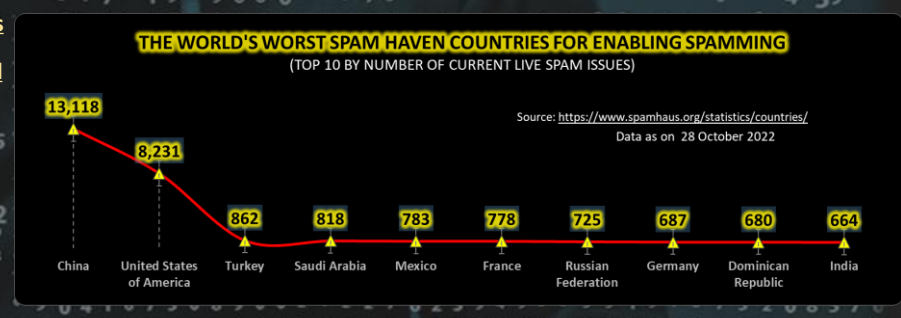
For Reporting Cyber Crime in the USA go to (IC3) , in SA go to Cybercrime, in the UK go to ActionFraud



Other Interesting News and Cyber Security bits:

- Listen to the eerie sounds of a solar storm hitting the Earth's magnetic field
- Elon Musk brings whole new meaning to 'high speed' satellite internet with vehicle-optimized Starlink terminal
- 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