On August 3, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Samba, Grails 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

05 August 2022

In The News This Week

Thousands of hackers flock to 'Dark Utilities' C2-as-a-Service

Security researchers found a new service called Dark Utilities that provides an easy and inexpensive way for cybercriminals to set up a command and control (C2) center for their malicious operations. The Dark Utilities service provides threat actors a platform that supports Windows, Linux, and Python-based payloads, and eliminates the effort associated with implementing a C2 communication channel. A C2 server is how adversaries control their malware in the wild, sending out commands, configurations and new payloads, and receiving data collected from compromised systems. The Dark Utilities operation is a 'C2-as-a-service' (C2aaS) that advertises reliable, anonymous C2 infrastructure and all the required additional functions for a starting price of just EUR 9,99. A report from Cisco Talos says that the service has around 3,000 active subscribers, which would bring the operators a revenue of about EUR 30,000. Dark Utilities emerged in early 2022 and offers full-blown C2 capabilities both on the Tor network and on the clear web. It hosts payloads in the Interplanetary File System (IPFS) - a decentralized network system for storing and sharing data. Multiple architectures are supported and it appears that the operators are planning on expanding the list to provide a larger set of options of devices that could be targeted. Read the rest of the post by Bill Toulas here: BleepingComputer

Microsoft's new security tool lets you see your systems like a hacker would

Microsoft has launched two security services that aim to boost the intelligence capabilities of an organization's security operations center (SOC) rather than solely protect devices. Microsoft has launched Defender Threat Intelligence and Defender External Attack Surface Management (EASM) — two new products that merge technology Microsoft gained after acquiring security firm RiskIQ last July for $500 million. There may appear to be some overlap between Microsoft's existing services, such as its Azure-powered Sentinel security information and event management (SIEM) service and Microsoft Defender Experts for Hunting... But Microsoft says these RiskIQ-based threat intel service offerings differ in that they provide customers with "direct access to real-time data" from Microsoft's security signals. Microsoft chief Satya Nadella last week said the firm receives **43 trillion** security signals each day. Read the full post by Liam Tung here: ZDNet

Thousands of Mobile Apps Leaking Twitter API Keys

Thousands of mobile apps are leaking Twitter API keys — some of which give adversaries a way to access or take over the Twitter accounts of users of these applications and assemble a bot army for spreading disinformation, spam, and malware via the social media platform. Researchers from India-based CloudSEK said they had identified a total of 3,207 mobile applications leaking valid Twitter Consumer Key and Secret Key information. Some 230 of the applications were found leaking OAuth access tokens and access secrets as well. Together, the information gives attackers a way to access the Twitter accounts of the users of these applications and carry out a variety of actions. This includes reading messages; retweeting, liking, or deleting messages on the user's behalf; removing followers or following new accounts; and going to account settings and doing things like changing the display picture, CloudSEK said... Read the rest of the article by Jai Vijayan. here - DarkReading

Bug bounties to become part of Swiss cyber-security arsenal

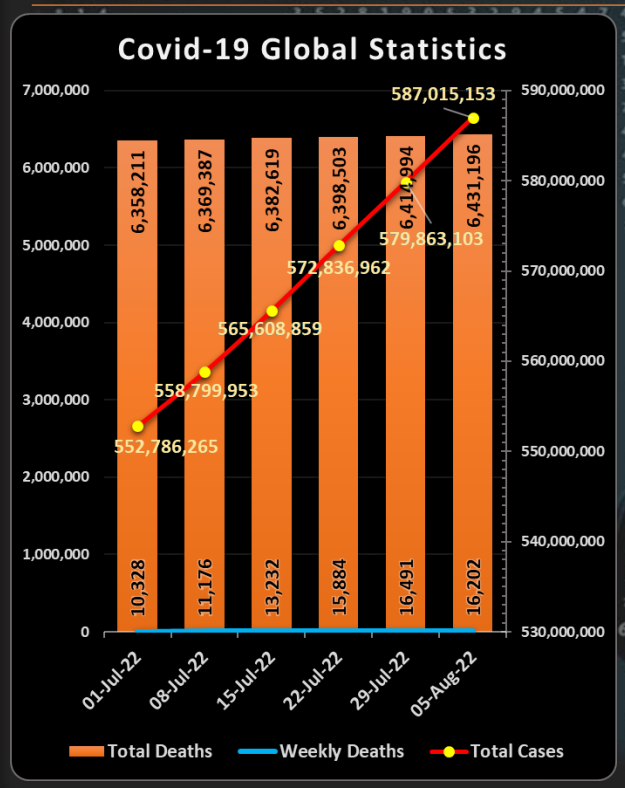
Switzerland - After a pilot project in 2021, authorities now want to systematically draw on the skills of "ethical hackers" to find flaws in government IT systems. - "Often, standardised security tests are no longer sufficient to uncover hidden loopholes" in official websites or software components, the finance ministry wrote this week. As a result, a centralised platform for bug bounty programmes (initiatives which offer financial rewards to hackers to identify cyber vulnerabilities) will be set up and run by the National Cybersecurity Centre (NCSC). This latter will work with Bug Bounty Switzerland SA, a company with expertise in the area and a large existing community of ethical hackers. The goal is to extend the schemes to cover "as many Federal Administration systems as possible", with the first projects to start already this year, the finance ministry said . Read the rest of the article here: SwissInfo

Ukraine takes down 1,000,000 bots used for disinformation

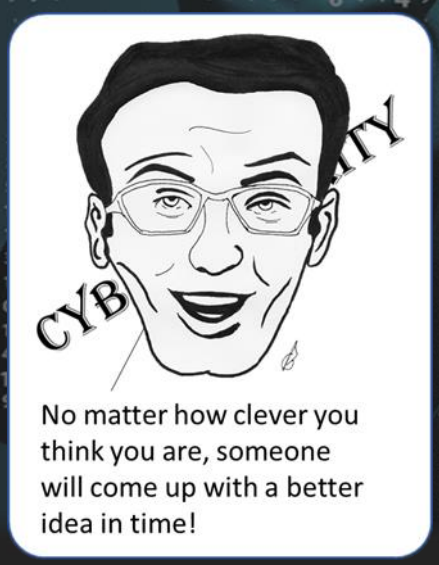
The Ukrainian cyber police (SSU) has shut down a massive bot farm of 1,000,000 bots used to spread disinformation on social networks. The goal of the bot farm was to discredit information coming from official Ukrainian state sources, destabilize the social and political situation in the country, and create internal strife. The messages spread by the bots were in line with Russian propaganda, so the operators of the disinformation machine are believed to be members of the Russian special services. In fact, SSU's investigation led to the criminal group's leader, a Russian "political expert" who in the past lived in Kyiv. "According to the investigation, this person was organizing information and subversive activities, which were ordered by one of the domestic political forces," explains SSU's announcement.... The bot farm dismantled by SSU was located in Kyiv, Kharkiv, and Vinnytsia and relied on 1,000,000 bots to spread disinformation. To create this online army, the threat actors used 5,000 SIM cards to register new social media accounts. Moreover, the operators used 200 proxy servers that spoofed the actual IP addresses and evaded detection of fraudulent activity and blocking by the social media platforms.... Read the full the story by Bill Toulas here: BleepingComputer

North Korea-backed hackers have a clever way to read your Gmail

Researchers have unearthed never-before-seen malware that hackers from North Korea have been using to surreptitiously read and download email and attachments from infected users' Gmail and AOL accounts. The malware, dubbed SHARPEXT by researchers from security firm Volexity, uses clever means to install a browser extension for the Chrome and Edge browsers, Volexity reported in a blog post. The extension can't be detected by the email services, and since the browser has already been authenticated using any multifactor authentication protections in place, this increasingly popular security measure plays no role in reining in the account compromise. The malware has been in use for "well over a year," Volexity said, and is the work of a hacking group the company tracks as SharpTongue. Read the full post by Dan Goodin here: ARSTecnica



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



Home Wi-Fi Security

I have written about home Wi-Fi security a number of times in this post over the years, and it is not something most people consider that important. Smart homes are becoming a norm rather than an exception, and with that comes more threats and more things to hack. Whether it is your neighbour who just wants a free Internet connection when his network is down or someone with a more sinister motive, news of digital home invasions is becoming more common than ever before. A recent post in WalesOnline said, "Research revealed that 4.3 million Brits are guilty of 'hacking' their neighbours Wi-Fi when their own internet has gone down". If you have an Internet-connected baby monitor, be careful as it seems to be a popular target for criminals. Can Smart Locks Be Hacked?, was a question recently posted in the popular MUO (Make-Use-Of) blog. If your Smart Home, including Smart Locks, is compromised, it is as good as leaving your front door wide open. The Daily Express reported 3 weeks ago that Smart Homes are "exposed" to more than **12,000** attacks per week. It all comes down to a secure home network. - With that in mind, I did my usual foraging through the Internet forest and found hundreds of sites offering advice on how to secure your Wi-Fi, and most offer more or less the same advice. Below is an extract of a post by CNET that covers the most important actions you can take to secure your home network.

Tips to Secure Your Home Wi-Fi Network: Banish Hackers and Freeloaders Now

Home network hacking happens all too frequently. Internet crime cost people in the US more than $6.9 billion in 2021, and while phishing and scams contributed to the losses, personal data breaches were also a significant factor. The average US home now has more than 10 devices connected to the home Wi-Fi network. From laptops and tablets to phones, smartwatches and streaming devices, things add up quickly. And with so much data stored on those devices -- credit card numbers, bank records, login credentials and other personal and private information -- you want to make sure you're protecting yourself from hackers if your network is ever compromised. A secure home network will help reduce the risk of getting hacked and someone accessing your sensitive information. Not only that, it will keep away any unwanted or unauthorized users and devices that would slow down your connection or freeload on the internet service you pay for.
It's fairly simple to create and maintain a secure home Wi-Fi network. Below, you'll find some tips for securing your network. Keep in mind that nothing can guarantee absolute security from hacking attempts, but these tips will definitely help to prevent it.

Place your router in a central location - Strong network security starts with a smart setup. If possible, place your router at the center of your home. Routers send wireless signals in all directions, so strategically placing your router in a central location will help keep your connection to the confines of your home. As a bonus, it will likely also make for the best connection quality. For example, if you have internet in an apartment where neighbours are immediately to the left and right of you, placing your router next to a shared wall could send a strong, and tempting, signal their way. Even if you aren't in an apartment, a good router can cast signals next door or across the street. Placing your router in a central location will help reduce how far those signals travel outside your home.

Create a strong Wi-Fi password and change it often - This should go without saying, but I'm going to cover it still to emphasize its importance. Creating a unique password for your Wi-Fi network is essential to maintaining a secure connection. Avoid easily guessed passwords or phrases, such as someone's name, birthdays, phone numbers or other common information. While simple Wi-Fi passwords make them easy to remember, they also make it easy for others to figure them out. (Here's how to access your router settings to update your Wi-Fi password.) Be sure to change your password every six months or so, or any time you think your network security may have been compromised.

Change the default router login credentials - Along the same lines of password-protecting your Wi-Fi network, you'll also want to keep anyone from being able to directly access your router settings. To do so, go ahead and change the admin name and password for your router. You can log in to your router settings by typing its IP address into the URL bar, but most routers and providers have an app that lets you access the same settings and information. Your router login credentials are separate from your Wi-Fi network name and password. If you aren't sure what the default is, you should be able to find it on the bottom of the router. Or, if it's been changed from the default somewhere along the way, again, here's how to access your router settings to update the username and password.

Turn on the firewall and Wi-Fi encryption - Most routers have a firewall to prevent outside hacking, as well as Wi-Fi encryption to keep anyone from eavesdropping on the data that's sent back and forth between your router and connected devices. Both are typically active by default, but you'll want to check to make sure they're on. Now that you know how to log in to your router settings, check to make sure the firewall and Wi-Fi encryption are enabled. If they're off for whatever reason, go ahead and turn them on. Your network security will thank you.

Create a guest Wi-Fi network - "Can I get the Wi-Fi password?" is undoubtedly something all hosts have heard. Before sharing access to your main home network, consider creating a separate guest network for visitors. I'm not suggesting your guests are going to attempt anything nefarious with your main Wi-Fi connection, but their devices or anything they download while connected to your network could be infected with malware or viruses that target your network without them even knowing it. A guest network is also ideal for your IoT devices, such as Wi-Fi cameras, thermostats and smart speakers -- devices that may not hold a lot of sensitive information and are perhaps more easily hackable than a smarter device such as a computer or phone.

Use a VPN - There are a few reasons to use a good VPN, and network security is definitely one of them. Among other things, a virtual private network hides your IP address and Wi-Fi activity, including browsing data. VPNs are probably more useful when connected to a public network, but they can still add a level of security and privacy to your home network. Some VPNs are better than others, but like anything, you often get what you pay for. Free VPN services are available, but paying a little extra (seriously, just a few bucks per month) will deliver a much better, more secure service.

Verify connected devices - Frequently inspect the devices that are connected to your network and verify that you know what they are. If anything on there looks suspicious, disconnect it and change your Wi-Fi password. You'll have to reconnect all your previously connected devices after changing your password, but any users or devices that are not authorized to use your network will get the boot. Some devices, especially obscure IoT ones, may have some odd default names of random numbers and letters that you don't immediately recognize. If you come across something like that when scrutinizing your connected devices, go ahead and disconnect it. Later on, when you can't start your robot vacuum cleaner from your phone, you'll know that's what it was.

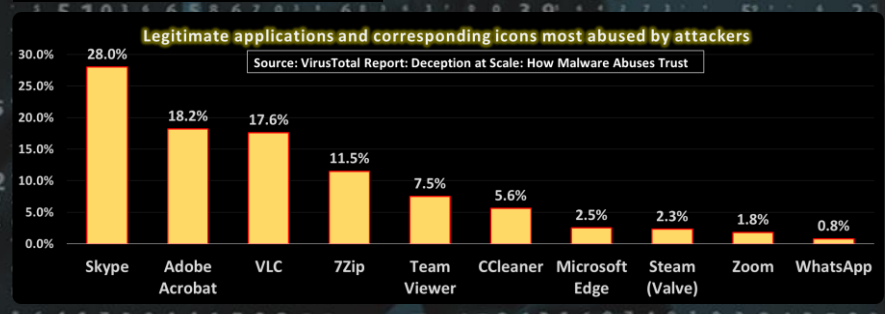
Find more tips and insights here: CNET, The Bronx, Trusted Reviews, Komando, Which

Other Interesting News and Cyber Security bits:

- UK Government - Cyber security breaches survey 2022
- Deception at Scale: How Malware Abuses Trust – A VirusTotal report
- Post-quantum crypto cracked in an hour with one core of an ancient Xeon
- Cadillac Unveils Electric Vehicle to Compete with Bentley and Rolls-Royce
- 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