On April 19, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google and Oracle 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

21 April 2023

In The News This Week

UK and US issue warning about APT28 actors exploiting poorly maintained Cisco routers

UK and US agencies have today (Tuesday) issued a joint advisory to help organisations counter malicious activity used by Russian cyber actors to exploit poorly maintained Cisco routers. APT28 – a threat group attributed to Russia's military intelligence service the GRU – has been observed taking advantage of poorly configured networks and exploiting a known vulnerability to deploy malware and access Cisco routers worldwide. In 2021, a series of attacks was carried out against a small number of organisations based in Europe, US government institutions and around 250 Ukrainian victims for reconnaissance purposes, with Jaguar Tooth malware then deployed against some targeted devices to enable unauthenticated access.
Read the full article here: National Cyber Security Centre (NCSC)

Yes, AI is a cybersecurity 'nuclear' threat (An opinion)

Microsoft just announced Security Copilot, their AI-powered assistant that will revolutionize cybersecurity defense by increasing efficiency and productivity. The tool will incorporate ChatGPT4 technology from OpenAI and a proprietary security specific model created by Microsoft from all the data they have. The Security Copilot is currently available to a small number of selected companies for testing with the official launch date still unknown. However, hackers are not waiting and have already started utilizing widely available AI tools to launch attacks. Waiting for this public release or any other official AI security defensive tools is leaving companies at a disadvantage, as they're easy targets for assailants fond of the new tech. Companies are postponing authorization because of the potential risks they believe it may bring. However, the utilization of AI in organizations brings potential benefits that far outweigh the risks of not using this technology. ...
Read the rest of this opinion by Rodrigo Loureiro here: Fox News

Bank of America warns Lloyd's over state-backed cyber attack exclusion

Bank of America raised concerns with Lloyd's of London about a move to exempt big "state-backed" cyber attacks from standard insurance policies, underscoring the concern among financial institutions about changes to a crucial safety net. The US lender expressed unease over the new rule in one of a series of discussions of the matter in recent weeks between Lloyd's and big clients, according to people familiar with the meetings, as the insurance market seeks to protect itself from systemic risk. Anxiety is growing among large corporations about the threat from state-sponsored cyber groups, including over whether the cost of attacks will be covered by their insurers.
A senior UK official warned on Wednesday over the threat from "ideologically motivated, rather than financially motivated" hackers allied to Moscow. Read the article by Ian Smith here: Financial Times

Sam Bankman-Fried's Legal Team Can't Figure Out How to Install Spyware on His Parents' Smartphones

- The disgraced FTX founder was supposed to be automatically monitored across devices, but some have proven resistant. - It turns out that installing spyware on smartphones isn't as easy as it sounds.
Lawyers for Sam Bankman-Fried said that they have encountered unexpected challenges while attempting to comply with specific bail conditions set forth by the court. The issue in question is installing software on his parents' smartphones that would take pictures of the user every five minutes in order to constantly monitor who was using them. "We learned recently that the monitoring software installed on the new cellphones we purchased for Mr. Bankman-Fried's parents cannot, in fact, automatically photograph the device's user every five minutes as required by the order," wrote attorneys Mark Cohen and Christian Everdell... Read the rest of the story by Jason Nelson here: Decrypt

Capita admits customer, supplier or colleague data may have been accessed by hackers

London UK - Capita, the outsourcing specialist and government contractor, has revealed that customer, supplier or colleague data may have been accessed during a cyber attack in March. - The company, which announced earlier this month that it had been targeted, said its investigations had identified that the attack on its systems first took place on or around 22 March. It said the unauthorized access was not interrupted until 31 March. It believed the hackers primarily impacted access to internal Microsoft Office 365 applications, admitting there was evidence of a "limited" data breach. "Capita continues to work through its forensic investigations and will inform any customers, suppliers or colleagues that are impacted in a timely manner," its statement said. - Read more by James Sillars here: Sky News

UK Warns of Russian Hackers Targeting Critical Infrastructure

The UK government's intelligence and security arm this week issued an alert on Russian state-aligned threat actors aiming to conduct disruptive and destructive attacks against critical infrastructure in Western countries. To date, says the National Cyber Security Centre (NCSC), these threat groups have focused on distributed denial-of-service (DDoS) attacks, defacements, and misinformation attacks. "Some have stated a desire to achieve a more disruptive and destructive impact against western critical national infrastructure (CNI), including in the UK," the NCSC warns. Read the full story here: SecurityWeek

iOS vs. Android – Which Is The More Secure Platform?

The debate around who has the best security between Apple iOS and Android has been raging on for about 15 years now. In the past, I reported on the topic in this forum a few times, but I thought it would be a good to revisit the latest reviews and views. Below is an extract of a post by Adeola Adegunwa of Information Security Buzz that gives as a fairly unbiased view.

Overview of Android and iOS Security - While Android and iOS have distinct security models, the end goal for both platforms remains the same – safeguarding user data and devices. Android is an open-source platform. This indicates that anyone can view and edit the code because it is publicly available. While this provides flexibility and customization for developers, it also makes the platform more vulnerable to security threats. It is because any malicious code can be easily integrated into the system, potentially compromising the device's security.
To mitigate these risks, Google has implemented various security measures in the Android platform. For example, Android has built-in security features such as Google Play Protect, which scans apps for malware and other security threats.
On the other hand, iOS is a closed system, meaning only Apple can access and modify the code. This makes it more secure than Android but also means that users have less control over their devices. However, iOS also has vulnerabilities that hackers can exploit.
Apple has implemented various security measures to ensure its platform's security. For example, iOS uses hardware-based encryption, which makes it more difficult for hackers to access user data. Additionally, iOS has a more stringent app review process, which includes manual reviews of each app before it is published on the App Store. It makes it less likely for malicious apps to make their way onto the platform.

iOS vs. Android: Homogeneous vs. Fragmented Ecosystems - One factor that can impact the security of a mobile platform is the ecosystem in which it operates. iOS has a more homogeneous ecosystem, meaning that most users are running the latest version of the operating system. In fact, 70% of iPhone users update their devices within 51 days of a patch being released. This is partly because Apple controls its products' hardware and software, enabling quicker and more effective updates. As a result, iOS devices receive security patches more quickly, which helps to lower the possibility of known vulnerabilities being exploited.
The Android ecosystem, in comparison, is more dispersed, with a wider variety of devices and operating system versions in use. This can make it more challenging for security updates to be rolled out quickly and efficiently, leaving some devices vulnerable to known exploits. Additionally, some device manufacturers may not prioritize security updates, leaving users with older devices at a higher risk of being targeted by attackers.

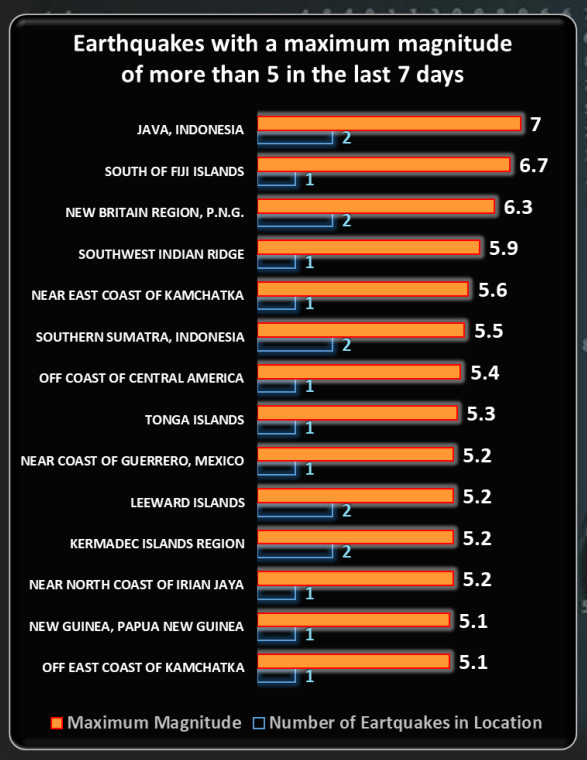
iOS vs. Android: Vulnerability Comparison - Overall, the number and severity of vulnerabilities may vary depending on the platform, but both Android and iOS are vulnerable to attacks. According to recent statistics, Android had 547 vulnerabilities in the year 2021, compared to 357 for iOS. While Android and iOS have vulnerabilities, these recent statistics suggest that Android has more overall vulnerabilities. But it's crucial to remember that a higher proportion of Android vulnerabilities are considered to have a low attack complexity, which means that they are easier to exploit. In contrast, iOS has more critical vulnerabilities, which suggests it is harder to compromise, but the rewards may be more significant.

iOS vs. Android: App Security - App security is a crucial aspect to consider when comparing iPhone and Android security. Though Apple's App Store and Google's Play Store have measures in place to limit exposure to malicious apps, the question remains how effective they are.
The Apple Store is the only source of apps for iPhone users unless the device is jailbroken. Although this may seem restrictive, it is a key component of Apple's overall security strategy. Each app on the App Store undergoes a manual review process by a member of the Apple Review team before being listed. However, even with Apple's stringent review policy, malicious apps have managed to slip through and make it to the App Store.
In contrast, Android users have access to a larger pool of apps than iPhone users. Google Play Protect checks apps for malware and other issues, and Google claims to scan more than 100 billion apps on the Play Store daily. Moreover, like iOS, Android apps are sandboxed, limiting their access to other apps and files.
However, installing third-party apps on Android devices outside the Play Store is easier than on iPhones. Despite Google's security measures, researchers frequently find malicious apps on the Play Store that have affected millions of Android devices.
Overall, while both Apple's App Store and Google's Play Store have allowed some malicious apps to slip through, more reports of this happening on the latter have been documented. Therefore, Apple provides better app security for iPhone users than Google does for Android users.

iOS vs. Android: Updates and Update Frequency - When it comes to updates and update frequency, iOS provides a better user experience than Android. Apple releases a new iOS version every year, delivering over 70 major updates in 15 years. There have been at least seven updates since iOS 16 was released in September 2022, and frequent patches are rolled out between major releases. All iOS devices receive updates at once, ensuring the timely delivery of vital security patches. Apple also supports devices with updates for up to seven years, which is longer than Android's three to five years.
In contrast, Android has received about 66 major updates since its launch in 2008, and updates can take significantly longer to roll out due to manufacturers independently testing them for compatibility issues. Android users receive updates less frequently than iPhone users, leaving them exposed to potential security vulnerabilities.
Although Android updates are not necessarily worse, data from cybersecurity firm Clario shows more search interest in iPhone update issues than Android over the last 12 years, indicating that Android may have fewer update issues. Nonetheless, Apple's control over its devices allows for the swift delivery of updates, making iOS a better option for users who prioritize security and functionality.

Conclusion: Which Platform is More Secure? - It's hard to determine which platform is more secure as both iOS vs. Android have their vulnerabilities. Android has more vulnerabilities, but they may be easier to exploit. iOS, on the other hand, is harder to compromise, but vulnerabilities can be more severe. The security of a mobile platform also depends on the user's behavior and security updates. Which platform to utilize ultimately comes down to personal preference and requirements. Android offers more customization, while iOS has consistent security updates and targeted exploits. Users need to stay vigilant, keep software updated, use strong passwords, and avoid downloading apps or clicking on links from unknown sources.

Please visit the Information Security Buzz site to read the full post with more comparison areas.

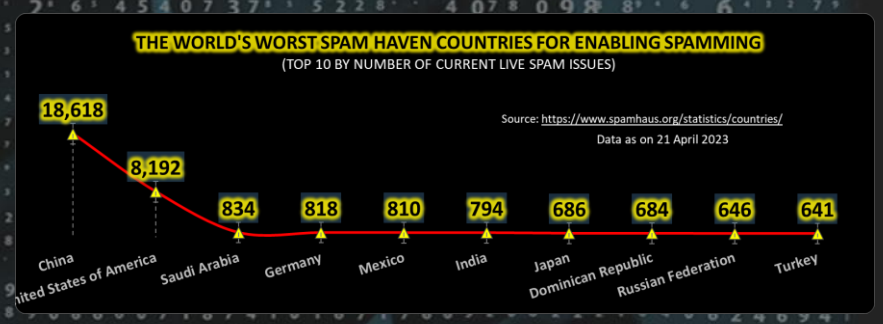


For Reporting Cyber Crime in the USA go to (IC3) , in SA go to Cybercrime, in the UK go to ActionFraud

Other Interesting News and Cyber Security bits:

- Mysterious flash of light over Kyiv sparks alarm and confusion after NASA denies its satellite crashed
- The Privacy Dilemma: How Autonomous Cars May Impact Your Personal Data
- Driving Toward a Safer Future: NVIDIA Achieves Safety Milestones With DRIVE Hyperion Autonomous Vehicle Platform
- 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