The Cyber Threat Alert Level was evaluated on May 12 2021, and was set to Blue (Guarded), and will remain at this level until a change is indicated by CIS.

Covid-19 Global Stats

Date	Confirmed Cases	Total Deaths
16 July	189,730,243	4,083,003

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

16 July 2021

In The News This Week

South Africa is Burning - Landlords beef up security and close malls as looters run amok

More than 200 retail centres have been damaged since the incarceration of Jacob Zuma. Mall owners have heightened their private security or closed their shopping centres to protect customers from looters and rioters especially in Gauteng and KwaZulu-Natal. More than 200 malls have been looted or destroyed and more than 600 stores have been torched or damaged since violence broke out at the weekend, the SA Property Owners Association (Sapoa) said in a statement on Tuesday. The body that represents 800 member companies and organisations said the situation is getting worse and that the authorities trying to calm the situation are overwhelmed. Sapoa CEO Neil Gopal said though President Cyril Ramaphosa had undertaken in his speech on Monday to provide sufficient security to prevent further destruction, "looting is continuing and the police and private security are not coping". "The capacity authorised for [the] South African National Defence Force (SANDF) seems insufficient to quell the unrest." Read more about the situation here: BusinessDay, TechCentral, BBC

German Cyber-Security Watchdog Confirms Country's First 'Cyber-Catastrophe'

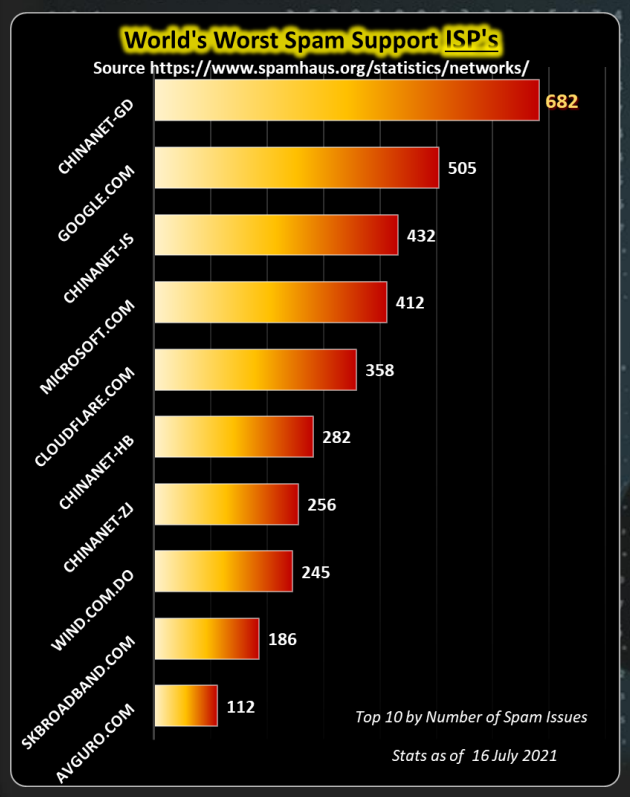
A district council in eastern Germany has declared a disaster after its computer systems were paralyzed by a hacker attack in what the federal cyber-security watchdog confirmed was the country's first-ever "cyber-catastrophe." Hackers knocked out the IT operations of the municipality of Anhalt-Bitterfeld, in the state of Saxony-Anhalt, on Tuesday, a spokesperson confirmed to Reuters on Saturday. "We are almost completely paralyzed," the spokesperson said, adding its offices would probably remain offline next week and giving no indication of when services would resume. The municipality declined comment on the identity of the attacker or whether they had made a ransom demand, citing a police investigation. Security sources say German local governments often run outdated and poorly maintained software systems that could be wide open to cyber attack. The rural district of Anhalt-Bitterfeld, with a population of 157,000, is for the time being unable to pay out welfare benefits. Its consequent catastrophe declaration is a formal step that allows it to call for federal help. Read the full story by Andreas Rinke here: Insurance Journal

China tightens control over cybersecurity in data crackdown

Tech experts in China who find a weakness in computer security would be required to tell the government and couldn't sell that knowledge under rules tightening the Communist Party's control over information. The rules would ban private sector experts who find "zero day," or previously unknown security weaknesses, and sell the information to police, spy agencies or companies. Such vulnerabilities have been a feature of major hacking attacks including one this month blamed on a Russian-linked group that infected thousands of companies in at least 17 countries. Beijing is increasingly sensitive about control over information about its people and economy. Companies are barred from storing data about Chinese customers outside China. Companies including ride-hailing service Didi Global Inc., which recently made its U.S. stock market debut, have been publicly warned to tighten data security. Read the full story by Joe McDonald here: ABC News

Google: Russian SVR hackers targeted LinkedIn users with Safari zero-day

Google security researchers shared more information on four security vulnerabilities, also known as zero-days, unknown before they discovered them being exploited in the wild earlier this year. The four security flaws were found by Google Threat Analysis Group (TAG) and Google Project Zero researchers after spotting exploits abusing zero-day in Google Chrome, Internet Explorer, and WebKit, the engine used by Apple's Safari web browser. "We tie three to a commercial surveillance vendor arming govt backed attackers and one to likely Russian APT," Google Threat Analysis Group's Director Shane Huntley said. "Halfway into 2021, there have been 33 0-day exploits used in attacks that have been publicly disclosed this year — 11 more than the total number from 2020," Google researchers added. - Google researchers said the attackers were part of a likely Russian government-backed actor abusing this zero-day to target iOS devices running older versions of iOS (12.4 through 13.7).
Read the full story here: Bleeping Computer, ZDNet, ThreatPost



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

Laptop Stolen?

This week Marshall Gunnell of PCWorld published a very useful article on what to do if your laptop is stolen and things you can do to soften the blow. Below is a condensed extract of the article.

What to do when your laptop is stolen (and how to prepare for it)

Having your laptop stolen isn't just stressful because you need to replace a pricey piece of hardware—it also poses a threat to your digital security. Fortunately, there are steps you can take to protect yourself both before and after your laptop goes missing. Read on to learn about how to prepare yourself against the possibility of notebook theft, how to report the theft if your laptop is stolen, and how to protect your data after it's in the hands of thieves.

How to prepare for possible laptop theft

Obviously, nobody expects their laptop to get stolen, but it can happen to anyone. It's important to take steps to protect yourself while your computer (and your sensitive data) is still in your possession, as it makes recovering from a notebook theft much easier. In particular, you should do the following:

Encrypt your data

You can encrypt your hard drive so that no one can access your sensitive information (like saved passwords and your credit card info) even if they have physical access to your laptop. If your computer is running Windows, take a few minutes to set up BitLocker, which can encrypt your drive. You'll need to pick a password to access your data, so make sure to follow all the usual password best practices. (Above all, don't write it on a post-it note and stick it on your laptop.) If you're open to using third party software, you can also download Absolute Home & Office (formerly LoJack for Laptops).

Keep a current backup

You should regularly back up your data so that if someone steals your laptop, your files aren't lost forever. You should be doing this even if you're not concerned about laptop theft, since data can be lost or damaged in dozens of different ways.

Enable your laptop's tracking feature

Lastly, you should enable your laptop's tracking feature. If it's stolen, you can use this to locate and lock it. In Windows 10, this feature is called Find My Device; in macOS, it's just called Find My.

To use the Find My Device feature in Windows, your laptop needs to be logged into a Microsoft Account and location services need to be enabled. To enable this feature — which, to be clear, you have to do before your laptop is stolen— **(1)** click the Start Menu in the bottom-left corner of your desktop and then click Settings. **(2)** In the Settings screen, click the button that says Update & security. **(3)** Next, click Find My Device in the sidebar. Click the button on the next screen that says "Change," and finally, toggle the slider to the "On" position under "Save my device's location periodically."

What to do when your laptop gets stolen

If someone does steal your laptop, you need to act fast. Take the following steps using another device you own or a loan device:

Locate and lock your laptop

You can only do this if you enabled the "Find My Device" feature, as described above. To locate your laptop after it's stolen, visit the devices page for your account on Microsoft's website. Click the tab that says "Find My Device" and select your laptop (look for the name it appeared under when you connected it to your local network). Click "Find." If everything goes according to plan, Microsoft will display a map showing your laptop's location. Take a screenshot—you'll want to provide it when you report the theft to the authorities, which you should do next.

To protect your data, click your laptop on the map and click Lock > Next. This will prevent anyone from using your laptop until you unlock it. That includes you, so if your laptop gets returned to you (keep your fingers crossed) you'll need to sign back into your Microsoft account before you can log in.

Report the theft

File a police report and alert your bank, if you ever shop online, your credit card information might be saved on your laptop. If you are insured, notify your insurance company and file an insurance claim.

Wipe your data

If your lost device is connected to the internet, you might be able to remotely erase your data (hopefully you have a backup). If you're using macOS and have the "Find My" feature enabled, you can mark your device as lost and remotely erase it using a similar process to "Find My Device," outlined above. This will also lock your device and disable Apple Pay. If you're on Windows and you installed the Absolute Home & Office software suite previously suggested, you can use that to wipe your data as well.

Change your passwords

Log into your online accounts and change your passwords. You should do this for every account you can remember accessing from your laptop, but pay particular attention to your email, bank logins, and social media profiles. When you're doing this, make sure not to update the autofill function so that the passwords on your missing laptop aren't synced and updated.

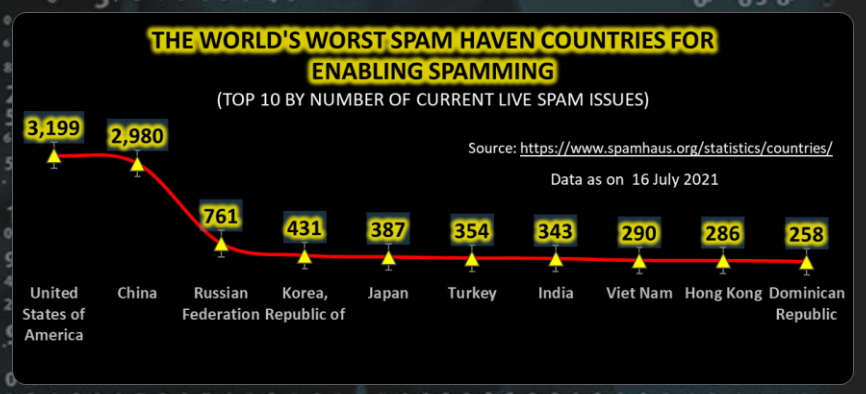
Clear your browsing data and deauthorise your account and devices

After changing your passwords, delete your browser data, such as your autofill settings and browsing history. If you use a Google account, sign out of Chrome remotely to deauthorize your device. Firefox and Safari also allow remote sign-outs. If you're using an Apple laptop, you can remotely log out of any device signed in with your Apple ID. Make sure you also turn off auto-sync between your linked devices to prevent your sensitive information from being synced on your missing laptop.

...Please read the full article here: PCWorld

Other Interesting News and Cyber Security bits:

- Harvard-MIT Quantum Computing Breakthrough – "We Are Entering a Completely New Part of the Quantum World"
- 'Lack of cybersecurity has become a clear & immediate danger to our society': Klaus Schwab
- Cyber Security in 7 Minutes for the uninformed



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