On September 20, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to a vulnerability in Mozilla 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
22 September 2023

In The News This Week

US DOD releases 2023 cyber strategy to combat emerging threats

The baseline document sets a new strategic direction for the US Department of Defense, supports priorities set out in the 2022 National Security Strategy, 2022 National Defense Strategy, and the 2023 National Cybersecurity Strategy, and builds upon the 2018 DOD Cyber Strategy. The classified cyber strategy, in its fourth iteration, establishes how the department will operate in and through cyber space to protect Americans and advance domestic defense priorities. It specially outlines threats from the People's Republic of China, Russia, North Korea, Iran, violent extremist organizations, and transnational criminal organizations. "As the department's cyber capabilities evolve, so do those of our adversaries. Both the People's Republic of China and Russia have embraced malicious cyber activity as a means to counter US conventional military power and degrade the combat capability of the Joint Force," the document stated.. Read the full article by Robert Dougherty here: CyberSecurityConnect

Satellite constellations taking on greater role in Japan's security

The Russia-Ukraine war, which started in February 2022, is sometimes described as an all-out war in the digital era, having a mix of old and new aspects of warfare. One of the latter is the Starlink satellite internet service used by the Ukrainian forces as telecommunication infrastructure. The service, a type of satellite constellation — a group of artificial satellites operated as a single system — has attracted great attention in the ongoing war. However, the use of satellite constellations is not limited to the Ukrainian government. The U.S. military has begun shifting its space system architecture to satellite constellations. Japan's Defense Ministry and Self-Defense Forces have also been conducting demonstration experiments for the use of Starlink satellites since March.."…. Read the rest of the story by Jane Wang here: TheJapanTimes

Junta shells out another 12 million euros on new 24-hour cyber threat monitoring centre in Malaga

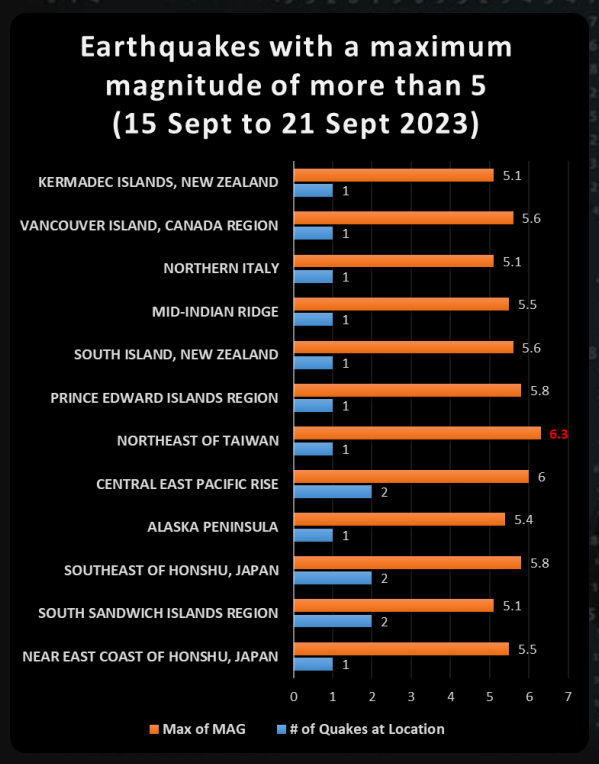
The Junta de Andalucía has pumped another 12 million euros into a new cyber security project located in the Spanish city centre of Malaga. The Centro de Ciberseguridad de Andalucía has been partially operating since the end of March in the Palmeral de las Sorpresas in Malaga, but lacks the "brain", the security operations centre that can monitor cyber threats 24 hours a day. However, a 12-million-euro cash injection, approved on Tuesday 19 September, will fund the nerve centre that will assess cyber risks at all times. Regional minister Antonio Sanz has said that the official opening date of the centre will be on 28 November. The regional cybersecurity centre will have seen a total an investment of 60 million euros and will act as a "centre point for the region to develop and promote everything related to its cybersecurity strategy", Sanz said. The space will also house facilities to offer training, innovation and awareness to companies, universities and the public..
Read the article by Nuria Triguero here: SUR

War crimes tribunal ICC says it has been hacked

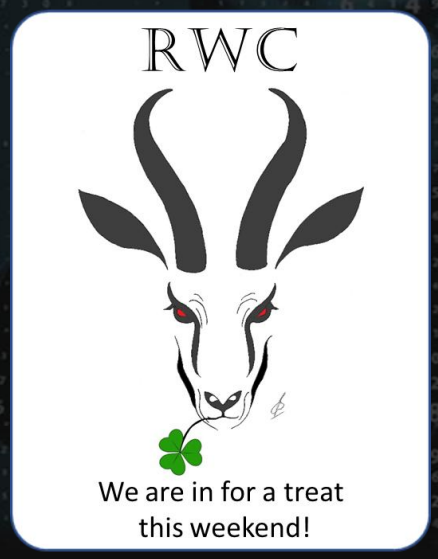
THE HAGUE, Sept 19 (Reuters) - The International Criminal Court (ICC) said on Tuesday its computer system had been hacked, a breach at one of the world's most high-profile international institutions and one that handles highly sensitive information about war crimes. The ICC said it had detected unusual activity on its computer network at the end of last week, prompting a response that was still ongoing. A spokesperson declined to comment on how serious the hack was, whether it has been fully resolved, or who might be behind it. "Immediate measures were adopted to respond to this cybersecurity incident and to mitigate its impact," the ICC said in a short statement. The ICC is the permanent war crimes tribunal in the Dutch city of The Hague, established in 2002 to try war crimes and crimes against humanity. Prosecutors at the court are currently conducting 17 investigations into situations in Ukraine, Uganda, Venezuela, Afghanistan and the Philippines, among others...
Read the full story by Toby Sterling and Stephanie van den Berg here: Reuters

China Accuses U.S. of Decade-Long Cyber Espionage Campaign Against Huawei Servers

China's Ministry of State Security (MSS) has accused the U.S. of breaking into Huawei's servers, stealing critical data, and implanting backdoors since 2009, amid mounting geopolitical tensions between the two countries. In a message posted on WeChat, the government authority said U.S. intelligence agencies have "done everything possible" to conduct surveillance, secret theft, and intrusions on many countries around the world, including China, using a "powerful cyber attack arsenal." Specifics about the alleged hacks were not shared. It explicitly singled out the U.S. National Security Agency's (NSA) Computer Network Operations (formerly the Office of Tailored Access Operations or TAO) as having "repeatedly carried out systematic and platform-based attacks" against the country to plunder its "important data resources." The post went on to claim that the cyber-warfare intelligence-gathering unit hacked Huawei's servers in 2009 and that it had carried out "tens of thousands of malicious network attacks" on domestic entities, including the Northwestern Polytechnical University, to siphon sensitive data, an allegation that was first leveled by China in September 2022...Read the rest of the article here: The Hacker News



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



Why You Need a VPN

Following on from last week's tech jargon post on Kerberos, this week we will have a look at VPNs, what it is, how it works, and why you would need it. I'm sure you come across the term many times on your daily online commute, but do you really know what it is and how you can benefit from using a VPN? Max Eddy from PC Magazine recently posted an article to give us some insight and today I'll share an extract of the article.

"A VPN can protect your privacy, if you use it right. We explain what VPNs do, what they don't, and how to get the most out of a VPN"

What Is a VPN?

VPN stands for Virtual Private Network. When we talk about VPNs, we're usually talking about a commercial VPN being sold directly to consumers for use in day-to-day life, but the idea of VPNs has much broader applications than that. Corporations have long used VPN technology to let workers access digital resources no matter where they are, long before COVID-19 made work from home the norm. When you switch on a VPN, it creates an encrypted connection (sometimes called a "tunnel") between your device and a remote server operated by the VPN service. All your internet traffic is routed through this tunnel to the server, which then sends the traffic off to the public internet as usual. Data coming back to your device makes the same trip: from the internet, to the VPN server, through the encrypted connection, and back to your machine.

Do VPNs Make You Anonymous Online?

By encrypting your traffic and routing it through a VPN server, it is harder but not impossible for observers to identify you and track your movements online. No VPNs provide total anonymity, but they can help improve your privacy. For example, your internet service provider (ISP) is probably the single entity with the most insight into what you do online. The FTC issued a report in 2021 outlining exactly how much your ISP knows about what you do online, and it's a lot. Worse, if you live in the US, thanks to Congress, your ISP can sell anonymized data about its customers. If you don't like that a company you're already paying is profiting from your data or if you have concerns about ISPs hoarding detailed information about your activities, a VPN will help. Not even your ISP can see your web traffic when you use a VPN. VPNs also make it harder for advertisers and others to track you online. Normally, data is transmitted from the internet to your device using its IP address. When the VPN is active, your true IP address is hidden, and anyone watching you can only see the IP address of the VPN server.
Despite that, VPNs do not make you fully anonymous online. Advertisers, for instance, have numerous ways to identify and track you as you move across the web. Trackers and cookies in websites try to uniquely identify you, and then watch for where you appear next...

Using Tor can guard your privacy even better than a VPN, and grant you access to the Dark Web. Unlike a VPN, Tor bounces your traffic through several volunteer server nodes, making it much harder to trace. It's also managed by a nonprofit organization and distributed for free. Some VPN services will even connect to Tor via VPN, making this arcane system easier to access. The cost to your internet connection is high, however, as using Tor will degrade your connection much more than a VPN. Tor isn't perfect either, and it too has plenty of weaknesses to consider.
Keep in mind that law enforcement and government agencies have access to more advanced and invasive techniques. Given enough time, a determined, well-funded adversary can usually get what it's after.

Do VPNs Protect Against Malware and keep you safe online?

Several VPNs say they include some protection against malicious files. Sometimes this is basic protection against known malicious sites and files. Some VPN services include dedicated antivirus tools as well, and some antivirus companies now offer VPNs. (But, since VPNs are generally viewed as a privacy tool, do not solely rely on it as malware protection. A VPN will hide the contents of your web traffic from some observers and can make it harder for you to be tracked online. But a VPN can, at best, provide only limited protection against the threats you're most likely to encounter on the web: malware, social engineering scams, and phishing sites. There are better ways to address these threats , and since VPNs are generally viewed as a privacy tool, do not solely rely on it as malware or phishing protection.

Do VPNs Hide Your Torrenting and Online Activity?

When a VPN is active, all your traffic is encrypted. This means your ISP can't see the sites you're visiting or the files you're moving. But while your ISP maybe can't see you're Torrenting the entire run of Great British Bake Off, they can surmise that you're using a lot of bandwidth. This alone may be a violation of your terms and conditions. Pirating content may also be a violation of your VPN's terms and conditions, so be sure to check carefully.

Can VPNs Bypass Censorship or regional streaming restrictions?

With a VPN, it's possible to connect to a VPN server in another country and browse the web as if you were physically where the VPN server is. This can, in some cases, get around local content restrictions and other kinds of censorship. It's easily the noblest use of a VPN, and VPN companies will often play up their role in protecting internet freedom. Although it should work, it's important to know that a VPN doesn't make your traffic invisible. Observers can see encrypted traffic, but they shouldn't be able to see the contents of the traffic. However, the encrypted traffic alone might attract unwanted attention. Some VPNs include modes that aim to disguise VPN traffic as more common HTTPS traffic.

Can You Trust a VPN?

The biggest problem with VPNs isn't an issue of technology, but one of trust. Because all your traffic is passing through its systems, a VPN company is in the same position as an ISP. It could, if it wished, see everything you do online and sell that data. It could inject ads into the websites you view. It could keep unnecessary amounts of data it could then be compelled to hand over to law enforcement. VPNs are eager to receive that trust, but proving they deserve that trust is difficult. When we review a VPN, we pore over its privacy policy and send out a questionnaire to get a sense of what efforts each company makes to protect customers' privacy. We know they could lie to us, but our goal is to put them on record.

Do I Need a VPN?

Nowadays, most web traffic is sent via HTTPS, which does encrypt your connection. Looking at HTTPS traffic, an ISP or someone spying on your network can only see the highest level of your traffic's destination. That's like seeing PCMag.com and not PCMag.com/max-is-great. Browser fingerprinting and other techniques mean a VPN's anonymizing abilities are curbed somewhat. Even a VPN's lauded ability to spoof locations, bypass censorship, and unblock streaming is less certain as companies and governments have become increasingly aggressive in detecting and blocking VPN traffic. But it depends on why you want a VPN. If, for whatever reason, you want your traffic to appear to be coming from another country, a VPN will do that, etc. A VPN will not make you invincible online, but it can help protect your privacy. It's a valuable part of your security and privacy toolbox, and like every tool a VPN works best when you use it for the right job.

Resources: PC Magazine, Also see - The Best VPN Services for 2023

Other Interesting News and Cyber Security bits:

- Estonian firm develops virtual 'shooting range' to test cyber defenses
- What Are the Best Vehicle Dash Cams?
- Mysterious 'Sandman' Threat Actor Targets Telecom Providers Across Three Continents
- Who's Hacked? Latest Data Breaches And Cyberattacks (Cybercrime Magazine)
- SANS Daily Network Security Podcast (Storm cast)

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