On November 30, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google 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
02 December 2022

In The News This Week

New LastPass Hack Confirmed—Here's What We Know So Far

On Wednesday, 30 November, LastPass CEO, Karim Toubba, confirmed that an unauthorized party had gained access to "certain elements of our customers' information" within a third-party cloud storage service. The data breach was, Toubba stated, made possible using information obtained from a previous hacking incident in August this year. At that time, Toubba said that portions of source code and some proprietary LastPass technical information had been accessed. It is not clear, however, what specific information enabled the threat actor to gain access to the cloud storage service in the latest breach. At this early stage in the investigation, Toubba said that work is underway to determine the scope of the breach and the specific nature of the customer information that has been accessed. "Our customers' passwords remain safely encrypted due to LastPass's Zero Knowledge architecture," Toubba confirmed. This, as in the August breach, is good news for users of the LastPass password manager. However, a single breach confirmation, let alone two within the space of four months, will not inspire confidence in a business whose sole function is security. Read the rest by Davey Winder here: Forbes

Breaking down the cybersecurity risks at Elon Musk's Twitter

A massive Twitter staff exodus in the first month of Elon Musk's ownership is only exacerbating the company's long list of existing data security problems, experts tell Axios. - Why it matters: While Twitter's list of cybersecurity challenges hasn't appeared to change yet, dwindling staff numbers mean the company could struggle to fix security flaws or respond in the event of a massive hack. The departures of Twitter's chief information security officer and other top security employees have created a new layer of concern about the company's long-existing data-security issues. The big picture: Twitter already had a troubled history of data breaches, account takeovers and poor internal cybersecurity hygiene. Earlier this year, former Twitter CISO Peiter "Mudge" Zatko filed a whistleblower complaint detailing the extent of Twitter's security problems, from a lack of employee access controls to a company culture that failed to take cybersecurity seriously. In 2020, a 22-year-old hacker broke into Twitter and took over accounts belonging to then-presidential candidate Joe Biden, former President Barack Obama and Musk himself..... Read the full story by Sam Sabin here: Axios

UK strikes digital trade deal with Ukraine

The digital trade agreement was struck at a London meeting of Trade Secretary Kemi Badenoch and Ukraine's Minister for Trade and Economy Yulia Svyrydenko. Trading digitally is particularly valuable, the UK government argues, because war and damage to Ukrainian infrastructure makes trading physically difficult. It is hoped the agreement will help bolster Ukraine's beleaguered economy. According to the Department for International Trade (DIT) it is hoped the agreement will help the UK and Ukraine make their digital identity systems work together. There is critical need for people who have lost documentation or been forced by the war to travel to new countries to be able to use digital tools to prove they are who they say they are, it said. The deal will also enable deeper cooperation on cybersecurity and help smooth flows of cross-border information between financial services firms an explanatory note says.. Read the article here: BBC News

Sony and Lexar-trusted encryption provider leaked sensitive data for over a year

ENC Security, a Netherlands software company, had been leaking critical business data since May 2021. - When you buy a Sony, Lexar, or Sandisk USB key or any other storage device, it comes with an encryption solution to keep your data safe. The software is developed by a third-party vendor – ENC Security. Netherlands-based company with 12 million users worldwide provides "military-grade data protection" solutions with its popular DataVault encryption software. As it turns out, ENC Security had been leaking its configuration and certificate files for more than a year, the Cybernews research team discovered. "The data that was leaking for over a year is nothing less than a goldmine for threat actors," Cybernews researcher Martynas Vareikis said. The company said a misconfiguration by a third-party supplier caused the issue and fixed it immediately upon notification.". Read the full story by Jurgita Lapienytė here: Cybernews

Self-Replicating Malware Used by Chinese Cyberspies Spreads via USB Drives

A China-linked cyberespionage group tracked as UNC4191 has been observed using self-replicating malware on USB drives to infect targets, and the technique could allow them to steal data from air-gapped systems, Google-owned Mandiant reports. UNC4191 has been observed targeting public and private entities in Southeast Asia, Asia-Pacific, Europe, and the US, with a focus on the Philippines, deploying legitimately signed binaries to side-load malware. As part of the investigated activity, the threat actor has used malware families such as the Mistcloak launcher, the Darkdew dropper, and the Bluehaze launcher. The attackers also deployed the NCAT command-line networking utility (for file download and upload purposes) and a reverse shell on the target machine, to achieve backdoor access to the compromised system...
Read the rest of the article by Ionut Arghire here: Security Week

Where does your IoT devices come from, and does it matter?

IoT devices have been at the center of many security talks and concerns in the last decade as many of these devices have hidden features built in that we don't always know about. These features could have been built in with no ill intent and are meant for manufacturers to update software or firmware when flaws are identified, or if a stolen device needs to be disabled. For example, as we learned in the looting riots in South Africa in the not-too-distant past, Samsung Smart TVs had a built-in feature that enabled the manufacturer to disable the stolen devices remotely. With that said, on the other side of the coin is manufacturers that deliberately build in hidden features that could allow them to hack into devices and connected networks. The fact is that these features exist and whether for good or bad intent, it leaves some sort of a doorway open that can be hacked or exploited by bad actors. With that on the table, Carsten Rhod Gregersen, CEO of Nabto posted a short piece in HelpNetSecurity this week that talks a little about the importance of where your IoT device comes from.

IoT device origin matters more than ever – by Carsten Rhod Gregersen
Recently, British politicians called on the government to crack down on the use of surveillance equipment from two Chinese companies, Hikvision and Dahua, which are already blacklisted by Washington. Not only did ministers criticize the state-owned companies as national security and cybersecurity threats, but they also brought into question their human rights record.
This story is not an outlier. From hard-coded admin passwords to "always-on" cloud features, cheap smart / connected devices with limited privacy or regulatory standards – largely from the Asian superpower – have flooded the market over the past decade.
It's clear that these connected devices pose major security risks to the public and private sectors. In this context, device buyers should consider where their devices come from and regional regulations. Let's look at why the origin of connected devices today matters more than ever.

The problem with devices from China - The Internet of Things (IoT) has grown in leaps and bounds over the past decade. In fact, the number of connected devices produced and sold has increased 10 times since 2012, to more than 16 billion worldwide. Powered by smaller, cheaper, and more efficient components, most of this growth comes from Chinese companies. But Chinese connected tech is notorious for low cybersecurity standards (and the companies for not respecting human rights).

Case in point: Hikvision. Cameras from this state-owned video surveillance manufacturer and supplier proclaim advanced capabilities such as facial recognition, person tracking and gender identification. The company claims its cameras can even detect emotion. However, human rights groups flag that the technology is abused for ethnic profiling of Uyghurs and other groups in Xinjiang. Meanwhile, Hikvision's state ownership raises additional data storage and retention questions.

And then there are the cybersecurity vulnerabilities. In the past, hackers have successfully exploited internet ports in Hikvision cameras to gain access without a username or password. Then, once inside, the remote attacker can use this entry to explore the entirety of the victim's network. Despite owning about 40% of the global surveillance camera market, Hikvision is increasingly blacklisted by Western governments for the above issues. In August, New Zealand joined the United States in banning equipment from the company. Around the same time, more than 60 parliament members across the United Kingdom called for a public sector ban. Minister David Davis called the devices "invasive and oppressive" that pose "a significant threat to civil liberties."

Device origin is more important than ever - Hikvision is but one example in an ocean of questionable tech from China. State ownership, ethical pitfalls and cybersecurity problems are unfortunately par for the course for these devices. Why? Undoubtedly one reason is that product quality and security superiority is sacrificed in a race for the lowest price. Meanwhile, another reason is a lack of consumer protections. Unlike other regions of the world, China counts few cybersecurity or privacy protections. As a result, devices are eminently more hackable and therefore dangerous.

On the other hand, consider the various rules and regulations which devices must comply with before hitting the market in Europe. The European Union's General Data Protection Regulation sets a very high standard on data protection and privacy. Additionally, the bloc is preparing to pass the European Cyber Resilience Act.

Publicly shared in September, the act would introduce "mandatory cybersecurity requirements for manufacturers and retailers ... with this protection extending throughout the product lifecycle." This includes the prohibition of default and weak passwords, support of software updates and mandatory testing for security vulnerabilities. Once passed, companies will have 24 months to get up to standard. Violating the new rules could impose fines of up to €15 million or 2.5% of a company's worldwide annual revenue (whichever is highest).

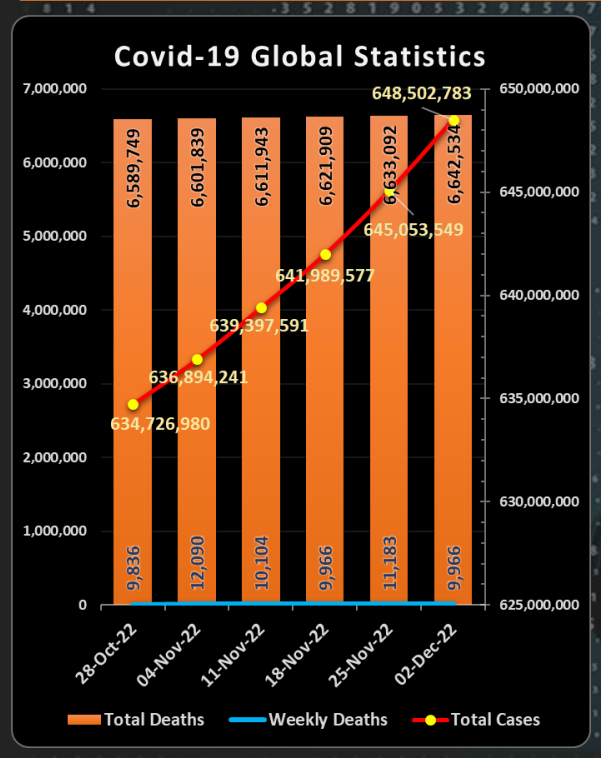
The differences between the two regions are night and day. For example, European manufacturers would be very unlikely to ship an entire line of products with a default password like "123456." In China, however, this not only happens but happens often. Moreover, Europe's new edict will now prevent manufacturers from setting such low cybersecurity levels and enforce stiff penalties.

For cybersecurity leaders, the difference between device cybersecurity and consumer protections could not be starker.

Think beyond price in your next purchase - My advice is to think beyond price. Sure, Chinese devices might be better for the bottom line, but they can also lead to very costly data breaches and open security holes into your home or workplace.

Likewise, remember that typical recommendations – such as changing default passwords or strict firewalling – will not always mitigate the whole range of issues. For example, millions of smart televisions from China have been shown to surreptitiously collect data about nearby networks and attached devices. Again, company and personal information security simply cannot be guaranteed based on the countless examples of dodgy devices from this part of the world.

Leaders: do your research, evaluate the risks and buy accordingly. You should take device origin into strong consideration. Your data is worth it..
Posted in HelpNetSecurity

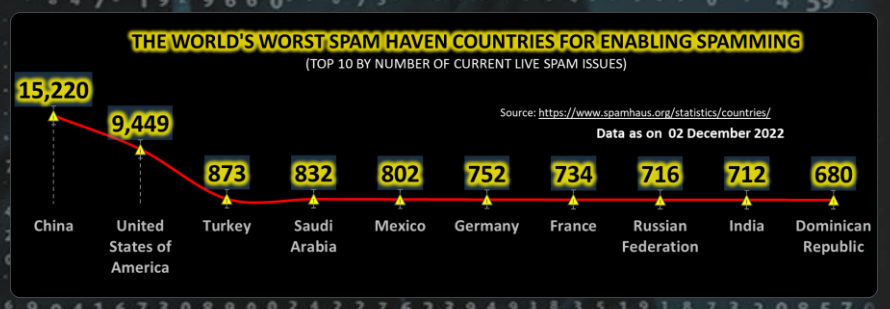


For Reporting Cyber Crime in the USA go to (IC3) , in SA go to Cybercrime, in the UK go to ActionFraud

Other Interesting News and Cyber Security bits:

- Zero trust to dominate cyber security in 2023
- World-first post-quantum biometric passport security demonstrated by Infineon, partners
- Sweden launches Europe's most advanced hub for automotive cyber security
- 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