On January 25, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Sophos, Apple, Google, and VMware 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
27 January 2023

In The News This Week

T-Mobile Breached Again, This Time Exposing 37M Customers' Data

This time around, weak API security allowed a threat actor to access account information, the mobile phone giant reported. - T-Mobile has disclosed a new, enormous breach that occurred in November, which was the result of the compromise of a single application programming interface (API). The result? The exposure of the personal data of more than 37 million prepaid and postpaid customer accounts. For those keeping track, this latest disclosure marks the second sprawling T-Mobile data breach in two years and more than a half-dozen in the past five years...And they've been expensive.... Last November, T-Mobile was fined $2.5 million for a 2015 data breach by the Massachusetts attorney general. Another 2021 data leak cost the carrier $500 million; $350 million in payouts to affected customers, and another $150 million pledged toward upgrading security through 2023. Now the telecom giant is mired in yet another cybersecurity incident.
Read the full article by Becky Bracken here: DarkReading

NIST working on 'potential significant updates' to cybersecurity framework

The National Institutes of Standards and Technology intends to release version 2.0 of its Cybersecurity Framework in the coming years, and this week, the agency teased some of the "potential significant updates" that may land in that new framework. On Thursday 19 January 2023, NIST published a concept paper outlining significant changes to the Cybersecurity Framework and opening them to public feedback over the next several weeks. The framework is a voluntary guide to help organizations in all sectors to better understand, manage, reduce, and communicate cybersecurity risks. It is used widely, along with NIST's Risk Management Framework, by federal agencies to plan their own cybersecurity approaches. Of the proposed changes in the concept paper, the most notable are broadening the scope of the framework beyond critical infrastructure use cases to better include other organizations like small businesses and higher education institutions; including more guidance for implementation; and emphasizing the importance of cybersecurity governance and cybersecurity supply chain risk management, among others. These updates come directly from responses to NIST's cybersecurity request for information opened last February. Read the full article by Billy Mitchell here: Fedscoop

LastPass owner GoTo shares more bad news about November's security breach

GoTo, the remote collaboration and IT software company that owns LastPass, has confirmed that, along with LastPass' password vaults, it had customer data taken by attackers during a November 2022 security breach (via TechCrunch).
The company, which was formerly known as LogMeIn, is updating its blog post about the breach for the first time since November 30th, when GoTo confirmed "unusual activity" within its development environment and cloud storage service. Many of GoTo's enterprise products were affected, including Central, Pro, join.me, Hamachi, and RemotelyAnywhere. GoTo CEO Paddy Srinivasan writes that a hacker "exfiltrated encrypted backups from a third-party cloud storage service" and acquired the encryption key for a portion of them — nearly two months ago. The information taken varies by product but "may include account usernames, salted and hashed passwords, a portion of Multi-Factor Authentication (MFA) settings, as well as some product settings and licensing information." Read the full article by Umar Shakir here: The Verge

British Cyber Agency Warns of Russian and Iranian Hackers Targeting Key Industries

The U.K. National Cyber Security Centre (NCSC) on Thursday warned of spear-phishing attacks mounted by Russian and Iranian state-sponsored actors for information-gathering operations. "The attacks are not aimed at the general public but targets in specified sectors, including academia, defense, government organizations, NGOs, think tanks, as well as politicians, journalists and activists," the NCSC said. The agency attributed the intrusions to SEABORGIUM (aka Callisto, COLDRIVER, and TA446) and APT42 (aka ITG18, TA453, and Yellow Garuda). The similarities in the modus operandi aside, there is no evidence the two groups are collaborating with each other. The activity is typical of spear-phishing campaigns, where the threat actors send messages tailored to the targets, while also taking enough time to research their interests and identify their social and professional circles. The initial contact is designed to appear innocuous in an attempt to gain their trust and can go on for weeks before proceeding to the exploitation phase. This takes the form of malicious links that can lead to credential theft and onward compromise, including data exfiltration. To maintain the ruse, the adversarial crews are said to have created bogus profiles on social media platforms to impersonate field experts and journalists to trick victims into opening the links.
The Russian state-sponsored SEABORGIUM group has a history of establishing fake login pages mimicking legitimate defense companies and nuclear research labs to pull off its credential harvesting attacks.. Read the story here: The Hacker News

Cybersecurity Expert Warns Investors: These Are The Most Common & Potent Cyber Threats | Forbes (Video, 20 mins) - Richard Seewald, Founder and Managing Partner at Evolution Equity Partners, joins "Forbes Talks" to discuss the cybersecurity threats facing investors, companies, and the US. Watch the video here: Forbes

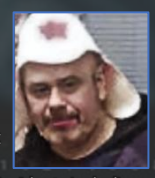
Meet the Cybercriminals of 2022

The year 2022 marked a significant increase in Cybercrime and state-sponsored Cyberattack activities, many of which were reported in this weekly post. The Russian invasion of Ukraine probably sparked most of the state-sponsored activities, but the Covid pandemic spawned a whole new breed of profit-seeking criminal conglomerates and individuals. As a horde of tech-savvy people lost their jobs and/or regular income streams, many of them turned to the Internet to look for alternative means to make a living. And so, the lure of a highly profitable "anonymous" Cybercrime world proved to be too good of an opportunity to let it go by. Many made millions without getting caught and are still out there, but some did get caught. Today I want to share extracts of a post by TechCrunch that highlight some of these.

Meet the Cybercriminals of 2022

Arrested, seized, doxed and detained. These are just some of the ways police and prosecutors around the world took down the biggest cybercrime operations of the year, even if it meant resorting to new and unconventional eyebrow-raising methods. From stashing billions of bitcoin under the floorboards to teenage hackers gatecrashing Fortune 500 networks, this year saw some of the most jaw-dropping breaches — and the highest-profile apprehensions. As the year closed out, we look back at the cybercriminals we lost in 2022... to the law...

Sanctions and seizures hit the crypto scene - U.S. officials scored some major wins against crypto-laundering in 2022. At the beginning of the year, the Justice Department said it had seized more than $3.6 billion worth of bitcoins allegedly stolen in the 2016 hack of crypto exchange Bitfinex and that it had arrested a married couple suspected of laundering the money. The couple — Ilya Lichtenstein, 34, and Heather Morgan, 31 — face up to 25 years in prison if convicted on charges of conspiring to launder money and defrauding the U.S. government.
Later in the year, the Office of Foreign Asset Control (OFAC), a watchdog within the U.S. Treasury tasked with enforcing sanctions violations, announced that it had sanctioned decentralized cryptocurrency mixing service Tornado Cash for its role in enabling billions of dollars' worth of cryptocurrency to be laundered through its platform.
Tornado Cash, along with other mixers such as AlphaBay, allows customers to conceal the source of their crypto funds when participating in a transaction in exchange for a fee. It blends potentially identifiable or tainted cryptocurrency funds with others to obfuscate the source and destination of crypto assets. More than $1.5 billion in proceeds of crime, like ransomware and fraud, has been laundered through Tornado Cash to date, experts estimate.



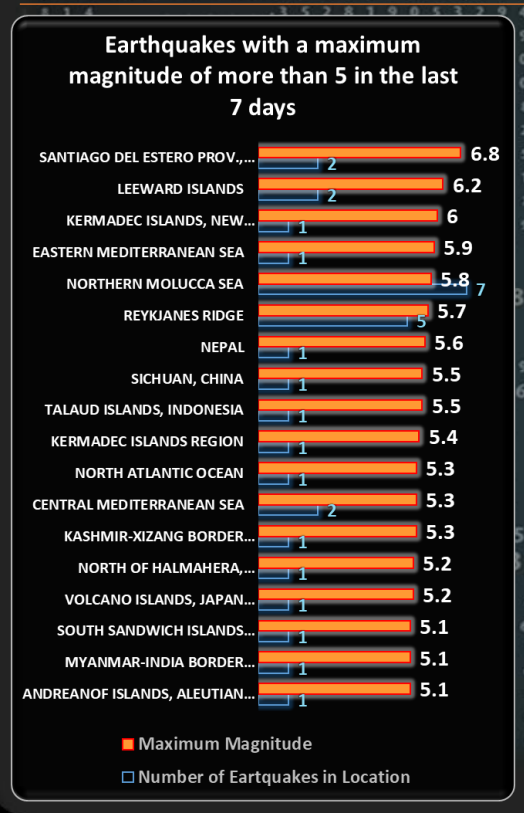
U.S. doxes alleged Conti ransomware member - In August, the U.S government shared an image of a suspected Conti ransomware operator known as "Target," the first time it has outed a major ransomware actor. The program also offered up to $10 million for information leading to the identification and location of Target, along with four other alleged Conti members known as "Tramp," "Dandis," "Professor" and "Reshaev." The State Department said Conti has carried out more than 1,000 ransomware operations targeting U.S. and international critical infrastructure. Most recently, the gang infiltrated 27 government institutions in Costa Rica and demanded a $20 million ransom.
Another gang dealt a devastating hit in 2022 was NetWalker, a ransomware gang that has been linked to numerous high-profile incidents including an attack on the University of California San Francisco, which paid a ransom demand of more than $1 million, and an attack targeting cyberthreat startup Cygilant. Between August 2019 and January 2021, ransomware attacks involving NetWalker pulled $46 million in ransom payments, according to cryptocurrency analysis firm Chainalysis. In October, Sebastien Vachon-Desjardins, a 34-year-old from Quebec, was sentenced in a Florida court in October after pleading guilty to charges related to his involvement with NetWalker. Vachon-Desjardins, who worked as an IT consultant for Public Works and Government Services in Canada, was previously arrested by Canadian police in January 2021 and sentenced to seven years in prison. During a search of his home, law enforcement officials discovered and seized 719 bitcoin and $790,000 in Canadian currency.

James Zhong, the hacker who stole billions of Silk Road's bitcoin - In a surprising yet anticlimactic conclusion to one of the government's longest-running cyber cases, the mystery of the notorious dark web drugs marketplace Silk Road's missing billions was solved. In November, U.S. federal agents said it found $3.36 billion worth of bitcoin that had been stashed in a popcorn can under the bathroom closet floorboards in the home of the hacker nearly a decade earlier. Prosecutors brought charges against the hacker, a Georgia resident named James Zhong, whose plea agreement with the feds saw him forfeit the huge cache of cryptocurrency, along with $600,000 in cash and other precious metals. Somewhat confusingly, Zhong is the second hacker to have ultimately turned over Silk Road's stolen billions — albeit at a lower exchange rate than today. In 2020, a hacker who went by the alias Individual X forfeited another huge cache of Silk Road's bitcoin that they had stolen years earlier during a hacking spree over 2012 and 2013. The Justice Department's latest forfeiture closed the door on another billion-dollar mystery, even if the feds kept secret how the funds were stolen or how they came to find the hacker, long after Silk Road's founder Ross Ulbricht was jailed.

Raccoon Stealer operator charged over mass password theft - U.S. officials in October charged a Ukrainian national over his alleged role in the Raccoon Infostealer malware-as-a-service operation that infected millions of computers worldwide. Mark Sokolovsky, who goes by the online handle "raccoonstealer," is accused of having a major role as a key administrator of the malware, which prosecutors say was used to steal more than 50 million unique credentials and forms of identification from victims around the world since February 2019. Sokolovsky is charged with computer fraud, wire fraud, money laundering and identity theft and faces up to 20 years in prison if found guilty. Sokolovsky is in Amsterdam awaiting extradition to the United States. Sokolvsky's arrest led to an uptick in new Mars Stealer campaigns, including the mass-targeting of Ukraine in the weeks following Russia's invasion and a large-scale effort to infect victims by malicious ads. However, in November, a security research and hacking startup told TechCrunch that it had found a coding flaw that allows it to lock out operators of the Mars Stealer malware from their own servers and release their victims.

That is all I have space for in this post but please visit the TechCrunch site to read the rest, and if the topic of anonymous cryptocurrency interest you, please check out the resources below.

Resources: FastCompany, Acuant, NDTV, NYTIMES, City A.M., Time, PandaSecurity



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

IRIS Interactive Earthquake Map

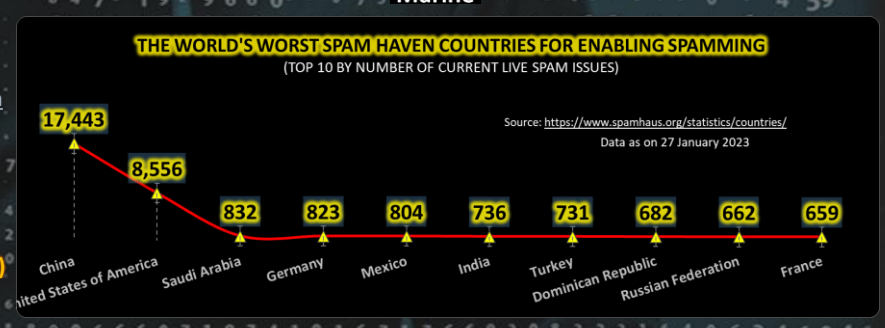
Other Interesting News and Cyber Security bits:

- Common Misconceptions About Modern Ransomware
- Ukraine: A world lesson in cyber warfare
- Cyber Operations Tracker (Listing of state-sponsored Cyber incidents since 2005)
- 'We hacked the hackers:' U.S. blocks ransomware gang (Video – 26 Jan 2023)
- SANS Daily Network Security Podcast (Storm cast)

flightradar24 LIVE AIR TRAFFIC Track any Aeroplane in flight globally

Marine Traffic

SatelliteXplorer Track satellites in orbit



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