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

On September 21, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Mozilla 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

23 September 2022

In The News This Week

Australia's Optus says up to 10 million customers caught in cyber attack

Australian No. 2 telco Optus, owned by Singapore Telecommunications Ltd (STEL.SI), said it will contact up to 10 million customers whose personal details were taken in a "sophisticated" hack, but added no corporate clients were compromised. Optus chief executive Kelly Bayer Rosmarin said she was angry and sorry that an offshore-based entity had broke into the company's database of customer information, accessing home addresses, drivers licence and passport numbers in one of the country's biggest cybersecurity breaches. Australian No. 2 telco Optus, owned by Singapore Telecommunications Ltd (STEL.SI), said it will contact up to 10 million customers whose personal details were taken in a "sophisticated" hack, but added no corporate clients were compromised. Optus chief executive Kelly Bayer Rosmarin said she was angry and sorry that an offshore-based entity had broke into the company's database of customer information, accessing home addresses, drivers licence and passport numbers in one of the country's biggest cybersecurity breaches. .
Read the rest here: Reuters

Grand Theft Auto VI footage leaked after hack, developer Rockstar confirms

More than 90 videos and images from the next edition of the Grant Theft Auto franchise have been leaked online by a hacker, the game's developers say. - The leaked content was posted on Sunday after what is being described as one of gaming's biggest security breaches. Rockstar Games said it remained unclear how the "network intrusion" occurred, but confirmed "early development footage" from GTA VI had been stolen. The footage was put on the GTAForums site by a user called teapotuberhacker. The hacker claimed to have gained access to the data by breaching Rockstar's internal feed on the Slack messaging app, and invited executives to negotiate to avoid further leaks. Additional revelations could include source code, assets, and testing builds from both GTA 5 and GTA 6, which could be damaging to the company's operations..
Read the full article by Matt Murphy here : BBC News

Microsoft Teams' GIFShell Attack: What Is It and How You Can Protect Yourself from It

Organizations and security teams work to protect themselves from any vulnerability, and often don't realize that risk is also brought on by configurations in their SaaS apps that have not been hardened. The newly published GIFShell attack method, which occurs through Microsoft Teams, is a perfect example of how threat actors can exploit legitimate features and configurations that haven't been correctly set. This article takes a look at what the method entails and the steps needed to combat it. Read more here: The Hacker News

Record DDoS Attack with 25.3 Billion Requests Abused HTTP/2 Multiplexing

Cybersecurity company Imperva has disclosed that it mitigated a distributed denial-of-service (DDoS) attack with a total of over 25.3 billion requests on June 27, 2022. The "strong attack," which targeted an unnamed Chinese telecommunications company, is said to have lasted for four hours and peaked at 3.9 million requests per second (RPS). "Attackers used HTTP/2 multiplexing, or combining multiple packets into one, to send multiple requests at once over individual connections," Imperva said in a report published on September 19. The attack was launched from a botnet that comprised nearly 170,000 different IP addresses spanning routers, security cameras, and compromised servers located in more than 180 countries, primarily the U.S., Indonesia, and Brazil. Read the full story by Ravie Lakshmanan: The Hacker News

IHG hack: 'Vindictive' couple deleted hotel chain data for fun (Why you should have a strong password)

Hackers have told the BBC they carried out a destructive cyber-attack against Holiday Inn owner Intercontinental Hotels Group (IHG) "for fun". - Describing themselves as a couple from Vietnam, they say they first tried a ransomware attack, then deleted large amounts of data when they were foiled. They accessed the FTSE 100 firm's databases thanks to an easily found and weak password, Qwerty1234. An expert says the case highlights the vindictive side of criminal hackers. UK-based IHG operates 6,000 hotels around the world, including the Holiday Inn, Crowne Plaza and Regent brands. On Monday last week, customers reported widespread problems with booking and check-in. For 24 hours IHG responded to complaints on social media by saying that the company was "undergoing system maintenance". Then on the Tuesday afternoon it told investors that it had been hacked. Read the full story by Joe Tidy here: BBC News *(Thanks to Graham Cartwright who pointed me to this story)*

In protest of Mahsa Amini's death, "anonymous" has declared cyber war against Iran

The voice from a video of the decentralized international hacktivist collective Anonymous resounded on Twitter on Tuesday afternoon as the Anonymous collective declared war on Iran and launched several strikes against the regime. Iran saw significant protests for many days after the brutal prison death of 22-year-old Mahsa Amini. In response, Anonymous ended its inaction and launched the OPIRan. Spid3r, the inventor of KromSec and an agent of Anonymous, alone brought down several websites after the discovery. The 22-year-old Iranian lady from the Kurdistan area died on Friday in Tehran, according to authorities and state media, after suffering a stroke and many heart attacks while being detained by Iran's purported morality police **because she was wearing an "improper" headscarf**.
Read the full story by Somya Agrawal here: The Tech Outlook

A look at the deployment of real life RoboCops

It has been more than five years since Dubai made headline news when it deployed humanoid robotic police officers to patrol its massive malls and busy streets. And, as A.I. and Machine Learning improved dramatically over the last few years, more police departments are following suit. They are either supplementing, or are planning to supplement their police force with law enforcement robots of some sort. Today I will take a look at a few of these and give you a glimpse of what is coming in the future, or not! Some recent deployments faced a heavy public backlash and were cut short. I will start with Dubai's "RoboCop"

Dubai

In May 2017, The Dubai police department deployed their first robot officers in preparation and anticipation for Expo 2020 which was postponed for two years due to the Covid-19 pandemic. The robot officer was first announced at the annual GITIX technology show in 2016 and was fitted with facial recognition to help police identify wanted criminals. Members of the public can talk to the robot to report a crime or communicate with it using a touch screen computer embedded in its chest to get local information, and they can even pay traffic fines. At the time, Dubai Police said it wants the unarmed robots to make up 25 percent of its patrolling force by 2030. The robots are built by Spanish based PAL Robotics.

New York - Digidog (Video)

Last year NYPD acquired a robotic police dog from Boston Dynamics that was hailed to be the answer to protect police officers from going into potentially life threatening and dangerous situations. The program was cut short however, as the department faced an unanticipated backlash from the public amidst privacy concerns. As cited in the New York Times ""*This dog is going to save lives," Inspector Frank Digiacomo of the department's technical Assistance Response Unit said in a television interview. "It's going to protect people. It's going to protect officers." Instead, the machine, which the police named Digidog, became a source of heated debate. After it was seen being deployed as part of the response to a home invasion in the Bronx in February, critics likened it to a dystopian surveillance drone. And when officers used it at a public housing building in Manhattan in February, a backlash erupted again, with some people describing the device as emblematic of how overly aggressive the police can be when dealing with poor communities*."

Israel's Dogo

Although not a fully-fledged autonomous AI robot, Dogo is designed to pack a 9mm Glock and laser sights to actually shoot someone. It can also be fitted with non-lethal options like pepper spray or teargas. Its design allows for it to go almost anywhere and stairs prove to be no obstacle for this little fella. Its manufacturer, General Robotics, says that together with the CHAMELEON, a throwable and climbing robot, forces are able to achieve full situational awareness and lethality.
Dogo actually reminds me of the Sphero Rover I bought for each of my boys a couple of years ago when they got interested in robotics.

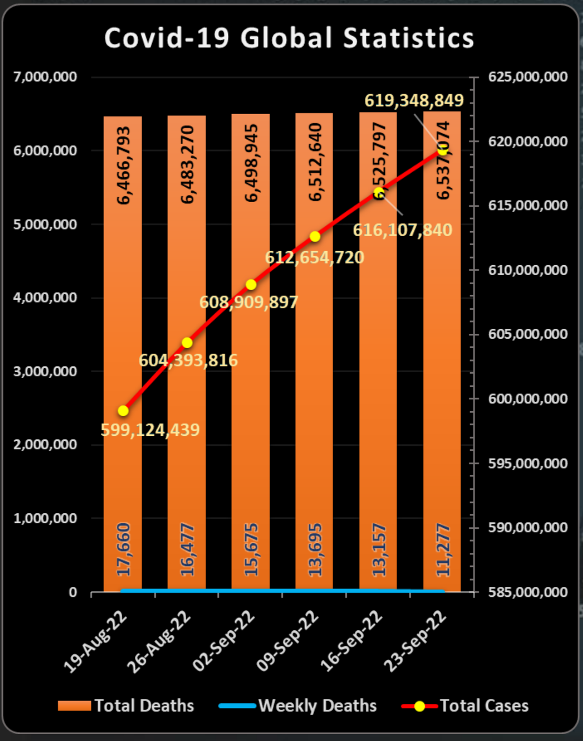
Tokyo's Persueusbot

In 2018, the Kei Yokota Seibu Railway Co. introduced Persueusbot to patrol the Tokyo railway stations in anticipation of the 2020 Olympics that were also postponed for 2 years due to Covid-19. It uses Artificial Intelligence linked with security cameras and is able to move around designated areas of a train station. The robot can then detect unfamiliar objects or people, who are exhibiting so-called 'unusual behavior'. It reports back to ground security staff via smartphone technology. The railway company anticipated potential terrorism threats during the Olympics and would not have enough staff to monitor all parts of the station at all times. This technology will enable them to monitor and react swiftly" (Video)

South Korea

Not so much RoboCops, but men in Ironman suits. In June this year, the South Korean police unveiled their plans for Iron Man Police to roam their streets possibly with Robo dogs to assist them. The 'Iron Man Police' is described to be human cops donning high-tech armor that enhance their strength and power. Their suits would also be equipped with an AI advisory system, not unlike Tony Stark's built-in smart butler/voice assistant J.A.R.V.I.S. from the Marvel movies. "*They'd be aided by quadruped robots, who will go on patrols and navigate harder-to-reach areas. With the landscape rapidly evolving into a technology-led one, the law enforcement agency anticipates that artificial intelligence, robotics, and advanced mobility will be the way to go to keep society safe*."
According to the Korea Herald, the national police force plans to deploy self-piloting robots, automated cars and, exoskeleton suits to aid body movement by 2050. Titled "Police Future Vision 2050," the NPA blueprint suggests five key strategies and 14 projects designed to help the law enforcement agency adapt to the fast-changing security environment along with technological advancement. The agency said the goal is to shift the police force away from a heavy reliance on manpower and human contact to an approach based on AI and science.

Other interesting initiatives I came across was the drone catching drones deployed in Japan to control restricted airspace. These are still remote pilot operated drones but can you imagine how effective it will be if countries deploy autonomous drone swarms to do this.. Just a parting thought.. (The Drone threat is discussed here: SIA)



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

Hey Olly, I'm going to get me one of them Iron Man suits
Now why on earth do you want to do that Stanley?
They say it will make me stronger than you, and I won't feel a thing if you hit me on the head

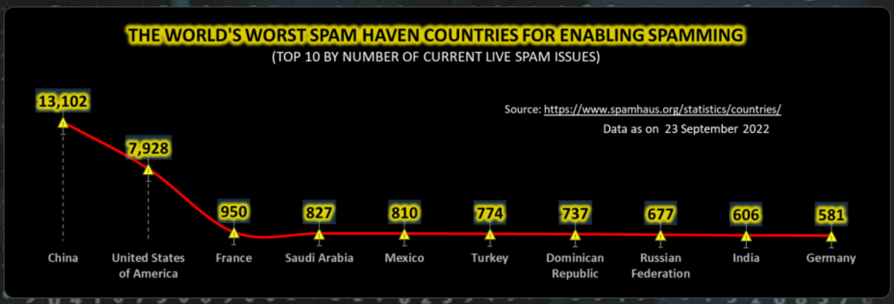
flightradar24 LIVE AIR TRAFFIC
Track any Aeroplane in flight globally

Marine Traffic
Track any Sailing Vessel globally

SatelliteXplorer
Track satellites in orbit

Other Interesting News and Cyber Security bits:

- What can you expect on Tesla AI Day?
- 'It's awesome': world's first flying bike makes U.S. debut
- Cyber Security At Sea: A Brand New Naval Cyber Framework
- SANS Daily Network Security Podcast (Storm cast)



Source: https://www.spamhaus.org/statistics/countries/
Data as on 23 September 2022

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