Low
Guarded
Elevated
High
Severe
Global Internet Security Alert Level
Source:
CIS. Center for Internet Security
By
Chris Bester

On July 6, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Mozilla and Google products.
CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
08 Jul 22	558,799,953	6,369,387

Deaths this week: 11,176

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

08 July 2022

In The News This Week

Hacker claims to have stolen 1 bln records of Chinese citizens from police

SHANGHAI, July 4 (Reuters) - A hacker has claimed to have procured a trove of personal information from the Shanghai police on one billion Chinese citizens, which tech experts say, if true, would be one of the biggest data breaches in history. The anonymous internet user, identified as "ChinaDan", posted on hacker forum Breach Forums last week offering to sell the more than 23 terabytes (TB) of data for 10 bitcoin , equivalent to about $200,000. "In 2022, the Shanghai National Police (SHGA) database was leaked. This database contains many TB of data and information on Billions of Chinese citizen," the post said. "Databases contain information on 1 Billion Chinese national residents and several billion case records, including: name, address, birthplace, national ID number, mobile number, all crime/case details.". So far, Reuters was unable to verify the authenticity of the post. Read the full article here: Reuters – **2 Days later, China censors block news of hack exposing data of 1 billion Chinese citizens**… Read the follow-up story by Grady McGregor here: Fortune .. and more here: Bloomberg

Cloud Misconfig Exposes 3TB of Sensitive Airport Data in Amazon S3 Bucket: 'Lives at Stake'

- The unsecured server exposed more than 1.5 million files, including airport worker ID photos and other PII, highlighting the ongoing cloud-security challenges worldwide. - A misconfigured Amazon S3 bucket resulted in 3TB of airport data (more than 1.5 million files) being publicly accessible, open, and without an authentication requirement for access, highlighting the dangers of unsecured cloud infrastructure within the travel sector. The exposed information, uncovered by Skyhigh Security, includes employee personal identification information (PII) and other sensitive company data affecting at least four airports in Colombia and Peru. The PII ranged from photos of airline employees and national ID cards — which could present a serious threat if leveraged by terrorist groups or criminal organizations — to information about planes, fuel lines, and GPS map coordinates. Read the full article by Nathan Eddy here - DarkReading

Google TAG exposes hack-for-hire groups targeting activists and sensitive data

Google Threat Analysis Group (TAG) exposed hack-for-hire groups operating in Russia, India and the United Arab Emirates (UAE), in a blog post released last Thursday - Hack-for-hire groups use various methods to pursue their targets, with some openly advertising their services, while other groups solicit business with a more select group of potential clients, according to researchers. TAG tracked a group of India-based threat actors, some of them with prior experience inside offensive security firms, including Appin and Belltrox. Researchers have linked the former employees to a new firm called Rebsec, which openly advertises corporate espionage.... Read the rest of the post by xxx here: Cybersecuritydive

North Korean State Actors Deploy Surgical Ransomware in Ongoing Cyberattacks on US Healthcare Organizations

- US government warns healthcare and public-health organizations to expect continued attacks involving the manually operated "Maui" ransomware. - The FBI, US Cybersecurity and Infrastructure Security Agency (CISA), and the Treasury Department on Wednesday warned about North Korean state-sponsored threat actors targeting organizations in the US healthcare and public-health sectors. The attacks are being carried out with a somewhat unusual, manually operated new ransomware tool called "Maui." Since May 2021, there have been multiple incidents where threat actors operating the malware have encrypted servers responsible for critical healthcare services, including diagnostic services, electronic health records servers, and imaging servers at organizations in the targeted sectors. In some instances, the Maui attacks disrupted services at the victim organizations for a prolonged period, the three agencies said in an advisory..
Read the full story by Jai Vijayan here: DarkReading (More here: Security Magazine)

Apple Introduces Lockdown Mode to Secure Its OSes Against Cyberattacks

The new Lockdown Mode announced by Apple, available now in the latest betas of iOS 16, iPadOS 16, and macOS Ventura, aims to provide a further level of protection to users at risk of highly targeted Cyberattacks. *"Lockdown Mode offers an extreme, optional level of security for the very few users who, because of who they are or what they do, may be personally targeted by some of the most sophisticated digital threats, such as those from NSO Group and other private companies developing state-sponsored mercenary spyware*". Turning on Lockdown Mode will require users to enable the corresponding option in Settings.app and restart their devices. This action will harden the OS defenses and limit a number of functionalities, thus reducing the attack surface available to cyberattackers.. Read the rest of the article by Sergio De Simone here: InfoQ

The British Army's Social Media Accounts Get Hit by Hackers

After falling victim to the latest cyber-attack, the British Army has gained control of its targeted social media accounts. According to sources, the hackers attacked the British Army's Twitter and YouTube accounts. The attackers renamed both accounts and used them to promote fraud cryptocurrency and non-fungible token (NFT) projects. Moreover, the promoted scam was an NFT and crypto project known as "ThePossessedNFT."… Read the rest of the article here: CoinCuora

Parenting Safety Tips For Teens On Mobile Phones & Tablets

The stark reality of the technology age we live in is that as good as it is for most things, the digital frontier is also a dangerous place. Like the Wild West of old, law enforcement is a huge challenge in the wide expanse of the Internet, and kids are the most vulnerable. Kids, especially teenagers, are also susceptible to peer pressure and the lure of cyber gangs that can land them in all sorts of trouble with very little or no escape route. If it comes to mobile phones, let's face it, there are no dumb phones anymore, they are all smartphones with more processing power than the Cyber 730 mainframe computer that was used to help land Apollo 11 on the moon. Most of the teenagers I know carry one, and they are constantly online.

So how do we protect our kids?

The last thing I want to do is to spy on my kids to see what they are up to, but maybe for some parents that could be the best way to protect them. If you have a strong suspicion that your kids are involved with something they should not be, then what do you do as a parent? My personal choice is to keep an open dialog with my two boys, not just about the dangers of cyberspace but also the good stuff. I believe the key is to stay connected with them on their level. Listen to their conversations and keep an eye out for those tell-tale signs we spoke of in last week's post. In today's post, I just want to introduce you to some ideas, concepts, and maybe some tools that can help you and put your mind at ease. The HelpYourTeenNow advocacy group posted a downloadable eBook on "How to keep your teen safe on mobile devices", which gives some insight into scary statistics. They also posted some tips on "How To Set Security Settings On Your Child's Mobile Device", and below is a short extract of this post.

How To Set Security Settings On Your Child's Mobile Device

Most phones come equipped with a few ways to set up restrictions for your teens and their phone usage.

iOS for iPhone & iPad Parental Restriction Settings

(1) Settings > General **(2)** Restrictions > Enable Restrictions **(3)** Create a parental passcode **(4)** Go through each setting type to enable the type of restrictions you'd like to put on your child's phone. The settings allow you to customize which apps and content types the phone is allowed to access. You can also prevent your teen from changing the privacy settings on specific apps (e.g., Facebook) after you've set them up.

Android Tablet Parental Controls - *[For Android 4.3 Jelly Bean or later.] - For Android phones, skip to the next set of instructions.*

(1) Pull down the top menu and tap Settings **(2)** Users **(3)** Add user or profile **(4)** Create a restricted profile **(5)** Enter a parental PIN (If you already have a PIN you won't see this step.) **(6)** Tap the Settings icon next to New Profile and give it a name (e.g., Teen) **(7)** Go through the list of apps and toggle off the apps you'd like to restrict. **(8)** Location sharing defaults to "OFF" unless it's been turned on by your child.
(9) You can also restrict access to the Google Play Store to prevent unauthorized purchases from your child's phone.

- Launch the Play Store
- Tap the menu and select Settings
- Enable the feature called "Password – Use password to restrict purchases"
- Enter the password for your Google account

Android Phone Parental Controls - *[For Android 5.0 Lollipop you have the options of limiting SMS & voice calls only. Additionally, earlier versions of Android don't have parental controls. In addition, some phones running Android 5.0 or newer still do not have the ability to create multiple users]*

(1) Tap the Profile icon (a white circle) in the notification bar **(2)** The Users menu appears **(3)** Tap Add User > OK **(4)** Tap Set Up Now **(5)** Tap the gear icon next to the User Name you just created **(6)** Slide the selector to the right to disallow SMS and phone calls
(7) You can also restrict access to the Google Play Store to prevent unauthorized purchases from your child's phone.

- Launch the Play Store
- Tap the menu and select Settings
- Enable the feature called "Password – Use password to restrict purchases"
- Enter the password for your Google account

Amazon Fire Tablet Parental Controls *[For Amazon Fire phones, see below.]*

(1) Swipe down from the top of the screen to show Quick Settings, and then tap More **(2)** Toggle the parental controls ON **(3)** Enter a password, confirm your password, and then tap Finish **(4)** From here you can restrict almost anything about the tablet, including: browsing, email, social sharing, the camera, and purchases.

Amazon Fire Phone Parental Controls

(1) From Settings > Applications & Parental Controls **(2)** Enable Parental Controls **(3)** Toggle the parental controls ON **(4)** Enter a password, confirm your password again, and then tap Submit **(5)** From here you can restrict almost anything about your child's phone, including: browsing, email, social sharing, the camera, and purchases.

Are Your Keeping Up With Your Teen & Mobile Technology? (Short extract of the eBook)

Today the world is changing at a rapid pace. With ongoing innovations in every area of our lives, it can be a challenge to keep up-to-date on all the new technology. As wave after wave of new devices and applications come in, you may feel at best overwhelmed or even like you could get left behind. However, it's extremely important that we keep children safe online and with mobile devices because with new frontiers come new dangers.

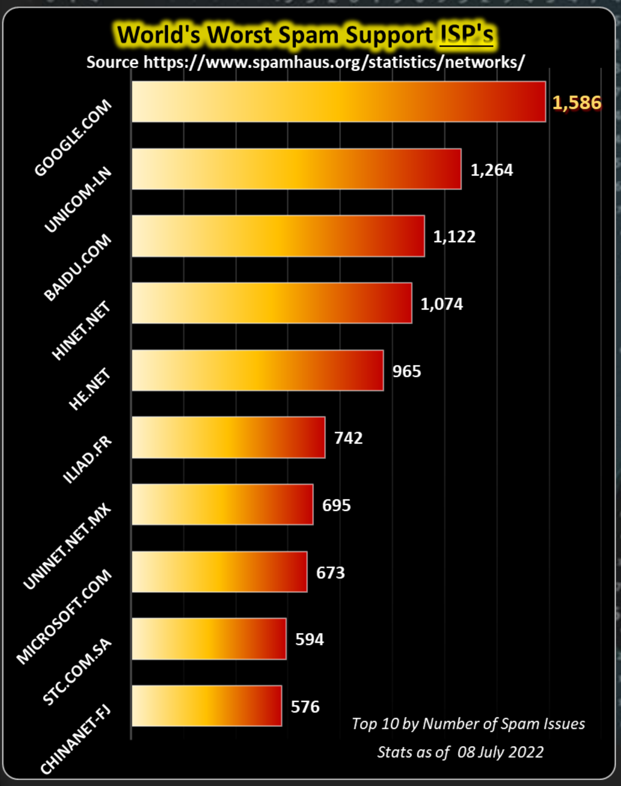
Numerous studies reveal the frightening threats to today's online teens. Parents believe they are in control when it comes to monitoring their teen's online behaviors. However, these studies show that many parents know very little about what their children are doing online — particularly with their mobile phones.

How much time does your child spend in front of mobile screens?

Studies vary wildly on how much screen time teens indulge in, particularly by country. However, a recent global study of 32 different countries found that teens spend about three hours on the mobile web per day.

A British study found that a child born in 2014 can expect to spend an entire year of his life (that's 365 days for 24 hours a day) in front of a screen by the age of seven. Another study found that people check their mobile devices on average over 200 times per day…. (the rest here)

Resources: HelpYourTeenNow, YourTeen, Top10-Parenting Control Apps, PCMag



World's Worst Spam Support ISP's
Source https://www.spamhaus.org/statistics/networks/

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

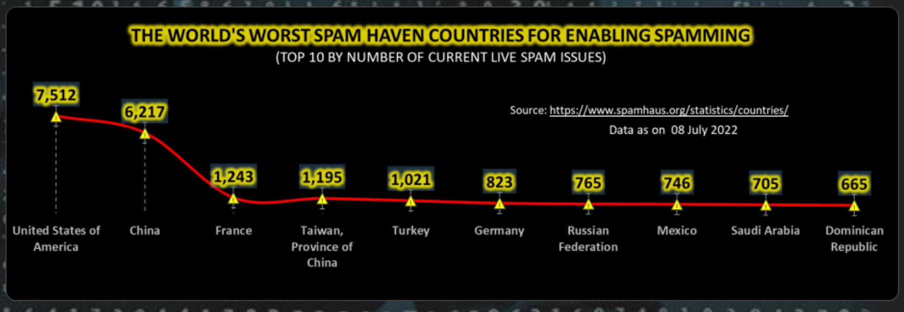
Pappa, come and see which cool group wants me to join them on Discord… They say they have some cool tools and stuff to share!
DANGER

Other Interesting News and Cyber Security bits:

- CERN is firing up its Large Hadron Collider at record energy levels, in search of dark matter
- To stop quantum hackers, the US just chose these four quantum-resistant encryption algorithms
- The top 3 scams targeting mobile phones
- SANS Daily Network Security Podcast (Storm cast)

flightradar24 LIVE AIR TRAFFIC
Track any Aeroplane in flight globally

Marine Traffic
Track any Sailing Vessel globally



THE WORLD'S WORST SPAM HAVEN COUNTRIES FOR ENABLING SPAMMING
(TOP 10 BY NUMBER OF CURRENT LIVE SPAM ISSUES)
Source: https://www.spamhaus.org/statistics/countries/
Data as on 08 July 2022

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