On September 14, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Apple, Microsoft, and Adobe 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
16 September 2022

In The News This Week

Uber security breach 'looks bad', potentially compromising all systems
Uber reportedly has suffered another massive security incident, which is likely more extensive than its 2016 data breach and potentially may have compromised its entire network. It also can result in access logs being deleted or altered. A hacker on Thursday was believed to have breached multiple internal systems, with administrative access to Uber's cloud services including on Amazon Web Services (AWS) and Google Cloud (GCP). "The attacker is claiming to have completely compromised Uber, showing screenshots where they're full admin on AWS and GCP," Sam Curry wrote in a tweet. The security engineer at Yuga Labs, who corresponded with the hacker, added: "This is a total compromise from what it looks like."....
Read the full story by Eileen Yu here: ZDNet

Self-Checkouts, IoT And The Rise Of Cyber Security Threats In Retail
Cyber security threats are a rising concern for retail companies as they increasingly adopt self-checkouts through Apple, Google Pay or other payment platforms. Since 2005, retailers have seen over 10,000 data breaches, mainly due to flaws and vulnerabilities in payment systems. Point of sale (POS) systems often utilize a plethora of external hardware, software, and cloud-based components. "At minimum, retailers must ensure that their contracted party complies with them and will observe the same security compliance requirements that the company itself has. There are numerous opportunities for a cybercriminal to take advantage of the system, whether this be at the source of the vendor providing the solution or when the technology is deployed onsite. ... There are also security threats that users face when using IoT devices in retail. Over 84 percent of organizations use IoT devices. However, less than 50% have taken solid security measures against cyber-attacks. ..."The introduction of these new payment mechanisms signals the beginning of a new technology adoption cycle. From the security point of view, this is when things are typically the most vulnerable".
Read the full article by Dennis Mitzner here : Forbes

Israel offers cyber aid to Albania, which severed Iran ties over hacking claim
Israel offered cyber defense assistance to Albania on Monday, days after the Balkan state severed its diplomatic ties with Iran, citing accusations that the Islamic Republic carried out cyberattacks against the country in July. Deputy Foreign Minister Idan Roll met with Albanian Foreign Minister Olta Xhacka on the sidelines of the Conference on Shaping Feminist Foreign Policy in Berlin, where he "offered to share our knowledge and experience in cyber defense" and "expressed Israel's appreciation" for Tirana's decision to kick out Iran's diplomats, he said in a tweet. "We will continue to tighten cooperation between Israel and Albania," Roll added. Read more here: TOI

Ukrainians hack consumer drones to fight Russia
High-tech drones are the latest big thing in modern warfare. But the kind you can buy off the shelf to play with at home can also be helpful in times of need, as Ukrainians are discovering... See the Video here: Deutsche Welle (DW)

Over 280,000 WordPress Sites Attacked Using WPGateway Plugin Zero-Day Vulnerability
A zero-day flaw in the latest version of a WordPress premium plugin known as WPGateway is being actively exploited in the wild, potentially allowing malicious actors to completely take over affected sites. Tracked as CVE-2022-3180 (CVSS score: 9.8), the issue is being weaponized to add a malicious administrator user to sites running the WPGateway plugin, WordPress security company Wordfence noted. "Part of the plugin functionality exposes a vulnerability that allows unauthenticated attackers to insert a malicious administrator," Wordfence researcher Ram Gall said in an advisory. WPGateway is billed as a means for site administrators to install, backup, and clone WordPress plugins and themes from a unified dashboard. The most common indicator that a website running the plugin has been compromised is the presence of an administrator with the username "rangex." Additionally, the appearance of requests to "//wp-content/plugins/wpgateway/wpgateway-webservice-new.php?wp_new_credentials=1" in the access logs is a sign that the WordPress site has been targeted using the flaw, although it doesn't necessarily imply a successful breach. Wordfence said it blocked over 4.6 million attacks attempting to take advantage of the vulnerability against more than 280,000 sites in the past 30 days.
Read the full article by Ravie Lakshmanan here: The Hacker News

A terrifying AI-generated woman is lurking in the abyss of latent space
"Loab is the last face you see before you fall off the edge." -There's a ghost in the machine. Machine learning, that is. We are all regularly amazed by AI's capabilities in writing and creation, but who knew it had such a capacity for instilling horror? A chilling discovery by an AI researcher finds that the "latent space" comprising a deep learning model's memory is haunted by least one horrifying figure — a bloody-faced woman now known as "Loab." But is this AI model truly haunted, or is Loab just a random confluence of images that happens to come up in various strange technical circumstances? Surely it must be the latter unless you believe spirits can inhabit data structures .... Read more here: TechCrunch (Warning, disturbing images on site)

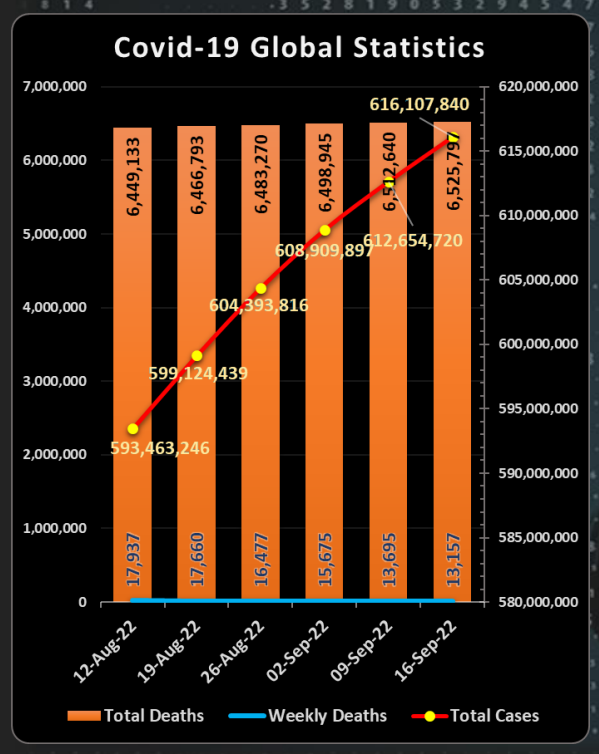
A look at Dark Web Markets

By now, most people has heard of or seen news casts of one of the original Dark Web market places called "Silk Road". "Silk Road" was taken down by federal agencies in 2013 for trading in illegal goods, including drugs. Since then, there were many spin-offs of the original dark market place idea, and many of them has short lived. But the battle of illicit traders and law enforcement agencies are raging on. In 2017 federal agents took down AlphaBay, which had been sited as one of the biggest dark markets ever. AlphaBay, however, has recently been resurrected by a person who goes by the handle of "DeSnake", who claims to have been the second in charge of the original AlphaBay. Although the Dark Web subject came up in earlier bulletins, today I want to take a deeper look into the resurrected AlphaBay. But first, for those who are not in the know, lets see what a Dark Web Market is all about.

What is a Dark Web Market?
Investopedia describes it as follows: "*Darknet markets are dark web black markets that offer illicit goods for sale, often using cryptocurrencies as a method of payment. Although some products for sale are legal, illicit goods such as drugs, stolen information, and weapons are common items in these markets. The transactions in darknet markets are anonymized. These markets exist on the Tor network in order to create security and anonymity for both users and darknet providers. Transactions take place via a cryptocurrency like Bitcoin using dark wallets to protect the seller and buyer. The payment is held in escrow by the site operator to discourage scammers. The only exposed link in the chain is the actual shipping of the goods through the postal system.*"
In essence, these markets are found on the Dark Web, a part of the internet that is not indexed and not searchable by normal search engines and intentionally hidden. So, mostly, if someone don't tell you were to look and how to look, it is very difficult to find. According to recent surveys, the Dark Web constitute about 96% of the internet, which means that what we see on the normal internet, or surface web, is a very small 4%.
There are thousands of Dark Markets abound, some here today and gone tomorrow, but here are some Dark Web Marketplaces (DWMs) that are deemed to be the leaders: ASAP Market, AlphaBay, Tor2Door Market, Vice City Market, Dark0de Reborn & Abacus. Goods traded on these notorious markets include: Drugs and other banned substances, firearms and weapons, illegal diamonds, hacking tools and services, cyber weapons, counterfeit documents and currencies, counterfeit goods, the list goes on.

The resurrected AlphaBay
Wired published a recent article on AlphaBay and below is an extract of the article that gives you a good overview.

Five years after it was torn offline, the resurrected dark web marketplace is clawing its way back to the top of the online underworld. - For years, dark web markets and the law enforcement agencies that combat them have been locked into a cycle of raid, rinse, repeat: For every online black market destroyed, another has always been there to take its place. But rarely has a dominant dark web market been busted by a massive law enforcement operation only to rise from the ashes half a decade later and regain its top spot—a feat that may very soon be achieved by AlphaBay, the once and future king of the contraband crypto-economy.
In July of 2017, a global law enforcement sting known as Operation Bayonet took down AlphaBay's sprawling narcotics-and-cybercrime bazaar, seizing the site's central server in Lithuania and arresting its creator, Alexandre Cazes, outside his home in Bangkok. Yet in August of last year, AlphaBay's number-two administrator and security specialist, publicly known only as DeSnake, suddenly reappeared, announcing AlphaBay's resurrection in a new and improved form. Now, 10 months later, thanks in part to a tumult of takedowns and the mysterious disappearances of competing dark web markets, DeSnake's reincarnated AlphaBay is now well on its way to its former heights atop the digital underworld. By some measures, it appears to have already regained that spot. *"Yes, AlphaBay is the #1 darknet marketplace right now," says DeSnake, writing to WIRED in a text-based conversation in June. "I did tell you we were going to be #1 before," he added, referring to our interview with AlphaBay's new admin at the time of its relaunch last summer. "As I have told you, I do what I say."*
DeSnake's boast is at least partly true: At the time, AlphaBay had more than 30,000 unique product listings—largely drugs, from ecstasy to opioids to methamphetamines, but also thousands of listings for malware and stolen data, like Social Security numbers and credit card details. That's up from a mere 500 listings in September of last year. Another older market called ASAP displays more than 50,000 listings. But ASAP is known to allow vendors to post duplicate listings. And according to security firm Flashpoint, which closely tracks the competing markets, AlphaBay had more than 1,300 active vendors in roughly the first six months of this year, compared to about 1,000 for ASAP. According to Flashpoint's data, AlphaBay's listings also appear to be growing significantly faster. Other markets touted in dark web forums like Archetyp and Incognito, meanwhile, have only a few thousand or just a few hundred listings.
AlphaBay's tens of thousands of product listings are still a tiny fraction of the more than 350,000 it offered before its 2017 takedown, when it was the biggest dark web market ever seen. By the FBI's estimate, it was 10 times the size of the legendary Silk Road drug market. DeSnake concedes that the new AlphaBay's revenue hasn't yet come close to the level of its 2017 peak, when blockchain analysis firm Chainalysis estimates that AlphaBay generated as much as $2 million a day in sales.
Also, unlike most competitors, the new version of AlphaBay only allows users to buy and sell in the privacy-focused cryptocurrency Monero, not Bitcoin, transactions of which can often be tracked through blockchain surveillance. That makes the site's sales difficult to measure and may mean it has fewer sales per listing, since many users prefer to trade in Bitcoin.
AlphaBay's quick growth—or regrowth—has been fuelled in part by what Ian Gray, a dark web analyst, calls "the Great Cyber Resignation." At least 10 dark web markets have dropped offline for various reasons in the last 18 months.... Please read or listen to the rest of the article here: Wired Other resources: CSO, Darknet One, Darknet Pages, SOCRadar, Rapid7

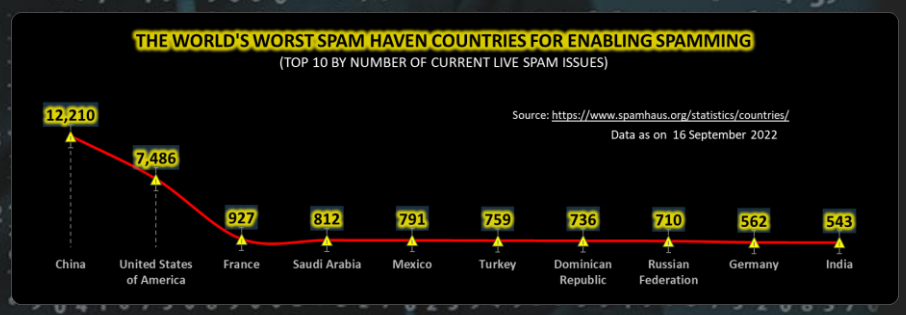


For Reporting Cyber Crime in the USA go to (IC3) , in SA go to Cybercrime, in the UK go to ActionFraud

Other Interesting News and Cyber Security bits:

- Queen Elizabeth II: A life in pictures
- The Cyber Security Head Game
- An Overview of Vehicular Cybersecurity for Intelligent Connected Vehicles
- 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