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

On May 12, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded). No further updates from CIS this week.

Covid-19 Global Stats

Date	Confirmed Cases	Total Deaths
04 June	172,893,291	3,716,836

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

04 June 2021

In The News This Week

JBS: World's largest meat supplier hit by cyber-attack

The world's largest meat processing company has been targeted by a sophisticated cyber-attack. Computer networks at JBS were hacked, causing some operations in Australia, Canada and the US to temporarily shut down, affecting thousands of workers. The company believes the ransomware attack originated from a criminal group likely based in Russia, the White House said. The attack could lead to shortages of meat or raise prices for consumers. In a ransomware attack, hackers get into a computer network and threaten to cause disruption or delete files unless a ransom is paid. The White House says the FBI is investigating the attack.

"JBS notified [the White House] that the ransom demand came from a criminal organisation likely based in Russia," White House spokeswoman Karine Jean-Pierre said on Tuesday.. Read the full story here: BBC News

South Africa - WhatsApp messages that can now land you with a fine and jailtime

President Cyril Ramaphosa has signed the Cybercrimes Bill into law, bringing South Africa's cybersecurity laws in line with the rest of the world. The bill, which is now an act of parliament, creates offences for and criminalises, amongst others, the disclosure of data messages which are harmful, says Ahmore Burger-Smidt, director and head of Data Privacy Practice at Werksmans Attorneys. Examples of such data messages include: (1) Those which incite violence or damage to property; (2) Those which threaten persons with violence or damage to property; (3) Those which contain an intimate image sent without the subject's consent.

Other offences include cyber fraud, forgery, extortion and theft of incorporeal property, said Burger-Smidt. The unlawful and intentional access of a computer system or computer data storage medium is also considered an offence along with the unlawful interception of, or interference with data." "This creates a broad ambit for the application of the Cybercrimes Act which defines 'data' as electronic representations of information in any form."

Read the rest of the story here: BusinessTech

Japanese Government Agencies Suffered Cyber Attack Exposing Proprietary Data

Several Japanese government agencies reportedly suffered data breaches originating from Fujitsu's "ProjectWEB" information sharing tool. ProjectWEB is a cloud-based enterprise collaboration and file-sharing platform launched in the mid-2000s. The cyber attack forced the Japanese IT equipment and services company to deactivate the software-as-a-service (SaaS) platform. Fujitsu had earlier disclosed that hackers gained unauthorized access to the system and stole customer data. The computer emergency response team is still investigating and trying to determine if government agencies were targeted or the incident was a software supply chain attack.

Read the article by Alicia Hope here: CPO Magazine

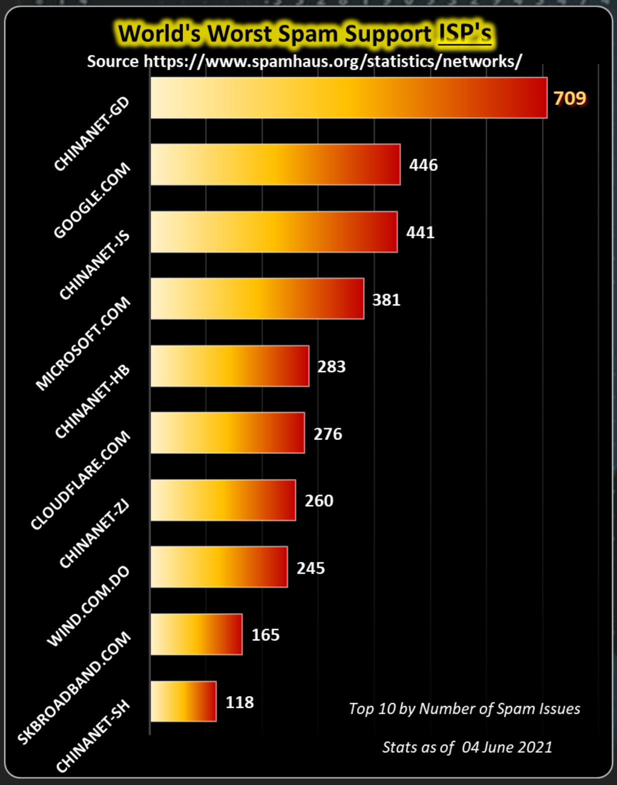
Cyber Security spend on the rise as it becomes more important than ever

Since the pandemic and the rise of people working from home, cyber criminals have had to adapt to their new environment prior to launching a cyber attack. The UK Government estimates that the cost of cyber crime is £27bn a year. The latest data released in the Hiscox Cyber Readiness Report shows that organisations are upping their defences against cyber crime, with cyber security taking up 21% of the average organisation's IT budget. This is a large jump from the 13% which was used for the same spend last year. Although more spend could be allocated to cyber security, the increase in this year's spend is being attributed to: (1) 43% of organisations experienced a cyber attack in 2021 compared to 38% in 2020; (2) Of those experiencing an attack, 73% of them experienced more than one attack in the last 12 months; (3) Only 9% of attacked organisations revealed that they were able to defend the attack with no impact to operations.

The report revealed that phishing was still the main way that cyber criminals were infiltrating businesses with 65% of organisations being attacked via this method, so ensuring employee vigilance is still key in the fight against crime. Read the story here: Today's Conveyancer

World's Worst Spam Support ISP's

Source https://www.spamhaus.org/statistics/networks/



Top 10 by Number of Spam Issues

Stats as of 04 June 2021

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

Mmmm, lets target the politicians with Android phones then...

Android vs. iOS

This week I stumbled on a recent report on digitaltrends by Simon Hill and Mark Jansen weighing up and comparing features between the two mobile platform giants, Android and iOS. Although my interest is more from a security perspective, they came up with quite a few interesting comparisons I thought worthy of sharing. For the sake of space limitations, I'll summarise some of the comparisons but please visit the site to read the complete article if this tickles your interest.

Security - Much has been supposedly "toxic stew" off apps on Android, but the threat of malware is exaggerated. The truth is that most people will never encounter a problem because they don't go outside the Play Store for apps. Some manufacturers have taken extra efforts to beef up security for the enterprise market, but the slow nature of updates on many Android devices can seriously delay important security patches. Speedy updates are now more important than ever because security breaches are becoming more serious. Android tends to generally lag in the update world unless you have a phone running Android One. The lack of update speed tends to mean Android is less secure to emerging threats. Because millions of Android phones are still running software that's years old, they can be vulnerable to serious hacks like Heartbleed and Stagefright.

Apple is firmly entrenched in corporate America and has also worked on improved security for general consumers, most notably with Touch ID and FaceID in the iPhone X and later. The tight oversight that Apple has on apps and the ability to push updates out to more devices more quickly gives it an edge over Android. The company also encrypts data in iMessage and its other apps. Apple prioritizes user privacy, so you can feel safe knowing your personal data is not stored or read by Apple. It is all encrypted, too.

Meanwhile, Android encrypts some data, but your privacy is less protected. Google mines your data for information that it can use to sell better ads and market products to you. Your data is also stored and read to provide you with a better A.I. experience.

Google claims it is committed to fully protect user privacy and still provide the A.I. services it offers, but some security experts and Apple argue that Google presents a false choice between A.I. and privacy. Apple even went to war with the FBI to guarantee your right to encryption. It's hard to beat that kind of dedication.

There's no denying that iOS is the most secure platform and the one that best protects user privacy. If you care about your privacy and security, go with an iPhone. Winner: iOS

Rooting, bootloaders, and jailbreaking - It's not for everyone, but if you want root access and complete control over your device, then rooting is the way to get it. Rooting gives you access to more apps, the latest OS updates without waiting, new software skins to get the aesthetic you want, the chance to get rid of bloatware from carriers and manufacturers, potential tweaks to boost your device's speed and battery life, and more. Many Android OEMs (original equipment manufacturers) also offer a way to unlock the bootloader, which determines how the OS loads up on your device. Apple is completely opposed to this kind of thing. Jailbreaking is an option for iOS, which lets you download and install apps from outside the App Store and bypass some other limitations. (My comment: Rooting and Jailbreaking, however, can open a security can of worms that can seriously sour up your day.)

Winner: Android

Updates - Apple's iOS offers consistent and timely software updates and security patches. If you want the same experience on Android, then you have to buy one of Google's Pixel phones or any phone running Android One. This is how iOS version shares break down according to the official Apple Developer website: iOS 14: 80%, iOS 13: 12%, Earlier: 8%

So, around 80% of all iOS devices are now running the latest version, and the numbers are even better when you look at devices introduced in the last four years. For those devices, 86% run iOS 14, 12% run iOS 13, and only 2% run an earlier version of iOS. That's impressive.

Is Android up to a similar standard? No. Android 11 is now available, but don't expect it to spread to a majority of devices for a while. Our Android stats come from Android Studio and don't seem to be updated as often as Apple's iOS distribution numbers. Android 11's distribution stats seem to be out now, but we wouldn't expect it to move into double digits for a while. Heck, according to Android Studio, it's struggling to hit a single percentage point. Android Studio stats: Android 11: <1%, Android 10: 8.2%, Android 9.0 Pie: 31.3%, Android 8.1 Oreo: 14% ; Android 8.0 Oreo: 7.3%, and so on. (See Android studio for the rest of the stats.)

While there are some notable exceptions for Google's own Pixel phones and those running Android One (like many of Nokia's phones), if you want the latest features, bug fixes, and security updates, then you should choose iOS. Winner: iOS

Alternative app stores and sideloading - It's relatively easy to sideload apps on Android. Tick a box in the settings, download an APK, and you're set. There are also a lot of alternative Android app stores beyond the Play Store, but sideloading can open you up to the risk of malware and isn't worth worrying about for most people. Apple is opposed to third-party app stores, and if you want to access them, you'll have to jailbreak your iPhone. If you want a wider choice of apps and easy sideloading, then your winner is obvious. Winner: Android

Customizability - This has always been one of Android's main strengths. It's very easy to customize your phone — you can set up the layout you want on your home screen, add widgets and shortcuts, and even change your entire user interface with launchers.

iOS 14 was something of a revolution for iPhone users, introducing far more support for widgets on the iOS home screen. While initially, this seems more like a bit of fun, some users have taken advantage of widget-customizing apps to dramatically change the look of their devices. However, it's still not up to the level of Android, which allows for third-party launchers that can completely change your phone into something else entirely. If you want a phone that embraces tinkering, or a truly unique, personalized look for your home screen, then Android is the platform for you. Winner: Android

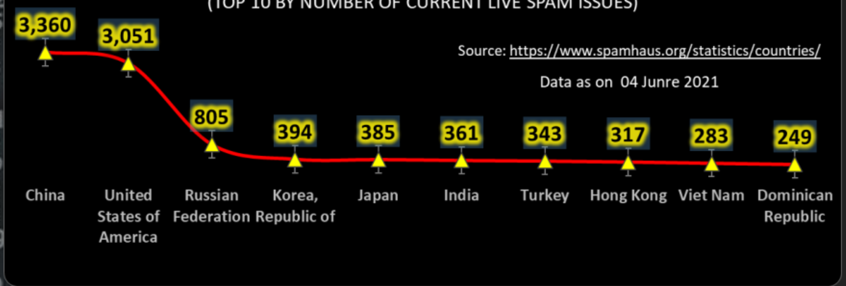
References: digitaltrends , IDC, Apple Developer, Statista, Alternative-Android-App-Stores, Android Studio

Other Interesting News and Cyber Security bits:

- Insights on the Data-centric Security Global Market to 2027 - Industry Analysis Report and Forecasts
- Microsoft continues IoT security push
- 2021 Cyber Security Statistics - The Ultimate List Of Stats, Data & Trends

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 04 Junre 2021

AUTHOR: CHRIS BESTER (CISA,CISM)

chris.bester@yahoo.com