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

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

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

31 March 2023

In The News This Week

White House Makes Moves To Secure Space Cyber Security

The US has opened discussions into the importance of securing the cyber security of space and the industry. - The White House held a forum with private industry leaders and government stakeholders, outlining plans to bolster cybersecurity for the US industry. "Public and private sector space actors — including stakeholders representing the diversity of the space ecosystem — must work together to proactively address cybersecurity challenges." The roundtable discussion was hosted by National Space Council Executive Secretary Chirag Parikh and Acting National Cyber Director Kemba Walden, who outlined three main directives for boosting space cybersecurity. First the Office of the National Cyber Director will host workshops for US industry leaders to gain perspectives on current policy and identify gaps that require "more specific guidance."
Read the rest of the post by Daniel Croft here: CyberSecurity Connect

The Treasury has kicked off a pay row after advertising for a Head of Cyber Security on a salary starting at slightly over £50,000. - London – "The advertised 'hybrid' job is described as being of 'mid-senior level' and pays a salary of between £50,550 and £57,500 per year. It involves managing a team of two other people and "advise seniors on cyber risks across our services and systems. It is described as "an exciting and meaningful opportunity to work on cyber security at the heart of Government in a time of momentous change.
"According to job site Glassdoor, the average salary for the position in the private sector is around £130,000 per year.
One security professional spotted the ad and posted online: "Head of cyber for the treasury of Britain. £57k. Head of cyber security for a trading company no-one has ever heard of, £450k." ☺ ... Read the story by Asher McShane here: LBC

Meta wants EU users to apply for permission to opt out of data collection

Instead of a yes/no consent, Meta users will fill out a form and include justification. - Meta announced that starting next Wednesday, some Facebook and Instagram users in the European Union will for the first time be able to opt out of sharing first-party data used to serve highly personalized ads, The Wall Street Journal reported. The move marks a big change from Meta's current business model, where every video and piece of content clicked on its platforms provides a data point for its online advertisers. People "familiar with the matter" told the Journal that Facebook and Instagram users will soon be able to access a form that can be submitted to Meta to object to sweeping data collection. If those requests are approved, those users will only allow Meta to target ads based on broader categories of data collection, like age range or general location....
Read the full story by Ashley Belanger here: ARSTechnica

3CX Supply Chain Attack — Here's What We Know So Far

Enterprise communications software maker 3CX on Thursday confirmed that multiple versions of its desktop app for Windows and macOS are affected by a supply chain attack. The company said it's engaging the services of Google-owned Mandiant to review the incident. In the interim, it's urging its customers of self-hosted and on-premise versions of the software to update to version 18.12.422. "3CX Hosted and Start UP users do not need to update their servers as we will be updating them over the night automatically," 3CX CEO Nick Galea said in a post on Thursday. "Servers will be restarted and the new Electron App MSI/DMG will be installed on the server." Read the rest of the story by Ravie Lakshmanan here: The Hacker News

Russia: the "Vulkan files" investigation reveals Moscow's secret weapons for cyber warfare

La Russia it has for years been held responsible for cyber attacks against other states, which it has repeatedly denied. Now, the "Vulkan Files" investigation, conducted by "Der Spiegel", "Zdf", "Sueddeutsche Zeitung" and other international media shows how a software company from Moscow, the Volcano, is developing digital weapons for Russian intelligence agencies. The material on which the research was based comes from an anonymous whistleblower and demonstrates how Russia can carry out cyber attacks on a global scale. As reported by "Zdf", according to "internal documents", Vulkan also works for the entire Russian intelligence apparatus: the internal secret service Fsb, the foreign one Svr and the military one Gru. From the material acquired by the media authors of the investigation, the objectives of a software developed by Vulkan emerge: "deactivation of the control systems of rail, air and maritime transport", "disturbance actions against energy companies and critical infrastructures", "identifying critical infrastructure vulnerabilities to attack them". Read more here: Nova

The Louisiana Cyberattacks That Weren't—or Maybe Were?

Last week, the Louisiana State Police Cyber Crime Unit tipped off five institutions—the University of New Orleans, River Parishes Community College, Nunez Community College, Southern University at Shreveport and Louisiana State University Agricultural Center—that their networks had possibly been compromised. The risks needed "immediate" attention, Quintin D. Taylor, chancellor of River Parishes Community College, wrote in an email to Inside Higher Ed, adding that the coordinated effort also included the Governor's Office of Homeland Security and Emergency Preparedness....
Read the full story by Susan D'Agostino here: Inside Higher Ed

What AI chatbots mean for the future of cybersecurity

ChatGPT and other AI chatbots are still the talk of the town since ChatGPT's launch last year, and we've read in the news how this can and is already revolutionizing the computing world as we know it. We've heard how it has been used by teachers, students, researchers, coders, security specialists, and also, cybercriminals. As a follow-up on the Q&A session post with Nvidia's CSO, David Reber on the topic in February, I wanted to look into what this so-called revolution really means to the cybersecurity community. With that in mind, I found a recent article by Danny Parker of ZDNet that summed it up for me in the following extract:

OpenAI's chatbot has many great uses -- but as with any new technology, there are people out there who will look to exploit it in ways that could cause problems. - OpenAI's chatbot has many great uses -- but as with any new technology, there are people out there who will look to exploit it in ways that could cause problems. From relatively simple tasks, such as composing emails, to more complex jobs, including writing essays or compiling code, ChatGPT -- the AI-driven natural language processing tool from OpenAI -- has been generating huge interest since its launch. It is by no means perfect, of course -- it's known to make mistakes and errors as it misinterprets the information it's learning from, but many see it, and other AI tools, as the future of how we'll use the internet.

OpenAI's terms of service for ChatGPT specifically ban the generation of malware, including ransomware, keyloggers, viruses or, "other software intended to impose some level of harm". It also bans attempts to create spam, as well as use cases aimed at cybercrime. But as with any innovative online technology, there are already people who are experimenting with how they could exploit ChatGPT for murkier ends.

Following its launch, it wasn't long before cyber criminals were posting threads on underground forums about how ChatGPT could be used to help facilitate malicious cyber activity, such as writing phishing emails or helping to compile malware. And there are concerns that crooks will attempt to use ChatGPT and other AI tools, such as Google Bard, as part of their efforts. While these AI tools won't revolutionize cyberattacks, they could still help cyber criminals -- even inadvertently -- to conduct malicious campaigns more efficiently. "I don't think, at least in the short term, that ChatGPT will create completely new types of attacks. The focus will be to make their day-to-day operations more cost-efficient," says Sergey Shykevich, threat intelligence group manager at Check Point, a cybersecurity company.

Phishing attacks are the most common component of malicious hacking and fraud campaigns. Whether attackers are sending emails to distribute malware, phishing links or are being used to convince a victim to transfer money, email is the key tool in the initial coercion. That reliance on email means gangs need a steady stream of clear and usable content. In many cases, especially with phishing , the aim of the attacker is to persuade a human to do something, such as to transfer money. Fortunately, many of these phishing attempts are easy to spot as spam right now. But an efficient automated copywriter could make those emails more compelling.

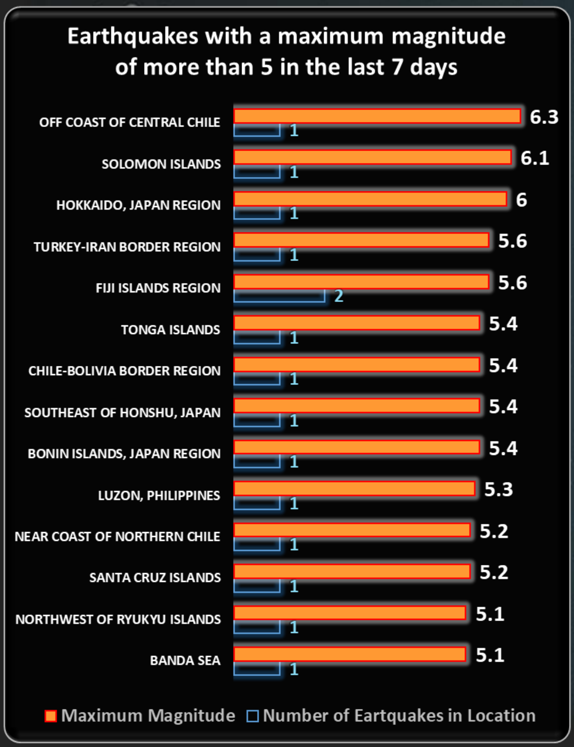
Cybercrime is a global industry, with criminals in all manner of countries sending phishing emails to potential targets around the world. That means language can be a barrier, especially for the more sophisticated spear-phishing campaigns that rely on victims believing they're speaking to a trusted contact , and someone is unlikely to believe they're speaking to a colleague if the emails are full of uncharacteristic spelling and grammar errors or strange punctuation. But if AI is exploited correctly, a chatbot could be used to write text for emails in whatever language the attacker wants.
"The big barrier for Russian cyber criminals is language -- English," says Shykevich. "They now hire graduates of English studies in Russian colleges to write for phishing emails and to be in call centres, and they have to pay money for this."
He continues: "Something like ChatGPT can save them a lot of money on the creation of a variety of different phishing messages. It can just improve their life. I think that's the path they will look for."

In theory, there are protections in place that are designed to prevent abuse. For example, ChatGPT requires users to register an email address and also requires a phone number to verify registration. And while ChatGPT will refuse to write phishing emails, it's possible to ask it to make email templates for other messages, which are commonly exploited by cyber attackers. That effort might include messages such as claiming an annual bonus is on offer, an important software update must be downloaded and installed, or an attached document needs to be looked at as a matter of urgency.
"Crafting an email to convince someone to click on a link to obtain something like a conference invite -- it's pretty good, and if you're a non-native English speaker this looks really good," says Adam Meyers, senior vice president of intelligence at Crowdstrike, a cybersecurity and threat intelligence provider. "You can have it create a nicely formulated, grammatically correct invite that you wouldn't necessarily be able to do if you were not a native English speaker."

But abusing these tools isn't exclusive to just email; criminals could use it to help write script for any text-based online platform. For attackers running scams, or even advanced cyber-threat groups attempting to conduct espionage campaigns, this could be a useful tool -- especially for creating fake social profiles to reel people in. "If you want to generate plausible business speak nonsense for LinkedIn to make it look like you're a real businessperson trying to make connections, ChatGPT is great for that," says Kelly Shortridge, a cybersecurity expert and senior principal product technologist at cloud-computing provider Fastly.

Various hacking groups attempt to exploit LinkedIn and other social media platforms as tools for conducting cyber-espionage campaigns. But creating fake but legitimate-looking online profiles -- and filling them with posts and messages -- is a time-consuming process. Shortridge thinks that attackers could use AI tools such as ChatGPT to write convincing content while also having the benefit of being less labour-intensive than doing the work manually. "A lot of those kinds of social-engineering campaigns require a lot of effort because you have to set up those profiles," she says, arguing that AI tools could lower the barrier to entry considerably. "I'm sure that ChatGPT could write very convincing-sounding thought leadership posts," she says. The nature of technological innovation means that, whenever something new emerges, there will always be those who try to exploit it for malicious purposes. And even with the most innovative means of attempting to prevent abuse, the sneaky nature of cyber criminals and fraudsters means they're likely to find means of circumnavigating protections. .....

That is all I have space for in this post, but please link to the ZDNet site and read the rest of Danny Parkers article.


Earthquakes with a maximum magnitude of more than 5 in the last 7 days

	Maximum Magnitude	Number of Eartquakes in Location
OFF COAST OF CENTRAL CHILE	6.3	1
SOLOMON ISLANDS	6.1	1
HOKKAIDO, JAPAN REGION	6	1
TURKEY-IRAN BORDER REGION	5.6	1
FIJI ISLANDS REGION	5.6	2
TONGA ISLANDS	5.4	1
CHILE-BOLIVIA BORDER REGION	5.4	1
SOUTHEAST OF HONSHU, JAPAN	5.4	1
BONIN ISLANDS, JAPAN REGION	5.4	1
LUZON, PHILIPPINES	5.3	1
NEAR COAST OF NORTHERN CHILE	5.2	1
SANTA CRUZ ISLANDS	5.2	1
NORTHWEST OF RYUKYU ISLANDS	5.1	1
BANDA SEA	5.1	1

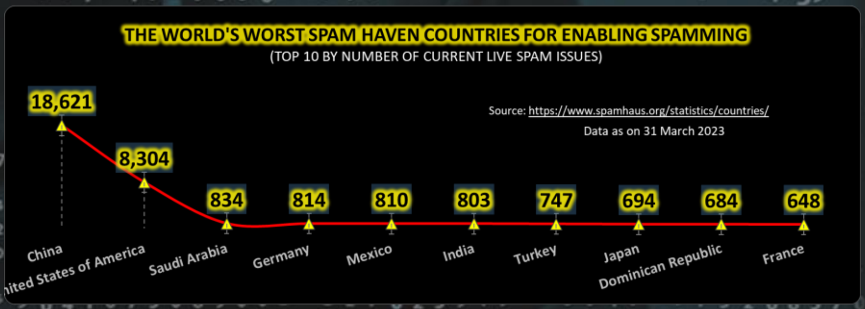
■ Maximum Magnitude □ Number of Eartquakes in Location

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

Other Interesting News and Cyber Security bits:

flightradar24 LIVE AIR TRAFFIC Track any Aeroplane in flight globally
IRIS Interactive Earthquake Map
Marine Traffic
SatelliteXplorer Track satellites in orbit

- There's a chronic shortage of talent in cybersecurity, Microsoft says (CNBC Video)
- How to use ChatGPT to write Excel formulas
- New Solid-State Battery Has 2x the Energy—and No Anode New coating helps solid electrolyte cells outpace traditional lithium ions
- SANS Daily Network Security Podcast (Storm cast)


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 31 March 2023

China	United States of America	Saudi Arabia	Germany	Mexico	India	Turkey	Japan	Dominican Republic	France
18,621	8,304	834	814	810	803	747	694	684	648

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