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

On May 10, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Mozilla, Microsoft, Aruba, 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

12 May 2023

In The News This Week

Cybersecurity firm Dragos discloses cybersecurity incident, extortion attempt

Industrial cybersecurity company Dragos today disclosed what it describes as a "cybersecurity event" after a known cybercrime gang attempted to breach its defenses and infiltrate the internal network to encrypt devices. While Dragos states that the threat actors did not breach its network or cybersecurity platform, they got access to the company's SharePoint cloud service and contract management system. "On May 8, 2023, a known cybercriminal group attempted and failed at an extortion scheme against Dragos. No Dragos systems were breached, including anything related to the Dragos Platform," the company said. "The criminal group gained access by compromising the personal email address of a new sales employee prior to their start date, and subsequently used their personal information to impersonate the Dragos employee and accomplish initial steps in the employee onboarding process." Get the full story by Sergiu Gatlan here: Bleeping Computer

Darkweb marketplaces offering deepfake videos at up to $20,000 per minute conference hears

Darkweb marketplaces are offering deepfake videos with prices varying from $300 to $20,000 per minute, an audience heard at the Kaspersky Cyber Security Weekend–META 2023 event held in Kazakhstan's commercial capital Almaty. Vladislav Tushkanov, a lead data scientist at Moscow-founded cybersecurity and anti-virus provider Kaspersky Lab, was quoted by trade media as addressing the dangers of deepfakes, synthetic media digitally manipulated to replace a person's likeness convincingly with that of another, leveraging machine learning and artificial intelligence (AI). "$300/per minute is the starting price for a deepfake on the darknet," was cited as saying by iTWeb, adding: "The higher limit was discovered to be about $20 000. "It's important to remember that deepfakes are a threat not only to businesses, but also to individual users: they can spread misinformation, be used for scams, or to impersonate someone without consent.".
Read the rest of the article here: Intellinews

Leak of Intel Boot Guard Keys Could Have Security Repercussions for Years

While Intel is still investigating the incident, the security industry is bracing itself for years of potential firmware insecurity if the keys indeed were exposed. - The potential leak from MSI Gaming of signing keys for an important security feature in Intel-based firmware could cast a shadow on firmware security for years to come and leave devices that use the keys highly vulnerable to cyberattacks, security experts say. Intel is still "actively investigating" an alleged leak of Intel Boot Guard private keys for 116 MSI products, the company told Dark Reading. The investigation comes after a claim by Alex Matrosov, CEO of firmware supply chain security platform Binarly, that leaked source code from a March 2023 cyberattack on MSI includes this data, as well as image-signing private keys for 57 MSI products. Read the story by Elizabeth Montalbano here: DarkReading

Minnesota Senate passes proposed bill addressing threats of 'deep fake' technology

In remarks on the Minnesota Senate floor Wednesday, Sen. Erin Maye Quade, DFL-Apple Valley, said "deep fake" technology is an insidious threat to Minnesotans and something poised to wreak havoc on society. Her speech preceded a 64-1 vote to pass a proposed bill lawmakers say will help protect Minnesotans from some of the potential harms caused by the rapidly-emerging, artificial intelligence technology. And Maye Quade's well-received speech itself represented a bit of what lawmakers are grappling with. "Everything I just read was actually produced for me by AI," she revealed to lawmakers, illustrating how quickly realistic, AI-generated material is becoming available. According to Maye Quade, 96% of "deep fake" material online is pornographic in nature. Read the article here: Bring Me The News

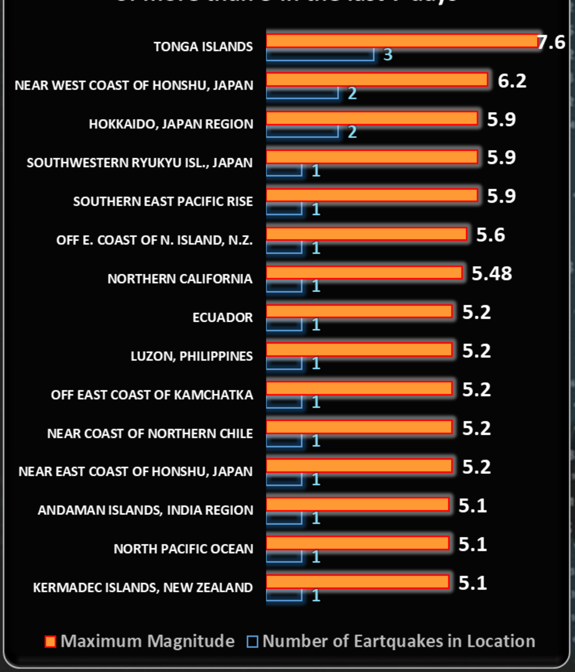
Bl00dy Ransomware Gang Strikes Education Sector with Critical PaperCut Vulnerability

U.S. cybersecurity and intelligence agencies have warned of attacks carried out by a threat actor known as the Bl00dy Ransomware Gang that attempt to exploit vulnerable PaperCut servers against the education facilities sector in the country. The attacks took place in early May 2023, the Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) said in a joint cybersecurity advisory issued Thursday. "The Bl00dy Ransomware Gang gained access to victim networks across the Education Facilities Subsector where PaperCut servers vulnerable to CVE-2023-27350 were exposed to the internet," the agencies said. Read the rest of the story by Ravie Lakshmanan here: The Hacker News

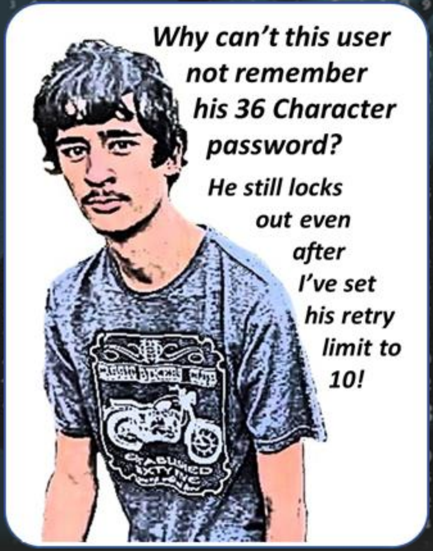
Multinational tech firm ABB hit by Black Basta ransomware attack

Swiss multinational company ABB, a leading electrification and automation technology provider, has suffered a Black Basta ransomware attack, reportedly impacting business operations. Headquartered in Zurich, Switzerland, ABB employs approximately 105,000 employees .... As part of its services, the company develops industrial control systems (ICS) and SCADA systems for manufacturing and energy suppliers.... On May 7th, the company fell victim to a ransomware attack conducted by Black Basta, a cybercrime group that surfaced in April 2022. The attack has affected the company's Windows Active Directory, affecting hundreds of devices. In response to the attack, ABB terminated VPN connections with its customers to prevent the spread of the ransomware to other networks. Read the full story by Lawrence Abrams here: Bleeping Computer

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



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


Why can't this user not remember his 36 Character password?
He still locks out even after I've set his retry limit to 10!

Deepfake Technology, what you need to Know

I've touched on "Deepfake" Technology in this forum before, but it stays a hot topic for discussion as we see in the attention it got in the media in the last few weeks. We even see that Governments are considering it a major threat as we see laws drawn up to control it.

First, for those not in the know, what are "Deepfakes"?

"Deepfake" is an umbrella term for various types of synthetic content, created or altered with the aid of artificial intelligence, which can appear to show events, scenes, or conversations that never happened. We also see the technology used to create special effects or morph some actor's face onto another actor's body as we see in movies like Wonder Woman where actress Linda Carter became a much younger Gal Gadot. Sometimes creators are doing it just for fun like when someone deepfaked Jim Carrey's face on Jack Nicolson's body as it appeared in Stephen King's "The Shining". But then again, Deepfakes are more in the news for the far more sinister side like fake presidential speeches and fake news to sway people's sympathy or mindset to a certain cause, or to gain public support for a hidden political agenda. These include videos and photos of Donald Trump's and Vladimir Putin's fake arrests to a video where President Joe Biden is portrayed as making a speech in the wrong state.

But for me, the real danger is that criminals can use this technology to manipulate someone to part with his or her well-earned money or even do something for them that they would normally never do. More examples can be seen here.

The scary part is that a lot of the technology is in everybody's grasp as free phone or PC apps. Yes, it is real fun to play around with and create funny videos to share with family or friends with apps like Avatarify, Wombo, or Reface, but in the hands of a criminal, some of these apps are tools of deception.

AI technology is exponentially getting better each day, and each of us can fall into the trap of believing something that is simply not true, no matter how vigilant or careful we are. That is why authorities are scrambling to get some legislation out there to control it, and to protect the common everyday person from harm.

But what can we do, and how can we spot whether it is a fake or not?

Not all deepfakes are created equal. And therefore, not every technique works everywhere. While some have tell-tale signs of being machine-made, others need careful observation or even other AI tools to differentiate.

Skin Tone

This is the first thing to take note of. The 'worked' portion (usually the face) will have slight differences in skin color, causing a mismatch with the rest of the visible body parts.

Expressions

This is the major giveaway, especially when amateurs masquerade as deepfakes experts. Their subpar creations often suffer from unnatural lip movement without human pauses helping to identify them as fake.
However, some algorithms do have provisions for breathing pauses. Still, you can tell the identical stoppages and head movements that follow similar patterns, generally too mechanic to ignore.
Likewise, blinking is another area that reveals deepfakes as such. This also goes through cycles (as written in their code), which isn't as human-like if you observe alongside a real video of the same person.
Another thing you can use to spot deepfakes is the eyeball movement. The AI, a machine lacking emotions and distractions, often appear more focused than an average human while talking.
Conclusively, deepfakes are easier to spot unless made with (almost) perfection by professionals.

Patches

So, how to tell that that isn't the real Morgan Freeman in this deepfake?
The best thing about the video is the high quality. You can switch to the highest resolution (4k available) to give yourself a chance to spot the artificial. And the bigger the screen, the better. Alternatively, you can screenshot and zoom in to see if some computer work is behind the obvious.
If you look closely, you can see the made-up skin. This is where algorithms fail, the small details, no matter how sophisticated. The skin kind of looks patchy, and the facial (and head) hair reproduction isn't natural and looks glued.

Details

There is a lot that goes on when we talk. Everyone has their own styles, which lead the lips, tongue, chin, cheeks, etc., to move in a certain pattern unique to them. Besides, deepfake tech is yet to master the inside-the-mouth-visuals while talking. For instance, you can't point out individual lower (mandibular) teeth in the Obama deepfake. All we see is a white strip at the bottom, and there are no signs of tongue movement at all.
You can watch any genuine Obama video and can observe the man is much more expressive with a lot of facial movement than this AI replica.
Besides, you can see the video itself isn't very clear. It's very low quality, compressed to hide the reality or due to computing limitations.

Transitions

One limitation in deepfake creation is their frame-by-frame generation. Every frame must be checked for perfect masking to keep the magic intact. Because of this, most convincing deepfake videos are extremely limited in facial movements. They only show frontal faces with no side views because the side-to-front transitions can reveal the creative bottlenecks.
Look at the Tom Cruise deepfake for instance, If you slow down the video and keenly observe from 35-40 seconds, the side-to-frontal transitions have some blurred portions. These are arguably the most difficult part to conceal and the best ones to uncover such AI creations.

Resources: Geekflare, Scientific Reports, MIT, Euronews, Telefonica, Q5id

Other Interesting News and Cyber Security bits:

- The End of Lithium P3! Elon Musk Revealed ALL-NEW Shock Battery Tech, Change Entire Industry! (30 Min Video)
- To Catch The Sun – How To Harness your own Solar Energy
- 12 Best Deepfake Apps and Websites You Can Try for Fun
- SANS Daily Network Security Podcast (Storm cast)

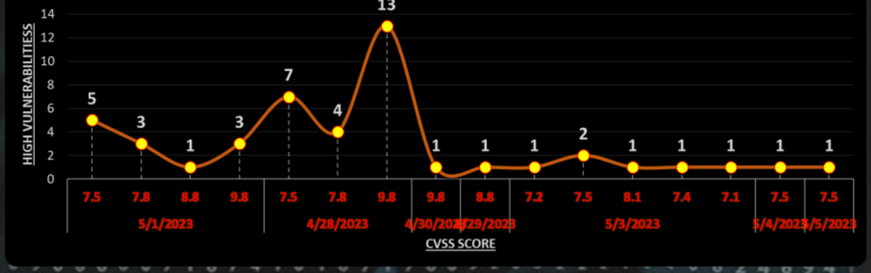
flightradar24 LIVE AIR TRAFFIC Track any Aeroplane in flight globally

www.iris.edu IRIS Interactive Earthquake Map

Marine Traffic

SatelliteXplorer Track satellites in orbit

46 New vulnerabilities classified as "High" in CISA's last report



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