On November 16, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Citrix, Apple, and Mozilla products. (No further updates this week)
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 November 2022

In The News This Week

This Android File Manager App Infected Thousands of Devices with SharkBot Malware

The Android banking fraud malware known as SharkBot has reared its head once again on the official Google Play Store, posing as file managers to bypass the app marketplace's restrictions. A majority of the users who downloaded the rogue apps are located in the U.K. and Italy, Romanian cybersecurity company Bitdefender said in an analysis published this week. SharkBot, first discovered towards the end of 2021 by Cleafy, is a recurring mobile threat distributed both on the Google Play Store and other third-party app stores. One of the trojan's primary goals is to initiate money transfers from compromised devices via a technique called "Automatic Transfer System" (ATS), in which a transaction triggered via a banking app is intercepted to swap the payee account with an actor-controlled account in the background. It's also capable of serving a fake login overlay when users attempt to open legitimate banking apps, stealing the credentials in the process. Often, such apps offer seemingly harmless functionality, masquerading as antivirus software and cleaners to sneak into the Google Play Store. But they also double up as droppers that, once installed on the device, can fetch the malware payload. The dropper apps, now taken down, are X-File Manager, FileVoyager & LiteCleaner M. Read the rest of the article here: The Hacker News

Medibank: Hackers release abortion data after stealing Australian medical records

Hackers who stole customer data from Australia's largest health insurer Medibank have released a file of pregnancy terminations. - It follows Medibank's refusal to pay a ransom for the data, supported by the Australian government. Medibank urged the public to not seek out the files, which contain the names of policy holders rather than patients. CEO David Koczkaro warned that the data release could stop people from seeking medical attention. Terminations can occur for a range of reasons including non-viable pregnancy, miscarriages and complications. "These are real people behind this data and the misuse of their data is deplorable and may discourage them from seeking medical care," he said. The data of 9.7 million Medibank customers was stolen last month - the latest in a string of major data breaches in Australian companies in recent months..... Read the full story by Frances Mao here: BBC News

Microsoft: Popular IoT SDKs Leave Critical Infrastructure Wide Open to Cyberattack

Chinese threat actors have already used the vulnerable and pervasive Boa server to infiltrate the electrical grid in India, in spate of malicious incidents. - Microsoft this week identified a gaping attack vector for disabling industrial control systems (ICS), which is unfortunately pervasive throughout critical infrastructure networks: the Boa Web server. The computing giant has identified vulnerabilities in the server as the initial access point for successful attacks on the Indian energy sector earlier this year, carried out by Chinese hackers. But here's the kicker: It's a Web server that's been discontinued since 2005. It may seem strange that a nearly 20-year-old end-of-life server is still hanging around, but Boa is included in a range of popular software developer kits (SDKs) that Internet of Things device developers use in their design of critical components for ICS, according to Microsoft. Read the full story by Elizabeth Montalbano here: DarkReading

Buvers call for clarity over cyber war exclusions

Zurich-Mondelez dispute highlights need for insurers to be clear on 'war' cover with customers. - Cyberattacks instigated by Russia could be set to cause more disputes between businesses and insurers following the Zurich-Mondelez case. Nearly one in 10 small and medium sized enterprises (SMEs) that bought cyber insurance in 2022 did so as a precaution against the Russia-Ukraine conflict, meaning many new customers will take payouts on cyber claims for this reason for granted. This is according to research by GlobalData. According to its survey, nine percent of SMEs in the UK that purchased cyber insurance in 2022 said the Russia-Ukraine conflict was a key trigger for their purchase. Ben Carey-Evans, senior insurance analyst at GlobalData, said: "While it ranked behind several other key factors, businesses that cited this factor will certainly expect to be paid out if they are victims of a cyberattack for this reason". Read more here: StrategicRISK

Hackers guessed the world's most common password in under 1 second—make sure yours isn't on the list

- NordPass, the password management tool from the team behind NordVPN, released its list of the 200 most common passwords in 2022 — and it turns out people are still using notoriously weak passwords. The most common password in the world this year was the infamously bad "password", and it took hackers under one second to crack it. The same goes for the second and third most common passwords: "123456" and "123456789", respectively. NordPass compiled its list with the help of independent cybersecurity researchers who analyzed a three-terabyte database to produce their findings. The list is full of fascinating (and cautionary) tidbits. For instance, nearly 5 million people around the world used "password" as their password. And of the 20 most common passwords, 18 were guessed in under one second. The most important takeaway, though? If your password is on the list, it's time to make a change. Find the list here: CNBC

2FA, 3FA, MFA... What does it all mean?

In the last few months, I had numerous conversations about the various digital authentication methods available and required by organisations nowadays. The conversations I had with people in the security fraternity hovered around the effectiveness and even the validity of multifactor authentication. On the other side of the coin, in conversations with the general security layman was all about "what is it?" and "which is better?" In this post, I want to address the "What is it?" question, as many people who are not part of the security fraternity are getting lost in the security acronym jungle. HELPNETSECURITY recently posted and article that I thought answer this question in simple language that you can even share with your grandmother or younger child.

2FA, 3FA, MFA... What does it all mean?

Simply put, authentication is the act of proving you are who you say you are. To gain access to protected information, systems or locations, the user must prove their identity by providing specific access credentials.
The system asks: "Who are you? Prove it." When the user successfully authenticates (and depending on the permissions associated with their account), the system allows them to perform specific actions, access specific information or specific physical locations.
Identification requires a user ID (e.g., a username). To prove their identity, users then provide a password or another authentication factor, which is then paired with the username. The combination may or may not result in the user gaining access to the system.
Multi-factor authentication (MFA) is the process in which the user must provide two or more pieces of evidence (i.e., factors) to a system or location, in order to be let in. MFA protects a system, location, or sensitive data from being accessed by an unauthorized user (and potential threat actor).

Types of authentication factors

There are several main categories of authentication factors:

- Knowledge factors (something the user knows): E.g., a password, a passphrase, or a PIN. Security questions fall in this category but are no longer recognized as an acceptable authentication factor because the widespread use of social media made the answers easily obtainable to attackers.
- Possession factors (something the user has): The user can verify their identity with an object in their possession, such as an access card, key fob, or another physical security token. MFA systems also consider a one-time password/code received by the user via SMS or authenticator app as a possession factor (a software token).
- Inherence factors (something the user is or does in a particular way): This type of authentication factor is based on a biometric characteristic of the user – fingerprint, palm print, iris, face – or on how the user uniquely performs an action (e.g., their typing or vocal timbre and pattern).

In an MFA setup, if one factor can't be provided or is incorrect, the user will not be given access!

Contextual information

Contextual information may also influence whether an authentication attempt will be successful. This information may not be an authentication factor by itself, but it may help authentication systems assess whether a login/access attempt is legitimate.
This information includes:

- Location: The physical location of the user/device when they are logging in. For instance, if all employees are in the US and the login request comes from an unknown/unsanctioned location or network, the system may deny access based on that information (because it believes the authentication credentials and factors have been compromised).
- Time: The specific timing of a login request may point to its potentially malicious nature. A system can be programed to deny login attempts outside of regular business hours, or to deny a login request seemingly made by the same user that logged in just moments before – if that second login request is apparently coming from another country.

What is 2FA?

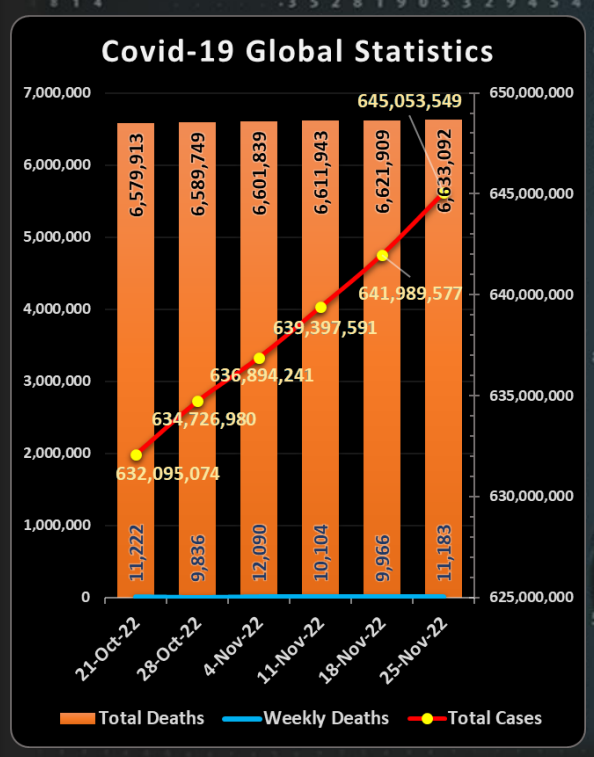
Two-factor authentication (**2FA**) is an authentication setup that requires the user to provide two authentication factors to be granted access. The withdrawal of money from an ATM is an example of 2FA in action: The user can withdraw money only with the correct combination of a bank card (possession factor) and PIN (knowledge factor). Another example: The user wants to access an online account protected by 2FA. They need to provide the correct password (knowledge factor) and one-time password (possession factor) available only on the users' device/smartphone (either sent via SMS or provided via an authentication app). 2FA is currently the most used MFA method, but as technology evolves and attackers come up with effective ways to bypass the protection it offers, businesses will have to implement 3FA, 4FA, etc.

What is 3FA?

Three-factor authentication (**3FA**) is a more secure authentication process that adds a third layer of protection to user accounts. It requires users to provide three distinct authentication factors. For example: a password, a security card, and their fingerprint (to be scanned and compared to a previously created record). Or a PIN, an OTP password, and their voice (to be compared with a recorded audio file).
With 3FA in place, stolen passwords become much less of a problem. 3FA is usually deployed by businesses and organizations that require a high level of security, e.g., banks, government agencies, airports, hospitals, etc.

Why do we need multi-factor authentication?

The threat landscape is constantly evolving. Attackers have noticed that more individuals work remotely than ever before and that cloud-based solutions have become standard across different sectors. As a result, securing access to various systems and assets has become paramount. Compromised user credentials represent one of the greatest risks to organizations. To better protect personal, commercial, and public resources from unauthorized access, employing multi-layered (multi-factor) authentication is becoming normal. Traditional passwords are simply not enough anymore, especially since users often reuse the same weak passwords on different websites and services.
Please read the rest of the article here if you want to know more.

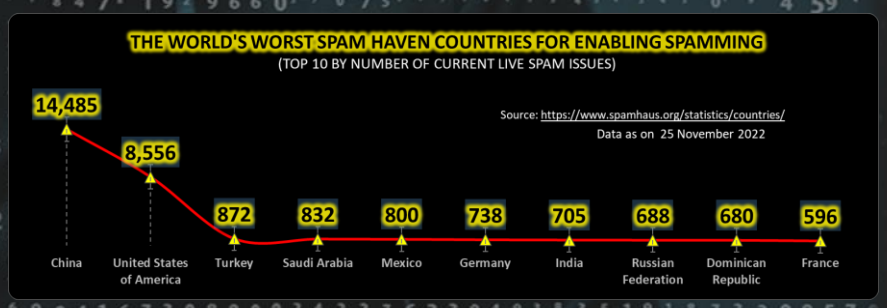


For Reporting Cyber Crime in the USA go to (IC3) , in SA go to Cybercrime, in the UK go to ActionFraud

Other Interesting News and Cyber Security bits:

- FP Summit Food + 2022 Food Security & Supply Chain Summit, 14 Dec 2022
- How BlackBerry moved from iconic cellphones to cybersecurity
- Is this really the end of Twitter?
- 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