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

On November 2, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Apple 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

04 November 2022

In The News This Week

Dropbox discloses unauthorized access to 130 GitHub source code repositories

According to the advisory published by Dropbox, the company was the target of a phishing campaign that resulted in access to the GitHub repositories. The investigation revealed that the code accessed by the attackers contained some credentials, primarily, API keys, used by the development team. The company pointed out that no one's content, passwords, or payment information were accessed, it also remarked that the issue was quickly resolved. Dropbox uses CircleCI for select internal deployments, and in early October, a phishing campaign targeted multiple Dropboxers using messages impersonating CircleCI. "While our systems automatically quarantined some of these emails, others landed in Dropboxers' inboxes. These legitimate-looking emails directed employees to visit a fake CircleCI login page, enter their GitHub username and password, and then use their hardware authentication key to pass a One Time Password (OTP) to the malicious site." reads the advisory published by the company. "This eventually succeeded, giving the threat actor access to one of our GitHub organizations where they proceeded to copy 130 of our code repositories.". Read the rest of the story by Pierluigi Paganini here: Security affairs

U.K. Reveals £6 Million Cybersecurity Support Package to Ukraine

The tempo of Russian cyber attacks against Ukraine increased significantly following its illegal invasion in February 2022, seeking to undermine Ukraine's sovereignty and strategic advantage in the war. - U.K. Foreign Secretary, James Cleverly, has revealed that the U.K. provided a £6.35 million support package to Ukraine to help protect its critical national infrastructure and vital public services from cyber attacks. The U.K.'s 'Ukraine Cyber Programme' was mobilized shortly after Putin's invasion in February to protect against increased Russian cyber attacks. The program has not been made public until now to protect its operational security. Utilizing the expertise of leading cybersecurity providers, the program has to date provided incident response support to Government of Ukraine entities, protecting them against destructive cyber attacks, including malware such as Industroyer2. This is preventing malicious actors from accessing vital information relevant to the war effort. The program has also limited attacker access to vital networks and supported Ukraine to harden their critical infrastructure against future attacks… Read the full article here: Homeland Security

Chinese Hackers Using New Stealthy Infection Chain to Deploy LODEINFO Malware

The Chinese state-sponsored threat actor known as Stone Panda has been observed employing a new stealthy infection chain in its attacks aimed at Japanese entities. Targets include media, diplomatic, governmental and public sector organizations and think-tanks in Japan, according to twin reports published by Kaspersky. Stone Panda, also called APT10, Bronze Riverside, Cicada, and Potassium, is a cyber espionage group known for its intrusions against organizations identified as strategically significant to China. The threat actor is believed to have been active since at least 2009. The group has also been linked to attacks using malware families like SigLoader, SodaMaster, and a web shell called Jackpot against multiple Japanese domestic organizations since April 2021, per cybersecurity firm Trend Micro, which is tracking the group under the name Earth Tengshe. The latest set of attacks, observed between March and June 2022, involve the use of a bogus Microsoft Word file and a self-extracting archive (SFX) file in RAR format propagated via spear-phishing emails, leading to the execution of a backdoor called LODEINFO. Read the full story by Ravie Lakshmanan here: The Hacker News

Bitdefender Upgrades Its Android Mobile Security With Real-Time Chat Protection

Chat Protection detects scam links sent through WhatsApp, Messenger, Discord, and Telegram. - Bitdefender just upgraded its mobile security suite for Android with real-time protection for your chat sessions on the most popular instant messaging apps. Bitdefender Mobile Security already offers protection for Android users against malware, scams, and suspicious apps, as well as the ability to remotely lock or wipe your device. However, a new feature has been introduced this week called Chat Protection. Chat Protection carries out real-time monitoring of your chat sessions in WhatsApp, Messenger, Discord, and Telegram in case someone sends you a malicious link. If they do, Chat Protection alerts the user and advises them not to forward the message and to instead delete it. Read the story by Matthew Humphries here: PC Mag

South Africa -The public sector must reimagine cybersecurity to enable e-government ideal

BCX -The South African government has demonstrated a deep understanding of how important the fourth industrial revolution (4IR) and a digital economy can be for our country's development. But security is the foundation and enabler of the 4IR and digital government and needs to be addressed first.

Critical infrastructure and government departments are under fire worldwide as cyber attackers target the most crucial systems for the largest payout. Power grids, ports, water and oil pipelines are being attacked, with IBM's latest Cost of a Data Breach Report saying 28% of breaches in critical infrastructure were ransomware or destructive attacks, with average breach costs topping $5.4-million in cases where organisations do not have Zero Trust strategies..

Read the full story by Sinamava Hina-Mvoko here: Mail&Guardian

Electric Vehicles and Cybersecurity, what's the fuss about?

As the world is pushing for green and renewable energy and technology is advancing at an enormous rate, Electric Vehicles (EVs) became more viable than ever before. As fossil fuel prices are going up and up, and mother nature is crying out for us to reduce emissions, people are ready to embrace EVs as the new norm. Up to now though, owning an electric vehicle was reserved for the few who can afford it. Not many people can go out and buy a Tesla, but the good news is that almost all manufacturers embarked on a race in the last few years to produce affordable EVs for the mass market. There is a slight problem though, EVs are running on batteries that needs to be recharged now and again. The infrastructure to sustain and maintain an array of charging stations across the length and breadth of a country is still lacking in most parts of the world. And then comes the cybersecurity issue as all EVs and many of their newer fuel-guzzling cousins are connected to the Internet. This is not necessarily a bad thing, but it opens up a myriad of risk factors that includes hacking. The bad guys have already compromised several "smart" vehicles in the last year and today I want to share an article by Ryan Owen of Finite State that talks about the cyber risks associated with EVs.

Electric Vehicle Cybersecurity: What Are the Risks?

A record 1.8% of US light vehicle registrations in 2020 belonged to electric vehicles (EV), according to research from IHS Markit, a division of S&P Global. For December 2020, that figure rose to 2.5%, a new monthly record. Those numbers represent a small fraction of all vehicles on US roads, but interest—and purchases—of EVs have continued to soar amid rising fossil fuel costs and concern for the environment. For the quarter ended **March 31, 2022**, over 200,000 EVs were sold in the United States, a new record high. And, by 2030, more than half of auto sales will be electric vehicles, according to American automotive executives interviewed by KPMG.

There's a dark side to this burgeoning interest, however. EVs are connected. They're like computers on wheels and rival our smartphones for the levels of technology they introduce into the driving experience of many Americans. Gone are the days when you could dismantle your muscle car with a suitcase of socket wrenches, an automotive repair manual, and the radio tuned to the sports team of your choice. EVs are complex wonders of technology, indeed. They come with 21st-century cybersecurity risks that never would have come to mind in the days of AM Top40 radio and roll-down window handles in your car.

The rising stakes of EV cybersecurity

Connected device technology brings innovation and potential to the future of our roads and how we experience them, but how does that connectivity translate into cybersecurity exposures? Could bad actors hack into the doors, steering mechanisms, and autonomous driving systems of our EVs? Could they hack into our charging stations? All these things can be connected, which means the risk exists. And those exposures have begun to materialize into exploits.

In January, a 19-year-old man exploited a weakness in a third-party app and was able to start 25 Tesla vehicles in 13 different countries—along with rolling down their windows and blasting their radios. Although more an annoyance than a dangerous cyberattack, if hackers had exploited the vulnerabilities in EV software directly, the results could have expanded beyond mere mischief. Those kinds of cyberattacks may be able to affect an EV's headlights, brakes, or even its steering, and potentially while the car is in operation.

As EV charging stations proliferate across the US and the world, stories of cybercrime exploits are surfacing. On the UK's Isle of Wright in April, hackers manipulated EV charging stations so they would display explicit content from adult websites instead of the usual content from the company's official website. In another incident, Russian EV stations were hacked to show pro-Ukrainian messages. Scarier, however, is the speculation surrounding how large-scale attacks on EV charging stations could affect victims. Research funded in part by the National Science Foundation speculates that hackers could simultaneously gain entry into many changing stations and repeatedly switch them on and off, causing irritation, inconvenience, but also potential mayhem if that attack stresses a regional power grid to the point of a failure that causes a blackout.

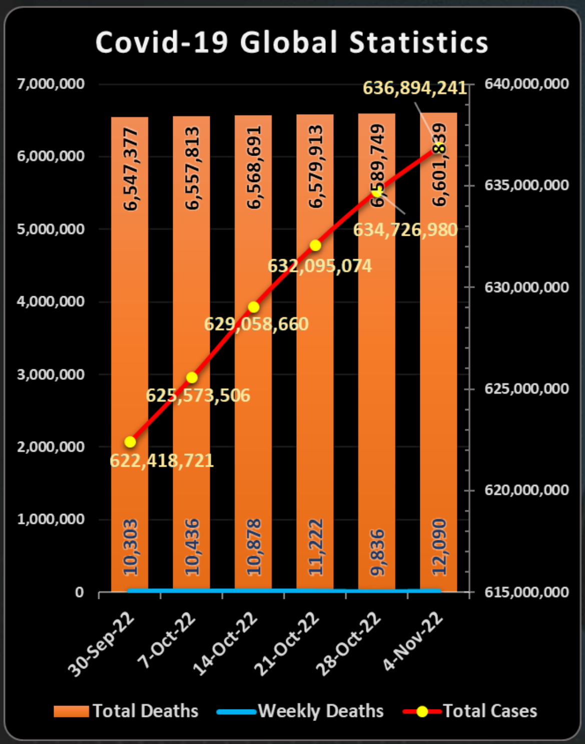
How can EV cybersecurity be improved?

Open the hood of any electric vehicle and see an ecosystem of components from brands you might recognize and some that you don't. It's hard to measure any one of those component makers' commitment to cybersecurity. In the future, evidence of that commitment could come in the form of attestations, perhaps a first-party attestation similar to the one created by SOX-302 requirements and signed by public-company executives who attest to the accuracy of their financials. President Biden's Executive Order (EO) 14028 could also create a framework for a third-party attestation model where an external party would certify the controls of a subject company.

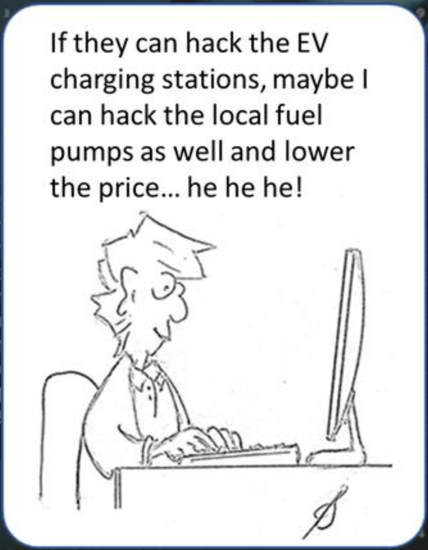
The Growing Need for Software Bills of Materials

While details like these are still being sorted out, recent regulatory developments suggest that manufacturers of connected devices—EVs included—could soon be required to disclose what goes into their connected products. Generally considered to have been issued in response to the 2020 SolarWinds attack, EO 14028 highlights the need for these connected-device inventories or Software Bills of Materials (SBOMs). SBOMs offer solutions to a key roadblock in improving EV cybersecurity. Without a comprehensive inventory of what lies within your product, you can't assess, improve, or mitigate its threats and vulnerabilities. You need a quality SBOM—linked with relevant vulnerability, weakness, and exposure data—to be able to meet the challenge of improving your product security, or the product security of an upstream supply chain partner. SBOMs remove some of the mystery behind the vulnerabilities that may be lurking within software, whether it's software that passed through your own product security process, or code that's come from your software supply chain lifecycle. While EV makers face the same pressures as other organizations—speeding time-to-market and reducing costs—it's important to prioritize the cybersecurity of the electric vehicles to which consumers entrust their lives. That can come through making real commitments to understanding the components that make up their products, as well as the code that makes them run. (Read the full article here: Finite State)

Other Resources: Upstream, NREL, The Hill, Axios, GovTech



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


If they can hack the EV charging stations, maybe I can hack the local fuel pumps as well and lower the price... he he he!

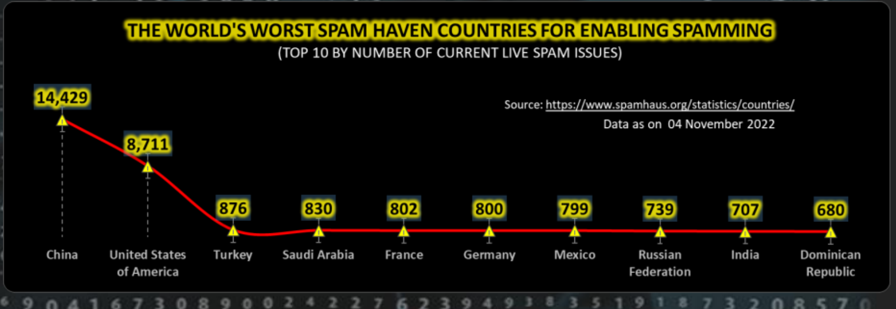
Other Interesting News and Cyber Security bits:

- Banker Oleg Tinkov renounces Russian citizenship over Ukraine
- Russia threatens commercial satellites that Pentagon sees as its future
- SANS Daily Network Security Podcast (Storm cast)

flightradar24 LIVE AIR TRAFFIC
Track any Aeroplane in flight globally

Marine Traffic
Track any Sailing Vessel globally

SatelliteXplorer
Track satellites in orbit



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