On June 21, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in MOVEit and Citrix 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
23 June 2023

In The News This Week

Russian APT Group Caught Hacking Roundcube Email Servers

A Russian hacking group has been caught hacking into Roundcube servers to spy on government institutions and military entities in Ukraine. - A prolific APT group linked to the Russian government has been caught exploiting security flaws in the open-source Roundcube webmail software to spy on organizations in Ukraine, including government institutions and military entities involved in aircraft infrastructure. According to an advisory from threat intelligence firm Recorded Future, the Roundcube server infections are being used to run reconnaissance and exfiltration scripts, redirecting incoming emails and gathering session cookies, user information, and address books. Recorded Future teamed up with Ukraine's Computer Emergency Response Team (CERT-UA) to document the activity, which is being attributed to Russia's GRU military spy unit...
Read the full article by Ryan Naraine here: Security Week

Why is it so rare to hear about Western cyber-attacks?

A cyber-attack that took over iPhones at a Russian technology company is being blamed on US government hackers. Could the attack, and the response from the Russian government, be rewriting the narrative of who the good guys and bad guys are in cyber-space? Camaro Dragon, Fancy Bear, Static Kitten and Stardust Chollima - these aren't the latest Marvel film superheroes, but the names given to some of the most feared hacking groups in the world. For years, these elite cyber teams have been tracked from hack to hack, stealing secrets and causing disruption allegedly under orders from their governments**. With dots** on a world map, marketeers at these companies regularly warn customers about where these "advanced persistent threats" (APTs) are coming from - usually Russia, China, North Korea and Iran. But parts of the map remain conspicuously empty.
So why is it so rare to hear about Western hacking teams and cyber-attacks? A major hack in Russia, unearthed earlier this month, might provide some clues.. Read the full article by Joe Tidy here: BBC news

Almost 770,000 Calpers members hit by cyber attack

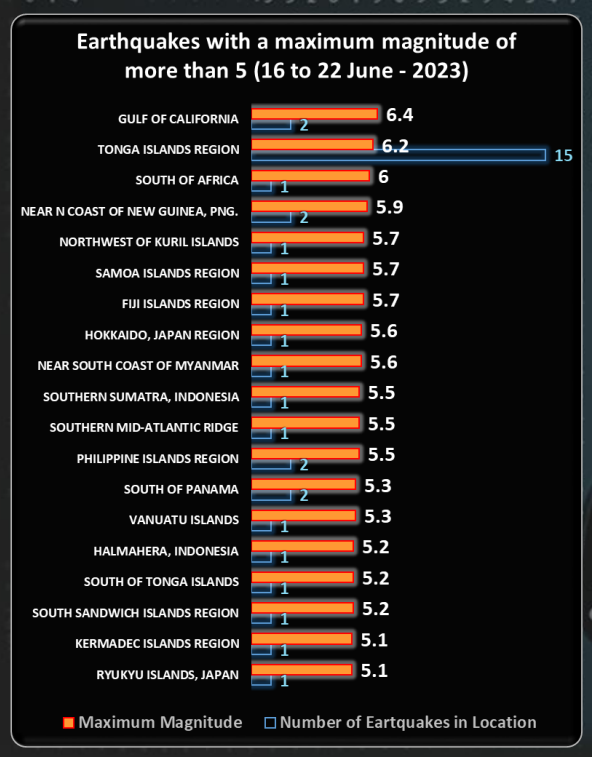
Calpers, the biggest public pension plan in the US, has become the latest organisation to be hit by the MOVEit cyber attack with about 770,000 of its members affected by the global data breach. In a statement published on its website, the $442bn pension fund alerted its retired members and their families that some of their personal information, including dates of birth and social security numbers, were downloaded during an incident impacting its contracted third-party provider PBI Research Services/Berwyn Group. The incident involved the MOVEit file transfer service.. Read more here: Financial Times

Luno launches Ethereum staking — earn rewards for helping secure the network

South African-born cryptocurrency exchange and wallet provider Luno has launched Ethereum staking. "Luno's staking feature will initially launch in South Africa with support for [Ethereum]," said Luno South Africa country manager Christo de Wit. "Customers simply open a staking wallet and can earn up to 4% per year in ETH by holding (hodl in crypto-speak) ETH." De Wit explained that the reward rate could fluctuate depending on the demand on the network and the number of active validators. "Rewards will be paid weekly, so you can automatically grow your stake and compound your rewards," he said. Rewards are paid in cryptocurrency every five days, and there is no minimum deposit requirement. There is no fee to stake or unstake, but Luno said it would deduct a staking service from the reward customers receive. Luno said that while they are staked, customers cannot sell or send their coins, but they can unstake at any time and remove their ether from their staking wallets. Ethereum switched from its proof-of-work transaction validation system to proof-of-stake in September last year through an upgrade called The Merge. In April this year, Ethereum added the ability to unstake with the Shangai upgrade....
Read the full article by Jan Vermeulen here: My Broadband

Experts Uncover Year-Long Cyber Attack on IT Firm Utilizing Custom Malware RDStealer

A highly targeted cyber attack against an East Asian IT company involved the deployment of a custom malware written in Golang called RDStealer. "The operation was active for more than a year with the end goal of compromising credentials and data exfiltration," Bitdefender security researcher Victor Vrabie said in a technical report shared with The Hacker News. Evidence gathered by the Romanian cybersecurity firm shows that the campaign – dubbed RedClouds – started in early 2022. The targeting aligns with the interest of China-based threat actors. In the early phases, the operation relied on readily available remote access and post-exploitation tools like AsyncRAT and Cobalt Strike, before transitioning to bespoke malware in late 2021 or early 2022 in a bid to thwart detection. A primary evasion tactic concerns the use of Microsoft Windows folders that are likely to be excluded from scanning by security software (e.g., System32 and Program Files) to store the backdoor payloads..
Read the rest of the article by Ravie Lakshmanan here: The Hacker News



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

Crypto Currency in the Underworld

The first cryptocurrency was Bitcoin, which was first released as open-source software in 2009. As of March 2022, there were more than 9,000 other cryptocurrencies in the marketplace, of which more than 70 had a market capitalization exceeding $1 billion, which is huge. From a Cybersecurity perspective, however, this is not always good news as cryptocurrency is the primary payment method demanded by ransomware gangs and is pretty much untraceable. Although authorities are constantly on the hunt and are succeeding to close down some of these criminal crypto "laundromats", the battle stays constant. The moment one is shut, another surface. How do these cryptocurrency 'Laundromats' work and where are they?
I recently stumbled on an article that I want to share that gives us some idea, but for most, it is still a mystery. I encourage you to follow some of the links in the resources section below to get a clearer picture, but I'll share the article by Andy Greenberg of Wired as a start.

Most Criminal Cryptocurrency Funnels Through Just 5 Exchanges

The crypto money-laundering market is tighter than at any time in the past decade, and the few big players are moving a "shocking" amount of currency. - For years, the cryptocurrency economy has been rife with black market sales, theft, ransomware, and money laundering—despite the strange fact that in that economy, practically every transaction is written into a blockchain's permanent, unchangeable ledger. But new evidence suggests that years of advancements in blockchain tracing and crackdowns on that illicit underworld may be having an effect—if not reducing the overall volume of crime, then at least cutting down on the number of laundering outlets, leaving the crypto black market with fewer options to cash out its proceeds than it's had in a decade.

In a portion of its annual crime report focused on money laundering that was published today, cryptocurrency-tracing firm Chainalysis points to a new consolidation in crypto criminal cash-out services over the past year. It counted just 915 of those services used in 2022, the fewest it's seen since 2012 and the latest sign of a steady drop-off in the number of those services since 2018. Chainalysis says an even smaller number of exchanges now enable the money-laundering trade of cryptocurrency for actual dollars, euros, and yen: It found that just five cryptocurrency exchanges now handle nearly 68 percent of all black-market cash-outs. In fact, Chainalysis saw just 542 cryptocurrency deposit addresses receive more than half of the $6.3 billion in total illicit funds it tracked to those cash-out services in 2022, and just four addresses received $1.1 billion of those funds.

That intense narrowing of so-called "off-ramps" for crypto crime is a result of an ongoing government crackdown on crypto money laundering and a sign of additional enforcement on the way, says Kim Grauer, Chainalysis' director of research. "It's shocking to see some of these deposit addresses moving more than a hundred million dollars in illicit funds and still operating when it's something that's extremely transparent and easy to see with blockchain analytics," Grauer says. "So, it does seem like a good chokepoint, where we can shut down and profile and—to some degree—eradicate this activity."

Whether the overall amount of crypto crime rose or fell in 2022, meanwhile, is far from clear: By some measures, Chainalysis' data has shown that criminal use of cryptocurrency increased last year despite the steep decline in cryptocurrency exchange rates. But those numbers include a huge spike in illegal transactions at sanctioned cryptocurrency exchanges—which may have less to do with a rise in crime than with the US Treasury's Office of Foreign Asset Control (OFAC) increasingly imposing those sanctions on major players in the crypto underground. In April of last year, for instance, OFAC sanctioned Garantex, an exchange based in Russia that it says laundered over $100 million in criminal proceeds, including ransomware payments. The year before, it sanctioned two other Russian exchanges, Chatex and Suex, which have since gone out of business. And just last week, OFAC sanctioned another exchange, Bitzlato, and the Justice Department indicted its Russian founder, Anatoly Legkodymov, and tore his operation offline.

"You don't carry out a ransomware attack if there's no way of converting that ransom into something usable," says Grauer. "What we're really seeing OFAC doing, and what we've really highlighted, is that the money-laundering off-ramps are what's facilitating crime. And I think the ongoing crackdown has shown that people understand they're at a point where there can be meaningful intervention."

Chainalysis declined to name the five exchanges it says enabled the majority of cryptocurrency money laundering. That's because, the company says, those exchanges may be the targets of ongoing investigations. (Chainalysis often works with law enforcement agencies in those investigations.) Further, the exchanges may not actually be aware that they're enabling that money laundering, since money launderers often take pains to hide the source of their funds before it hits an exchange. In fact, Chainalysis found that a large chunk of the illicit cash-outs went through two types of intermediaries that might obfuscate criminal funds: Many were traded through "nested services," essentially exchanges that appear to be independent but actually use a larger exchange to carry out their trades. In those cases, the nested service, rather than the underlying exchange, is often responsible for complying with "know-your-customer" requirements, even as the larger exchange provides the cash reserves for transactions.

In another growing subset of cases, Chainalysis says, criminals are turning to individual dark-web-based money-laundering services, many of which offer to hide the origin of funds by combining them with other users' transactions in a "mixer." As law enforcement has cracked down on major mixing services in recent years—seizing and tearing offline the mixers Bitcoin Fog and Helix and sanctioning the mixing service Tornado Cash, for instance—more criminals have turned to smaller dark-web services that Chainalysis' Grauer refers to as "mom-and-pop" mixers, whose distributed nature makes them harder to seize or disrupt. Despite its reluctance to name the top five money-laundering exchanges in its most recent report, in another report in February of last year Chainalysis did point to a collection of Russia-based exchanges it says have cashed out large sums of criminal proceeds.

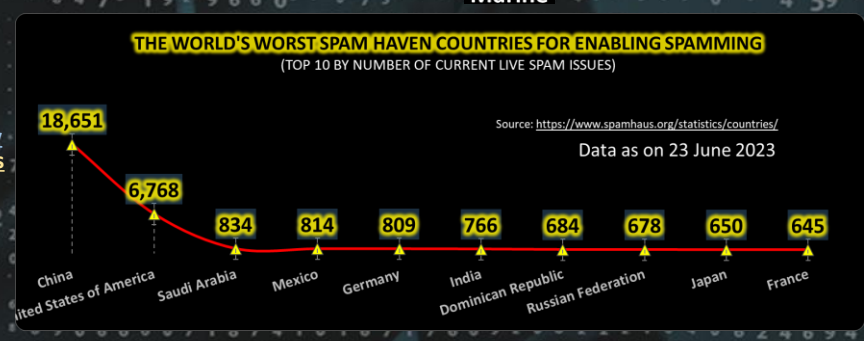
When WIRED reached out to the US Treasury, an official there declined to comment on any specific exchanges or ongoing investigations. The official, who asked to remain unnamed due to the sensitive nature of sanctions policies that are coordinated between multiple government agencies, also suggested that Chainalysis' data offered only one incomplete perspective on the crypto money-laundering landscape and that much of the consolidation it describes might simply be due to 2022's crypto crash and the resulting bankruptcy of several exchanges—particularly more "fly-by-night" ones with looser compliance rules..... That is all I have space for in this post, please visit WIRED to read the full article.

Resources: Investing, Bitcoinist, USN, Be(In)Crypto, & Sense, Tom's Guide, Apple

Other Interesting News and Cyber Security bits:

- How vertical farming can save water and support food security
- 5 ways generative AI will help bring greater precision to cybersecurity
- Security forum hears risks of quantum computing and threats to energy companies
- SANS Daily Network Security Podcast (Storm cast)

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



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