On May 31, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google Chrome.
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
02 June 2023

In The News This Week

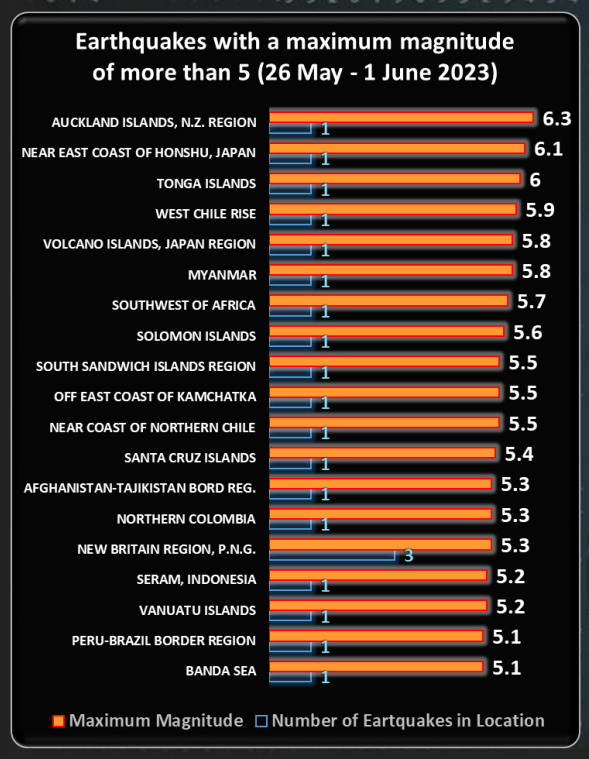
Russia's intelligence Federal Security Service (FSB) said that the recent attacks against iPhones with a zero-click iOS exploit as part of Operation Triangulation were carried out by US intelligence.
Researchers from the Russian firm Kaspersky have uncovered a previously unknown APT group that is targeting iOS devices with zero-click exploits as part of a long-running campaign dubbed Operation Triangulation. The experts uncovered the attack while monitoring the network traffic of its own corporate Wi-Fi network dedicated to mobile devices using the Kaspersky Unified Monitoring and Analysis Platform (KUMA). According to Kaspersky researchers, Operation Triangulation began at least in 2019 and is still ongoing. The attack chains commenced with a message sent via the iMessage service to an iOS device. The message has an attachment containing an exploit. The expert explained that the message triggers a remote code execution vulnerability without any user interaction (zero-click). Shortly after Kaspersky's disclosure, Russia's FSB accused the US intelligence for the attacks against the iPhones. According to Russian intelligence, thousands of iOS devices belonging to domestic subscribers and diplomatic missions and embassies have been targeted as part of Operation Triangulation.
Read more by Pierluigi Paganini here: Security Affairs

Improved BlackCat Ransomware Strikes with Lightning Speed and Stealthy Tactics
The threat actors behind BlackCat ransomware have come up with an improved variant that prioritizes speed and stealth in an attempt to bypass security guardrails and achieve their goals. The new version, dubbed Sphynx and announced in February 2023, packs a "number of updated capabilities that strengthen the group's efforts to evade detection," IBM Security X-Force said in a new analysis. The "product" update was first highlighted by vx-underground in April 2023. Trend Micro, last month, detailed a Linux version of Sphynx that's "focused primarily on its encryption routine." BlackCat, also called ALPHV and Noberus, is the first Rust-language-based ransomware strain spotted in the wild. Active since November 2021, it has emerged as a formidable ransomware actor, victimizing more than 350 targets as of May 2023...
Read the rest of the article by Ravie Lakshmanan here: The Hacker News

Greece Orders Probe Into Massive School Exam Cyber-Attack
Ministries described the disruptive large-scale DDoS attacks as 'the most significant attack ever made on a Greek public government organisation' - Greece's Supreme Court Public Prosecutor Isidoros Dogiakos ordered an investigation into a cyber-attack on the data bank providing the school exam questions, with the assistance of the Police's Cyber Crime Unit. End-of-high-school exams in Greece were disrupted on Monday and Tuesday by a massive cyber-attack on the data bank providing the questions, causing delays, cancellation of exams, and havoc among teachers and students. The caretaker Ministries of Education and Religious Affairs and Digital Governance, in a shared press release, said the school exams platform received large-scale and long-lasting distributed denial-of-service, DDoS, attacks (up to 280,000 connections per second). DDoS attacks aims to disrupt the normal traffic of a system and bring it down. "The exam bank platform received 165 million hits from 114 countries. It is the most significant attack ever made on a Greek public government organisation," the ministries said.
Read the full story by Eleni Stamatoukou here: BalkanInsight

Canada to set up cyber security certification for defence contractors
OTTAWA, May 31 (Reuters) - Canada will work with the United States to draft a cyber security certification framework for defense contractors that will be identical for both countries as incidents of malicious hacking increase, the defense minister said on Wednesday. Russian President Vladimir "Putin's war on Ukraine has reminded all of us that the cyber domain is crucial to our national security," Canadian Defense Minister Anita Anand said at CANSEC, an annual defense trade show in Ottawa. "Here at home, malicious cyber activities have targeted defense contractors and subcontractors across Canada, leaving classified information vulnerable," she said. Without certification, which should be in place by the end of next year, Canadian suppliers' risk being excluded from future international defense procurement opportunities, the defense ministry said in a statement. Read the full article here: Reuters

Google triples reward for Chrome full chain exploits
The Chrome Vulnerability Rewards Program, which started on June 1, is set to run until December 1, 2023. During this period, bug hunters who report security bugs that can be chained together to fully exploit Chrome can get up to $180,000.
To further encourage researchers, Google has implemented an additional reward structure. When submitting subsequent full chain exploits, bug hunters will get the opportunity to earn up to $120,000.
"We're always interested in explorations of new and novel approaches to fully exploit Chrome browser and we want to provide opportunities to better incentivize this type of research," said Amy Ressler from the Chrome Security Team.
Read the full story by Helga Labus here: HelpNetSecurity



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

How to protect your phone from juice jacking attacks

"Juice Jacking" is something everyone should be aware of, whether you are a frequent traveler, a holidaymaker, or anyone that finds themselves in unfamiliar surroundings and desperately needs to charge your phone, tablet, or PC. So, what is juice jacking? Today, I want to share an extract of a recent post by Ema Globytė from NordVPN that gives you some insight into what it is and how to prevent being a victim.

What is juice jacking?
Juice jacking is a cyberattack where a public USB charging port is used to steal data or install malware on a device. Juice jacking attacks allow hackers to steal users' passwords, credit card information, addresses, names, and other data. Attackers can also install malware to track keystrokes, show ads, or add devices to a botnet. The term "juice jacking" was coined in 2011 by investigative journalist Brian Krebs after he conducted a proof-of-concept attack at DEFCON. A juice jacking attack can happen in any public place with portable wall chargers or public USB charging stations, like shopping centers, hotels, or cafes. Hackers infect the USB port or the charging cable before the user connects. Once your phone is connected and charging, the attacker can upload malware to your device, initiate data transfers, or monitor your keystrokes. Let's look at how juice jacking attacks work in more detail.

How juice jacking works
Juice jacking exploits a device's vulnerability when it's connected to a public charging station. Most attacks target mobile devices, such as Android and iOS phones. Older Android versions are particularly susceptible to juice jacking attacks. When you charge your phone by connecting it to your laptop's USB port, you can also transfer data between the two devices. That's because USB ports are not just power sockets: they have multiple pins, but only one is needed to charge your device. Two of the other pins are used for data transfers. When a user connects their device to a USB port to charge, they make it possible to move data between devices. Hackers use this USB connection functionality at public charging stations to hack into mobile devices and steal your personal data.

Types of juice jacking - Several types of juice jacking attacks exist, with differences between each attack method. Here are the four main juice jacking types:

- **Data theft** - Data theft juice jacking is when a hacker steals data from your device while you're charging your phone using a USB port. The process is typically fully automated, so you probably won't see a suspicious-looking character lurking nearby and waiting to transfer your personal data onto their device. Hackers often use crawlers to search your device for personally identifiable information (PII), banking details, or account passwords. They may also use malicious apps to clone all your mobile device's data to another phone. This method includes using additional hardware (e.g., a Mac or Windows computer) as an intermediary. After cloning your data, cybercriminals can harm you in many ways, from identity theft and impersonation to financial damage.
- **Malware installation** - Cybercriminals may also use juice jacking to install malware or viruses on connected devices (e.g., adware, ransomware, spyware, or trojans). Each malware type can be used by hackers in different ways. For example, ransomware may encrypt your files so that the criminals can ask for ransom, while spyware allows hackers to monitor and track your activity over a longer period. Cybercriminals may also use malware to steal personal information and gather data like social media interactions, photos, or call logs. Many of today's malicious software is designed to be indetectable, so a user may never realize they have malware on their device.
- **Multi-device attack** - A multi-device juice jacking attack also infects your device with malware. However, on top of infecting your mobile phone, it's designed to continue spreading malware without hackers having to do anything. Once your device is infected, it becomes a carrier designed to infect other USB ports. Multi-device attacks allow cybercriminals to scale up their attacks and infect multiple devices simultaneously.
- **Disabling attack** - A disabling juice jacking attack locks the device owner out of their device, giving full access and control to the hacker. When the phone is connected to the infected USB cable, the attacker loads malware onto the device, disabling it so the user can't access it anymore. They won't be able to do anything even if they notice suspicious activity on their phone..

Where juice jacking attacks can occur - Juice jacking can happen in any public place that provides USB charging stations, including **Airports., Hotels and hostels, Charging kiosks, Coffee shops, and Train stations**. You may think that hackers only target places offering a free charge, but that's not always the case. Even the public charging stations that you typically have to pay for may have malware installed.

Detecting juice jacking attacks - Juice jacking attacks can be difficult to detect. If your device has already been compromised, you may notice some suspicious activity – but that won't always be the case. For example, you may notice something you don't recognize on your phone — like purchases you didn't make or calls that look suspicious. Your phone may also start working unusually slowly or feel hotter than usual. Chances are, you may have picked up malware. For a full list of signs to watch out for, check out this article on how to know if your phone is hacked.

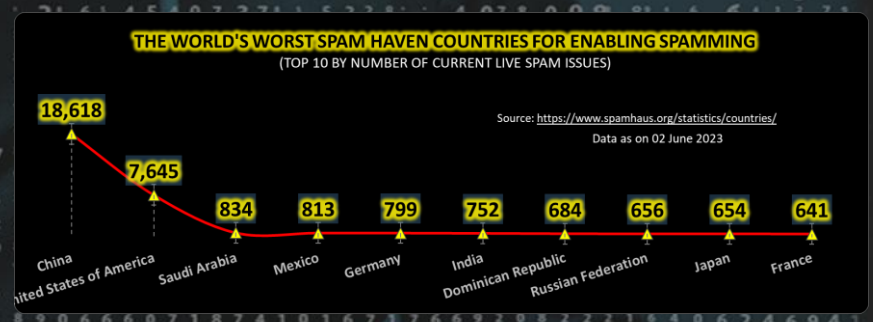
How to prevent juice jacking - Because these attacks mostly happen when charging at a public charging station through a USB port, the best thing you can do is not use them. Here are a few other tips for keeping your phone's data safe:
Get a power bank - Power banks are a safe and convenient way to charge your device on the go. Getting a portable power bank means that you'll never have to use public charging stations where juice jacking attacks occur. Always ensure your power bank is fully charged so you can use it on the go.
Use a USB data blocker - A USB data blocker is a device that protects your phone from juice jacking when you're using a public charging station. It plugs into the charging port on your phone and acts as a shield between the public charging station's cord and your device. USB data blockers (also known as "USB condoms") work by blocking data transfer through a charging cable. When you're using a USB data blocker, hackers have no way to load malware onto your device or steal your data.
Use a power socket instead - Juice jacking attacks only happen when you're connected to a USB charger. If you absolutely need to charge your phone in public, avoid the risk of infected cables and USB ports and use a power outlet with your own charger and cable. This is typically a safe way to charge your mobile device and other devices in public.

There is much more to say on the subject, so please read the full article here.

Other Interesting News and Cyber Security bits:

- The top 5 Cybersecurity online courses
- The best dash cam in 2023: security and protection for you and your vehicle
- NVIDIA is upgrading the in-car experience with AI, streaming, and advanced safety features
- Organizations are placing OT cybersecurity responsibility on CISOs
- SANS Daily Network Security Podcast (Storm cast)

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



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