On May 11, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in F5, Google, Microsoft, and Adobe products..
CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
13 May 22	519,878,295	6,284,865

Deaths this week: 12,693

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
13 May 2022

In The News This Week

Beware: This cheap and 'homemade' malware is surprisingly effective

A powerful form of trojan malware that offers complete backdoor access to Windows systems is being sold on underground forums for the price of a cup of coffee – and it's being developed and maintained by one person. Known as DCRat, the backdoor malware has existed since 2018 but has since been redesigned and relaunched. When malware is cheap it's often associated with only delivering limited capabilities. But DCRat – offered online for as little as $5 – unfortunately comes equipped with a variety of a functions, including the ability to steal usernames, passwords, credit card details, browser history, Telegram login credentials, Steam accounts, Discord tokens, and more... Read the rest of the story by Danny Palmer here: ZDNet

Spain's Intelligence Service Leader Is Ousted

MADRID — The chief of Spain's intelligence agency was ousted by the government on Tuesday following the disclosure that her agency had used powerful spyware to infiltrate the cell phones of Catalan separatist politicians. The government's dismissal of Paz Esteban — who was the first woman to run the intelligence agency, known in Spain as C.N.I., for the Centro Nacional de Inteligencia — is the most serious consequence so far of a phone-hacking scandal involving the Pegasus spyware developed by an Israeli company, an issue that has been roiling Spanish politics. Ms. Esteban was removed only days after she appeared before a parliamentary committee to discuss how her agency had used Pegasus... Read the article by Raphael Minder here: New York Times

South Africa - 3.7 million client records compromised in Dis-Chem data 'incident'

JSE-listed Dis-Chem Pharmacies has disclosed that a data "incident" involving a "third-party service provider or operator" has led to the compromise of millions of client records containing personal information. It has not named the third party. Dis-Chem revealed the incident in a notification published on its website in terms of section 22 of the Protection of Personal Information Act. The incident affects almost 3.7 million Dis-Chem customers, with the following information compromised: First names and surnames, E-mail addresses, & Cell phone numbers. "Based on the categories of personal information impacted, there is a possibility that any impacted personal information may be used by the unauthorised party to commit further criminal activities, such as phishing attacks, e-mail compromises, social engineering and/or impersonation attempts," Dis-Chem said. Read the rest of the story by Duncan McLeod here: TechCentral

Russia's RuTube knocked out for second day by Victory Day cyber attack

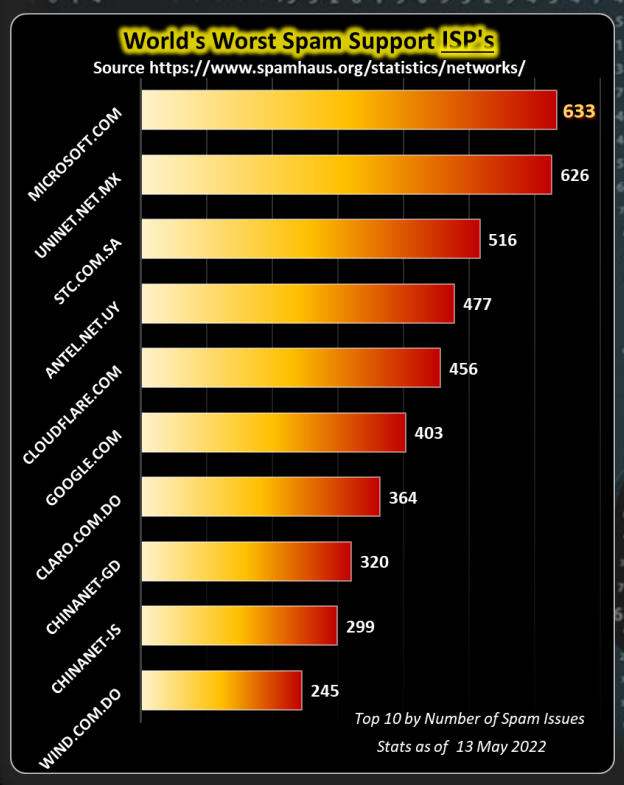
RuTube, Russia's answer to YouTube, was crippled for a second day on Tuesday by a cyber attack whose timing it linked to this week's anniversary celebrations of victory over Nazi Germany in World War Two. Usually packed with video content, RuTube's site is currently black, with a short message reading: "Attention! The site is undergoing technical work. The site was attacked. At the moment the situation is under control. User data has been saved. "The attack began on Monday, a major national holiday when Russia commemorated the Soviet victory over Adolf Hitler and President Vladimir Putin delivered a speech likening that struggle to the current war in Ukraine. "Someone really wanted to prevent RuTube from showing the Victory Day parade and celebratory fireworks," RuTube said. "It is not a sin to remember the battles our guys won. The battle for RuTube continues." Read the rest of the article here: Reuters & Daily Swig

Sinister Russian hacking group threatens to shut down hospital ventilators in Britain

A shadowy Russian hacking group has threatened to shut down ventilators at British hospitals after an alleged member of their gang was arrested in the UK. The hacker, 23, was arrested in Tottenham, north London on Monday after Romanian government websites were attacked. Now, members of the sinister Killnet Russian hacking group have demanded his release and threatened to target life-saving ventilators if their demands aren't met. It is unclear if Killnet are supported by the Russian government - though spy agencies from the Five Eyes alliance - made up of Australia, Canada, New Zealand, the UK and US - have described it as a Russian-aligned group acting in the Kremlin's interests..
Read the full article by Danyal Hussain here: Daily Mail

Hackers Infiltrated Multiple U.S. Law Enforcement Data Systems

The hacker apparently gained access to the databases May 8 through the DEA's EPIC System portal, which is distinct from the esp.usdoj.gov portal that requires much more strict government authentication. Krebs wrote that the EPIC system apparently only requires a username and password without even a request for two-step authentication.
Read the full article by Kyle Barr here: Gizmodo



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

Do an Internet search on yourself, you will be surprised by what you will discover! There might even be something you didn't know about yourself!

How to remove yourself from Internet search results and hide your identity

Charlie Osborne posted a step-by-step guide this week in ZDNet's Zero Day blog on reducing your digital footprint online, whether you want to lock down data or vanish entirely. I'm sure that it will be an interesting read for many in this day and age of digital identity theft. Below is an extract of her post.

Charlie Osborne wrote:

There is now a very thin line, easily broken, which separates our physical and digital identities. Social networks have evolved from the days of MySpace to valuable, data-slurping machines that have information on everything from our friends and family to our voting habits. When you apply for a new job, many employers will try to find and evaluate your social media presence to ascertain if you are a suitable candidate. A Google search that reveals an old conviction can make it more difficult to get hired, and -- whether true or not -- allegations of criminal conduct spread online can cause misery and impact your mental wellbeing and job prospects in the long term. The internet never forgets. As I discovered, old online posts can come back to haunt you. A misjudged tweet from years ago or an inappropriate Facebook photo can destroy future job prospects or ruin a career. If you want to take control of your privacy and online data, here are some tips to get you started.

Google and other search engines - The Google search engine, among others such as Bing and Yandex, can be used to uncover exactly what information about you is public and what the average person can quickly find out without the need for advanced tools, social engineering, or Open-source intelligence (OSINT). Once you know what is online, you can start tackling the problem. Run a quick search and note any website domains that flag you, social media account links, YouTube videos, and anything else of interest.
The Have I Been Pwned service is run by cybersecurity expert Troy Hunt and can be a useful tool to discover if any account information belonging to you has been compromised or included in a data breach. If you find an email address connected to you has been pwned, check to see what data breaches you have become embroiled in -- and make sure you change your passwords as quickly as possible.
Google accounts - Make sure you visit the Google Account page, where there are numerous settings that can boost your privacy, reduce data collection, or remove you altogether from the ecosystem. The Google Privacy checkup allows users to prevent Google from saving your searches and other Google activity to your Google Account and turn off your location history. You can also choose to disallow Google from saving web and app activities, Chrome history, YouTube history, voice and audio, and other data. Google has also introduced an auto-delete function for data stored. In this section, you can also choose whether or not to allow Google to use your information for tailored advertising. The Google Security checkup can be used to show you which devices have access to your account, including laptops, PCs, and handsets. You can also find a list of any third-party applications which have been granted permission to access your account. Revoke permissions as necessary. In addition, if Google finds an online account with your email and password, you will see an alert here. Delete me; found under Account Preferences, Google's deletion service can be used to delete select products or remove your account entirely. You can also download a copy of all your data.

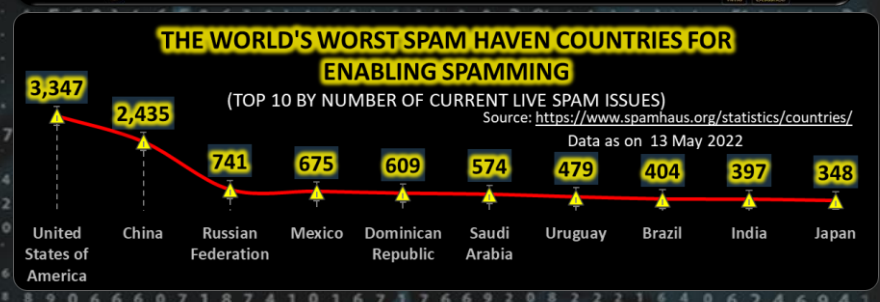
Lockdown your social media accounts or delete primary accounts entirely

Facebook: In the Settings tab, you can download all of Facebook's information on you. You should also take the opportunity to lock down your account. In the Privacy tab, you should restrict your posts to 'friends only,' limit your past posts, and you can also decide to disallow lookups through your provided email address or phone number. An important element that shouldn't be overlooked here is the option to remove your Facebook profile from search engine results outside of the social networking platform. Under the Location tab, consider turning off location data collection by Facebook, too.
Twitter: Twitter also allows users to request their archive, which is all the information collected from you. This option can be found under the Settings and privacy tab. In the settings area, you can also choose to lock down your account entirely and make tweets private and only viewable by those with your approval; you can turn off tweets containing location data; you can decide whether or not to allow email and phone number searches to connect others to your profile, and you can choose whether or not to allow others to tag you in photos. Under the Safety portion of the tab, you can prevent your tweets from appearing in the search results of those you have blocked on the micro-blogging platform. You can also deactivate your account entirely.
Instagram: Facebook-owned Instagram has a number of privacy settings you can also change to maintain an acceptable level of privacy. By default, anyone can view your photos and videos on your Instagram account unless you are a minor. However, by going to your profile, clicking Settings, Account Privacy, and switching 'Private account' on, you can make sure your content is only viewed by those you approve.
Remove everything: A more extreme option is to delete all of your primary social media accounts completely. In order to do so on Facebook, you can go to Settings & Privacy>Settings>Your Facebook Information>Deactivation & Deletion to deactivate it. This gives you the option to return at a later time and does not delete your data. Your settings, photos, and other content are saved, but you will not appear beyond unclickable text. Deactivating your account gives you the option to take a break and return later and will take you off searchable results. However, you can also permanently delete your account. If you have trouble finding this setting, you can also type "delete Facebook" in the Help Center tab. A grace period of 90 days is given before the deletion of content starts.
In order to deactivate Twitter, you need to click on Settings and privacy from the drop-down menu under your profile icon. From the Account tab, you can then click deactivate.
To delete your Instagram account, log in and go to the request deletion page. Once you have submitted an answer as to why you are deleting your account, you will be prompted to re-enter your password, and then a delete account option will appear.

That is all I have space for in this post, but there is much more to be said in Charlie's post, please check it out on ZDNet

Other Interesting News and Cyber Security bits:

- Beach Bot, an AI rover that will clean up the beach
- IBM dumping Watson Health is an opportunity to re-evaluate artificial intelligence
- SANS Daily Network Security Podcast (Storm cast)



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