On May 18, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Adobe, HP, Zyxel, SonicWall and Apple products.
CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
20 May 22	526,028,990	6,297,334

Deaths this week: 12,469

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

20 May 2022

In The News This Week

FBI: North Korea's tech workers are posing as freelance developers, helping hackers

Skilled software and mobile app developers from North Korea are posing as US-based remote workers to land contract work as developers in US and European tech and crypto firms. The warning comes in a new joint advisory from The US Department of State, the US Department of the Treasury, and the Federal Bureau of Investigation (FBI) outlining the role North Korean IT workers play in raising revenue for North Korea, which contributes to its weapons of mass destruction (WMD) and ballistic missile programs, in violation of U.S. and UN sanctions. Hackers working for North Korea – officially known as the Democratic People's Republic of Korea (DPRK) – have gained notoriety for sophisticated hacks on cryptocurrency exchanges during the past five years. In 2021 alone they stole over $400 million worth of cryptocurrency for the DPRK. Read the rest of the story by Liam Tung here: ZDNet

Tesla cars are susceptible to hacking due to bluetooth locks, cybersecurity firm says

Teslas are among the most susceptible vehicles to be hacked due to their Bluetooth locks, cybersecurity firm NCC Group said. The cars can be remotely unlocked and controlled by hackers that can exploit a vulnerability in the Bluetooth system's security, the group said. NCC Group researcher Sultan Qasim Khan was shown in a video opening, then driving a Tesla using a small relay device attached to a laptop. The device bridged a large gap between the Tesla and the Tesla owner's phone, Reuters said. "This proves that any product relying on a trusted BLE connection is vulnerable to attacks even from the other side of the world," NCC said in a statement. BLE means Bluetooth Low Energy, and is a technology utilized in vehicles and Bluetooth locks that will automatically unlock or unlatch when an authorized device is nearby. While it is a convenience feature, it is not immune to attacks, which was the point of NCC's experiment. The hack was performed on a 2021 Tesla Model Y, but NCC Group maintains that any lock utilizing BLE technology, including residential smart locks, could be unlocked in the same manner. Read the full article by Joey Klender here: Teslarati

Cyber security: Global food supply chain at risk from malicious hackers

Modern "smart" farm machinery is vulnerable to malicious hackers, leaving global supply chains exposed to risk, experts are warning. It is feared hackers could exploit flaws in agricultural hardware used to plant and harvest crops. Agricultural manufacturing giant John Deere says it is now working to fix any weak spots in its software. A recent University of Cambridge report said automatic crop sprayers, drones and robotic harvesters could be hacked. The UK government and the FBI have warned that the threat of cyber-attacks is growing. John Deere said protecting customers, their machines and their data was a "top priority". Smart technology is increasingly being used to make farms more efficient and productive - for example, until now the labour-intensive harvesting of delicate food crops such as asparagus has been beyond the reach of machines. The latest generation of agricultural robots use artificial intelligence, minimising human involvement. They may help to plug a labour shortage or increase yield, but fear of the inherent security risk is growing, adding to concern over food-supply chains already threatened by the war in Ukraine and Covid... Read the rest of the story by Claire Marshall & Malcolm Prior here: BBC News

Collective Cyber Defence and Attack: NATO's article 5 after the Ukraine conflict

With the Russian invasion of Ukraine on February 24, 2022, US and Western European pundits predicted devastating and crippling cyber effects predicating kinetic warfare. However, over the past weeks, numerous Russian actions in cyberspace have largely flown beneath the radar due to actions by the cyber-security industry, or so-called "patriotic hackers", who have taken it upon themselves to counter Russian cyber aggression and attack Russian cyber infrastructure. In light of developments such as these, the North Atlantic Treaty Organisation (NATO) should consider and create policy for collective cyber defence, and potentially offense, under Article 5 of the NATO Charter. Cyberspace has proliferated across the globe, particularly in critical infrastructure, as technology has eclipsed traditional definitions of computing. Non-traditional computers reside in pockets, are able to make phone calls, and, increasingly, take high-resolution photographs. These non-traditional computers also maintain proper food temperatures in kitchens, give directions in cars, and track movement and health on people's wrists. But more importantly, these non-traditional computers reside in critical infrastructure centres displaying data for operators in the form of large screen monitors on walls, showing the physical environment through closed circuit television cameras. Many of these devices, which frequently lack anti-virus protection and utilise vulnerable protocols, exist within critical infrastructure, either natively or brought into these environments by employees.... Read the rest of the article by Michael Klipstein and Tinatin Japaridze here: European Leadership Network

IoT and Wi-Fi 6 GHz (802.11ax)

The question came up this week if your home wireless security system will perform better on Wi-Fi 6 (Also known as 802.11ax) rather than on versions 4 & 5, and if it is worth it to upgrade your router?

What is Wi-Fi 6 GHz 802.11ax

IEEE 802.11 is part of the IEEE 802 set of local area network technical standards and specifies the set of media access control and physical layer protocols for implementing wireless local area network computer communication. These Wi-Fi standards are introduced and managed by the Wi-Fi Alliance which comprises of a worldwide network of companies that has a common vision to connect everyone and everything, everywhere.

The Legacy 802.11 standard, released in 1997, had a maximum data rate of 2 Mbps and operated on the 2.4 GHz frequency band. The more recent, and most widely used Wi-Fi 4 (802.11n) was released in 2009. It operates on the 2.4 GHz and 5 GHz frequencies and can transmit data up to a rate of 450 Mbps. Wi-Fi 5 (802.11ac) was released in 2014 and can transmit data at a rate of 1.73 Gbps and operates on a 5GHz frequency. Wi-Fi 6, officially released in late 2019, is the next-generation wireless standard, and with a data rate of 2.4 Gbps, is the fastest yet. Wi-Fi 7 (802.11be) is currently under development.

In basic terms, 6 GHz Wi-Fi can operate on a less congested Wi-Fi spectrum, allowing devices equipped to work on this band to maximize their performance. Up to now, most Wi-Fi ran over the 2.4 GHz and 5 GHz bands. Both home and work access points use these lines to communicate with equipment.

The 2.4 GHz band is the narrowest, with a frequency range of only about 70 MHz. It has limits on how much data it can send but can send it a fair distance. With the 5 GHz band, there are 500 MHz of bandwidth, helping it transmit more data. The drawback is that this band can't transmit the data as far. Now, 6 GHz represents a third band that will broadcast and receive Wi-Fi signals, and devices connected to it will have less competition for bandwidth. In essence, 6 GHz increases the amount of Wi-Fi space available by a factor of two. The 6 GHz band offers 1,200 MHz of additional bandwidth, allowing it to transmit massive amounts of data. It does have an issue, though, as its range limitations mean it's best suited for data transfers between devices in the same room..

With that being said, let's look at the pros and cons of upgrading to Wi-Fi 6.

Pros

Apart from the massive 2.4 Gbps data transmission rate, Wi-Fi 6 also uses Target Wake Time (TWT), which allows devices to determine when they will normally wake up to begin sending and receiving data. This extends the battery life of mobile devices such as smartphones and tablets, as well as battery-powered smart home devices such as security cameras and video doorbells. The new standard also takes advantage of previously unused radio frequencies to provide faster 2.4GHz performance, and it uses refined bandwidth management to provide enhanced Quality of Service (QoS) options. Additionally, Wi-Fi 6 offers eight-stream uplink and downlink Multi-User Multiple Input Multiple Output (MU-MIMO), which streams data simultaneously rather than sequentially, allowing a more equitable sharing of bandwidth among connected MU-MIMO enabled clients. Wi-Fi 5 MU-MIMO topped out at four streams.

Aside from the capabilities mentioned above, Wi-Fi 6 also offers features like beamforming, which transmits Wi-Fi signals directly to clients rather than over a broad spectrum. All Wi-Fi 6 devices can also handle WPA3 encryption, which is the newest iteration of Wi-Fi security. It will use features like robust password protection and 256-bit encryption algorithms to make it harder for people to hack into your network.

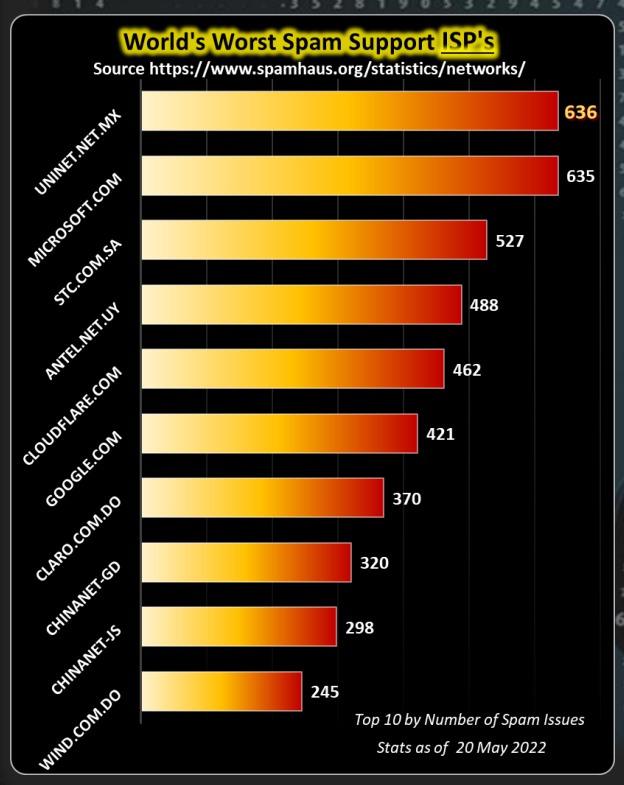
Your network will also run faster due to background networking improvements, like support for 1,024-QAM (Quadrature Amplitude Modulation), a method that allows more data to be packed into each signal for increased throughput. This can deliver up to 25 percent more capacity than the 256-QAM method used in most Wi-Fi 5 routers.

All this jargon is a lot to unpack, but rest assured that any device you get that supports the final Wi-Fi 6 standard will have all these features in place. On the other hand, there are some Wi-Fi 6 devices with enhanced capabilities that go beyond the basic features that the Wi-Fi Alliance certified. Called Wi-Fi 6E, these products support a 6 GHz wireless spectrum. Essentially, this means Wi-Fi 6E enables faster speeds and lower latencies than Wi-Fi 6 and earlier iterations. Wi-Fi 6E devices will be backward compatible with Wi-Fi 6 and earlier Wi-Fi standards, but to use the new 6GHz channels, you'll need a Wi-Fi 6E router and a Wi-Fi 6E client device (meaning computers, phones, smart home devices, cameras, and other gadgets that support Wi-Fi 6E).

Cons

The main disadvantage of Wi-Fi 6 is the range limitation. The broadcast range is significantly shorter than the previous versions, and therefore you will need to invest in a mesh network to get full coverage of your home, and this will obviously have a cost implication. A mesh network is a group of devices that act as a single Wi-Fi network; so there are multiple sources of Wi-Fi around your house, instead of just a single router. Rather than broadcasting Wi-Fi signals from a single point, mesh router systems have multiple access points. One node links to the modem and acts as the router, while one or more other access points, often called satellites, capture the router's signal and rebroadcast the signal.
Apart from range limitation and associated cost implications, I couldn't find any other significant disadvantages to upgrading to Wi-Fi 6. One thing to keep in mind though, when you are scanning the market for a Wi-Fi 6 router, make sure it is backward compatible and still supports the older 2.4 GHz and 5 MHz standards as some of your legacy devices may not support 6 GHz. Most of them do though but there are some out there that supports 6 GHz only.

Resources: BitPipe, How-to Geek, Wi-Fi Alliance, Intel, PCMag, CEOViews, BinaryTides



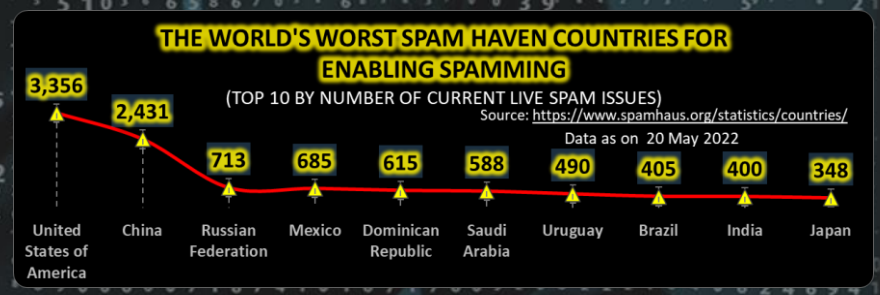
For Reporting Cyber Crime in the USA go to (IC3) , in SA go to Cybercrime, in the UK go to ActionFraud

Other Interesting News and Cyber Security bits:

- Cybersecurity critical to advance a sustainable energy system
- FBI and NSA say: Stop doing these 10 things that let the hackers in
- How to Turn a Coke Can Into an Eavesdropping Device
- 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