On January 4, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to a vulnerability in Brocade Fabric OS.
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
06 January 2023

In The News This Week

Biden Signs Quantum Computing Cybersecurity Act

U.S. President Joe Biden signed the Quantum Computing Cybersecurity Preparedness Act into law last month to address the migration of federal agency systems to post-quantum cryptography (PQC) that can better resist attacks from quantum computers. The legislation required the Office of Management and Budget (OMB) to prioritize the post-quantum cryptography migration within a year after the National Institutes of Standards and Technology (NIST) issues post-quantum cryptography standards, which are expected to publish by 2024. It also asked OMB to submit a strategy to address the security risk posed by the vulnerabilities of agency information technology systems to the potential capability of a quantum computer and report ongoing coordination efforts with international standards development organizations for PQC standards. The act mentioned that Congress finds cryptography essential for national security and the functioning of the economy and notes the potential risks posed by "harvest now, decrypt later" attacks. "Quantum computers might one day have the ability to push computational boundaries, allowing us to solve problems that have been intractable thus far, such as integer factorization, which is important for encryption," the act states. Read the rest of the article by Nancy Liu here: sdxcentral

New Phishing Campaign Impersonates Flipper Zero to Target Cyber Professionals

Several social media accounts and fake websites are pretending to sell the sought-after hacking tool Flipper Zero to lure cybersecurity professionals into making cryptocurrency transactions. This new campaign of angler phishing – a type of social media phishing that involves impersonating corporate social media accounts to interact with their customers – was first uncovered by security researcher Dominic Alvieri on December 2, 2022. On Twitter, Alvieri warned of three distinct Twitter accounts and two websites impersonating the official Flipper Zero seller to lure potential buyers into sending cryptocurrencies – without sending them the Flipper Zero device in exchange.
At first glance, one of the Twitter accounts looked very similar to the official Flipper Zero. However, upon closer examination, the researcher discovered that the fake account's handle used a capital "I" instead of an "l." after the "F."r...
Read the full story by Kevin Poireault here: Infosecurity-magazine

Ransomware group LockBit apologizes saying 'partner' was behind SickKids attack

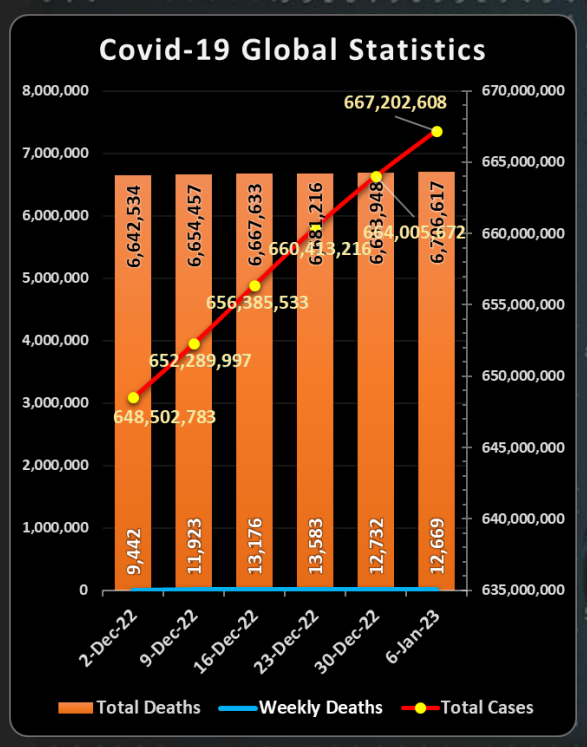
A global ransomware operator has issued a rare apology after it claims one of its "partners" was behind a cyberattack on Canada's largest pediatric medical centre. LockBit, a ransomware group the U.S. Federal Bureau of Investigation has called one of the most active and destructive in the world, posted a brief statement on what cybersecurity experts say is its data leak site claiming it has blocked its partner responsible for the attack on Toronto's Hospital for Sick Children and offering the code to restore the system. SickKids acknowledged Sunday it was aware of the statement and says it was consulting experts to "validate and assess the use of the decryptor," adding it has not made a ransom payment. The hospital has said last month's attack delayed lab and imaging results, knocked out phone lines and shut down the staff payroll system.
It says 60 per cent of its priority systems have since been brought back online and restoration efforts are "progressing well." Cybersecurity experts say even if SickKids decides to use a decryptor, they face the often lengthy and costly task of fully restoring the systems and potentially rebuilding their cybersecurity architecture to prevent another attack...
Read the full article here: CBC News

Twitter Whistleblower Joins Rapid7, a Cybersecurity Company

The former head of security at Twitter Inc., Peiter Zatko, is joining cybersecurity company Rapid7 Inc., following a whistleblower complaint to federal authorities last year in which he alleged security risks and mismanagement at the social media giant. Mr. Zatko's part-time role at Rapid7 will entail advising the company's executives and customers, including board members, on using data to make cyber decisions, a spokeswoman for the Boston-based company said. In a July whistleblower complaint, Mr. Zatko alleged Twitter lied about its computer security problems and failed to protect users' privacy. The filing was shared with the Securities and Exchange Commission, the Federal Trade Commission and the Justice Department, triggering investigations into Twitter's actions. Read the full story by Catherine Stupp here: The Wall Street Journal

Rackspace: Ransomware Attack Bypassed ProxyNotShell Mitigations

The hosting provider had not applied Microsoft's new patch due to publicly reported issues with the update. - Managed cloud hosting services company Rackspace Technology has confirmed that the massive Dec. 2 ransomware attack that disrupted email services for thousands of its small-to-midsized business customers came via a zero-day exploit against a server-side request forgery (SSRF) vulnerability in Microsoft Exchange Server, aka CVE-2022-41080. Karen O'Reilly-Smith, chief security officer for Rackspace, told Dark Reading in an email response. "Microsoft disclosed CVE-2022-41080 as a privilege escalation vulnerability and did not include notes for being part of a remote code execution chain that was exploitable." - CVE-2022-41080 is a bug that Microsoft patched in November. Read the full article by Kelly Jackson Higgins here: Dark Reading



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

Tech Support Opportunists

In recent months we saw numerous news reports of shadowy computer technicians that are doing more than they should when unsuspecting customers entrust their computers to the so-called computer expert for repairs. We also saw reports of criminals impersonating technicians of well-known and above-board support companies through E-mail scams or phone calls. Finding a trustworthy tech support company or person is not that easy and finding tech support online is risky. Even taking a device back to the store you bought it from is risky, who knows what the technician is doing with your data in the back room? Today I want to highlight one of these and offer some words of advice from the experts. The examples and links discussed are mostly North American, but these scams and activities are happening across the globe, and I urge you to apply the same vigilance in your own regions.

Geek Squad scam

Geek Squad Inc. is a subsidiary of American and Canadian multinational consumer electronics corporation Best Buy, headquartered in Richfield, Minnesota, and servicing the US, Canadian and Mexican market. It offers a tech support subscription service covering almost all electronic devices ranging from computers and cell phones to appliances and smart home setups.

Cybercriminals wield the Geek Squad name in various scams, knowing that some people will take the bait. Crooks often impersonate well-known brands and services as a form of social engineering. You trust these names, so you're likelier to fall for a trick. Scammers can contact you via phone call, text, email or even a pop-up on your computer. Here are five Geek Squad scams that you need to watch out for.

Phishing emails - Phishing scams are among the most common criminal campaigns, and email makes for a perfect delivery system. Crooks can send thousands of messages at once, and even a tiny percentage of success can net them big bucks. Let's say you get an email claiming that your annual Geek Squad security services plan has been renewed at $400 or more. But wait, you didn't have a subscription to begin with! The message uses eye-catching words, such as "charged," "transaction" and "payment mode," among others. It goes on to say that the renewal charge will be deducted from your account.

Pop-up scams - You're browsing the web and you get a pop-up claiming that your computer has been infected with malware or a virus. There's a number to call the Geek Squad and have them come to the rescue. Well, guess what? The pop-up and the number are both phony. Call them and you'll be handing over personal and financial information to a scammer. Komando Content Director Allie recently got a similar pop-up from McAfee claiming her subscription expired. She was also warned about being exposed to viruses and malware.

Remote access scam - When you have a problem with your computer, tech support can remotely access it to diagnose and fix it. This is a very risky move. If you let the wrong person in, they'll have free rein to do whatever they want on your computer. Scammers will tell you that Geek Squad needs to access your machine. They'll provide a link that will either open the door to your system or implant malware that gives them access to everything.

Refund scam - You'll get a message saying you overpaid for a service or have money owed to you for some reason. You call the provided number, and the person claims you need to pay a fee to unlock the funds you have coming to you. They'll often ask for payment in gift cards. One thing you should know: when you hear the words "gift card," get your guard up. It's more often than not a scam.

Ransomware/recovery scams - Once you've fallen for their tricks, scammers will go a step further and ask for payment to get back access to your own files. They'll either reveal they're crooks or continue posing as Geek Squad technicians. They'll demand money in exchange for your stuff or (you guessed it) ask for payment in gift cards.

Words of advice

Follow these tips and checks to distinguish a scam email from an original, real one:

1. Check the email content for spelling or grammar errors.
2. Inspect the scammer's email address and see if it contains the misspelled company name or if it looks pretty generic and so not official.
3. Check if the scammer addressed you by name. It's a scam if no name is mentioned anywhere, or you are only addressed as "Dear Sir/Madam."
4. Never click on links in emails. If you're not sure, use a link-checking website to make sure they don't redirect you to a random, unofficial address.
5. Is the transaction in the same currency as your bank account? The email is likely from a scammer if it's different.
6. Subscribers usually have a seven-day period to cancel their subscriptions. Be wary of emails that tell you to contact them within one to two days—the scammer is trying to cause you to panic and make a mistake.
7. Is the email you received from Geek Squad sent to the same email address you signed up with?
8. Does the email ask you to reply on the same email address as official support or a random one?
9. Check if this is a scam by confirming that no transaction has been made from your bank account.

In case you become a victim of the Geek Squad or any other email scam, here is what you should do:

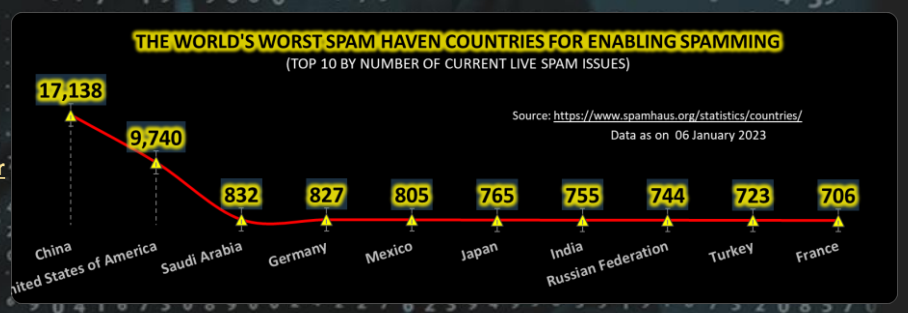
1. Don't act on anything they tell you to do if you have only spoken with the scammers.
2. To avoid scammers contacting you again, block the number you just called.
3. Call your bank and freeze your funds if you've shared your personal data, such as credit card information.
4. Check your computer for viruses if you've downloaded software or any files from the email.
5. You shouldn't use the same login details on numerous accounts, but many people do anyway. Change your login details immediately if you have signed up using a link scammers sent you using your email address.
6. To prevent scammers from recording you unknowingly, temporarily disable your webcam if it's enabled.

Resources: Komando, MUO, YouTube, Security Boulevard, Security Boulevard(2), Florida News, BestBuy

Other Interesting News and Cyber Security bits:

- Cost of a data breach 2022 - IBM Report
- Japan's new national security strategy is making waves
- Electronics repair technicians snoop on your data
- 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