On July 6, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Mozilla and Google products.
(No update this week)
CIS Security Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
15 Jul 22	565,608,859	6,382,619

Deaths this week: 13,232

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
15 July 2022

In The News This Week

Ex-CIA engineer convicted of biggest theft of secret information in agency's history

A former CIA programmer was convicted Wednesday of federal charges in connection to the massive Vault 7 theft of secret information provided to WikiLeaks in what the Justice Department describes as "one of the most brazen and damaging acts of espionage in American history." Joshua Adam Schulte was once a CIA programmer "with access to some of the country's most valuable intelligence-gathering cyber tools used to battle terrorist organizations and other malign influences around the globe," according to a statement released by U.S. Attorney Damian Williams. However, when Schulte "began to harbor resentment toward the CIA, he covertly collected those tools and provided them to WikiLeaks, making some of our most critical intelligence tools known to the public – and therefore, our adversaries," Williams, of the Southern District of New York, said. .. Read the full story by Danielle Wallace here: Fox News

10,000 organisations targeted by phishing attack that bypasses multi-factor authentication -

Microsoft has shared details of a widespread phishing campaign that not only attempted to steal the passwords of targeted organisations, but was also capable of circumventing multi-factor authentication (MFA) defences. The attackers used AiTM (Attacker-in-The-Middle) reverse-proxy sites to pose as Office 365 login pages which requested MFA codes, and then use them to log into the genuine site. According to Microsoft's detailed report on the campaign, once hackers had broken into email inboxes via the use of stolen passwords and session cookies, they would exploit their access to launch Business Email Compromise (BEC) attacks on other targets. By creating rules on victims' email accounts, the attackers are able to then ensure that they are able to maintain access to incoming email even if a victim later changes their password. The global pandemic, and the resulting increase in staff working from home, has helped fuel a rise in the adoption of multi-factor authentication. Cybercriminals, however, haven't thrown in the towel when faced with MFA-protected accounts...
Read the full story by Graham Cluley here: TripWire .. and more here: Bleeping Computer

The Man at the Center of the New Cyber World War

Yurii Shchyhol's job is to protect Ukraine against ongoing Russia cyberattacks. But the war he's fighting is global, he says — and he has some advice for the rest of us. Ukraine has long been Russia's cyberwarfare sandbox, a proving ground for the Kremlin to trial new techniques and new malware viruses. Since Russia launched a full-scale invasion of the country on Feb. 24, Ukraine has seen those attacks increase threefold, according to Ukrainian officials — hitting everything from civilian and military agencies to communications and energy infrastructure. Those attacks have not been isolated to the roughly 40 million residents of Ukraine. Russian cyberespionage and cyberattacks since the start of the invasion have been recorded in 42 countries across six continents — the majority of which are NATO countries or those that supplied aid packages to or voiced support for Ukraine. In April, the Department of Justice said that U.S. officials had discovered malware planted by Russian military forces in computers across the world and had removed the malware before it could be activated into a "botnet," a network of computers used in mass cyberattacks... Read the full article by Kenneth R. Rosen here - Politico

Man hacks woman's Instagram account ahead of wedding!

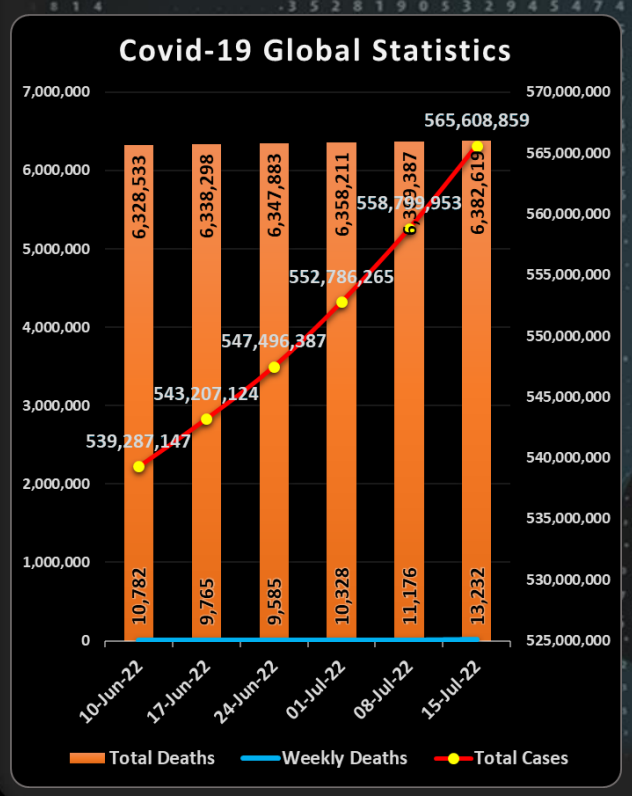
India, Mumbai - Man arrested for hacking woman's Instagram account in a bid to defame her name. - A man from Uttar Pradesh has been arrested for allegedly hacking a city woman's Instagram account days before her wedding and announcing that she was going to run away before the wedding. The woman, a resident of Goregaon east, was engaged in May and got married last month. The woman's parents had posted her wedding invitation on social media and also sent soft copies of the invitation to their relatives through WhatsApp on June 10. A day later, the woman noticed that her Instagram account had been hacked by an unidentified person and her wedding invitation card was posted on it with a message: "This woman is going to leave her groom and run away from her wedding." The accused also claimed that the woman was known to him and was in his contact. "As soon as the woman learnt about the hack, she informed her parents and finance, who approached the police and reported the incident. Based on their complaint, we registered a case against the unidentified person," said a police officer from Vanrai police station.... Read the rest of the post here: Hindustan Times

PayPal phishing kit added to hacked WordPress sites for full ID theft

A newly discovered phishing kit targeting PayPal users is trying to steal a large set of personal information from victims that includes government identification documents and photos. Over 400 million individuals and companies are using PayPal as an online payment solution. The kit is hosted on legitimate WordPress websites that have been hacked, which allows it to evade detection to a certain degree. Researchers at internet technology company Akamai found the phishing kit after the threat actor planted it on their WordPress honeypot. The threat actor targets poorly secured websites and brute-forces their log in using a list of common credential pairs found online. They use this access to install a file management plugin that allows uploading the phishing kit to the breached site. Read the rest of the article by Bill Toulas here: Bleeping Computer

Johnson & Johnson CISO Marene Allison: 'You can't sit on today's technology'

The CSO Hall of Fame inductee stresses the importance of having a roadmap that allows you to anticipate what's coming and pivot quickly. . The oath Marene Allison took years ago to defend and protect the United States is the same tenet that now guides her work maintaining cybersecurity at one of the largest pharmaceutical and consumer packaged goods manufacturers in the world. "It's like I raise my hand [in an oath] every morning and the mission is to protect and ensure the viability of my company in the cyber world," says Allison.
Read her story by Sharon Gaudin here: CSO



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

Privacy on Social Media Guards Against Identity Theft

I am sure that most of you have heard or know someone who has been a victim of some sort of online fraud where the victim's private identity information was used to commit the crime. In fact, we hear about it so often in the news that we became a little desensitized to the severity of the problem. Social media is one of the prime sources of personal information which lies ripe for criminal pickings. Julie Myhre of Business News Daily recently posted an article with some tips and pointers on social media privacy which I felt is worth sharing today in the extract below.

How to protect your privacy on social media

By definition, social media is all about sharing information, whether it's photos, articles or even your thoughts. But how safe is it to be sharing your personal identity and private information on social media? Active social media users are 30% more likely to be affected by identity fraud; account holders on Snapchat, Facebook and Instagram are the most likely victims, with a 46% higher risk.
More than 5% of 2019 consumers were victims of identity theft for almost $17 million in damages – an increase of over $2 million from the previous year – according to the 2020 Identity Fraud Report by Javelin Strategy & Research, one of the top comprehensive analysts of identity fraud.

1. Keep your personal information private.
A previous Javelin report studied media behaviors and found that 68% of people with public social media profiles shared their birthday, with 45% of those users sharing their full birthdate; 63% shared the name of their high school; 18% shared their phone number; and 12% shared their pet's name. It is always safer to omit information about yourself than include it on your social media. Just because there is an option to include your current city doesn't mean you have to. Give a generalized version of that information or no information at all. For example, the San Francisco Bay Area is a general option for Burlingame, California. This still gives some information, but makes it a little more difficult to figure out your ZIP code or home address.
2. Set strict privacy settings - Go into the settings for your Facebook, Twitter, Pinterest, Instagram, and LinkedIn to edit your privacy settings. Make sure all of your personal information – such as your birthday, current location and workplace – is private or visible only to your friends. When your privacy settings are more lenient, you're giving strangers easy access to all of your information. They won't even have to hack into your account to discover everything they might be looking for.
3. Don't tag or post your specific location - The location tag is a fun feature, but not everyone needs to know where you are at all times. It makes you and your home vulnerable, especially if your profile is public. It's cool to let your social media friends know that you're at Disneyland with your sister, but you're also letting everyone know that you're more than 100 miles away from your home, which makes it available for break-ins.
4. Know your friends/connections - It's important not to make yourself or your information vulnerable to people you have never met in real life. A lawyer, Steven J.J. Weisman said that befriending people you don't know makes it easier for them to use the information on your social media to find out more about you. "These 'friends' who don't know you gain access from your Facebook page to personalized information that often can be used to make you a victim of identity theft," he said, "often by providing information that can permit someone to learn or reasonably guess your email address or answer your security questions." Don't add someone as a friend just because they send you a request. There is a "decline" button, and you should use it on a suspicious friend request.
5. Always log out of your social media - This is especially important when you use a public computer, such as at a library or hotel. The reality is that we all have some private information on our social media account – even if it's only our name and a photo – and you don't want to give someone easy access to your identity. Leaving your account open allows anyone who next sits down at that computer to see all of your recovery email addresses, phone numbers, credit card information, private messages, and friends and family.
6. Use strong passwords - Passwords are one of the keys to your identity, so make them effective. The best passwords combine letters, numbers and punctuation marks in randomized, nonsequential order. Avoid using full words and anything related to your birthday or current and previous addresses, these are the first keywords hackers will guess when attempting to log in to your accounts.
7. Use an internet security software suite - Internet security software protects your identity when you're surfing the web or using social media. As Weisman said, sometimes you will open a link or download a file in a message from a "friend," and it contains a keystroke malware program that can steal all your personal information from your computer. One way to prevent this is to get antivirus software that detects and removes malware. Most internet security software suites have identity theft protection features like anti-keyloggers, secure environments and encrypted password protection. While all of these steps can help prevent social media identity theft, Ravi Bhatia, founder and director of outreach at Ashland Prep, said the only way to truly protect your identity on social media is to not use it.
"People should use social media only if they're willing to accept the small chance that it can ruin them," he said. "If they fear the consequences, then they should avoid them at all costs."
Scams to watch out for - Social media identity fraud can be difficult to recognize, because the most dangerous scams constantly change to reflect current events and take advantage of consumer patterns. Recent scams have shifted from email phishing to account fraud, leveraging fears about the COVID-19 pandemic. These fraudulent accounts pose as government agencies and post vaccine misinformation or dangle fake employment opportunities, enticing unsuspecting users to provide their contact or billing information in an effort to learn more. These are some common schemes:

- **Impersonation:** A hacker can message friends of the compromised account and ask for favors. Some messages may be innocuous, asking your friends about your weekend plans or work hours to learn when your home will be vacant. Others are more overt. These messages may claim that your friend is in some form of trouble and urgently needs money. Never consider sending money without **verifying that the request is genuine.**
- **Quizzes:** These scams pose as fun games to post publicly and share with friends. Many quizzes ask questions about the street of your childhood home, the name of your first pet, or your favorite restaurants. These sound familiar because old password prompts asked the same questions. Posting your filled-out questionnaires offers potential hackers an easy opportunity to learn your passwords.
- **Business opportunities:** When looking into employment opportunities, remember one golden rule: If you have to pay for anything, you are their customer, not their employee. These offers often come in the form of a pyramid scheme. The messaging party, who is almost always unsolicited, promises to send you a starter pack that you can sell. But first, of course, you need to provide your credit card information. Never, under any circumstances, provide credit information unless it is to make a purchase through a secured company page.

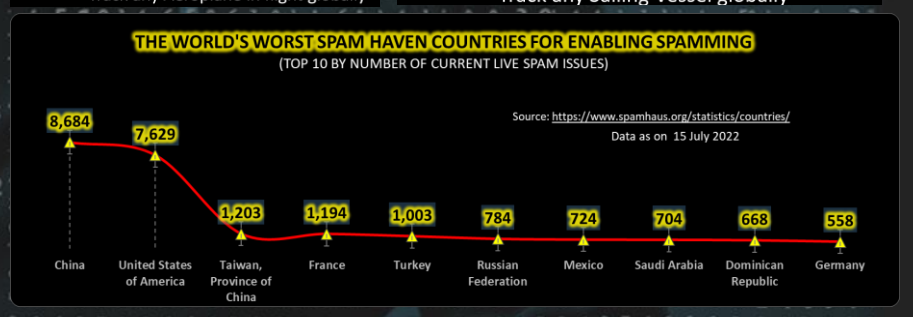
Resources: Business News Daily

Other Interesting News and Cyber Security bits:

- NIST Announces First Four Quantum-Resistant Cryptographic Algorithms
- Instagram is testing an AI tool that verifies your age by scanning your face
- How old are you? Lets see how accurate a computer can guess your age
- Hubble and James Webb Space Telescope Images Compared
- SANS Daily Network Security Podcast (Storm cast)

flightradar24
LIVE AIR TRAFFIC
Track any Aeroplane in flight globally

Marine Traffic
Track any Sailing Vessel globally



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