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

On April 22, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded).

Covid-19 Global Stats

Date	Confirmed Cases	Deaths
23-Apr	145,332,791	3,085,234

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

23 April 2021

In The News This Week

FBI cleans web shells from hacked Exchange servers in rare active defense move

The FBI has been deleting backdoors placed by cyberespionage group Hafnium on Microsoft Exchange servers. The court order allowing them to do so signals a more active defense approach. - In a move that has been described as unprecedented, the FBI obtained a court order that allowed it to remove a backdoor program from hundreds of **private** Microsoft Exchange servers that were hacked through zero-day vulnerabilities earlier this year. The operation shows that the FBI is ready to take a more active approach in responding to cyber threats that goes beyond its traditional investigatory role, but also raises questions about where the limits should be with such actions. Earlier this week, the Department of Justice announced that the FBI was granted a search and seizure warrant by a Texas court that allows the agency to copy and remove web shells from hundreds of on-premise Microsoft Exchange servers owned by private organizations. A web shell is a type of program that hackers install on hacked web servers to grant them backdoor access and remote command execution capabilities on those servers through a web-based interface. In this case, the warrant targeted web shells installed by a cyberespionage group dubbed Hafnium that is believed to have ties to the Chinese government.

Read the story by Lucian Constantin here: CSO

US sanctions Russian government, security firms for SolarWinds breach, election interference

- The Biden administration places economic sanctions on Russian government organizations, individuals, and companies including several security firms. -The Biden Administration announced a robust, coordinated series of punitive measures to confront Russia's growing malign behavior, including its massive hack of SolarWinds's software, attempts to interfere with the 2020 elections, and other destructive deeds against the US. The administration's actions levy financial sanctions on the country and the companies usually involved in malicious cyber activity against the US. It also exposes previously withheld details about the Russian ruling regime's digital and disinformation operations. In addition to the White House, the National Security Agency (NSA), Federal Bureau of Investigation (FBI), Department of Homeland Security, and Treasury Department all play a role in the complex set of actions against Russia. Read the rest of the article here: CSO

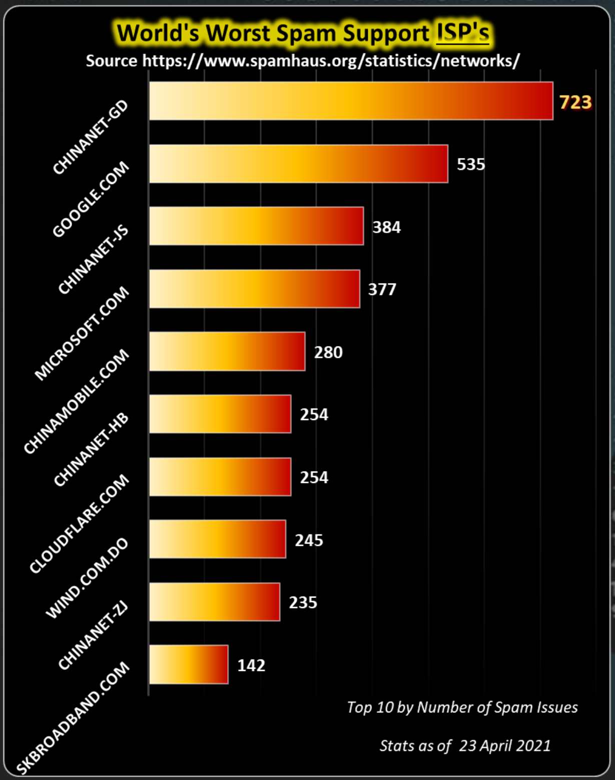
China behind another hack as U.S. cybersecurity issues mount

China is behind a newly discovered series of hacks against key targets in the U.S. government, private companies and the country's critical infrastructure, cybersecurity firm Mandiant said Wednesday. The hack works by breaking into Pulse Secure, a program that businesses often use to let workers remotely connect to their offices. The company announced Tuesday how users can check to see if they were affected but said the software update to prevent the risk to users won't go out until May. The campaign is the third distinct and severe cyberespionage operation against the U.S. made public in recent months, stressing an already strained cybersecurity workforce. The U.S. government accused Russia in January of hacking nine government agencies via SolarWinds, a Texas software company widely used by American businesses and government agencies. In March, Microsoft blamed China for starting a free-for-all where scores of different hackers broke into organizations around the world through the Microsoft Exchange email program. In all three campaigns, the hackers first used those programs to hack into victims' computer networks, then created backdoors to spy on them for months, if not longer.

Read the full article by Kevin Collier here: NBCNews

Hungary - Cyber Security Centre Issues Warning over Blackmailing Emails

The Hungarian cyber security centre NKI has renewed its warning over masses of blackmailing emails sent to Hungarian state offices, local municipalities, public institutions and private individuals. NKI said the emails inform the recipient that his or her computer has been infected by a trojan which has copied their data, including video recordings of their activities while visiting adult websites. The sender of the email threatens the recipient with forwarding the compromising recordings to friends or publishing them on public media unless payment is transferred.. Read the story here: HungaryToday

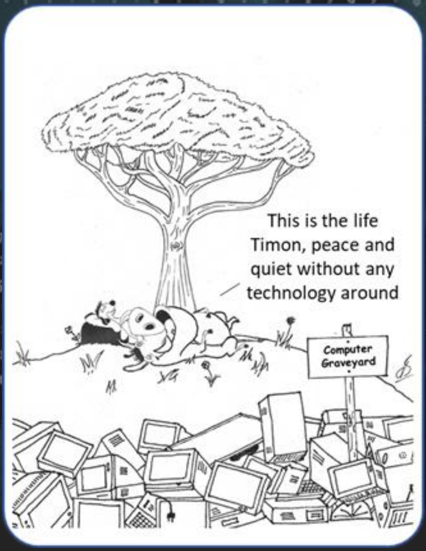

World's Worst Spam Support ISP's

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

Top 10 by Number of Spam Issues

Stats as of 23 April 2021

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


This is the life Timon, peace and quiet without any technology around
Computer Graveyard

Smartphone Security

The topic of Smartphone or Mobile phone security has been covered in many forms in this bulletin in the past but due to the nature of the ever-changing and evolving threat landscape, it is always good to revisit the subject from time to time. The recent WhatsApp debacle on privacy and what is gleaned off your phone brought home the fact that we have to be ever vigilant and always keep safeguarding our personal information in mind. To this effect, I want to share an extract of a recently updated Reader's Digest article that gives a good overview and tips on how to maintain security on your smartphone. Deep dive into the links provided in the article to get an even better understanding.

Smartphone Security: Everything You Need to Know to Keep Your Phone Safe

These days, your smartphone is more than just a way to call or text people, it serves as an external backup brain that more often than not holds all the important data in your life. Here's how to protect all your precious data. Considering our smartphones are now home to everything from emergency contacts to banking information, keeping those assets out of the wrong hands is more important than ever. Read on for all the mobile security threats you need to be on the alert for and what steps experts recommend you take to protect your device.

Phone security best practices

Ignore and avoid phishing attacks - Hackers and digital thieves are becoming craftier than ever in an attempt to steal the keys to your identity. Once you're aware of their tricks and know about the latest scams, including Apple ID phishing scams and vishing, you won't fall victim or mistakenly download a virus to your phone. Your first line of defense: immediately delete any questionable emails or texts and learn how to stop spam texts altogether.

Use antivirus for phones - Did you know that even with the latest iPhone security updates, iPhones can get viruses, too? Android users will want to know the ins and outs of Google Play Protect. If you should accidentally download a virus, we have you covered for that as well and can fill you in on how to remove hidden malware on an Android phone. Of course, investing in one of the most secure phones is essential to preventing security problems in the first place.

Secure your messages to maintain privacy - Whether you're in a career that demands privacy or you're simply planning a surprise birthday party for a friend, you'll want to know about these strategies for keeping your texts and phone calls secure. Start by learning how to hide text messages on an iPhone. Then consider if you need an encrypted phone, find out what this buzzword actually means and why and how to encrypt your iPhone or Android phone. The most secure messaging apps are a must for anyone with privacy concerns.

Manage your app permissions - Your smartphone and the apps you download to your phone know a lot about you, sometimes even too much. One of the quickest ways to keep your personal information private is by paying attention to your app permissions. For example, does your rideshare app really need access to your contact list or your calendar? Both iPhones and Androids have made it easier than ever to control app permissions, but you still need to do your homework in order to limit them to the ones the app truly needs. Apple devotees will want to know how to delete apps on an iPhone and iPhone privacy settings they should check ASAP. Also, everyone should know how to clear cookies from your phone; cookies are little bits and pieces of data that can reveal your likes, dislikes, and habits—and they reveal a lot about you.

Lock your phone - According to a 2017 Pew Report, almost 30 percent of smartphone owners do not even use a screen lock or other security features; yet the easiest and most obvious way to keep your phone protected is to regularly lock your home screen and use two-factor authentication. Additionally, experts recommend that you go the extra mile, so make sure you don't have a weak password and learn how to lock apps on your phone.

Be wary of public Wi-Fi - Sure, it can be convenient to check your email while waiting for your subway or bus and you may occasionally go to the coffee shop down the street to work. But logging on to an open Wi-Fi network could potentially open your device up to hackers, if you're not careful.

Use a recovery app to find a lost phone - A lost or stolen iPhone may feel like the worst thing in the world that can happen, but there are steps you can take immediately to protect yourself and your information. Plus the built-in Find My iPhone app can help you reconnect with your lost phone. Lost phones aren't the only way your data can be stolen, so be sure you know how to factory reset your iPhone or Android and do so before turning it in or recycling.

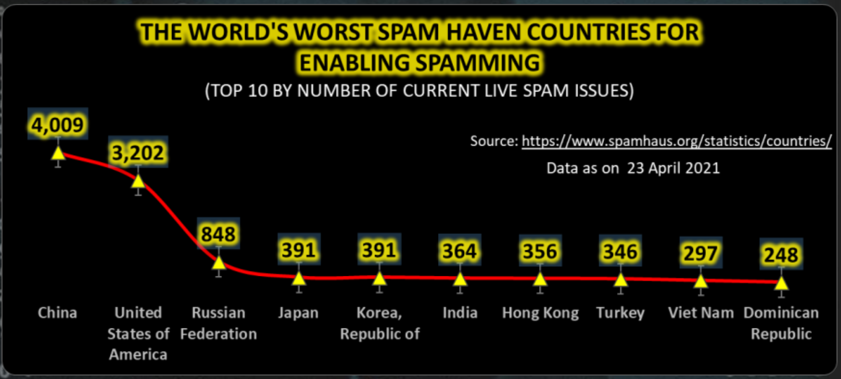
Don't jailbreak or root your device - Finally, experts strongly recommend against jailbreaking your iPhone or rooting your Android. Why? Even though jailbreaking your phone may seem appealing, no customization is worth making your phone vulnerable to hacking or other viruses.

Bottom line - While iPhone and Android are constantly employing better and more sophisticated security measures—and these are the most secure phones on the market—at the end of the day, keeping your phone and personal data safe is largely up to you. If you get a suspicious scam text or an iPhone virus warning, think twice before automatically clicking on any links to open it. Look to see if there are any tell-tale misspellings? Does the URL start with "https:"? And remember, that Apple (and other legitimate companies, such as your bank) will never ask for your password in a text message. Common sense will always be your best defense.

Reader's Digest Article

Other Interesting News and Cyber Security bits:

- First multi-node quantum network paves the way for the quantum internet
- UK - NCSC offers teachers free cyber security training
- How Cyber-Attack Automation Turned SMEs into Sitting Ducks: And How to Change This


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 23 April 2021

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