On October 11, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Cisco, Atlassian, Progress, Google, Apple, and Microsoft 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 October 2023

In The News This Week

Manufacturing giant dealing with 'disruptive' cyberattack

A major U.S. manufacturer of building materials said on Tuesday that it is dealing with a cyberattack disrupting its business operations – becoming the latest manufacturing firm in recent weeks to face operational issues due to a cyber incident. Simpson Manufacturing Company told the U.S. Securities and Exchange Commission (SEC) that on Tuesday, it experienced disruptions to its IT infrastructure after malicious activity was discovered. The company took systems offline immediately. "The incident has caused, and is expected to continue to cause, disruption to parts of the Company's business operations. The Company has engaged leading third-party cybersecurity experts to support its investigation and recovery efforts," Brian Magstadt, Chief Financial Officer told regulators and investors this week. "The investigation to assess the nature and scope of the incident remains ongoing and is in its early stages." The company did not respond to requests for comment about the nature of the attack. Read the full story by Jonathan Greig here: The Record

Microsoft Defender Thwarts Large-Scale Akira Ransomware Attack

Microsoft on Wednesday said that a user containment feature in Microsoft Defender for Endpoint helped thwart a "large-scale remote encryption attempt" made by Akira ransomware actors targeting an unknown industrial organization in early June 2023. The tech giant's threat intelligence team is tracking the operator as Storm-1567. The attack leveraged devices that were not onboarded to Microsoft Defender for Endpoint as a defense evasion tactic, while also conducting a series of reconnaissance and lateral movement activities prior to encrypting the devices using a compromised user account. But the new automatic attack disruption capability meant that the breached accounts are prevented from "accessing endpoints and other resources in the network, limiting attackers' ability to move laterally regardless of the account's Active Directory state or privilege level." Read the rest of the here: The Hacker News

Israeli cyber security professionals band together amid Gaza war

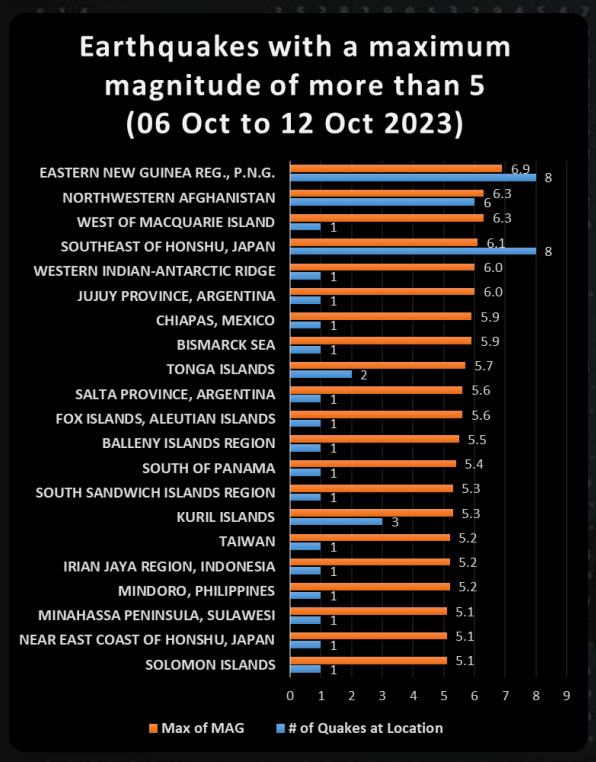
As Israeli children listened to their teacher over Zoom, the image of a gun-toting man in fatigues appeared on the screen, according to a screenshot shared with Reuters. In another case, a video showed a billboard in the central Israeli city of Holon displaying images of rockets and a burning Israeli flag. Israeli information security professionals are banding together to provide free cybersecurity services to Israeli companies amid a spike in hacktivist activity sparked by the war in Gaza, volunteers said. Reuters could not independently verify the school incident. The screenshot was provided by Yossi Appleboum, the chief executive of cybersecurity company Sepio. Appleboum said he received the screenshot via a person in direct contact with the children's families. In a statement, Zoom said that it was "deeply upset" to hear about the disruption, and that it had offered its help to enable schools in Israel to continue operating remotely.
Read the full article by Christopher Bing, Raphael Satter and James Pearson here: Reuters

FCA fines Equifax £11 million for role in cyber-security breach

The Financial Conduct Authority (FCA) has fined Equifax £11.2m for failing to manage and monitor the security of UK consumer data it had outsourced to its parent company based in the US. The breach allowed hackers to access the personal data of millions of people and exposed UK consumers to the risk of financial crime. In 2017, Equifax's parent company, Equifax was subject to one of the largest cybersecurity breaches in history. Cyber-hackers were able to access the personal data of approximately 13.8 million UK consumers because Equifax outsourced data to Equifax Inc's servers in the US for processing. The UK consumer data accessed by the hackers ranged from names, dates of birth, phone numbers, Equifax membership login details, partially exposed credit card details, and residential addresses. Read the post by John Kirwan here: MotorTrader

Largest DDoS attacks ever reported by Google, Cloudflare and AWS

Internet infrastructure providers Google Cloud, Cloudflare and Amazon Web Services have reported the largest ever distributed-denial-of-service (DDoS) attacks. The DDoS attacks were reported on October 10, with the cloud service providers noting that the attacks were part of a mass exploit of a zero-day vulnerability. The DDoS attacks themselves started during August and are still continuing as of the time of writing. In a blog post about the DDoS attacks, Google explained that it was the largest DDoS attack "to date", with the requests per second (rps) peaking at over 398 million, making it seven and a half times larger than the previous record-breaking DDoS attack. Google noted that 398 million rps is equivalent to "more requests than the total number of article views reported by Wikipedia during the entire month of September 2023". The DDoS attacks were launched using a threat vector previously unseen. The malicious actors "relied on a novel HTTP/2 "Rapid Reset" technique based on stream multiplexing" and impacted multiple internet infrastructure companies.
Read the rest of the post by Olivia Powel here: Cyber Security Hub



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

DIY home security projects using a Raspberry Pi

Last week we discussed some DIY projects to build a home security system or part of it with a small cheap Arduino microcontroller. In the post, I mentioned the differences between a microcontroller and a single-board computer (SBC) like the Raspberry Pi, but we focused on the Arduino microcontroller. The fact is, we can do the same with a single-board computer, it is just a tad more complicated, but you can build a much more sophisticated system. There are several different SBCs available out there, but I'll pick the one that I am more familiar with for this post, the Raspberry Pi. The Raspberry Pi is about the same physical size as the Arduino Uno, but it really is a full-blown computer with a quad-core processor and built-in Wi-Fi, Bluetooth, Ethernet, etc. In a post quite some time ago, I even mentioned how hackers used a Raspberry Pi to hack NASA. Many retailers are starting to use Raspberry Pi's as point of sale (POS) machines, that is how powerful they are, all you need is to add a keyboard and screen. It is a bit more expensive than the $10 - $20 Arduino though, as you are looking more in the region of $60 - $80, depending on the model.

Keeping the same format as last week, I'll share some DIY home security projects I found in the Internet jungle, but first, I'll talk more about the Raspberry Pi.

More about the Raspberry Pi

A Raspberry Pi is a small, affordable single-board computer that was originally developed by the Raspberry Pi Foundation, a UK-based charity organization. It was designed to promote computer science education and make computing more accessible to people of all ages and skill levels, but it evolved into much more than that, and tons of organizations are using it in loads of commercial applications.
The Raspberry Pi is about the size of a credit card and comes in various models and versions, each offering different capabilities. They typically include a processor, memory (RAM), USB ports, HDMI ports for connecting to displays, GPIO (General Purpose Input/Output) pins for hardware interfacing, and a microSD card slot for storage. It comes preloaded with an open-source Raspberry Pi OS (on a MicroSD card) based on the Debian distribution of Linux, and runs a suite of open-source software, but you can essentially run Windows or other flavors of Linux on it.
It is powered by a 5v power supply, or battery pack, or Power Over Ethernet (PoE).

DIY Security System Projects using the Raspberry Pi

Project 1 – Raspberry Pi-based smart home security system
Home Security Systems are a need in modern-day houses. It is possible to design a simple home security solution by using Raspberry Pi and utilizing the power of Internet of Things. The home security system designed in this project is a simple and easily installable device built using Raspberry Pi 3, a Web Cam, and PIR Motion Sensor. The Raspberry Pi 3 Model B comes equipped with onboard Bluetooth (BLE) and Wi-Fi (BCM43438 Wireless LAN), so, it can be easily connected with a Wi-Fi Router to access a cloud service.
The device designed in this project can be installed at the main entrance of a house. It detects motion of any visitor with the help of PIR sensor and starts capturing the images with the help of a USB webcam. The images are temporarily stored on the Raspberry Pi and pushed to the Google Cloud from where they are sent as email alerts to the homeowner. So, the user gets the images of any visitor immediately on email which he can check from his smartphone.

Project 2 - Home Alarm System Project for your Raspberry Pi
JemRF, aka PrivateEyePi, runs a site for Raspberry Pi projects aimed at the Raspberry Pi enthusiast wanting to build home security/automation systems and at the same time learn programming and electronics. You will find several projects on the site you can dabble into, and I've just picked one to post here, visit the site for more.

Project 3 - Build Your Own Surveillance System Using Raspberry Pi
Raspberry Pi is a tiny computer that can be used for pretty much anything. People use this tiny computer for a variety of things, including IoT projects, network monitoring systems, automating infrastructures, photo and video editing, gaming, crypto-mining, and the list never stops here. In this post, we will show you a step-by-step procedure to build your own surveillance system using Raspberry Pi.

Project 4 – Wi-Fi Security Camera With a Raspberry Pi Zero 2W

Have you ever left home and felt that something was wrong in your house? Well, worry no more! With this feature-packed yet incredibly simple setup, you can monitor your house whenever you like with just a click on your device. This project uses just a $15 Pi Zero 2W and a small camera to make a simple, fully functioning, and compact Wi-Fi security camera. The webcam continuously captures frames and sends them to the computer, and when it detects a sudden difference in consecutive frames due to some kind of motion, the camera records a short video. It then saves the video to the Pi Zero, uploads it to Google Drive, and sends a web request to IFTTT and thus, alerts the user in some way. The live camera feed can be viewed from any device with just one click. Pretty cool, right? In this detailed guide, I will walk you through every step in building this awesome project from scratch. Although this might seem very long, it is a very fun process, and the end result is definitely worth the patience.

Project 5 - Smart Greenhouse Controlled Using a Raspberry Pi 4 (Yes, not a security project but a fun one anyway ☺)

Welcome to this step-by-step instructables guide on how to create your very own smart greenhouse controlled by a Raspberry Pi! If you have a passion for gardening and technology, this project will undoubtedly pique your interest. By harnessing the power of the Raspberry Pi, we will build a greenhouse that not only protects your precious plants but also monitors their vital conditions. Imagine having the ability to remotely control and track the temperature, humidity, soil moisture, and even the amount of sunlight your plants receive. With this smart greenhouse, you can create the ideal environment for your beloved flora, ensuring they thrive and flourish under your attentive care.

Resources: Instructables, Engineers Garage, Cavelab, Hackster.io, PrivateEyePi, Raspberry Pi Handbook 2022, Raspberry Pi Handbook 2023

Other Interesting News and Cyber Security bits:

- Emerging cyber security threats in 2023: ChatGPT and beyond
- What Role Does AI Play In Enhancing Aviation Cybersecurity?
- Who's Hacked? Latest Data Breaches And Cyberattacks (Cybercrime Magazine)
- SANS Daily Network Security Podcast (Storm cast)

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

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