On April 12, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google, Apple, Mozilla, Microsoft, Adobe, and Fortinet 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

14 April 2023

In The News This Week

LockBit 3.0 Posts Dubious Claims of Breaching Darktrace Cybersecurity Firm

LockBit 3.0, a notorious ransomware gang known for its high-profile and some time making up attacks, has claimed to have successfully hacked, prominent Cambridge, United Kingdom-based Darktrace cybersecurity company. The gang announced the breach on its dark web portal, where they posted images of Darktrace's CEO Poppy Gustafsson that are already publicly available. Although LockBit 3.0 claims to have published the alleged stolen data, clicking the download links on the gang's website only redirects users to Darktrace's official website. Darktrace, on the other hand, has issued a statement acknowledging the claims made by LockBit 3.0, but denying any breaches or malicious activity.
Read the rest of the post by Waqas here: Hack Read

Python head hisses at looming Euro cybersecurity rules

The Python Software Foundation (PSF) is concerned that proposed EU cybersecurity laws will leave open-source organizations and individuals unfairly liable for distributing incorrect code. "If the proposed law is enforced as currently written, the authors of open-source components might bear legal and financial responsibility for the way their components are applied in someone else's commercial product," the PSF said in a statement shared on Tuesday by executive director Deb Nicholson. "The existing language makes no differentiation between independent authors who have never been paid for the supply of software and corporate tech behemoths selling products in exchange for payments from end-users."...
Read the full story by Thomas Claburn here: The Register

Banning TikTok could weaken personal cybersecurity

TikTok is not be the first app to be scrutinized over the potential exposure of U.S. user data, but it is the first widely used app that the U.S. government has proposed banning over privacy and security concerns. So far, the discussion has focused on whether TikTok should be banned. There has been little discussion of whether TikTok could be banned, and there has been almost no discussion of the effects on cybersecurity that a TikTok ban could cause, including encouraging users to sidestep built-in security mechanisms to bypass a ban and access the app. As a cybersecurity researcher, I see potential risks if the U.S. attempts to ban TikTok. The type of risk depends on the type of ban. Read the article by Robert Olson here: The Conversation

AI-created malware sends shockwaves through cybersecurity world

See how ChatGPT could be used as a cyber weapon - ChatGPT has caused a lot of buzz in the tech world these last few months, and not all the buzz has been great. Now, someone has claimed to have made powerful data-mining malware by using ChatGPT-based prompts in just a few hours. Here's what we know. Forcepoint security researcher Aaron Mulgrew shared how he was able to create this malware by using OpenAI's generative chatbot. Even though ChatGPT has some protections that prevent people from asking it to create malware codes, Aaron was able to find a loophole. He prompted ChatGPT to create the code function by function with separate lines. Once all the individual functions were compiled, he realized that he had an undetectable data-stealing executable on his hands that was as sophisticated as any nation-state malware. Read the rest of the story by Kurt Knutsson here: Fox News

New Python-Based "Legion" Hacking Tool Emerges on Telegram

An emerging Python-based credential harvester and a hacking tool named Legion is being marketed via Telegram as a way for threat actors to break into various online services for further exploitation. Legion, according to Cado Labs, includes modules to enumerate vulnerable SMTP servers, conduct remote code execution (RCE) attacks, exploit unpatched versions of Apache, and brute-force cPanel and WebHost Manager (WHM) accounts. The malware is said to bear similarities to another malware family called AndroxGh0st that was first documented by cloud security services provider Lacework in December 2022. Cybersecurity firm SentinelOne, in an analysis published late last month, revealed that AndroxGh0st is part of a comprehensive toolset called AlienFox that's offered to threat actors to steal API keys and secrets from cloud services.
Read more by Ravie Lakshmanan here: The Hacker News

Pentagon super-leak suspect cuffed: 21-year-old Air National Guardsman

When bragging about your job on Discord gets just a little out of hand? - The FBI has detained a 21-year-old Air National Guardsman suspected of leaking a trove of classified Pentagon documents on Discord. In the past few minutes, US Attorney General Merrick Garland confirmed the arrest, saying Jack Douglas Teixeira of the United States Air Force National Guard in Massachusetts was nabbed earlier today. The suspect was being held "in connection with an investigation into alleged unauthorized removal, retention, and transmission of classified national defense information," the AG said. The Washington Post reported yesterday that whoever leaked the files was thought to be a twenty-something American who liked gaming and guns and worked on a military base. It's said he also controlled a private Discord server, and allegedly posted photographs of the classified Pentagon documents to impress the private group's 25 members... Read the full story here: The Register

My phone, my credit card, my hacker, and me

Today I want to share a story of someone whose phone was hacked and the subsequent turmoil that followed. The post below is an extract of the person's account of the events. (You can read the full post here: Insider)

Verizon, Chase, the police - they were all useless when my identity got hacked. Then Psycho Bunny came to the rescue

It was a Friday in July when I first noticed something seemed off. I was spending some time with my family on a gorgeous summer day, swimming and drinking beer and ignoring my phone as much as possible. When I finally checked my notifications, I had two alerts from Verizon. Both contained authorization codes - the kind of security measure they take when you make changes to your account. There was also a receipt from Verizon for $0 and a message thanking me for activating my new device. I immediately checked my Verizon account, but nothing seemed amiss. The receipt seemed like a glitch - as if Verizon had belatedly billed me for the phone, which I'd activated four months prior. In hindsight, I should have been more suspicious. I should have called Verizon right away. But why would I want to spend the day in customer-service hell when I could spend it on a boat?

The next morning, though, something else strange happened. When I went to send a text, I realized I didn't have service. I tried flipping cell service on and off, restarting my phone - nothing. I couldn't text and I couldn't make calls. I asked my fiancé to check for a local Verizon outage, but nothing turned up. I wondered whether maybe I was just in a dead zone, but I'd never had this problem before. And then I started to feel that slowly dawning sense of dread.

A few days earlier, my colleague Rob Price had published a terrifying story about hackers who waged a campaign of harassment and intimidation to steal Instagram handles and other coveted usernames on social media. Tucked into that story was a phrase I hadn't heard before, a type of hack I'd had to look up: SIM swapping. In a SIM swap, the hacker doesn't need to physically steal your SIM card - the thing in your phone that identifies it as your phone. They just pretend to be you and persuade an employee at your telecom provider to activate a new SIM card for them, using your phone number. Once that happens, your phone immediately loses service - and the hacker can now use your number to wreak havoc on your life. They can send messages to others pretending to be you, intercept texts from your bank, and even reset your passwords to lock you out of your own accounts.

SIM swapping hasn't been around long. It started in about 2018 as a way for gamers to steal other people's cryptocurrency, which is pretty easy to do once you have full access to someone's phone. But now, experts say, the crime has become more pervasive - and far more organized. In 2021, the FBI reports, SIM swaps robbed victims of more than $68 million. "You could think of these people as petty thieves," says Allison Nixon, the chief research officer at Unit 221b, a cybersecurity firm. "But after 2018, these are petty thieves that became millionaires."

I borrowed a phone and called Verizon, which confirmed I'd been SIM swapped. While I was vacationing in western New York, more than four hours away, the hacker had shown up at a Verizon store in Columbus, Ohio, pretending they were me, complete with a fake ID. They told a store employee their phone had been destroyed and asked to use my phone number to activate an older iPhone they'd brought with them.
I remembered that strange $0 receipt I'd gotten the day before and checked the store address at the bottom. Sure enough, it was from a Verizon store in the Columbus area.

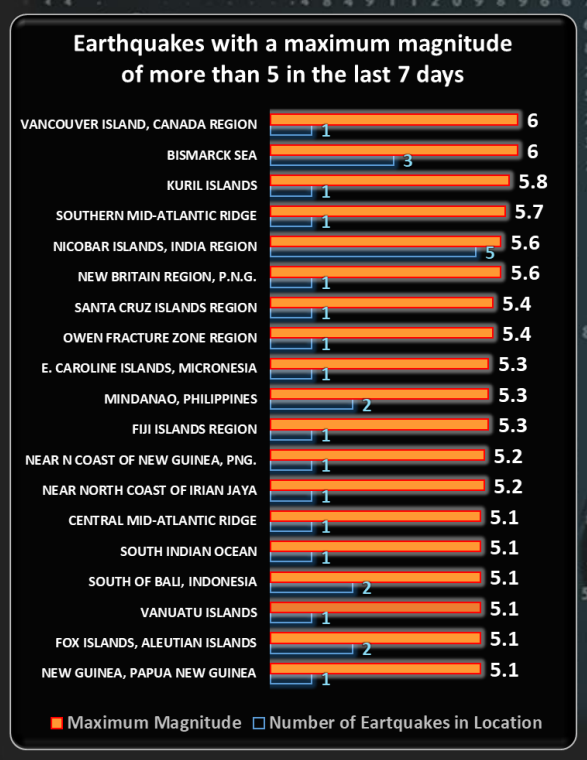
I was floored by how easily someone could steal my phone; surely it must have been a major screwup on the part of the store employee. But when I spoke with higher-ups at Verizon, they explained that their device-activation process had worked precisely the way it was supposed to. When two-factor authentication isn't possible - like when a phone has been lost, stolen, or destroyed - an ID card will suffice. All the hacker needed was a knowledge of the glaring loophole in Verizon's security, a phony piece of plastic, and a little chutzpah.
Verizon immediately deactivated the phone that belonged to the hacker and reinstated mine. But the employee I talked to warned me that this was probably just the beginning of the scam. - It turned out he was right.

Once the hacker had control of my phone number, they didn't waste much time. They left the Verizon store and went to a nearby Apple store, where they used my Chase credit card to spend $6,370. Then they drove to a mall across town to shop at Gucci, where they made two separate transactions totaling $2,956. They finished at a clothing store called Psycho Bunny, where they spent about $452. All told, they racked up nearly $10,000 in purchases on my card in just a few hours. The next morning, perhaps testing their luck, they tried to make another purchase at Best Buy. But this was after I'd spoken with Verizon and locked my card. So, they just opened a Best Buy credit card in my name instead.

Still, something about all the transactions kept bugging me. I noticed that the hacker never logged in to my Chase account or my social-media accounts - they just racked up charges on my card. I couldn't figure out why they needed my phone number in the first place. But when I scoured my text logs, I realized what they were up to. Chase, aware that I don't typically spend $10,000 in a single afternoon, sent out fraud alerts via text each time the hacker tried to make a big purchase. I could see in my text logs that each time a fraud alert came in, the hacker used my phone to respond, allowing the charges to go through.

That mystery was easily solved. But there was something else I couldn't figure out: How did the hacker make so many purchases on my card in the first place? I could see in my account that the charges had occurred at physical stores, not online. The hacker never logged into my iCloud account to set up Apple Pay, and my credit card had been safely tucked into my wallet the entire time.

I decided to call each of the stores where the hacker went shopping, to try to figure out what happened. I tried Gucci first. A representative at a centralized Gucci switchboard informed me that Gucci doesn't even have telephone numbers for its individual retail locations, and that the only way to learn more about how the purchase was made would be to visit the store. Given that I was back home in New York City, more than 14 hours away, I decided to try my luck at Apple. Apple was equally unhelpful.... I decided to give it one last shot with Psycho Bunny, a menswear retailer. A helpful store manager looked in the store's system and confirmed that yes, someone who said their name was Avery H. had made a purchase of $452 using my card number. The shopper had even supplied a phone number that was one digit off from mine, the manager said. .... Disheartened, I hung up...Then, about 15 minutes later, my phone rang. It was the store manager, calling back. She and her team had decided to go through the security footage from the day the purchase was made, and they'd found footage of the thief standing at the store counter. ..... Read the rest here: Insider

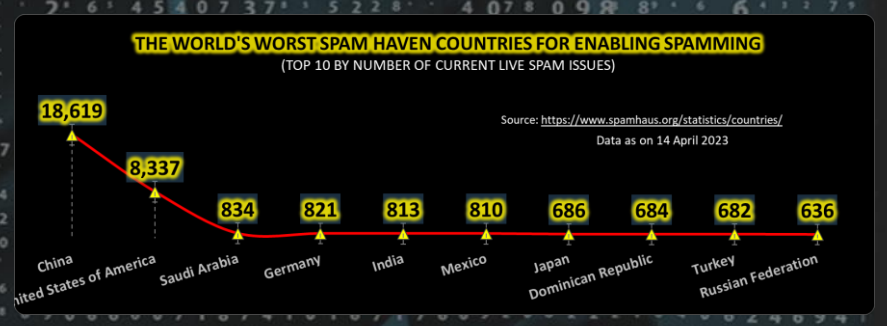


For Reporting Cyber Crime in the USA go to (IC3) , in SA go to Cybercrime, in the UK go to ActionFraud

Other Interesting News and Cyber Security bits:

- Bizarre object 10 million times brighter than the sun defies physics, NASA says
- Juice mission delayed: The European Space Agency's mission to find alien life on Jupiter's moons
- Were you caught up in the latest data breach? Here's how to tell
- 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