The Cyber Threat Alert Level as evaluated by CIS remains at Blue (Guarded)
Last Advisory 04 AUG 2021
Multiple Vulnerabilities in Google Android OS Could Allow for Remote Code Execution

Covid-19 Global Stats

Date	Confirmed Cases	Total Deaths
06 Aug	201,629,866	4,279,216

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
06 August 2021

In The News This Week

Apple to scan U.S. iPhones for images of child sexual abuse

Apple unveiled plans to scan U.S. iPhones for images of child sexual abuse, drawing applause from child protection groups but raising concern among some security researchers that the system could be misused, including by governments looking to surveil their citizens. The tool designed to detected known images of child sexual abuse, called "neuralMatch," will scan images before they are uploaded to iCloud. If it finds a match, the image will be reviewed by a human. If child pornography is confirmed, the user's account will be disabled and the National Center for Missing and Exploited Children notified. Read more coverage here: ABC News, Business Insider, USA Today

Microsoft tests Super-Duper Secure Mode for Edge

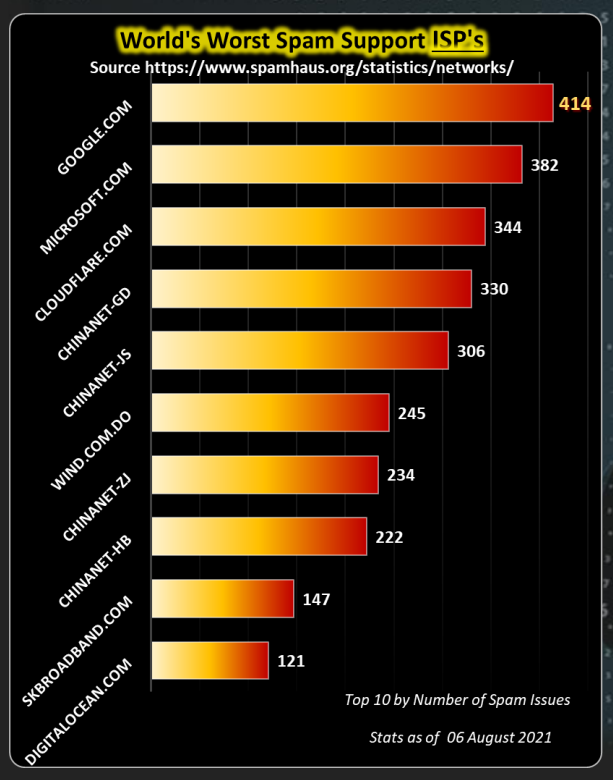
Microsoft's Edge Vulnerability Research (VR) team is testing a new feature they've christened, "Super Duper Secure Mode" (SDSM). Super-Duper Secure Mode is all about making Edge more secure without negatively impacting performance. SDSM works by removing Just-In-Time compilation from the V8 processing pipeline, which will reduce the attack surface that can be used to hack into Edge's systems, as Bleeping Computer (where I first saw the SDSM information) explains. In addition to disabling the JIT, SDSM enables "new security mitigations" to make Edge a more secure browser. "JavaScript plays a key role in any browser story. JITs exist for a reason, and that is to optimize JavaScript performance," the Microsoft browser researchers noted in their August 4 blog post about SDSM. However, so far, the researchers said they don't see much of a change in performance with JIT disabled; most of their tests remained unchanged. By disabling the JIT, roughly half of the V8 bugs that must be fixed would be removed. This would mean less frequent security updates and fewer emergency patches for users, the researchers noted.
SDSM is still considered to be in the experimental stage. Still, Edge preview testers -- in the Canary, Dev and Beta rings -- can enable it now with a flag by going to edge://flags/#edge-enable-super-duper-secure-mode and turning on the new feature. Read the story here: ZDNet

Zoom to pay $85M for lying about encryption and sending data to Facebook and Google

Zoom has agreed to pay $85 million to settle claims that it lied about offering end-to-end encryption and gave user data to Facebook and Google without the consent of users. The settlement between Zoom and the filers of a class-action lawsuit also covers security problems that led to rampant "Zoombombings."
The proposed settlement would generally give Zoom users $15 or $25 each and was filed Saturday at US District Court for the Northern District of California. It came nine months after Zoom agreed to security improvements and a "prohibition on privacy and security misrepresentations" in a settlement with the Federal Trade Commission, but the FTC settlement didn't include compensation for users. Read the full story here: ARSTechnica

Prometheus TDS: The $250 service behind recent malware attacks

Security researchers investigating multiple malware distribution campaigns found that an underground traffic distribution service called Prometheus is responsible for delivering threats that often lead to ransomware attacks. Among the malware families that Prometheus TDS has dished out so far are BazarLoader, IcedID, QBot, SocGholish, Hancitor, and Buer Loader, all of them commonly used in intermediary attack stages to download more damaging payloads.
Trojan delivery service - A traffic direction system (TDS) allows redirecting users to content based on specific characteristics (e.g. location, language, device type) that determine further action. Threat actors have been using such tools for more than a decade. A 2011 report from Trend Micro details an upgrade of the Koobface botnet with a TDS component that increased profits by driving traffic to affiliate advertising websites. Researchers at cybersecurity company Group-IB found that the Prometheus TDS malware-as-a-service (MaaS) operation is being advertised on underground forums since at least August 2020 for $250 per month.
A user called Main is promoting it as a "professional redirect system" with anti-bot protection that is suitable for email marketing, generating traffic, and social engineering.. Read the rest of the story here: BleepingComputer



For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov

Home router set-up

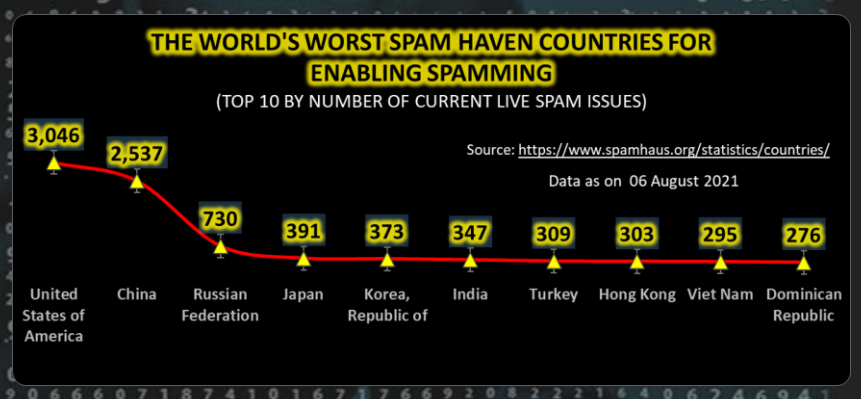
I have written about router and Wi-Fi set-ups numerous times in the past but I often get asked by my not-so-technical friends if there is not a step-by-step guide they can follow to set up their home router. Circumstances changed and the reality of Covid-19 forced a vast number of people across the globe to work from home. Threat actors have jumped on the opportunity to pry on the weaknesses of home network setups and the ignorance of the common user. To that end, I found this handy guide by PC Mag that would help you with the basic setup steps without too much technical jargon. Below is a shortened extract of the article.

How to Set Up and Optimize Your Wireless Router for the Best Wi-Fi Performance and Security

While manufacturers have been making installation utilities easier over the years, getting the best out of your new wireless router purchase usually means delving a little deeper than the standard installation routine will go. Just because you've plugged everything in and all the blinking lights have turned green doesn't mean your network's performance or its security are as good as they could be. Follow these basic steps to properly configure your router and optimize your wireless network.
How Do I Connect My Wi-Fi Router? - These steps assume that you've already found the right router for your home. As part of router selection, two additional questions you'll need to answer are whether you want a Wi-Fi 6 router or a Wi-Fi mesh system or even both in one. Wi-Fi 6 is an emerging standard that is finally seeing a widening selection of compatible routers coming to market. If you're looking to replace your current router and it's more than three years old, or if you're simply looking for the latest in terms of speed and security, Wi-Fi 6 is what you want. Wi-Fi mesh systems are for folks willing to pay a little more for two primary benefits: easy basic setup and whole-home Wi-Fi coverage. While you can increase the coverage in your home with a standard router and a wireless range extender, that solution tends to make users jump through a few additional hoops to get things working smoothly, notably forcing users to log into different wireless networks depending on where they are in the home. Wi-Fi mesh makes all that go away with a very quick and easy path to initial setup and a series of compatible "nodes" that integrate seamlessly into a single wireless network that blankets your entire home. Newer Wi-Fi mesh systems combine Wi-Fi 6 and mesh technology into a single package. (If you are into gaming, check out the gaming router guide)
Placement and Setup - Before getting started, you need to consider where you'll place your router. Finding an open space toward the center of your residence is the best way to ensure optimal coverage. Be aware that walls and floors will impede Wi-Fi signals, so the more obstructions you have between your devices and your router, the weaker the signal will be. Wi-Fi mesh systems get around this problem by letting you place an attractively designed node wherever coverage is weakest. But for those working with standard routers or even wireless range extenders, this will require some patience and testing to see where your optimal placement areas are. Start this process by connecting your router to your modem. For this, you'll need an Ethernet cable, which you'll want to plug into the WAN (wide-area network) port on your router's rear face. This port might look slightly different from router to router, but it will usually have a distinct colour from the other ports and be labelled "WAN," "Internet," or something similar. From the WAN port, connect the other end of the Ethernet cable to the Ethernet port on the back of your modem and switch it on. (The modem is the communication device that your Service Provider supply and will either be connected to a phone or Fibre connection).
Typically, there is a dedicated website URL that loads the router's internal configuration page. You can find this URL by connecting your computer to any of the router's LAN ports via Ethernet cable and entering 192.168.1.1 or a similar address (as specified by the router's documentation) into your browser search bar. (If you are already connected you can also determine the router address by typing "ipconfig /all" in the command line on your computer and look for the IP address of the "Default Gateway")
The first step to get your network up and running will be to set up a username and password. If you happen to have a pre-owned router, the username and password can be reset to factory defaults by holding a recessed button somewhere on the router (usually the back). Most often, these defaults are something like "admin" and "admin," which every would-be hacker knows, so make sure to change these right away. Be sure to use a secure password that includes a mix of uppercase and lowercase letters, numbers, and symbols. (Check out this link to find the most common default usernames, passwords and IP address)
How Do I Configure My Router? - With the username and password set, you can proceed to configure your router's settings. As with cooking dinner, there's no "right" way to install a router, and every model is likely to have its own unique steps, depending on its features. Because of this, trying to describe every possible configuration path here would be exhausting and pointless. We recommend consulting your router's manual for specifics. That said, we do have a few points of advice: Use the easy setup wizard. Most routers provide some form of brief setup routine that asks for little more than the SSID and password. If in doubt, start with this. (The SSID is your router's Wi-Fi name, feel free to change it).
Use the WPS button to connect Wi-Fi devices. - If you've ever paired two Bluetooth devices, such as a smartphone with headphones, then you already have a basic understanding of how this works. On your laptop, you'll see your router's SSID pop up on the list of visible wireless networks. When you select the SSID and attempt to connect, Windows will prompt you to enter the network security key or password. At this stage, press the WPS button on your router. You should allow at least a minute for the router and laptop to find each other and successfully pair. Keep in mind that WPS only works with Windows and Android devices.
Simply checking the Dynamic Host Configuration Protocol (DHCP) box in your router's settings will ensure IP addresses are automatically assigned to devices.
Connect to the 2.4GHz or 5GHz Band? - 5GHz connections will provide better performance at short ranges than 2.4GHz. This is because 5GHz, while somewhat faster, can't travel as far or transmit through some objects due to that band's shorter wavelengths.
Taking It To The Next Level - With most routers, simply activating your network and connecting to the internet is only scratching the surface of what you can do. While a tab name like "advanced settings" may seem a bit intimidating, the menus contained here often allow you to control some of your router's most helpful features. Read the rest of this article to go to the next level ....

Other Interesting News and Cyber Security bits:

- Washington ready to tax cryptocurrency trades, eyes $28 billion to help pay for infrastructure
- Microsoft will end 'classic' method of recording Teams meetings despite transcription concerns
- Raspberry Pi-Powered Speed Trap Collects Your Lead-Footed Driving Data



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