On March 22, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google Chrome.
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
24 March 2023

In The News This Week

JCDC Cultivates Pre-Ransomware Notification Capability

In today's blog post, Associate Director of the Joint Cyber Defense Collaborative (JCDC) Clayton Romans highlighted recent successes of pre-ransomware notification and its impact in reducing harm from ransomware intrusions.
With pre-ransomware notifications, organizations can receive early warning and potentially evict threat actors before they can encrypt and hold critical data and systems for ransom. Using this proactive cyber defense capability, CISA has notified more than 60 entities of early-stage ransomware intrusions since January 2023, including critical infrastructure organizations in the Energy, Healthcare and Public Health, Water and Wastewater Systems sectors, as well as the education community. The pre-ransomware notification was cultivated with the help of the cybersecurity research community and through CISA's relationships with infrastructure providers and cyber threat intelligence companies. For more information, visit #StopRansomware. To report early-stage ransomware activity, visit Report Ransomware. CISA also encourages stakeholders and network defenders to review associate director Romans' post, Getting Ahead of the Ransomware Epidemic: CISA's Pre-Ransomware Notifications Help Organizations Stop Attacks Before Damage Occurs, to learn more about CISA's Pre-Ransomware Notification Initiative. Read the CISA blog here: CISA

Details Of 16.8 Crore (168 Million) Citizens Leaked, 7 Arrested

Hyderabad, India: A massive data breach that has implications for national security was unearthed by Cyberabad Police here, who arrested seven people of a gang allegedly involved in the theft and sale of sensitive data of the government and important organisations, including details of defense personnel as well as the personal and confidential data of about 16.8 crore citizens. The accused persons were found selling more than 140 different categories of information, which include sensitive information such as details of defense personnel and the mobile numbers of citizens and NEET students, among others, Cyberabad Police Commissioner M Stephen Raveendra told reporters here on Thursday.
Seven data brokers were arrested from Delhi, police said adding that the accused had been operating through three companies (call centres) in Noida and other places. So far it has been found that the accused sold data to at least 100 fraudsters. Investigations are still on, police said... Read more here: NDTV

TikTok CEO: Company 'is not an agent of China'

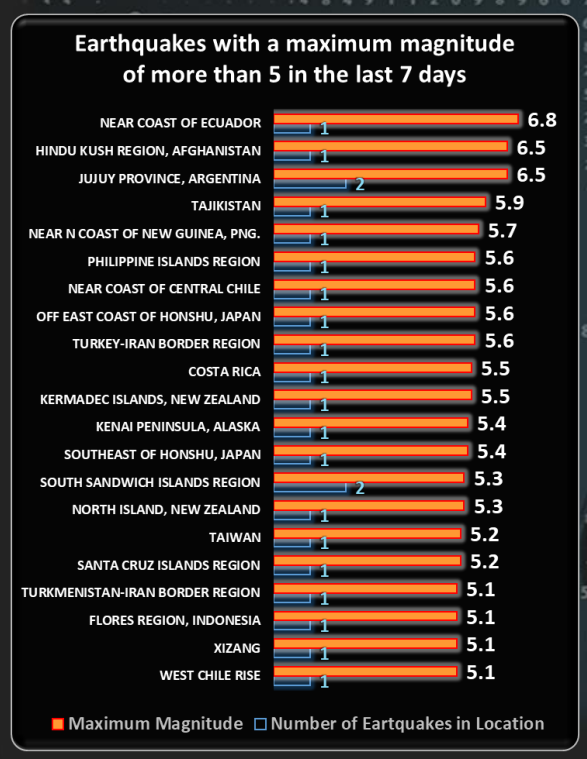
In front of a panel of skeptical and hostile U.S. representatives, TikTok CEO Shou Zi Chew tried to make the case for why the popular app is not a security threat to the country -- and why a government ban of the app would be the wrong course of action. A U.S. ban of the app would hurt the country's economy, reduce competition and "silence the voices of over 150 million Americans," Chew said in testimony submitted to the House Energy and Commerce Committee. The hearing, titled "TikTok: How Congress Can Safeguard American Data Privacy and Protect Children from Online Harms," was held Thursday morning in Washington, D.C. The Biden administration recently demanded that ByteDance divest its ownership stake in TikTok or potentially be banned in the U.S. over national-security concerns given TikTok's Chinese ownership...
Read the full story by Todd Spangler here: SIW

Fake ChatGPT Chrome Browser Extension Caught Hijacking Facebook Accounts

Google has stepped in to remove a bogus Chrome browser extension from the official Web Store that masqueraded as OpenAI's ChatGPT service to harvest Facebook session cookies and hijack the accounts. The "ChatGPT For Google" extension, a trojanized version of a legitimate open-source browser add-on, attracted over 9,000 installations since March 14, 2023, prior to its removal. It was originally uploaded to the Chrome Web Store on February 14, 2023. According to Guardio Labs researcher Nati Tal, the extension was propagated through malicious sponsored Google search results that were designed to redirect unsuspecting users searching for "Chat GPT-4" to fraudulent landing pages that point to the fake add-on.
Read the rest of the story by Ravie Lakshmanan here: The Hacker News

The DEA Quietly Turned Apple's AirTag Into A Surveillance Tool

In May last year, border agents intercepted two packages from Shanghai, China. Inside one was a pill press, a machine used to compress powders into tablets, in the other some pill dyes. Believing that they were destined for an illegal narcotics manufacturer, the Drug Enforcement Agency was called in. DEA investigators inspected the devices but rather than cancel the shipment or pay a visit to the intended recipient, they tried something they'd never been known to try before: they hid an Apple AirTag inside the pill press so they could track its movements. Revealed in a search warrant obtained by Forbes, it appears to be the first known case of a federal agency turning Apple's location-tracking device into a surveillance technology. It shows how the tech giant's miniature tracker has gone from giving consumers a handy way to keep tabs on luggage and other valuables, to a remote spy tool..
Read the full story by Thomas Brewster here: Forbes



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

No ma'am, according to our policy, your password must contain some numbers, a mix of upper and lowercase letters, a special character, a smiley face, a sprig of hyssop, an Egyptian scarab, and must be at least 64 characters long..

Dark Web: The Good, Bad and Ugly of This Online Underworld

If you haven't heard of the Dark Web or Dark Net, you probably lived in a remote cave or been stranded on a desert island or something for the last 20 years. The Dark Web is notorious for criminal activity, but as Nidhi Singh explained in a recent article, there is a good side to it as well. Below then is an extract of Nidhi's post that will give you some insight into the digital underworld.

The dark web is infamous for hosting illegal activities, but there are legitimate uses like combating censorship and protecting individuals - The internet is a vast network of information, but beyond the surface-level web that we all use every day, there lies a hidden world known as the dark web. The initial version of the current dark web first emerged in March 2000 with the introduction of Freenet by Irish student Ian Clarke. Freenet employs a decentralized network of users to enable anonymous online communication. Nonetheless, it was The Onion Router (Tor), a program that was launched on September 20, 2002, that popularized the dark web.
While the dark web has a notorious reputation for hosting illegal activities such as drug trafficking, weapons sales and human trafficking, not everything on the dark web is negative. It also provides a haven for journalists, activists, and individuals seeking anonymity for legitimate reasons. In this article, we will explore the complex and often challenging aspects of the dark web, delving into its good, bad, and ugly sides to provide a comprehensive overview of this enigmatic and intriguing realm.

Open web vs. deep web vs. dark web: What's the difference and why it matters - The internet is composed of three main layers: the open web, the deep web and the dark web. The surface web, or the open web, is the most visible and accessible layer of the internet. It can be accessed through commonly used browsers like Chrome, Firefox, Edge or Safari. This very article is a part of the surface web, which can be accessed from anywhere and at any time as long as there is an internet connection and a web browser. However, the surface web only represents a small portion of the entire internet, accounting for just five percent of its information.
The deep web, which constitutes the second layer of the internet, consists of content that is not indexed by search engines. This includes web pages and websites that may contain password-protected content, resources personalized for individual users and private forums. Examples of deep web content include online banking, cloud storage and private social media pages and profiles. The deep web accounts for approximately 95 percent of the internet's content.
Within the deep web lies the dark web, which comprises hidden sites and can only be accessed through specialized networks like Tor. Tor is an open-source privacy browser that offers confidentiality and anonymity by routing messages through a network of interconnected Tor relays. As the message passes from one node, or a configured computer in the network, to another, it becomes encrypted, ensuring that each relay only has knowledge of the machine that sent the message and the machine to which it is being sent. Like the open web, the dark web is a small part of the internet, accounting for approximately 5 percent of its content.

A breeding ground for illegal activities: The dark side of the dark web - While the deep web is often used for legitimate purposes such as private forums and research databases, the dark web has a reputation for hosting illegal activities, such as drug trafficking, extortion and cyber fraud. This is because the dark web offers a level of anonymity that attracts those who seek to operate beyond the reach of law enforcement.
In 2015, Daniel Moore and Thomas Rid from King's College London conducted a study on the dark web by examining the content of 2,723 active websites over a period of five weeks, revealing that 57% of these websites contained illegal material.
One of the most infamous activities on the dark web is the existence of assassination markets. These markets operate via crowdfunding, allowing users to pay for the assassination of a specific target, usually high-profile individuals such as politicians, celebrities or businessmen. While some of these markets may seem credible and functional, most are likely scams to defraud users and steal their money or personal information for identity theft or other illegal activities.
The prevalence of illegal activities on the dark web underscores the importance of exercising caution when accessing the platform With its hidden infrastructure and untraceable transactions, the dark web presents a unique challenge to law enforcement agencies worldwide.

The positive part of the dark web: Legitimate uses and tools for combating censorship - Despite its reputation as a breeding ground for illicit activities, the dark web also has its fair share of legitimate uses. The dark web provides tools for combating censorship and protecting individuals from persecution for their beliefs or actions. It also serves as a secure and anonymous platform for legitimate organizations like WikiLeaks to share information and avoid retaliation. . Initially, the organization utilized the Tor network to receive data, which enabled the whistleblowers to remain anonymous and avoid potential retaliation from governments and powerful entities.
Another Tor-based service that is widely used by media organizations, including The New Yorker and The Guardian, is SecureDrop. This service allows journalists and whistleblowers to securely exchange content without fear of their identities being revealed or their communications being intercepted by third parties.
According to Human Rights Watch, Tor has also been used by Chinese dissidents to bypass internet censorship and access blocked websites. In countries where internet freedom is restricted, such as China, Tor has become a crucial tool for evading government surveillance and censorship.
Overall, while the dark web does have a seedy underbelly, it also has its positive aspects and should not be dismissed entirely.

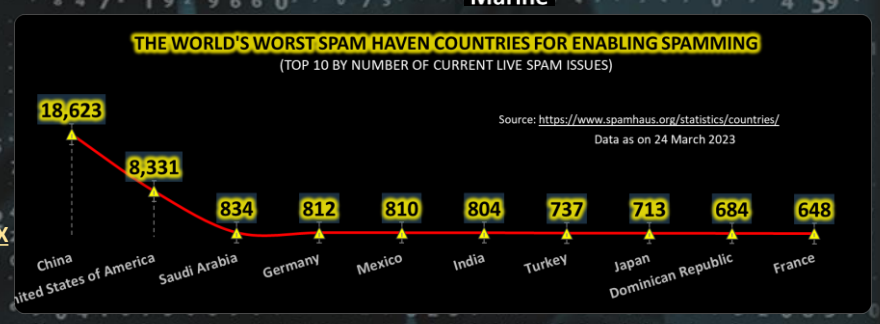
Tips to safely browse the dark web - Given that the dark web is a hotspot for cybercriminals who engage in illegal activities, such as identity theft, hacking and fraud, you must stay extra vigilant when browsing it. Here are several important steps you should take to safely browse the dark web: (1) Use a secure and anonymous browser such as Tor , but keep in mind, it is not foolproof, the Tor network can be compromised, exposing your online activity to potential attackers. (2) Always use a virtual private network (VPN) to protect your IP address. (3) Be cautious of any links or downloads and avoid clicking on anything that looks suspicious. (4) It is important to never give out any personal information or engage in any illegal activity on the dark web. Use common sense and exercise caution when interacting with other users.

In conclusion, the dark web is a double-edged sword that presents opportunities and dangers to internet users. The anonymous browsing and secure communication features it offers have proven crucial for individuals and organizations fighting against oppressive regimes, censorship and discrimination. On the flip side, it is also home to a thriving criminal underworld... Resources: Jumpstart, ZDNet, Kaspersky, Investopedia

Other Interesting News and Cyber Security bits:

- It Looked Like A Nice Family Home. Cops Suspect It Was A Secret Drone Airport For MDMA (ecstasy) Drop-offs
- New 'Bad Magic' Cyber Threat Disrupts Ukraine's Key Sectors Amid War
- Amazon is about to go head-to-head with SpaceX in a battle for satellite internet dominance
- SANS Daily Network Security Podcast (Storm cast)

flightradar24 LIVE AIR TRAFFIC Track any Aeroplane in flight globally
IRIS Interactive Earthquake Map
Traffic Marine
SatelliteXplorer Track satellites in orbit



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