On August 11, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in NicheStack, Mozilla, Microsoft, and Adobe products.
See Latest Advisory 11 AUG 2021

Covid-19 Global Stats

Date	Confirmed Cases	Total Deaths
13 Aug	206,155,806	4,346,672

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 August 2021

In The News This Week

Over $600 Million Stolen in Biggest Ever Cryptocurrency Theft

Over $600 million has been stolen from DeFi platform Poly Network in one of the biggest crypto heists of all time - but the hacker has returned some of the cash already - Cryptocurrency worth over $600 million were stolen from decentralized finance platform Poly Network, in one of the biggest crypto heists ever on Tuesday, with developers putting out a plea on Twitter to the hacker asking for the money back - which the thieves have appeared to respond to. Poly Network announced the hack on Twitter, noting the attack took place on across the binance, polygon and ethereum blockchains and involved various tokens, including shiba inu, wrapped ether, wrapped bitcoin, uniswap and a series of stablecoins. The platform also published the hacker's wallet addresses and urged crypto exchanges and miners to halt tokens from these addresses. In response, around $33 million of stablecoin Tether that were part of the hack were frozen by its issuer, Paolo Ardoino, its chief technology officer said on Twitter. They also said they had found the vulnerability on the platform that the hacker used to seize the coins. Poly Network last said it had started receiving money back from the hacker, sharing on Twitter that polygon tokens worth over $1 million had been returned.. Read more coverage here: Yahoo, Infosecurity Magazine

Accenture Confirms LockBit Ransomware Attack

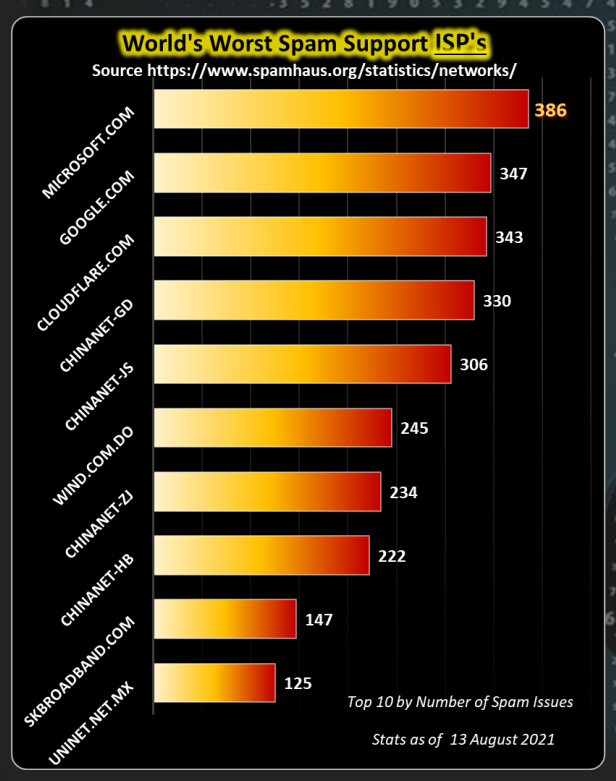
LockBit offered Accenture's purported databases and made a requisite jab at its purportedly sad security. Accenture says it recovered just fine from backups. - The LockBit ransomware-as-a-service (RaaS) gang has published the name and logo of what's purportedly one of its latest victims: Accenture, the global business consulting firm with an insider track on some of the world's biggest, most powerful companies. Accenture's clients include 91 of the Fortune Global 100 and more than three-quarters of the Fortune Global 500. According to its 2020 annual report; that includes e-commerce giant Alibaba, Cisco and Google. Valued at $44.3 billion, Accenture is one of the world's largest tech consultancy firms, and employs around 569,000 people across 50 countries. In a post on its Dark Web site, LockBit offered up Accenture databases for sale, along with a requisite jab at what the gang deemed to be Accenture's pathetic security. Read more here: ThreatPost, Economic Times

NSA Issues Warning Concerning Public Wi-Fi Networks

National Security Agency cautioned public servants against hackers that can benefit from public Wi-Fi in coffee shops, airports, and hotel rooms. NSA stated, "The Biden administration would like you to get a vaccine and wear a mask. Oh, and one more thing: It has just proclaimed that it's time for government employees and contractors to get off public Wi-Fi, where they can pick up another kind of virus." The National Security Agency released a strangely specific warning late last week cautioning that logging in for public Wi-Fi Network "may be convenient to catch up on work or check email," in a notification to every federal employee, leading defense companies and the 3.4 million uniformed, civil and reserves personnel serving on the military. In an eight-page report, the agency describes how the click on the local coffee shop's network caused problems in a year highlighted by ransomware attacks on pipelines, meatpackers, and even police forces in Washington, DC.
"Avoid connecting to public Wi-Fi, when possible," the warning read, stating that even Bluetooth connections can be compromised. . Read the story here: E-Hacking News

May cyberattack cost Scripps nearly $113M in lost revenue

A massive cyberattack May 1 cost Scripps Health $112.7 million through the end of June, with lost revenue bearing most of the cost. The non-profit San Diego-based hospital system reported the impact during its second-quarter earnings filed Tuesday. The attack led to a major disruption in patient care and forced providers to use paper records. Scripps said at the time that its facilities remained open for care but hasn't until now divulged the financial impact of the attack. Scripps restored all its systems May 26 after hiring computer consulting and forensic firms to help investigate the attack and restore its systems. "As of June 30th, we estimate total lost revenues to be $91.6 million and incremental costs incurred to address the cyber security incident and recovery were estimated at $21.1 million," the earnings report said. Read the rest of the story here: FierceHealthcare



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

How Wi-Fi Hotspot Hacks Occur

In light of the NSA's warning about public Wi-Fi Networks this week, I decided to re-visit the topic and share an extract of an article written by Jared Howe a while back. Jared highlights a few types of hacks or attacks, but as you know, the methods used by attackers are constantly evolving. I, therefore, encourage you to always be on the lookout for any strange behaviour on your computer or any unfamiliar pop-ups, especially when you are traveling.

How safe are Wi-Fi Networks

Many of us assume that using a Wi-Fi network at a hotel, coffee shop, or airport is the same as logging into our network at home or at the office. But the risks of using Wi-Fi networks at a hotel or airport are exponentially greater than those experienced at home or in an enterprise setting. Most private networks use firewalls to defend users against Internet-based attacks. This is not necessarily true in public wireless networks. You may assume you are safe from outside attacks, but you really have no idea whether any firewall lies between your laptop data and the Internet. It is literally impossible to tell the safe networks from the bad ones. Wireless eavesdropping is possible everywhere.

So What Should I Be Worried About?

Okay, so now you are probably aware that using a public Wi-Fi network while on the road exposes you to a lot of security risks. But what risks are we talking about exactly?

The following is a list of different types of hacks that can occur in public WiFi hotspots:

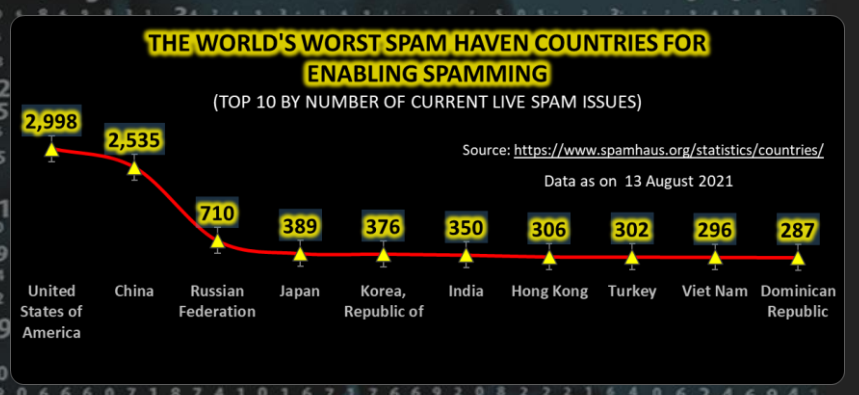
Sniffers: Software sniffers allow eavesdroppers to passively intercept data sent between your web browser and web servers on the Internet. This is the easiest and most basic kind of attack. Any email, web search or file you transfer between computers or open from network locations on an unsecured network can be captured by hackers. Sniffing software is readily available for free on the web and there are 184 videos on YouTube to show budding hackers how to use them. The only way to protect yourself against Wi-Fi sniffing in most public WiFi hotspots is to use a VPN, such as PRIVATE WiFi™ or similar VPNs available in the market.
Sidejacking: Sidejacking is a method where an attacker uses packet sniffing to steal a session cookie from a website you just visited. These cookies often contain usernames and passwords, and are generally sent back to you unencrypted, even if the original log-in was protected via HTTPS. Anyone listening can steal this log-in information and then use it to break into your Facebook or Gmail account. This made news in late 2010 because a programmer released a program called Firesheep that allows intruders sitting near you on a public WiFi network to take over your Facebook session, gain access to all of your sensitive data and send viral messages and wall posts to all of your friends.
Evil Twin/Honeypot Attack: This is a rogue Wi-Fi access point that appears to be a legitimate one, but actually has been set up by a hacker to eavesdrop on wireless communications. An evil twin is the wireless version of the "phishing" scam: an attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider. When a victim connects, the hacker can launch man-in-the-middle attacks, listening in on all Internet traffic, or just ask for credit card information in the standard pay-for-access deal. Tools for setting this up are easily available (e.g., Karma and Hotspotter). One recent study found that over 56% of laptops were broadcasting the name of their trusted Wi-Fi networks, and that 34% of them were willing to connect to highly insecure Wi-Fi networks.
ARP Spoofing: Address Resolution Protocol (ARP) spoofing, also known as ARP flooding, ARP poisoning or ARP Poison Routing (APR), is a technique used to attack a wireless network. ARP spoofing allows an attacker to sniff traffic on a LAN and modify or stop the traffic altogether. This attack can only occur on networks that make use of ARP and not another method of address resolution. ARP spoofing sends fake, or "spoofed", ARP messages to a LAN which associates the attacker's MAC address with the IP address of the victim. Any traffic meant for the victim's IP address is mistakenly sent to the attacker instead. The attacker could then forward the traffic to the actual default gateway (passive sniffing) or modify the data before forwarding it (man-in-the-middle attack). The attacker could also launch a denial-of-service attack against a victim by associating a non-existent MAC address to the IP address of the victim. A successful APR attempt is invisible to the user.
"Free Public WiFi" Rogue Networks: "Free Public Wi-Fi" networks are ad-hoc networks advertising "free" Internet connectivity. Once you connect to a viral network, all of your shared folders are accessible to every other laptop connected to the network. A hacker can then easily access confidential data on your hard drive. These viral networks can be used as bait by an Evil Twin. "Free Public Wi-Fi" networks turn up in many airports. Don't connect to these networks and you won't infect your laptop. If you find this kind of network on your laptop, delete it and reconfigure your adapter to avoid auto-connecting to any wireless network.
Man-in-the-middle Attacks: Any device that lies between you and a server can execute man-in-the-middle attacks, which intercept and modify data exchanged between two systems. To you, the man-in-the-middle appears to be a legitimate server, and to the server, the man-in-the-middle appears to be a legitimate client. In a wireless LAN, these attacks can be launched by an Evil Twin.

So How Can I Protect My Laptop?

Here are some proactive steps you can take to protect yourself when using such networks, and services you can use that provide laptop security: **(1)** Disable or block file sharing; **(2)** Enable your Windows / iOS Firewall or install a third party personal firewall; **(3)** Enable Windows / iOS file encryption; **(4)** Make use of a VPN.
If you read the disclaimers, the one thing that they all have in common is that it is **your** responsibility to protect yourself. One of the best ways to protect your sensitive information is to use a Virtual Private Network (VPN), which encrypts the data moving to and from your laptop. The encryption protects all your Internet communication from being intercepted by others in Wi-Fi hotspots. In addition, VPNs can prevent hackers from connecting to your laptop and stealing your data files... Read the full article here

Other Interesting News and Cyber Security bits:

- The Misunderstood Security Risks of Behavior Analytics, AI & ML
- Food, Farms and Cyber Security: Agriculture Faces a Growing Problem
- After Data Is Posted On Conspiracy Website, Colorado County's Voting Machines Are Banned



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