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

On January 11, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Microsoft, Adobe, and Google 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

13 January 2023

In The News This Week

US domestic flights delayed after FAA system outage. Here's what we know

Flights across the US are slowly returning to normal after being grounded because of a system outage on Wednesday at the Federal Aviation Administration (FAA). The FAA is the US government agency which oversees many aspects of America's aviation, including air traffic management. The issue affected the Notice to Air Missions (NOTAM) system, which provides pilots with real-time information about changes and potential hazards on flight routes. "The FAA is working to restore its Notice to Air Missions System. We are performing final validation checks and reloading the system now. Operations across the National Airspace System are affected," the FAA said in a tweet posted early Wednesday morning.

Read the rest of the article by Danny Palmer here: ZDNet

Royal Mail services hit by major cyber attack

The UK's Royal Mail has been forced to suspend overseas services amid serious disruption caused by a cyber attack of an as-yet unspecified nature. The attack has hit its international export services and means it is currently unable to dispatch letters or parcels outside the UK. Computer Weekly understands that domestic services are unaffected. "Royal Mail is experiencing severe service disruption to our international export services following a cyber incident," said a spokesperson. "We are temporarily unable to dispatch export items including letters and parcels to overseas destinations. We have asked customers temporarily to stop submitting any export items into the network while we work hard to resolve the issue. Some customers may experience delay or disruption to items already shipped for export. Our import operations continue to perform a full service with some minor delays. "Our teams are working around the clock to resolve this disruption and we will update customers as soon as we have more information.

Read the full story by Alex Scroxton here: ComputerWeekly, and more here: DailyMail

Meta sues Voyager Labs, saying it created fake accounts to scrape user data

Meta (owner of Facebook, Instagram & WhatsApp) filed a complaint against Voyager Labs on Thursday, alleging that the startup created fake Facebook accounts as part of a scheme to collect information from real Facebook users, which it then used for its own business purposes. Voyager Labs specializes in investigative software and services intended to help law enforcement and companies obtain information about suspects, among other uses. Meta alleged that Voyager Labs' software was powered by data that it improperly gathered from Facebook and Instagram in addition to other sites like Twitter, YouTube, Twitter, and Telegram. According to the filing in the District Court for the Northern District of California, Meta alleged that Voyager Labs created over 38,000 fake Facebook user accounts. These helped the startup scrape publicly posted information from more than 600,000 other Facebook users, including things like posts, likes, photos, and lists of friends. "Scraping" generally refers to the automated process of using software to scan a web page and compile information on it.

Read the full article by Jonathan Vanian here: CNBC News

Guardian confirms it was hit by ransomware attack

The Guardian has confirmed it was hit by a ransomware attack in December and that the personal data of UK staff members has been accessed in the incident. The Guardian Media Group's chief executive, Anna Bateson, and the Guardian's editor-in-chief, Katharine Viner, confirmed the news in an update emailed to staff on Wednesday afternoon. They described the incident as a "highly sophisticated cyber-attack involving unauthorized third-party access to parts of our network", most likely triggered by a "phishing" attempt in which the victim is tricked, often via email, into downloading malware.

Read the full story here: The Guardian

Copper Mountain reopens mine after ransomware attack

Copper Mountain Mining (TSX: CMMC) said it reopened its mine in southern British Columbia this week following a December 27 ransomware attack that left deliveries unaffected. The Vancouver-based company restarted the primary crusher at its mine near Princeton about 300 km east of Vancouver on Jan. 1 and resumed operations at the mill "shortly thereafter," Copper Mountain said in a news release last Friday. "On Jan. 4, the mill was at full production and the operation is currently being stabilized as the remaining business systems are fully restored," the company said. "Throughout this downtime, which resulted from the attack on its IT systems, the company has been shipping copper concentrate to the port of Vancouver from mine inventory and has maintained its planned shipping schedule." The shutdown was a preventative measure as Copper Mountain assessed the extent of the attack on its systems at the mine and its corporate offices, the company said. Copper Mountain Mining's update last Friday didn't mention any damage, the identity of the attackers, dollar amounts they may have sought, or any amounts paid to the hackers. A spokesperson for the company didn't immediately reply to emailed questions..

Read the full article here: Mining(dot)com

The EMP Threat

The Electro Magnetic Pulse threat, often referred to as EMP, has been discussed in Cyber circles for many years but gained renewed interest in the media recently as a result of the Ukraine Russia conflict and the tension that is building up between US and China. Speculations has been thrown around of the possibility of a man-made EMP event that could potentially wipe out all electronic devices in large geographical areas. Such an event can disrupt all forms of electronic communication temporarily, or for an extended time period, we just don't know. An EMP event has no direct effect on humans or living organisms, but the residual effects of electronic devices that stop working can be catastrophic. Imagine a surgeon busy with a delicate operation and his or her precision equipment stops working. Or an autonomous car, if the electronics stops working it can crash and injure or kill its occupants.

What is an EMP event and why is it a threat?

EMP events occur naturally due to solar flares and resultant geomagnetic storms from our own Sun. The biggest EMP event ever recorded, known as the Carrington Event, happened on 1 September 1859 and in a close second place was the geomagnetic storm on 13 May 1921, known as the New York Railroad Storm. On 23 July 2012, another solar storm was recorded with a similar magnitude that barely missed Earth with a margin of approximately nine days. The equator of the Sun rotates around its own axis with a period of about 25 days, and lucky for us, the region that produced the outburst was thus not pointed directly towards Earth at that time.

The Uptime Institute describes an EMP and its possible effects as follows: "*Electromagnetic pulse (EMP) is a rapid discharge of electromagnetic energy from a natural or artificial source. The resulting electric field acts upon conductive materials in electric and electronic equipment, inducing electric currents that can disrupt equipment operation and may cause permanent damage. Susceptible conductors, depending on the characteristics of the EMP, range from the wires that make up the electrical grid or a data center's power distribution system to the microscopic features on silicon chips.*"

If the Carrington event or a geomagnetic storm of this magnitude happened today it would cause widespread electrical disruptions, blackouts, and damage due to extended outages of the electrical power grid. (Maybe the 2012 close miss was what the ancient Mayan prophecy was talking about ☺ *tongue in cheek*)

An EMP event from a natural source is somewhat predictable and can be managed accordingly, but the real threat comes in man's ability to create an EMP artificially. This can be achieved by an intentional missile or nuclear explosion at high altitude, or, as some publications put it, a madman's junkyard invention targeting a data center or power utility. With the current military and political tensions across the globe, many state-sponsored programs for intentional EMP attacks are already in full swing. In 2020, Forbes reported on China's Super-EMP weapons and abilities. The US and some EU countries have been testing portable high-powered microwave radio frequency units that can for instance target drone invasions. We also know that Russia possesses a range of non-nuclear EMP munitions that could be launched from the ground using specialized shells.

In a Taskforce report from Homeland Security, the following was stated - North Korea's KMS-3 and KMS-4 satellites orbit over the U.S. daily. Their trajectory is similar to that planned for a Soviet-era secret weapon called the Fractional Orbital Bombardment System (FOBS) deployed by the USSR to make a surprise High-altitude EMP (HEMP) attack on the United States. Trajectories of North Korea's KMS-3 and KMS-4 satellites are near optimal for a HEMP attack on the U.S., if they are nuclear-armed. HEMP attack does not require much accuracy or a reentry vehicle capable of penetrating the atmosphere and is well within North Korea's technological capabilities.

What is the US Government doing about it?

The US started looking at the EMP threat in 2015. In a Hearing of the House of Representatives of the US Government on 13 May 2015, the following was written: "An electromagnetic pulse could be created through an attack from a missile, nuclear weapon, radio frequency weapon, or geomagnetic storm caused by the sun. Fallout from an EMP event, either man-made or natural, could be extremely significant ranging from the loss of electrical power for months, which would deplete energy sources of power such as emergency batteries and backup generators have cascading consequences for supplying basic necessities such as food and water, and result in loss of life". As per the hearing records, many states already started to put emergency response plans in place back then, should this happen.

The Department of Defense moved the North American Aerospace Defense Command, NORAD back inside Cheyenne Mountain in Colorado in the same year because the mountain is EMP hardened and would allow the military to sustain communications and homeland defense operations despite an EMP event. But this measure would not do much for the citizens and everyday business operations.

In October 2018, the Department of Homeland Security published its "Strategy For Protecting And Preparing The Homeland Against Threats Of Electromagnetic Pulse And Geomagnetic Disturbances" where one of the goals was to "Enhance capabilities to protect critical infrastructure from the impact of an electromagnetic incident".

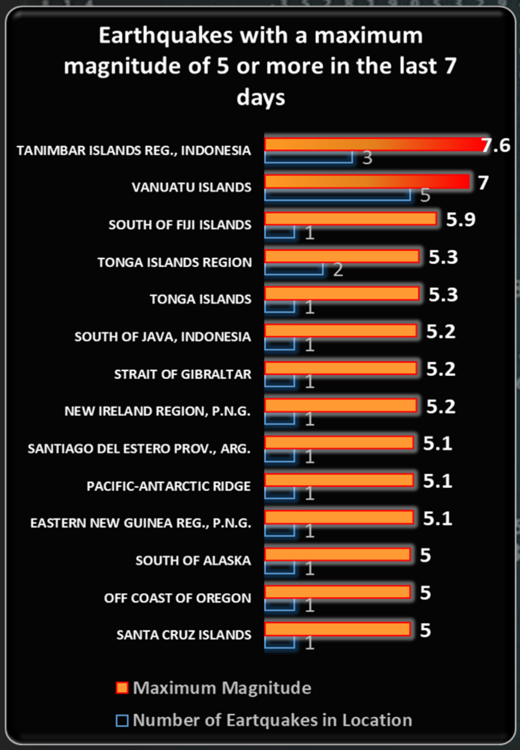
In other countries like Japan, the Defense Ministry is planning to move command centers underground at four Self-Defense Forces facilities by fiscal 2028 and implement measures against electromagnetic pulse attacks at five Air Self-Defense Force bases by fiscal 2029. My question is, will that not be too late?

Business and Commercial

From a commercial point, EMP Shield is offering EMP protection for vehicles, solar & wind installations, homes, and radio services. From a business perspective, since the world is transitioning to a cloud environment, maybe the question that needs to be asked is, are the data centers of your cloud service provider EMP hardened?

I'll leave you with this food for thought, please visit the resources below if you are interested to learn more.

Resources: Uptime Institute, US Gov, DHS, GC Gokce, OFFGRID, Eurasian Times, iNews, Forbes



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

IRIS Interactive Earthquake Map

Is your cloud service provider protected against an EMP event?

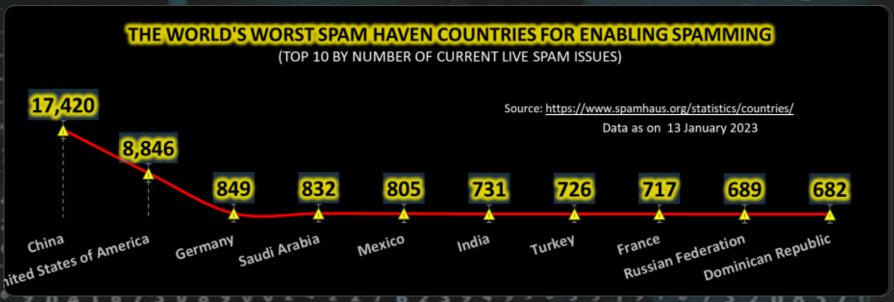
Other Interesting News and Cyber Security bits:

- Darktrace Publishes 2022 Cyber-Attack Trend Data for Energy, Healthcare & Retail Sectors Globally
- Apple accumulates a whopping 900 million subscribers across its services
- Russia's largest hacking conference reflects isolated cyber ecosystem
- SANS Daily Network Security Podcast (Storm cast)

flightradar24 LIVE AIR TRAFFIC Track any Aeroplane in flight globally

Marine Traffic

SatelliteXplorer Track satellites in orbit



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