On August 23, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Juniper 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
25 August 2023

In The News This Week

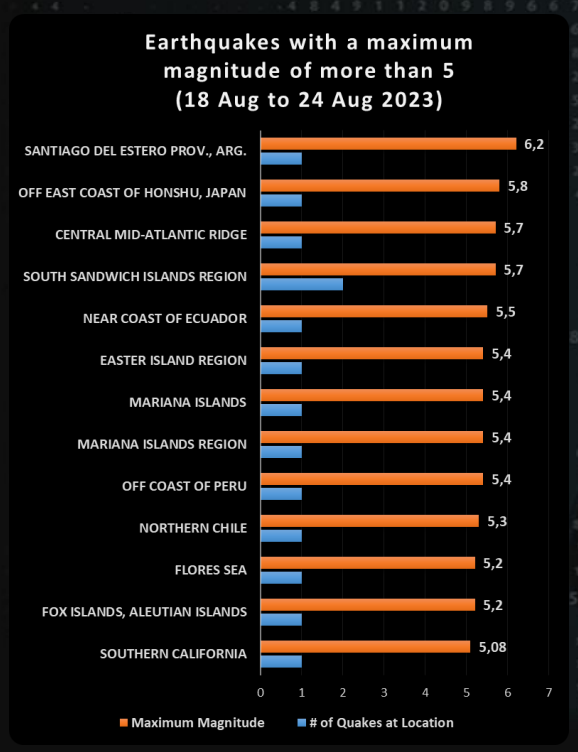
Check your SSDs: What to know about the SanDisk/Western Digital data loss disaster
If you use an SSD made by SanDisk or Western Digital, here's what you need to know and do now. - Are you backing up data to an external SSD made by SanDisk or Western Digital? Then you need to read on because you could be sitting on a ticking data loss time bomb that could cause you no end of headaches. Back in May, several outlets reported that Reddit users were complaining about failing SanDisk Extreme SSDs. Subsequently, replacement drives provided by Western Digital, SanDisk's parent company, were also reported to be failing. Western Digital then released a firmware update to address the issue. There was no mention of what users who had lost data should do, and it's unclear if this update fixed the issue.... According to the Western Digital's firmware update page, the impacted products are from the SanDisk Extreme Portable SSD V2, SanDisk Extreme Pro Portable SSD V2, and WD My Passport SSD line, and lists the models as follows: SanDisk Extreme Portable 4TB (SDSSDE61-4T00); SanDisk Extreme Pro Portable 4TB (SDSSDE81-4T00); SanDisk Extreme Pro 2TB (SDSSDE81-2T00); SanDisk Extreme Pro 1TB (SDSSDE81-1T00); WD My Passport 4TB (WDBAGF0040BGY). Users can enter their drive's serial number to find out if it is affected. According to reports, the drives appear to hit a problem once they are around half full, at which point they will start throwing up read and write errors. The drive then shows up as unformatted, and reformatting doesn't fix the issue. Is the data gone? Yes. There's nothing that the end user can do to recover it!
Read the full post by Adrian Kingsley-Hughes here: ZDNet

How Scammers Exploited ChatGPT To Unleash A Cryptocurrency Botnet On X (Twitter)
ChatGPT may well revolutionize web search, streamline office chores, and remake education, but the smooth-talking chatbot has also found work as a social media crypto huckster. - Researchers at Indiana University Bloomington discovered a botnet powered by ChatGPT operating on X—the social network formerly known as Twitter, in May of this year. The botnet, which the researchers dub Fox8 because of its connection to cryptocurrency websites bearing some variation of the same name, consisted of 1,140 accounts. Many of them seemed to use ChatGPT to craft social media posts and to reply to each other's posts. The auto-generated content was apparently designed to lure unsuspecting humans into clicking links through to the crypto-hyping sites." Read the rest of the story here: Verve Times

TP-Link Smart Bulb Vulnerabilities Expose Households to Hacker Attacks
Four vulnerabilities identified by academic researchers from Italy and the UK in the TP-Link Tapo L530E smart bulb and its accompanying mobile application can be exploited to obtain the local Wi-Fi network's password. - Currently a best-seller on Amazon Italy, the TP-Link Tapo smart Wi-Fi light bulb (L530E) is cloud-enabled and can be controlled using a Tapo application (available on both Android and iOS) and a Tapo account. The most severe of the identified issues is described as a "lack of authentication of the smart bulb with the Tapo app", which allows an attacker to impersonate a smart bulb and authenticate to the application. The issue has a CVSS score of 8.8.. Read the article by Ionut Arghire here: SecurityWeek

Tesla says data breach impacting 75,000 employees was an insider job
Tesla has said that insider wrongdoing was to blame for a data breach affecting more than 75,000 company employees. Tesla, the electric car maker owned by Elon Musk, said in a data breach notice filed with Maine's attorney general that an investigation had found that two former employees leaked more than 75,000 individuals' personal information to a foreign media outlet. "The investigation revealed that two former Tesla employees misappropriated the information in violation of Tesla's IT security and data protection policies and shared it with the media outlet," Steven Elentukh, Tesla's data privacy officer, wrote in the notice.." Read the story by Carly Page here: TechCrunch

Four teens hacked the MBTA (Massachusetts Bay Transport Authority) for free rides
About 15 years ago, three MIT undergrads found themselves in legal trouble for speaking out about security vulnerabilities in the MBTA payment system. By hacking the Charlie Ticket magstripe paper cards, the three students were planning on presenting their findings to a hacker conference with an enticing question: Want free subway rides for life?
Though the MIT students' talk was cancelled, the slides were published online. 15 years later, four high schoolers — Matty Harris, Scott Campbell, Noah Gibson and Zack Bertocchi — decided to pick up where the MIT students left off to see if the transit system fixed those exposed vulnerabilities. Spoiler alert: they didn't.
Two of the students, Harris and Campbell, joined All Things Considered host Arun Rath to explain their findings. What follows is a lightly edited transcript.....
Read the rest of the story by Kana Ruhalter and Arun Rath here: GBH



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

Choosing a Password Manager

After the LastPass breach, most computer users are a bit sceptical, and some are outright afraid to use a password manager. For those who do not know, LastPass, one of the most well-known password managers out there, where breached in late 2022, and the master password was stolen (to put it in simple terms). It had huge repercussions and the fallout went on until around May this year, and some are still affected. Yes, like with any piece of software, there is always a risk of something going wrong or someone compromising it, but the likelihood of the risk culminating is mostly very small, and the benefits could outweigh the risk.
Today I want to talk about password managers, how they work, why you would need a password manager, and how to choose one should you go that route.

Why do you need a Password Manager?

In today's electronic age we live in, we all need to register accounts on various online platforms like banking, social media, tax, insurance, etc. just to name a few, and all of these need a password or some form of authentication mechanism that includes a password. Like most people, you probably hate the fact that you have to remember a whole bunch of different passwords, or you take the easy way out and use the same password for most accounts. And, to remember the password, even the one you re-use all the time, you pick something easy. Well, easy for you is normally very easy for criminals to crack as well. However, it's the year 2023, and there are solutions to the problem, it is called password managers.

What is a Password Manager and how does it work?

Password managers are software applications (apps) that manage all your online logins and the password you need to authenticate your credentials for that specific site. The password manager generates new, random passwords for all the sites you visit. They store these encrypted credentials for you in a secure virtual or digital vault. At first, the password manager creates a master password. This master password is the only one you need to remember. The password manager then uses this master password to encrypt and decrypt your stored passwords. Then, when you visit a site or open an app where you need to log in, the password manager automatically fills in your login name and password for you. Most password managers can also fill in your personal information, like name, address, and credit card number on web forms to save you time during account creation or checkout when purchasing online. Some password managers can store your important documents or other credentials like safe codes and medical information in the vault, too.

There are multiple ways to categorize password managers, and some of the providers are offering a combination of the categories. For now, though, we will look at three of the technologies available and explain how they work. – These are: Locally installed or offline password managers, Web-based or online password manager services, and Stateless or token-based password managers.

Locally installed or offline password managers - As the name implies, locally installed password managers, also known as offline password managers, store your data on your device. It can be your computer or a smartphone, depending on your preference. You will find your passwords in an encrypted file, separately from the password manager itself. Some managers also allow storing each password in a separate file, greatly increasing overall security. As always, you need a master password to access your offline vault. If it's a strong one, there's a minimal chance that either the government or some hackers will break into your local database. That's because brute-forcing military-grade encryption requires a significant amount of time. What's more, if you keep that device with all passwords offline, there's no way to access it without seizing it. Naturally, offline password managers have some inherent flaws. For starters, using them on multiple devices might prove challenging. There's only one location, and other devices somehow have to sync with the one that has the vault.
✓ Pros: - (1) Minimises the risk that someone will breach your password vault, (2) Usually, it's a free service. ✗ Cons: - (1) You can access your vault on only one device, (2) If you lose your device, you lose your vault.

Web-based or online password manager services - By far, the most popular type, web-based password managers, store your passwords on a cloud, which is usually the provider's server. Such setup means that you can access your passwords from anywhere anytime, without the need to install the online password manager software. If accessing your vault via a web application is not possible, you would only need a browser extension or a mobile app. But how can one know if their passwords are not accessible to the provider? Well, all reputable online password managers use zero-knowledge technology. It means that they encrypt your data on your device before sending it to the server. It also means that your vault is available for access attempts to third-parties 24/7. What's more, all security measures mean nothing if there's key logger malware on your device, and you're not using two-factor authentication. Normally you won't even need to install the password manager client – most of the time, a browser extension will suffice.
✓ Pros: - (1) You can sync your vault across all your devices, (2) Premium subscription normally includes benefits like ark Web scanning, etc. ✗ Cons: - (1) You'll need Internet connectivity for authentication, (2) Your credentials are stored in an unknown location, (3) If the service provider is compromised, you are compromised (See LastPass reference above)

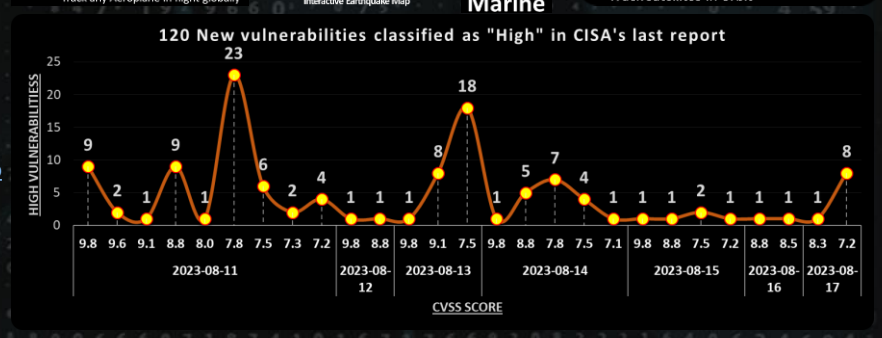
Stateless or token-based password managers - Last on the list are token-based or stateless password managers. In this scenario, a local piece of hardware, such as a flash USB device, contains a key to unlock your particular account. There's also no such thing as a password vault because the password manager generates them anew every time you log in. For additional safety, we recommend using not only the token but your master password too. This way, you'll be implementing two-factor authentication.
Stateless password managers don't require synchronization between your devices because there's no database in the first place.
✓ Pros: - (1) Your credentials are stored in a separate device ✗ Cons: - (1) If you lose your device, you lose your access, (2) This method usually requires proprietary hardware and software.

What Do You Look for When Picking a Password Manager? – (1) Security: Are you comfortable with the security the cloud-based provider is offering, or instead a vault created on your own device? The cloud-based option tends to be more popular, however, some people are more comfortable storing their details away from the cloud. (2) Compatibility: Will the app work with all your hardware and software and can it be accessed from any device? (3) Ease of use: Does it have a user-friendly interface? The system should use plain language, and browser extensions must work automatically. (4) Value: Free password management systems exist, but paid services may have better security and features. Look for unlimited password storage and features that offer the best value for your money.

Resources : CNET, PC Mag, CyberNews, PassworManager, How-to Geek

Other Interesting News and Cyber Security bits:

- Maru Towers secures infrastructure with cloud-based access control (Video)
- This AI-generated crypto invoice scam almost got me, and I'm a security pro
- 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