On July 5, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google and Mozilla products.
CIS Security Advisories

CISA Releases Three Industrial Control Systems 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
07 July 2023

In The News This Week

China's Mustang Panda Linked to SmugX Attacks on European Governments

Attackers use HTML smuggling to spread the PlugX RAT in the campaign, which has been ongoing since at least December. - A Chinese threat group has adopted a sneak HTML technique long-used by its counterparts to target European policy-makers, in a campaign aimed at spreading the PlugX remote access Trojan (RAT). Over the course of the last two months, Check Point Research (CPR) analysts have been tracking the activity, which they've dubbed SmugX because it uses an attack vector called HTML Smuggling — a technique for planting malicious payloads inside HTML documents, the researchers revealed in a report published earlier this week. The campaign has been ongoing since at least December and appears to have a direct link to a previously reported campaign attributed to Chinese APT RedDelta, as well as the work of Chinese APT Mustang Panda (aka Camaro Dragon or Bronze President), although there is "insufficient evidence" to definitively link SmugX to either group, according to the research..... Read the rest of the story by Elizabeth Montalbano here: Dark Reading

INTERPOL Nabs Hacking Crew OPERA1ER's Leader Behind $11 Million

A suspected senior member of a French-speaking hacking crew known as OPERA1ER has been arrested as part of an international law enforcement operation codenamed Nervone, Interpol has announced. "The group is believed to have stolen an estimated USD 11 million -- potentially as much as 30 million -- in more than 30 attacks across 15 countries in Africa, Asia, and Latin America," the agency said. The arrest was made by authorities in Côte d'Ivoire early last month. Additional insight was provided by the U.S. Secret Service's Criminal Investigative Division and Booz Allen Hamilton DarkLabs. The financially motivated collective is also known by the aliases Common Raven, DESKTOP-GROUP, and NXM. Its modus operandi was first exposed by Group-IB and Orange CERT Coordination Center (Orange-CERT-CC) in November 2022, detailing its intrusions on banks, financial services, and telecom companies between March 2018 and October 2022....
Read the full story by Ravie Lakshmanan here: The Hacker news

Cl0p's MOVEit Campaign Represents a New Era in Cyberattacks

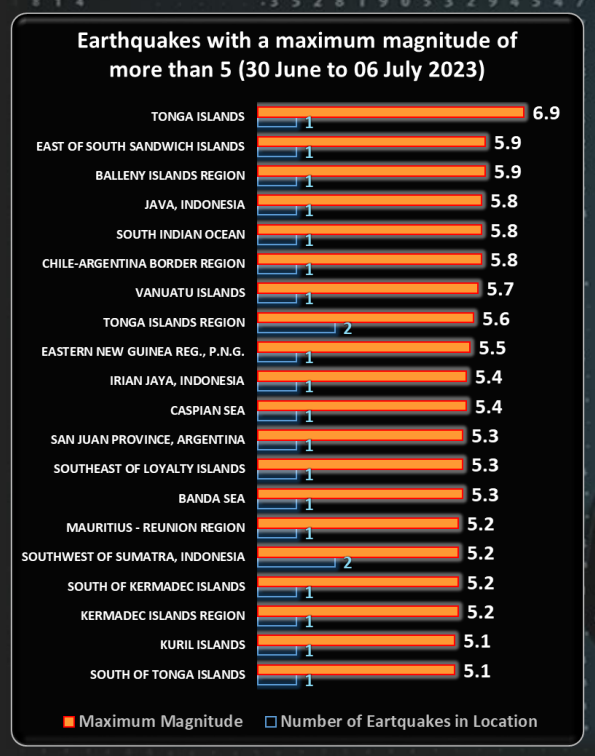
The ransomware group shows an evolution of its tactics with MOVEit zero-day — potentially ushering in a new normal when it comes to extortion supply chain cyberattacks, experts say. - The MOVEit file transfer zero-day vulnerability, first discovered on June 1, was used to breach at least 160 confirmed victims by June 30. The successful mass extortion campaign represents an evolution of tactics by the Russian-backed Cl0p ransomware group, which experts say is likely to catch the attention of rival threat actors. Threat researchers note that the MOVEit campaign has some clues about how to respond to future of supply chain cyberattacks for defenders as well. So far, the breached organizations include a who's who of international brands, like Avast's parent company, British Airways, Siemens, UCLA, and more. Reports say the ransomware group pulled off the technically detailed mass exploitation after at least two years of careful development, patiently plotting and planning when and where to strike, armed with the secret flaw in the MOVEit file transfer software.
Read the rest of the article by Becky Bracken here: Dark Reading

Dutch Critical OT Systems Vulnerable to Hacks

Critical services in the Netherlands could be a potential target of ransomware and hacktivist attackers with ties to Russia as a means to sow large-scale disruptions in the country, according to a Dutch National Cyber Security Center warning this week. Although the Russian invasion of Ukraine did not immediately result in a high level of attacks as anticipated, the Dutch NCSC said the country continues to experience a high volume of attacks compared to previous years. These attacks include an influx of ransomware, hacktivist, espionage activities from groups with political affiliations to Russia. Though these incidents have not led to major disruptions, the agency warned the Netherlands is likely to face "dynamic, complex and broader threat," especially against critical infrastructure, in the coming years. The country's operational technology networks, including industrial automation and control systems, are particularly at risk because they tend to be "insecure by design," the agency warned.... Read the full article by Akshaya Asokan here: Bank Info Security

Australian horse riding organisations caught up in cyber attack impacting 10,000 people

Cyber criminals have followed through on their threats of leaking the sensitive details of 10,000 people, after the company refused to bow to their extortion attempts. - Last month, the data of a little-known company called Event Secretary was published on an online forum. Unfortunately, Event Secretary was the platform that several major Australian horse-riding organisations used to book and enter equestrian competitions, and this has exposed riders and other admin users to hackers. In fact, Event Secretary was involved in the running of multiple events, including an international level event which is used for Olympic qualifications..... Read the full article by Alex Turner-Cohen here: News AU



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

Shared from an anonymous source on WhatsApp

ADD COMMAS TO YOUR PASSWORDS TO MESS WITH THE CSV FILE THE HACKERS USE TO DUMP IT INTO AFTER BEING LEAKED

Smart Home Security

Many homeowners have embarked on either some or a full home automation journey in the last couple of years which in most cases means that you can control these smart home systems via the Internet from any point on the globe that has Internet coverage. And, as you all know by now, this convenient connectivity to these systems comes with its own security challenges. I myself started the journey some time back and I must say, the convenience of monitoring and managing some of my appliances and my solar energy system from afar is all the money worth I spent on it. Today, I want to share an extract of a recent post by Pam Baker, published on The Verge, that addresses some of the questions and challenges around smart home security.

To worry or not to worry: answering questions about smart home security

You've heard the stories about safety issues of smart home devices — but are those stories fact or fiction? Here are some answers on what are and are not legit concerns.

If you're worried about security and data privacy in your smart home, believe me, you're not alone. "Considering that two-thirds of consumers agree it is impossible to keep data completely secure, it's no surprise that 55 percent are 'very concerned' — rating 6-7 on a 7-point scale — about personal data security," says Chris White, research director at Parks Associates, a consumer technology research firm.

Concern is not unwarranted, given that data breaches make the news headlines regularly. Some of those news stories are closer to home than others. Take, for example, the recent Amazon Ring settlement with the FTC for $5.8 million for alleged privacy and security violations.
"The FTC complaint makes it clear that this practice ceased after Amazon acquired Ring," says Cobun Zweifel-Keegan, managing director, DC, of the International Association of Privacy Professionals (IAPP), a not-for-profit global information privacy community and resource. "Other companies are hopefully closely watching this FTC enforcement and ensuring that their internal access controls ensure unauthorized access to video data does not happen."

Amazon was hit with another $25 million in penalties for Alexa violations of the Children's Online Privacy Protection Act Rule (COPPA Rule). "Last week's FTC action against Amazon's Alexa service alleged that the company was using some of these audio recordings and transcripts to help improve its speech recognition capabilities. The fact that children's voices could be captured and might be used for training models [algorithms] even after the audio files were deleted was a problem for the FTC," says Zweifel-Keegan. That's likely an issue with many parents as well....

Taking steps to ensure your personal data remains private and secure is always prudent. However, going overboard won't accomplish the goal. It's important to know which devices and circumstances pose a potential threat and which likely don't. That way, you'll know what to do to protect your data. To help you sort out the risks, here are solid answers to a few common concerns about smart home privacy and security.

Is my smart speaker listening to me? Why, yes, it is. But it is only "always listening" for when you say its wake word. That's when it will start to record and then analyze your words. "While it's a common belief that smart home devices are always monitoring you, that's not entirely accurate. They typically only record or listen when you use a specific wake word or command," says Doug Roberson, COO at Allterco, which offers a smart home automation product line called Shelly.
"However, it's crucial to remember that smart assistants are essentially voice-operated search engines, and these services often generate revenue through advertising. You can enhance your privacy by choosing an unusual wake word, if possible, [to prevent unwanted accidental recordings] and by regularly deleting stored data from your account," Roberson adds. Whether a company uses its smart assistant for advertising depends on which you're using. Apple is one of the only companies that has stated categorically that it doesn't use its assistant (Siri) to build a marketing profile....

Does my smart home know everything about me? Smart home devices need access to some personal data in order to provide you with the best service so that the information they provide is both relevant and tailored to your personal preferences and circumstances, such as your location for weather reports. But giving wide access to your personal data feels risky.
"Commercial smart home systems rely on a wide range of sensors to collect data about the environment, some of which may be personal data or could be used to infer personal data," says IAPP's Zweifel-Keegan. "Microphones and cameras are widely understood, but consumers may not recognize ultrasound sensors or spatial mapping systems that may be incorporated into smart speakers and virtual reality headsets, for example," that could be used to collect or infer information, such as your location within your house.
Keeping an eye on what data is collected and how companies are collecting it, as well as how they use it and protect it after collection, is key to keeping your family's information private. Most companies adhere to general privacy standards and consumer protection laws. But it's prudent to be aware of each company's data privacy policies....

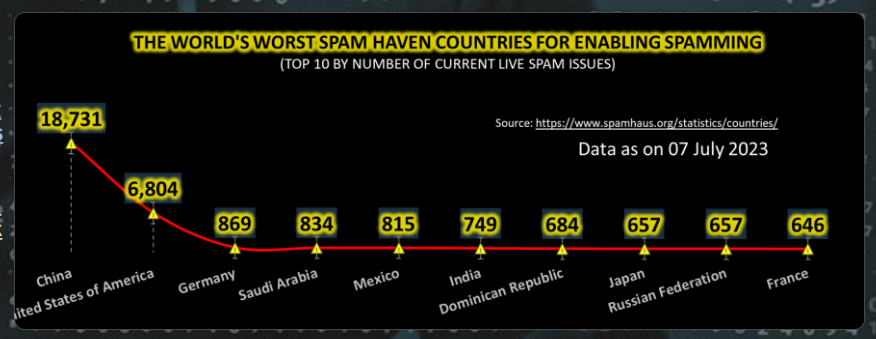
Can my smart lock be hacked? It's true that nothing on this earth is unhackable. However, it is also true that no physical lock is unbreakable.
"Both smart locks and regular locks are ultimately vulnerable to a strong brute-force attack. If someone comes at your door with a police-style battering ram, there's not a lot you can do to keep them out. Beyond that, traditional locks can be picked; smart locks [without keyways] can't. That in itself makes smart locks safer," says Rob Gabriele, home security expert at SafeHome.org, a provider of home security products.
The important thing to remember is that you want to make breaking into your home so difficult that it simply isn't worth the effort. In the case of physical locks, physical attributes matter most. In the case of smart locks, buying from reliable vendors is an absolute must....

Can someone access my security camera video footage? The most publicized smart home camera hacks have come from security company employees acting improperly to spy on customers or from outside hackers gaining access to your login information via phishing and other means. A camera company could also provide police and other law officials access to your footage without your permission or knowledge. The list goes on, but at issue is a basic lack of control over videos that can reveal quite a lot about your personal life.
The best way to prevent your smart home cameras, including security and nanny cams, from being hacked is to buy them from well-known vendor. (their reputation are key for staying in business)....
That is all I have space for in this post, please visit "The Verge" site to read this and more topics on smart home security

Other Interesting News and Cyber Security bits:

- Chatbot showdown: ChatGPT, Google Bard, and Bing Chat put to a real-world test
- Will AI take programming jobs or turn programmers into AI managers?
- Surviving the 800 Gbps Storm: Gain Insights from Gcore's 2023 DDoS Attack Statistics
- SANS Daily Network Security Podcast (Storm cast)

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



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