On December 21, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to a joint cybersecurity advisory that was released by FBI and CISA.
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
23 December 2022

In The News This Week

'Russian Hackers' Help Fraudsters Hijack JFK Airport's Taxi Dispatch

DoJ charges allege they hacked into the taxi dispatch system for profit, selling the ability for cab drivers to skip the line for picking up a fare at JFK terminals. - Two Americans have been indicted for hacking the New York taxi industry. With the help of two Russian nationals, Daniel Abayev and Peter Leyman are accused by the Department of Justice and the Port Authority of New York and New Jersey of breaching the John F. Kennedy International Airport taxi dispatch system and selling slots to cabbies who wanted to skip to the head of the line to pick up the next airport fare. New York cabs at JFK airport are required to wait in a holding lot, and line up and pick up the next fare in the order they arrive. During their intercepted text messages with the Russian nationals, Abayev asked the hackers, "I know that the Pentagon is being hacked, so why can't we hack the taxi industry?" Read the rest of the article here: DarkReading

LastPass Admits to Severe Data Breach, Encrypted Password Vaults Stolen

The August 2022 security breach of LastPass may have been more severe than previously disclosed by the company. The popular password management service on Thursday revealed that malicious actors obtained a trove of personal information belonging to its customers that include their encrypted password vaults by using data siphoned from the earlier break-in. Also stolen is "basic customer account information and related metadata including company names, end-user names, billing addresses, email addresses, telephone numbers, and the IP addresses from which customers were accessing the LastPass service," the company said. The August 2022 incident, which remains a subject of an ongoing investigation, involved the miscreants accessing source code and proprietary technical information from its development environment via a single compromised employee account. Read the full story by Ravie Lakshmanan here: The Hacker News

Canada - Toronto's Hospital for Sick Children dealing with cybersecurity incident

Toronto's Hospital for Sick Children is still dealing with a cybersecurity incident so serious it declared a 'Code Grey' — meaning an IT system failure. On Monday, the hospital said the incident appears to have only impacted a few internal clinical and corporate systems, as well as some hospital phone lines and webpages. "All patient care is continuing while SickKids investigates and works to resolve the situation," the hospital said in a statement. "Upon learning of this incident, we immediately activated the hospital's incident management command centre and launched an investigation to determine the nature and scope of the incident. At this time, the incident appears to have only impacted a few internal clinical and corporate systems, as well as some hospital phone lines and webpages. Downtime procedures have been activated where needed." It has notified the province and expert third parties to resolve the incident as soon as possible. For now, the public may experience difficulties calling into the hospital, and accessing some webpages such as AboutKidsHealth.ca (SickKids' health information site) and the hospital's Careers application portal, the hospital said.
Read the article by Howard Solomon here: ITWorld Canada

Ghana - Unlicensed cyber security providers can't operate from Jan. 2023

Effective January 2023, cyber security service providers, cyber security establishments and cyber security professionals who fail to register and obtain licenses from the Cyber Security Authority (CSA) cannot provide services for any entity or individual. This follows the strict enforcement of a mandatory licensing regime for cyber security professionals by January next year as part of measures to sanitise Ghana's cyberspace. Firms and individuals who fail to comply with the directive will attract both criminal and administrative sanctions. This came to light in a speech read on behalf of the Director-General of the CSA, Albert Antwi-Boasiako, by the Deputy Manager in charge of International Cooperation at the authority, Emmanuella Darkwah, at the opening of a national roundtable on addressing Ghana's cyber security capacity need.
Read the full story here: BussinessGhana

Ransomware gang uses new Microsoft Exchange exploit to breach servers

Play ransomware threat actors are using a new exploit chain that bypasses ProxyNotShell URL rewrite mitigations to gain remote code execution (RCE) on vulnerable servers through Outlook Web Access (OWA). - Cybersecurity firm CrowdStrike spotted the exploit (dubbed OWASSRF) while investigating Play ransomware attacks where compromised Microsoft Exchange servers were used to infiltrate the victims' networks.llars. To execute arbitrary commands on compromised servers, the ransomware operators leveraged Remote PowerShell to abuse the CVE-2022-41082, the same bug exploited by ProxyNotShell. "In each case, CrowdStrike reviewed the relevant logs and determined there was no evidence of exploitation of CVE-2022-41040 for initial access," the researchers said. "Instead, it appeared that corresponding requests were made directly through the Outlook Web Application (OWA) endpoint, indicating a previously undisclosed exploit method for Exchange." ...
Read the full story by Sergiu Gatlan here: Bleeping Computer

Safeguard Technology Christmas gifts before wrapping it.

Sunday the world will celebrate Christmas, and as many parents' pockets are emptied on technology gifts for their kids, we must remember that threat actors are waiting for those new unprotected gifts to get online. Whether it is a phone, tablet, game console, or computer, by the time it hits the shelves, those devices are at least three months behind in security updates. Although manufacturers are trying their utmost to ship these devices with the latest security controls in place, new threats are emerging so fast that the device can be outdated before it is even boxed. With this in mind, The Argus published an article this week with some advice for parents on how to safeguard your children before even wrapping up their new devices. From a personal view, I also recommend changing the default DNS settings on your kid's computers to point to a "safe" DNS service like Cisco's OpenDNS Family Shield, or other offerings depending on your DNS needs, its free.

Set up safety features on devices before Christmas, parents advised (The Argus)

Child psychologist Dr Linda Papadopoulos, who is an ambassador for child online safety group Internet Matters, said setting up new gadgets ahead of time could help parents "stay in control" of what their children access. Internet Matters' guidance suggests parents download any apps their child may use ahead of time, so it is ready to go when handed to them and to use available parental controls for internet browsers and app stores to ensure their children do not encounter any inappropriate content.

Dr Papadopoulos said: "Enforcing internet safety with children can feel overwhelming for parents, especially during the Christmas break when children have ample time to game or they're using new digital devices they received as a gift that parents might struggle to wrap their heads around. "The dos and don'ts of internet safety can feel overwhelming, especially during the festive season when time feels like it's moving faster. "With this in mind, setting up safety features straight away will ensure you can stay in control of what your children can access and when, to give them a better experience from the get-go." A range of online guides and resources can be found on the Internet Matters website, with Dr Papadopoulos recommending learning about whatever device or platform your child will end up using.

Additionally, she also encouraged parents to talk to their children generally about internet safety to make it easier for youngsters to come to them should they encounter any issues online. She said: "Talk to your child about their digital life this festive season, so they feel comfortable coming to you if something goes wrong. "Talking to them from an early age makes it easier to maintain good communication. Be sure to have bitesize conversations that are relevant to them. "Choose to talk when you are due to spend some time together, like over a meal or during their bedtime routine. Bring digital experience into normal, everyday conversations."

"Internet Matters has many online guides, but for the sake of space in this post, I had to choose one the most common phones and tablets kids are using and as Apple is first in the list, I list controls for these devices. For Android and other devices, please visit Internet Matters – Parental Controls"

Apple iPhone & iPad Controls & Settings guide – restrictions you can apply (A pictorial of the steps below is available here)
(1) **Enable screen time** - Using Screen Time to set content privacy restrictions and manage in-app purchases - Go to "Settings" and tap "Screen Time".
(2) Tap Continue, then choose "This is My [Device]" or "This is My Child's [Device]." - If it's a shared device and you'd like to ensure settings are not changed then tap "Use Screen Time Passcode". Then re-enter the passcode to confirm. If it's a child's device, you can follow prompts until you get to Parent Passcode and enter a passcode. Re-enter to confirm.
(3) Tap Continue, then choose "This is My [Device]" or "This is My Child's [Device]." If it's a shared device and you'd like to ensure settings are not changed then tap "Use Screen Time Passcode". Then re-enter the passcode to confirm. If it's a child's device, you can follow prompts until you get to Parent Passcode and enter a passcode. Re-enter to confirm.
(4) **Managing in-app purchases in Screen Time** - Tap "iTunes & App Store Purchases". Choose a setting and set it to "Don't Allow". Please note you can also change your password settings for additional purchases from the iTunes & App Store or Book Store. Follow steps 1-3, then choose Always Require or Don't Require.
(5) **Guided Access** - Guided Access allows you to lock your iPhone or iPad when in an app. This may be useful for children as they won't be able to come out of that particular app and will stop them from accessing other apps and settings. To enable: Go to your "Settings" tap "Accessibility" then scroll down and tap "Guided Access".
(6) Tap the Guided Access toggle so it turns green. Then to start the Guided Access, tap the side (power) button three times. When enabled, the buttons and touchscreen will be disabled. In this section, you can also set a passcode, time limit and enable auto-lock features.
(7) You can change the options which will appear in the bottom left of your screen which will allow the configure the settings for the app you or your child is on. Tip: Alternatively, you can easily turn on Guided Access by giving the command to Siri which Siri will automatically do for you.
(8) **Prevent web content** - iOS can automatically filter website content to limit access to adult content in Safari and apps on your device. You can also add specific websites to an approved or blocked list, or you can limit access to only approved websites. Follow these steps: Go to Settings, then Screen time. Tap 'Content & Privacy Restrictions' and enter your Screen Time passcode. Then, tap 'Content Restrictions', then tap 'Web Content'. Choose one of the following: Unrestricted Access, Limit Adult Websites, or Allowed Websites Only.
(9) **Restrict game centre** - Go to Settings, then Screen time. Tap 'Content & Privacy Restrictions' and enter your Screen Time passcode. Then, tap 'Content Restrictions' Scroll down to Game Center, then choose your settings. You can restrict these Game Center features: – Multiplayer Games, Adding Friends, Screen Recording - To turn it off, tap the side button three times.
(10) **Turn off tracking** - If you have the iOS 14.5 update or above, the App Tracking Transparency feature lets you decide if you want apps to track your activity for advertising purposes. This may not be suitable for children as it may encourage in-app spending. To disable: Go to Settings, then 'Privacy'. Tap 'Tracking'. The toggle button should be grey – this means the feature is disabled. Green means enabled.
(11) **Allow changes to privacy settings** - The privacy settings on your device give you control over which apps have access to information stored on your device or the hardware features. Go to Settings, then Screen time. Tap 'Content & Privacy Restrictions' if asked, enter your Screen Time passcode. Tap 'Privacy', then choose the settings you want to restrict.
(12) Allow changes to other settings and features - You can allow changes to other settings and features, the same way you can allow changes to privacy settings. Go to Settings, then Screen time. Tap 'Content & Privacy Restrictions' if asked, enter your Screen Time passcode. Always Allowed, select the features or settings you want to allow changes to and choose Allow or Don't Allow.

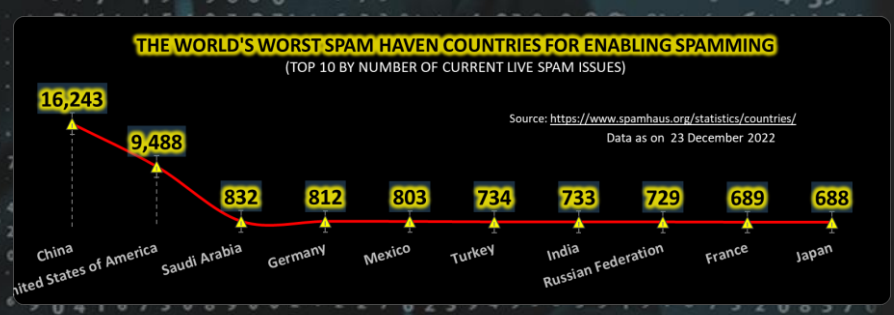
Visit Internet Matters

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:

- LinkedIn has massively cut the time it takes to detect security threats. Here's how it did it
- 18 cybersecurity predictions for 2023
- I started my own Mastodon server on a Raspberry Pi. Here's what I learned
- 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