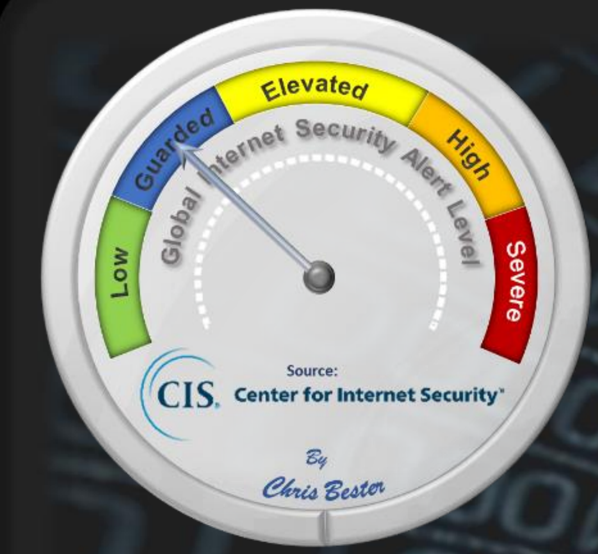

Low
Guarded
Elevated
High
Severe
Global Internet Security Alert Level
Source:
CIS. Center for Internet Security
By
Chris Bester

On June 29, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in WatchGuard products.
CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
01 Jul 22	552,786,265	6,358,211

Deaths this week: 10,328

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

01 July 2022

In The News This Week

NATO sends nuclear retaliation warning to Russia and China

NATO is putting Russia and any other "nuclear-armed peer-competitors" on notice that the trans-Atlantic alliance can and will retaliate against any nuclear attack. The latest edition of the security bloc's guiding strategic concept evinces a more muscular posture regarding NATO's nuclear forces than the 2010 document, which characterized Russia as a "partner" just four years before the Kremlin seized Crimea from Ukraine. And the latest document implies that as North Atlantic allies send a stronger signal about threats from Russia's nuclear threats, they also won't fail to keep an eye on China's nuclear arsenal. "We have a wartime strategic concept, actually, not a peacetime one, so [we] want to use stronger language," a senior European official told the Washington Examiner. The balance of nuclear military power emerged as a burning issue in the last several months, as Russian President Vladimir Putin has invoked Moscow's arsenal to deter at least some Western support or intervention for Ukraine. His nuclear saber-rattling has spurred some European officials to wonder if Putin thinks he could win a limited nuclear war; the allies, for their part, asserted such a conflict would be a losing proposition for their enemies.....
Read the full article by Joel Gehrke here: Washington Examiner

Spy agencies need 'independent authorisation' to access telecoms data, say judges

United Kingdom - The High Court has ruled that UK intelligence agencies should seek independent authorisation before accessing phone and internet records during criminal investigations. - The security and intelligence services will have to obtain independent authorisation before accessing citizens' private phone and internet records during criminal investigations following a landmark High Court decision. Two High Court judges have ruled that MI5, MI6 and GCHQ have been unlawfully given permission to access individuals' communications data for the prevention or detection of serious crime under the Investigatory Powers Act 2016, known as the Snoopers' Charter. Lord Justice Singh and Justice Holgate found that the ability of the UK's intelligence services to authorise their own access to the private communications data of the public for investigating crime is incompatible with EU laws that have been retained by the UK legal system after Brexit. The case brought by the campaign group Liberty represents a partial victory for the civil society group, which began its first legal challenge against the lawfulness of the state's bulk surveillance powers five years ago in 2017...
Read the report by Bill Goodwin here - ComputerWeekly

South African Police to deploy drones across SA to fight crime

he South African Police Service (SAPS) is looking to make use of drones across the country to fight crime. This is according to police minister Bheki Cele, responding to a parliamentary question by the Freedom Front Plus on whether the SAPS has purchased any drones to be used specifically for rural security. In his written response, Cele says SAPS is in the process of purchasing drones to be used as part of policing, including in rural areas, as per the implementation requirements of the Rural Safety Strategy. "The SAPS is in the process of acquiring 166 drones, in three phases, for use in various policing environments," the minister says... Read the rest of the post by Admire Moyo here: ITWeb

FBI warning: Crooks are using deepfakes to apply for remote tech jobs

Scammers or criminals are using deepfakes and stolen personally identifiable information during online job interviews for remote roles, according to the FBI. The use of deepfakes or synthetic audio, image and video content created with AI or machine-learning technologies has been on the radar as a potential phishing threat for several years. The FBI's Internet Crime Complaint Center (IC3) now says it's seen an increase in complaints reporting the use of deepfakes and stolen personally identifiable information to apply for remote work roles, mostly in tech. With some offices asking staff to return to work, one job category where there has been a strong push for remote work to continue is in information technology.
Reports to IC3 have mostly concerned remote vacancies in information technology, programming, database, and software-related job functions. ... Read the post by Liam Tung here: ZDNet

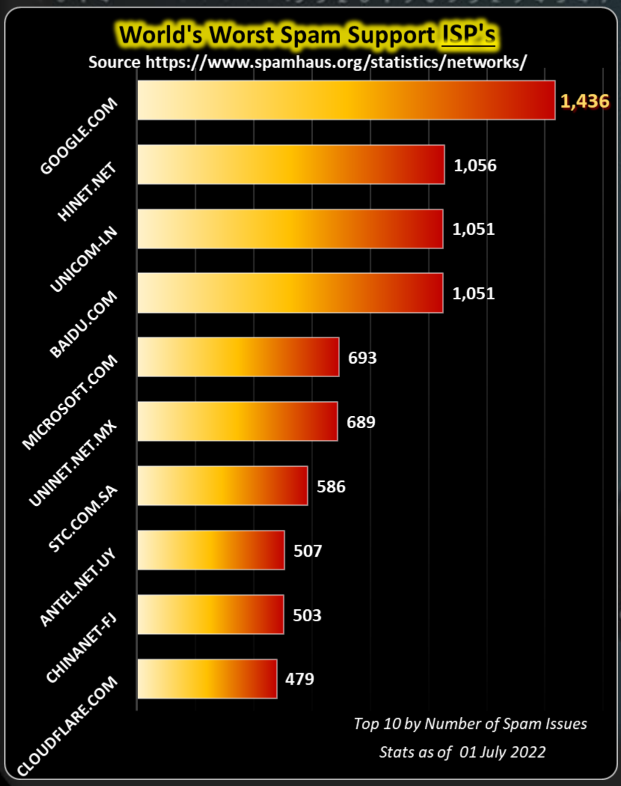
Russian hackers claim responsibility for cyberattack on Lithuania

Russian hacker group Killnet has claimed responsibility for a denial-of-service (DDOS) cyberattack on Lithuania, saying it was in response to the decision by Vilnius to block the transit of some sanctioned goods to the Russian exclave of Kaliningrad. Lithuanian state and private institutions were hit by the denial-of-service cyberattack on Monday. "It is very likely that attacks of similar or greater intensity will continue in the coming days, especially in the transportation, energy and financial sectors," the National Cyber Security Centre said. Read the rest of the article here: Aljazeera

Major Iran steel company halts production after being hit by cyber attack

A major Iranian steel company has been forced to shut down production after it was hit by a cyber attack, in what is the latest of a series of attacks on Iranian sites in recent months. According to Iranian media, the state-owned Khuzestan Steel Company said that experts had determined that its steel plant halt production until further notice "due to technical problems". The company's CEO, Amin Ebrahimi, stated that it managed to thwart the cyber attack and prevented any serious structural damage. Read the rest of the article here: MEMO

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



Top 10 by Number of Spam Issues
Stats as of 01 July 2022

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

Why is my bandwidth usage so high this month?! I wonder what my kids are up to?

Social Media Platforms Used to Create Hacking Culture

In the news this week we read about teenage hacking groups using social media platforms like Discord and the like to promote and share hacking fetes, tools, and ideas, to the dismay of many parents and the digital community at large. In the forming years of the Internet, youngsters quickly figured out that they can manipulate the then immature technology to their advantage. It was kind of cool for a teenager to break into a Government site just to gain bragging rights for doing so. With movie influences like Wargames with Matthew Broderick in the early eighties, it soon became a trend and organisations had to find ways to deal with this "new" threat of what we then called "Script Kiddies". We have come a long way since the eighties and the difference between the "Script Kiddies" of then and modern-day teenage hackers of today is that you don't need to be any kind of programming Wizkid. With an array of tools and step-by-step guides available on social media platforms, all you need is the ability to read and click a button. The other difference is that in the Eighties, kids mostly did it for fun, nowadays, criminal intent is much more prominent than "just having fun". On that note, I did a bit of browsing around and came across several articles covering the subject of social media influences on our kids and I want to share an extract of a blog by Emma Mcgowan of Avast looking at the problem of kids forming hacking groups online.

Kids are forming hacking groups online. Here's what to do about it.

The digital world comes with its own unique opportunities and potential dangers. But you, as the parent, have the tools to guide your kids and teens in the right direction. - When people hear the word "hacker," they probably picture a man sitting alone in a dark room in front of a computer. He has a black screen with green computer code in front of him. What they probably don't picture is their teenage kid.

But maybe they should, as Avast has discovered an online community creating, exchanging, and spreading malware on the popular communication platform Discord. The group advertises easy-to-use malware builders and toolkits so that users can DIY their own ransomware, information stealers, and crypto miners. And while there are many hacking forums on Discord, this one is composed mainly of teenagers.

Avast malware researcher Jan Holman says that kids and teens are attracted to the groups because they see hacking as cool and fun. The malware builders provide an easy entry — they require no actual programming, just customization of functions and appearance — into this activity and allow kids to prank people and make money. "However, these activities by far aren't harmless, they are criminal," Holman says. "They can have significant personal and legal consequences, especially if children expose their own and their families' identities online or if the purchased malware actually infects the kids' computer, leaving their families vulnerable by letting them use the affected device. Their data, including online accounts and bank details, can be leaked to cybercriminals."

So what can parents do about it? First, let's take a look at Discord — what it is, why kids love it, and what else parents should be aware of — and then we can explore some alternative ways to channel that energy.

What is Discord? - Discord is a communication platform for mobile or PC that was originally used by gamers who wanted to chat and hang out while playing video games in different physical locations. But it has expanded in recent years to include communities that convene around a range of topics. Users can communicate on Discord via voice, video, or text and it also facilitates doing group activities together, like playing video games, watching movies — or hacking teachers.

Discord is organized by "servers," which are created by users, some of which require an invite to get into and others of which are public. A server will be dedicated to a main topic and then will have "channels" underneath it for specific sub-conversations around that same topic. Anyone can set up a Discord server and decide the rules of that particular space.

For kids and teens, Discord offers a place to do what kids and teens love to do best: Hang out with their friends. Because servers are created around interests, kids can hang out while they play Fortnite or talk with other kids about their latest interests, whatever that might be. Discord has become especially popular since the start of the Covid-19 pandemic, allowing kids and teens to hang out without the possibility of exposure to the virus. Plus, it's not as "mainstream" as other social networks and is likely outside of the view of their parents, who may be listening in on other platforms.

How do I talk to my kids about online safety on Discord? - The minimum age to be on Discord is 13, but it's definitely an all-ages platform. That means some servers are very adult and include not only adult conversations but sometimes pornographic imagery and other adults-only content. Those servers are required to have an age-restricted label, but teens and kids are often savvy enough to get around those types of restrictions, so it's something to be aware of and speak with your kids about.

But as a parent, the best move isn't to tell your teen "Don't go into these adult rooms! They're not for you!" Psychotherapist and author Catherine Knibbs — who works with clients who have experienced trauma online — suggests asking kids questions that help promote critical thinking about what's going on in different online spaces to help guide them to their own decision.

"Rather than saying 'there are bad people out there online,'" Knibbs previously told Avast, "say something like, 'Who are your friends online? How do you know they're friends and not just someone you talk to? How do you know it's a genuine person?'"

What should I do if I find out my kid is into hacking? - Despite the fact that it's almost always portrayed negatively in common parlance and media, hacking per se isn't about breaking the law. While some hackers are cybercriminals, others work in cybersecurity or for other legitimate tech companies with the goal of protecting them.

"If your child shows an interest in hacking, encourage it, but also talk about issues of consent," Avast Global Head of Security (and parent of two teens with black hoodies) Jeff Williams says. "Hacking by itself is not a bad thing – understanding how things work and don't work deepens an understanding of the technology in question. It's when that knowledge is used against another party that it becomes problematic."

Williams says that there are some specific signs that your kid might be getting into hacking. He suggests being on the lookout for things like: **(1)** They start using terms like dox and DDoS and bot. **(2)** They receive packages or start wearing new things you didn't buy them and you are uncertain how they would have paid for the items. **(3)** Your parental control software suddenly stops working. **(4)** Massive bandwidth usage on the home network or cap exceeded on their phone.

Unfortunately, this is all I have space for in this post. Please read the rest of Emma's blog here: Avast

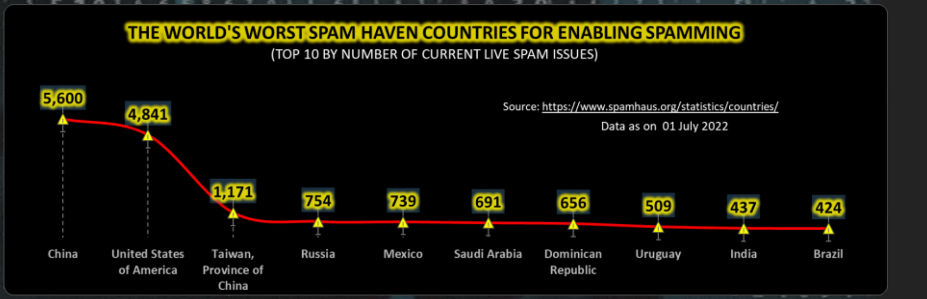
Other Interesting News and Cyber Security bits:

- War in Ukraine. Deep fake. The mayor of Berlin spoke to Fake Vitalize Gliska
- Subcommittee Wrestles with Quantum Computing and Deepfakes Issues
- Researchers Warn of Teen Hacking Group on Discord
- 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 01 July 2022

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