On June 8, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Mozilla, Atlassian, and Google products.
CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
10 JUN 22	539,287,147	6,328,533

Deaths this week: 10,782

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

10 June 2022

In The News This Week

Russia's government website hacked with pro-Ukraine message displayed instead

A Russian government website appears to have been hacked over the weekend, causing an Internet search for the site to lead to a "Glory to Ukraine" sign in Ukrainian. Russia's Ministry of Construction, Housing and Utilities website was targeted after many of the country's state-owned companies and news organisations suffered hacking attempts since the Russian government's invasion of Ukraine on February 24. Russia's state news agency RIA quoted a ministry representative on Sunday as saying that the site was down but users' personal data were protected. The website was working as normal by Monday. RIA said that other media had reported that hackers were demanding a ransom to prevent the public disclosure of users' data. Russia's war on Ukraine is being fought not only with bombs but with bytes as cyber warfare plays an increasingly major role in the invasion. - Read the rest of the story by Pascale Davies here: Euronews

Italian city of Palermo shuts down all systems to fend off cyberattack

The municipality of Palermo in Southern Italy suffered a cyberattack on Friday, which appears to have had a massive impact on a broad range of operations and services to both citizens and visiting tourists. Palermo is home to about 1.3 million people, the fifth most populous city in Italy. The area is visited by another 2.3 million tourists every year. Although local IT experts have been trying to restore the systems for the past three days, all services, public websites, and online portals remain offline. According to multiple local media outlets, the impacted systems include the public video surveillance management, the municipal police operations center, and all of the municipality's services. It's impossible to communicate or request any service that relies on digital systems, and all citizens have to use obsolete fax machines to reach public offices. Moreover, tourists cannot access online bookings for tickets to museums and theatres (Massimo Theatre) or even confirm their reservations on sports facilities. Read the full article by Bill Toulas here: BleepingComputer

Cyber security isn't an IT or business problem, it's an "us" problem

Cyber security and cyber crime is affecting every aspect of our lives. It has evolved from being an IT problem, to being a business problem and now it is an 'us' problem. Giving a keynote address at the Cape Town leg of ITWeb's Security Summit, **Wayne Olsen**, managing executive for Cyber Security at BCX, noted that society's mass move to digital is exciting but it introduces a whole new world of risks because our digital transformation is often being done with cyber security as an afterthought. When the pandemic hit, we literally had to take our entire business operations online and do everything in very different ways, he continued. But many did so in a rush and didn't think about the cyber security implications of their digital transformation. "As we make this massive leap towards digitisation, we have become more and more susceptible to cyber attacks," he said, noting that cyber criminals picked up on this; cleverly tapping into popular culture and human emotion to gain illicit access. "According to Forbes survey, there will be around 27 billion devices connected to the Internet of things by 2025. That is 27 billion ways for us to enhance our economy, 27 billion ways for us to have a better social life but also 27 billion additional ways for attackers to get to us," he explained.
Read the rest of the article by Joanne Carew here: ITWeb

Gone in 130 seconds: New Tesla hack gives thieves their own personal key

You may want to think twice before giving the parking attendant your Tesla-issued NFC card. -Last year, Tesla issued an update that made its vehicles easier to start after being unlocked with their NFC key cards. Now, a researcher has shown how the feature can be exploited to steal cars. For years, drivers who used their Tesla NFC key card to unlock their cars had to place the card on the center console to begin driving. Following the update, which was reported here last August, drivers could operate their cars immediately after unlocking them with the card. The NFC card is one of three means for unlocking a Tesla; a key fob and a phone app are the other two. Martin Herfurt, a security researcher in Austria, quickly noticed something odd about the new feature: Not only did it allow the car to automatically start within 130 seconds of being unlocked with the NFC card, but it also put the car in a state to accept entirely new keys—with no authentication required and zero indication given by the in-car display... Read the rest of the article by Dan Goodin here: ARSTechnica

Hackers Breach 4 Discord NFT Servers Following BAYC Server Hack

After the June 4 Bored Ape Yacht Club (BAYC) Discord community hacks, four more Discord NFT communities were compromised and phished of NFTs. The four NFT communities are the Yung Ape Squad, Apocalyptic Apes, Aiternate, and Bubbleworld. The hacks happened on June 6, only 2 days after the BAYC hacks happened. The hackers had the exact similar modus operandi as the BAYC Discord hacks. Firstly, the hackers take the account of one of the Discord moderators and then spam malicious links on servers disguised as announcements. Once a user clicks on the links, their wallets are compromised and they lose their NFTs. The NFT communities have officially addressed the matter and warned its members not to click links at the risk of losing their NFTs. Apocalyptic Apes lost 21 NFTs, meanwhile, Bubbleworld lost 160 NFTs. Read the rest of the story by Connor Jones here: Investing.com

IoT Security: Be Aware of What You Connect at Home

Modern technology In our mega-interconnected world is ultimately designed to make life easier and convenient for us, and in some cases safer. The problem, however, is that the criminal element in our world are always looking for ways to exploit this convenience and are constantly looking for loopholes to profit from or disrupt your life. With more and more IoT (Internet of Things) devices that become available, people tend to want it all. Yes, that is our nature, whether we can afford it all is a different story, but the fact is that we are bringing more and more of these devices into our homes. And, with each device you add, you are expanding what we call the attack surface of your home. The more we get connected, the more we need to think of security. I've reported many horror stories in this post previously where people's homes were "digitally" invaded and the turmoil following after the event. With this in mind, I toiled through the Internet forest and I came across this article by Mike Elgan, giving you something to think about when you connect your next device.

IoT Security: Be Aware of What You Connect at Home

Home IoT device adoption has grown by leaps and bounds. It's a time of connected gadgets everywhere, and with them, comes security risks. McKinsey predicts the total number of IoT-connected devices will be 43 billion by 2023, with the vast majority being consumer devices. Most of these new devices connect via home routers (another IoT device), 5G mobile broadband and satellite internet. These are new frontiers for threat actors, which means a new set of security concerns if you are not prepared.

Routers Can Be the Biggest Security Issue

The more devices connected at home, the bigger the attack surface. One of the biggest unsolved problems is the point of access — the router that IoT, mobile and wearable devices often connect to. For one, these devices aren't designed well enough or configured by the users properly. However, the real problem is that routers can still be breached and lead to compromise on the devices they connect. Ever since the Mirai botnet distributed denial of service in 2016, in which a single person weaponized 400,000 IoT devices (including home routers), IoT breaches based on these seemingly harmless gadgets have been a concern. Since then, the number and kinds of attacks involving IoT security breaches have grown each year.

Security Improvements?

A great many groups, both industry and federal, have published guidelines, recommendations and laws to address the manufacturing, provision and use of the IoT for better security. These include standards and guidelines from Federal and regional government entities across the globe. To date, these standards are not consistent and overlap. They still place burdens on the user or entity for IoT security.

Emerging Solutions - So, how do you keep IoT security in mind over all those connected devices at home?
(1) Built-In Security - While many device makers leave it up to consumers, consumers believe it should be built in. A Karamba Security survey found that 87% of consumers say that device makers, not users, should take the lead on making sure IoT devices are secure. New laws (California, Oregon and federal) focus on unique passwords and needs for the user to change authentication methods. These laws balance safety and convenience, and are not enough for enterprise use on their own. **(2) Biometrics -** Biometrics could standardize defense across devices. The mainstreaming of first fingerprint scanners and then face recognition in smartphones has gotten consumers used to this kind of interface. Scans can provide both defense and convenience. Behind the scenes, researchers have developed and nearly perfected a wide range of biometric solutions. From voice recognition to vein pattern scans to sensors tracking gait, they could help secure the future smart home. **(3) Labelling -** Another upcoming idea is the use of relevant labels on consumer devices, warning buyers about the risks of each product. This could affect product reviews and motivate creators to add better and easier security in consumer products.

How to Protect Yourself When Using Consumer Gadgets

There is no such thing as a one-button fix for IoT security threats to mobile and wearable devices for consumers. But, you can stay safe by following these best practices:

Buying IoT Devices

Choose products that emphasize digital safety. Key features to look for include how often firmware updates, data handling features, the option to turn off needless features and the option to limit access.

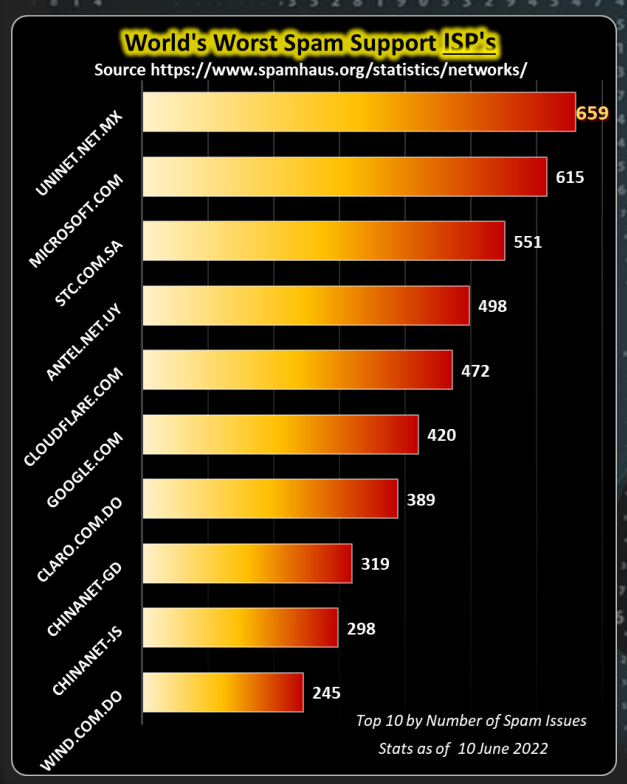
Using IoT Devices

(a) Use multifactor authentication whenever possible. (b) Next, use biometric security whenever possible. (c) Always change the default passwords for every device you use. Use a password-management solution, and use a different strong password for every device. In addition, change passwords often. (d) Turn off devices completely when they're not in active use. (e) Always keep devices updated with the latest firmware. Your router is the most important one to check. (f) Lastly, for mobile devices, including smartphones, turn on location services only for apps that truly need it.

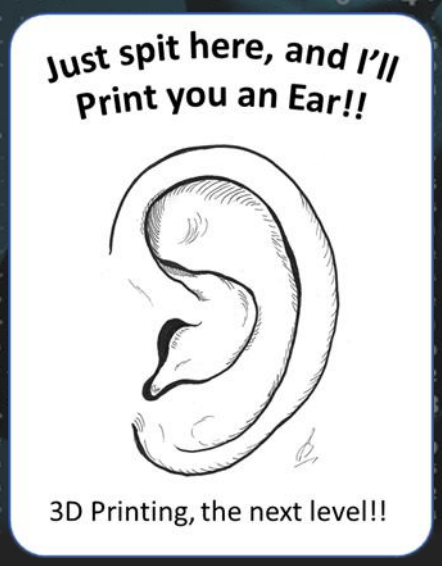
Managing IoT Devices Across Your Network

Use three different Wi-Fi networks if possible — one for work devices, one for home computing devices and another for IoT devices. (Follow manufacturers' instructions for segmenting networks.) This reduces the attack surface and makes it easier to track and contain breaches. Know your home routers' features and access the admin panel only via Ethernet. Change the name of the network, disable remote access, turn on encryption and enable the router's firewall feature.
In the era of the smart home, connected car and wearable computing device, we also see attacks plaguing consumers at a whole new level. With a mix of purchasing incentives, new tech and a new emphasis on defense by device makers, software companies and consumers alike, we can maximize consumer IoT safety going forward.

Read the full articled and other topics here: Security Intelligence

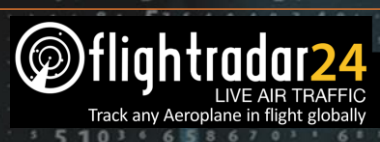


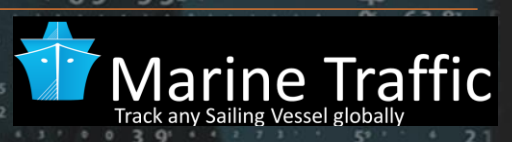
For Reporting Cyber Crime in the USA go to (IC3) , in SA go to Cybercrime, in the UK go to ActionFraud

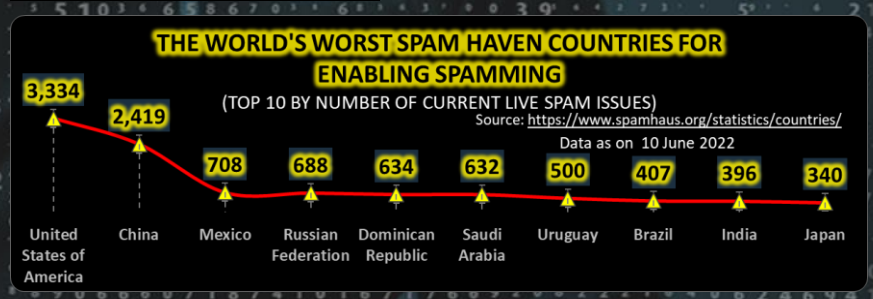


Other Interesting News and Cyber Security bits:

- Encryption Security for a Post Quantum World
- 3D Printing - Tissue printer creates lifelike human ear
- Introducing: Hack Me If You Can - Podcast
- SANS Daily Network Security Podcast (Storm cast)







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