On September 27, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Drupal, Apple, and 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
29 September 2023

In The News This Week

Sony investigates after ransomware group claims to have breached company's systems

Sony has said it has launched an investigation after a ransomware group claimed to have breached the company's systems. Cyber Security Connect reported that a ransomware group calling itself Ransomed.vc claimed it had breached Sony Group and threatened to sell stolen data. "We have successfully compromised [sic] all of sony systems," Ransomed.vc claimed on both on the clear and dark nets, as reported by Cyber Security Connect. "We won't ransom them! We will sell the data. Due to Sony not wanting to pay. DATA IS FOR SALE." - While the claims are unverified at this stage, Cyber Security Connect said Ransomed.vc posted proof-of-hack data that includes screenshots of an internal log-in page, an internal PowerPoint presentation outlining test bench details, and a number of Java files. There's also a file tree of the entire leak, which appears to have less than 6,000 files. Cyber Security Connect described this cache of data as "small" relative to the "all of Sony systems" claim... Read the full article by Wesley Yin-Poole here: IGN

Volkswagen stuck in neutral after 'IT disruption'

Some of Volkswagen's operations have screeched to a halt after some sort of cyber incident, according to German media reports. The event has halted large parts of the car manufacturer's IT and production systems at locations around the globe, according to daily business newspaper Handelsblatt. A VW spokesperson confirmed the disruption to the German publication, describing it as an "IT disruption of network components at the Wolfsburg location." It reportedly began at 1230 local time on Wednesday, and the full extent of the shutdown remains unknown. Volkswagen did not immediately respond to The Register's inquiries about the IT incident, but we will update this story as soon as we hear back from the automaker..
Read the rest of the story by Jessica Lyons Hardcastle here: The Register

Over 700 Dark Web Ads Offer DDoS Attacks Via IoT in 2023

The year 2023 has seen a surge of over 700 advertisements on the dark web offering Distributed Denial of Service (DDoS) attacks through Internet of Things (IoT) devices, suggests a new report by Kaspersky. These services come at varying price points, depending on factors like DDoS protection and verification on the target's end, ranging from $20 per day to $10,000 a month. On average, these services cost around $63.50 per day or $1350 per month. The dark web also serves as a hub for exploits targeting zero-day vulnerabilities in IoT devices and bundled IoT malware complete with infrastructure and tools. In the realm of IoT malware, numerous strains exist, many originating from the infamous 2016 Mirai malware...
Read the post by Alessandro Mascellino here: Infosecurity Magazine

Johnson Controls International Disrupted by Major Cyberattack

Johnson Controls International (JCI) this week reported in a filing with the US Securities and Exchange Commission (SEC) that it had suffered a cyberattack that caused disruptions to its internal IT infrastructure. In addition, two of the company's subsidiaries, Simplex and York, are reportedly displaying messages of a "technical outage" on customer portals and login pages. Gameel Ali, a researcher at Nextron Systems, shared a tweet including a ransom note from cybergang **Dark Angels** in its VMware ESXi encryptor, stating: "*HELLO dear Management of Johnson Controls International! If you are reading this message, it means that: your network infrastructure has been compromised, critical data was leaked, files are encrypted, backups are deleted.*" The note went on to say, "*The best and only thing you can do is to contact us to settle the matter before any losses occurs.*" The gang has allegedly stolen over 27TB of data and encrypted the company's VMware ESXi machines in a ransomware attack.... Read the full story here: Dark Reading

China looks to relax cross-border data security controls

China has moved to water down some of its tough cross-border data controls amid complaints from foreign businesses and a teetering economy. The Cyberspace Administration of China unveiled rules on Thursday evening which look to clarify and simplify the transfer of data out of the country for ordinary business activities. Beijing's move to walk back part of its burdensome regime comes amid efforts to reassure foreign businesses concerned about deteriorating US-China relations and the creeping influence of its own security apparatus. Under the security rules in place, CAC has been reviewing reams of data export submissions from foreign groups wanting to share "important data" abroad. However, the rules "created an untenable situation, with people unsure if they should apply for the data reviews and unsure on what counted as important data", said Graham Webster, a China expert at the Center for International Security and Cooperation at Stanford University. "These changes would create a more clear path for most data to be sent abroad," he said....
Read the rest of the article by Ryan McMorrow here: The Financial Times

IoT Security: Safeguarding Against Digital Assaults

IoT is short for Internet of Things, and it has become an integral part of modern life where everything talks to everything that can "see" the Internet. Whether that connection to the Internet is through a Mobile Network, Wi-Fi, Bluetooth, or a Satellite connection, combined with AI (Artificial Intelligence) it is busy to revolutionize life as we know it. The uses of IoT range from fridges ordering food replenishments based on the current content of the fridge, to someone's pacemaker "talking" to the health care provider's computer systems to alert doctors, or even automatically adjust the tempo when necessary. These are just two small examples of a vast array of IoT applications out there, and they can range from small unsophisticated to highly complex units. The scary thing though, is the vast amount of data that traverses through these networks and can typically contain Personal Identifiable Information (PII), especially in medical applications and personal wearable devices like a Fitbit or smartwatch, and so forth. Gartner predicts that there will be approximately 25 billion IoT devices by 2025. And this is where the security concerns are coming in. Other than computers and smartphones etc., IoT device manufacturers, in many cases, do not put a proportionate emphasis on security, which makes these devices vulnerable to hacking or other types of digital attacks. Just imagine if someone takes over control of a person's pacemaker remotely, it can have deadly consequences.
So, in today's post, I want discuss some of the security concerns on IoT security, and I found a post by Christian Henke of Emnify that sums it up nicely. Below is an extract of Christian's post.

IoT Security Risks

Weak authentication - Passwords are one of the first lines of defense against hacking attempts. But if your password isn't strong, your device isn't secure. Most default passwords are relatively weak, because they're intended to be changed, and in some cases, they may be publicly accessible or stored in the application's source code. End users may also set the password to something that's easy to remember. But if it's easy to remember, it's probably easy for a bot to guess it. Many IoT devices have little or no authentication at all. Even if there's no important data stored on the device itself, a vulnerable IoT device can be a gateway to an entire network, or it can be assimilated into a botnet, where hackers can use its processing power to perform DDoS attacks.

Low processing power - Most IoT applications use very little data. This reduces costs and extends battery life, but it can make them difficult to update Over-the-Air (OTA) and prevents the device from using cybersecurity features like firewalls, virus scanners, and end-to-end encryption. This ultimately leaves them more vulnerable to hacking. This is where it's crucial that the network itself has built-in security features.

Legacy assets - If an application wasn't originally designed for cloud connectivity, it's probably ill-equipped to combat modern cyber attacks. For example, these older assets may not be compatible with newer encryption standards. It's risky to make outdated applications Internet-enabled without making significant changes—but that's not always possible with legacy assets that have been cobbled together over years.

Shared network access - It's easier for IoT device to use the same network as the end user's other devices—such as their Wi-Fi or LAN—but it also makes the entire network more vulnerable. Someone can hack an IoT device to get their foot in the door and gain access to more sensitive data stored on the network or other connected devices. Likewise, another device on the network could be used to hack the IoT device. Every IoT application should use a separate network and/or have a security gateway or firewall—so if there's a security breach on the device, it remains isolated to the device. (This is one of the advantages of cellular IoT.) A Virtual Private Network (VPN) helps protect your devices from outside the network, but if your application shares a connection with other devices, it's still vulnerable to attacks from them if they become corrupted.

Inconsistent security standards - Within IoT, there's a bit of a free-for-all when it comes to security standards. There's no universal, industry-wide standard, which means companies and niches all have to develop their own protocols and guidelines. The lack of standardization makes it harder to secure IoT devices, and it also makes it harder to enable machine-to-machine (M2M) communication without increasing risk.

Lack of encryption - One of the greatest threats to IoT security is the lack of encryption on regular transmissions. Many IoT devices don't encrypt the data they send, which means if someone penetrates the network, they can intercept credentials and other important information transmitted to and from the device.

Missing firmware updates - Another of the biggest IoT security risks is if devices go out in the field with a bug that creates vulnerabilities. Whether they come from your own developed code or a third party, manufacturers need the ability to issue firmware updates to eliminate these security risks. Ideally, this should happen remotely, but that's not always feasible. If a network's data transfer rates are too low or it has limited messaging capabilities, you may have to physically access the device to issue the update.

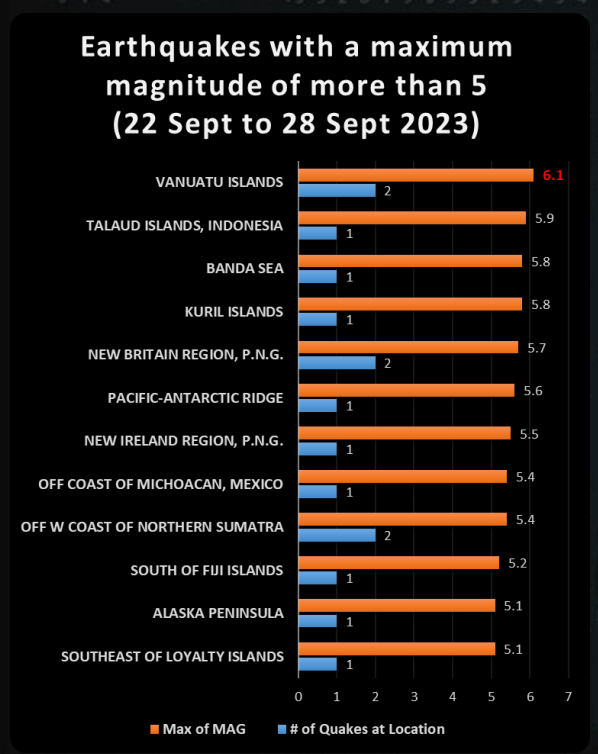
Gaps between mobile networks and the cloud - Many IoT devices regularly interact with cloud-based applications. And while the cellular network an IoT device uses may be secure, and the cloud application may be secure, transmissions from the network to the cloud typically pass through the public Internet, leaving them vulnerable to interception and malware. Even these small gaps can compromise an entire IoT deployment. Thankfully, IoT manufacturers and their customers can close them with cloud-based connectivity solutions.

Limited device management - Businesses often lack the visibility and control they need to see when a device has been compromised and then deactivate it. Every Mobile Network Operator (MNO) has their own connectivity management platform, and some give customers very little insight or functionality. Hacked or compromised devices tend to consume data differently, and so end users should be able to detect anomalous behavior and remotely deactivate these devices before they have opportunities to cause greater harm.

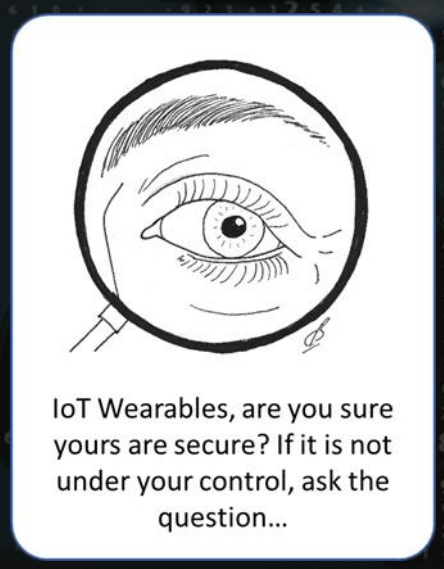
Physical vulnerabilities - Not all IoT devices operate in remote areas. Some regularly come into contact with people, which opens the door to unauthorized access. In fleet management, for example, it's not uncommon for drivers to steal SIM cards from their vehicle's GPS trackers to use them for "free data." Other thieves may steal SIM cards to commit identity theft. People can also physically access IoT devices for more nefarious purposes, like accessing a network or stealing information. End users can't always watch their IoT devices to ensure no one is physically accessing them, so it's important to consider ways to harden devices with better components and security features.

That is all I have space for in this post, please link to Christian's post to see more or visit some of the resources below.

Resources: Emnify, EC Council, LinkedIn, IEEE Computer Society



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:

- Food for a mission to Mars: This Finnish firm wants to feed astronauts proteins from microbes
- Remote workers are more aware of cybersecurity risks than in-office employees: new study
- 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