On November 3, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Adobe, Cisco, and Google products.
See Latest CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
05 Nov	249,343,498	5,045,077

Deaths this week: 47,938

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
05 November 2021

In The News This Week

Senate panel passes slew of cybersecurity bills

The Senate Homeland Security and Governmental Affairs Committee passed a slew of cybersecurity related legislation Wednesday, including bills that would put new cybersecurity guardrails around government artificial intelligence programs, bolster the federal cybersecurity workforce, implement a number of recommendations from the Cyberspace Solarium Commission on securing critical infrastructure, establish a national cyber exercise program to game out incident response capabilities and codify one of the government's primary cloud security certification programs. One of the most significant was the Defense of United States Infrastructure Act, which would implement a number of recommendations from the Cyberspace Solarium Commission. The legislation would develop a national strategy to protect critical infrastructure from cyber and physical attacks, establish grant programs to increase resiliency of critical infrastructure, give the National Cyber Director new hiring authorities and create a Bureau of Cybersecurity Statistics to track data around incidents and defense…
Read the full story by Derek B. Johnson here: SC Media

Iran Suffered A Cyber Attack Shutting Down Smart Gas Stations

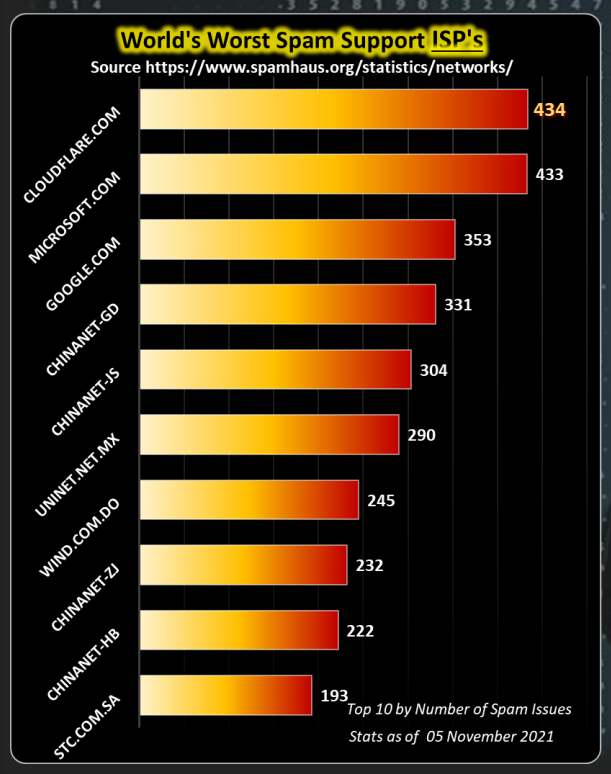
Iran's President Ebrahim Raisi acknowledged a massive cyber attack that disrupted gas stations across the country, blaming it on an unnamed country allegedly seeking to create disorder and disruption. The attack disabled a system that allows consumers to buy subsidized fuel with government-issued electronic cards. - The semi-official ISNA news agency reported that buyers encountered a cryptic message reading, "cyberattack 64411." The numbers represent a telephone hotline to Iran's Supreme Leader Ayatollah Ali Khamenei that answers questions on Islamic law. ISNA later withdrew the report claiming it was also a victim of a cyber attack, a tactic frequently used to avoid offending the powerful clergy. Read the story here: CPO Magazine

Singapore cyber-security firm blacklisted by the US along with those linked to Pegasus spyware

- A Singapore cyber-security company has been blacklisted by the US Department of Commerce for allegedly selling hacking tools that were used against individuals and organisations worldwide. Computer Security Initiative Consultancy (Coseinc) was one of four companies blacklisted on Wednesday (Nov 3) for malicious cyber activities. It was added to the blacklist alongside three other companies, including Israel's NSO Group and Candiru, which have been accused of developing and supplying the notorious Pegasus spyware. The uncovering of the Pegasus spyware sparked global outrage after it was found to have been used against government officials, journalists and activists internationally. The spyware could remotely tap phones, allowing malicious actors to turn on cameras and access data on the phone without the victims having any inkling on what was going on. Pegasus was uncovered in 2016, but it was found to have been used from as early as 2012, and was reportedly still widely used in July this year. A press release by the US Department of Commerce on Wednesday said Coseinc was blacklisted because it had trafficked in cyber hacking tools. The release did not provide details on the tools Coseinc had purportedly sold. Read the full story by David Sun here: Straitstimes

Phishing Attack Blends Spoofed Amazon Order and Fraudulent Customer Service Agents

It's the latest in a series of clever brand impersonation scams that use multiple vectors to lure victims - A new multistage phishing campaign spoofs Amazon's order notification page and includes a phony customer service voice number where the attackers request the victim's credit card details to correct the errant "order." The campaign, highlighted in new research from Avanan on Thursday, underscores how phishing attacks are growing in sophistication by using a combination of email and voice lures and leveraging popular brands such as Amazon to scam potential victims. Gil Friedrich, CEO at Avanan, now owned by CheckPoint, says that starting in October, Avanan observed a new attack in which the attacker spoofed a typical Amazon order notification page. The attack works like this: The victim receives an email showing their supposed Amazon order that totals more than $300. The victim, realizing they didn't place the order, clicks on a link in the email, which takes them to the actual Amazon website. A customer service number in the phishing email, which has an area code from South Carolina, doesn't answer when they try to call… Read the full story by Steve Zurier here: DARKReading



For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov

Understanding disinformation as a cyber threat

I spoke about fake news and disinformation, and how to recognise it, in this bulletin several times in the past. But do we fully understand how it is used as a lucrative cyber tactic or even as an effective political weapon? The EU DisinfoLab did some research on the subject and gave us the following breakdown of the disinformation playing field.

Why Disinformation is a Cybersecurity Issue

"Drawing on our research into coordinated disinformation campaigns and our own experience as an NGO in the field, we wish to highlight four areas of convergence between disinformation and cybersecurity of relevance to EU policymakers: the "terrain" on which disinformation is distributed (the social web and the internet stack, networking infrastructure, routing services), the "tactics" that increasingly combine disinformation as part of the cyberattack delivery package, the "targets" leading to victims of cyberattacks simultaneously being victim of disinformation, and what we could call the "temptation", i.e.. the lucrative possibility of both disinformation campaigns and cyberattacks.

1. ***Terrain:*** *While there is much focus on disinformation across major social media platforms, disinformation is an inherently distributed phenomenon. Disinformation campaigns continue to make use of networking infrastructure and routing services, leveraging different levels of the internet stack. As EU DisinfoLab's recent investigations have demonstrated, social media platforms often serve as gateways and amplifiers of disinformation websites. In this way, disinformation and cybersecurity implicate many of the same members of the private sector and the internet technical community.*
2. ***Tactics:*** *There is significant overlap between disinformation and cybersecurity regarding the tools and methods of attack. Disinformation is increasingly part of the cyberattack delivery package, used to deliver malware by manipulating people's fears and heightened emotions (for instance the deployment of "fearware", a subset of phishing lures that rose in prominence during the pandemic and rely on anxieties and informational deficits). The continuous proliferation of hack and leak operations as well as the coordination between hybrid tactics (illustrated in the Sandworm case) demonstrates this convergence. There is also significant convergence between disinformation campaigns and the tactics used in cybercrime, for example, via illegal dark web transactions, illegally obtained documents, and various kinds of fraud.*
3. ***Targets:*** *Disinformation campaigns and cyberattacks can cause similar harms and are sometimes combined to reach the same targets. While a data breach can compromise information security, so can the manipulation of data. We saw an example of this related to Covid-19 vaccines early this year, when hackers stole confidential documents from the European Medicines Agency (EMA) a European Union regulatory body to sew mistrust in the Pfizer-BioNTech vaccine. Meanwhile, so-called "anti-democracy attacks" and "cyber influencing attacks" like media manipulation and astroturfing in the context of elections illustrate the hybrid nature of interference in democratic processes.*
4. ***Temptations:*** *Hacking, cybercrime and influence operations are lucrative endeavours, often outsourced to skilled professionals. While individuals and businesses may have increased their readiness for ransomware attacks, disinformation strategies like defamation and extortion are now being used to cause reputational damage and seek profit. These activities all have strong financial incentives and as yet insufficient consequences, due in part to the challenges of attribution but also to the lack of dissuasive/restrictive measures. "*

Disinformation as an insider threat

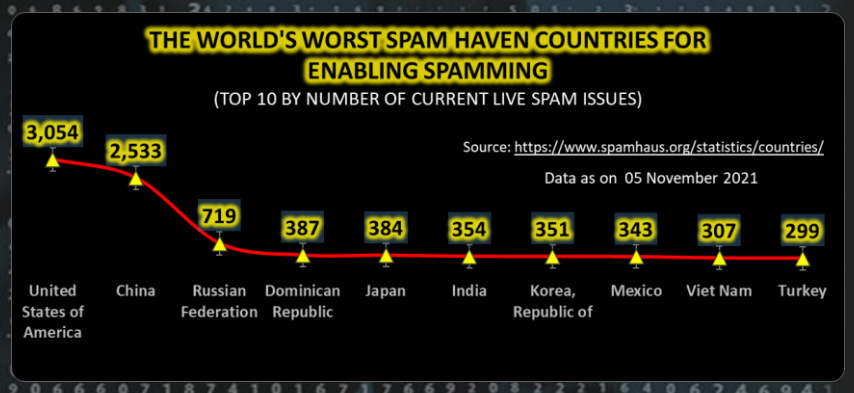
Christopher Burgess of the CSO wrote in a recent post that disinformation has not made it to the priority list of many CISO's who are facing real challenges to react to this threat vector.

CISO's challenge re disinformation *- This perspective is shared by Armaan Mahbod, director, counter insider threat, security and business intelligence at DTEX Systems. "The sharing of disinformation/ misinformation happens all the time, whether or not there are positive or negative intentions and outcomes behind the act," he says. "It's challenging for executives and organizations to refute the information because oftentimes they don't have visibility into what even might be being shared, so they're unaware that there's a need for a response." "On top of a lack of visibility, many organizational leaders are struggling to answer basic questions about their business and their team as it is, including: Who are my employees and where are they? How does my business actually function? How active is business (i.e., regionally, departmentally, etc.)? On top of the thousand other more nuanced and granular questions surrounding companies that play into an org's overall cybersecurity posture," Mahbod continues. Adam Flatley, director of threat intelligence at Redacted, sees the CISO's challenge wrapped within how disinformation campaigns external to the organizations "drive their victims to believe certain false narratives, drive wedges between them and those who provide contrary factual information, and get them addicted to information that feeds their confirmation bias." Flatley continues that "the next-level danger for a CISO is when that addiction to information feeding confirmation bias really sinks its hooks into victims (employees). It makes them more likely to click on phishing emails, text message links, and other types of lures which are tailored to the theme they hunger for, which can lead to stolen credentials or direct exploitation."*

Disinformation feeds social engineering opportunities *- Then there is the area of social engineering for which the individual employee must be prepared to deflect and for which the CISO must be prepared. Malicious actors are watching the disinformation firestorms, be they on global topics or topics unique to a given entity, and these miscreants then, "build personas to foster online relationships with their victims. They feed them information that not only manipulates them, but builds trust, which leads them to naturally visit websites sent to them by their 'true believer friend.' It establishes a comradery that would make victims more likely to open files sent to them, which could contain malware," warns Flatley. "In effect, before victims even take the step to being a witting insider threat, they could be used to compromise the network totally unwittingly, which is much easier for a threat actor to do than to truly recruit a malicious insider." –* CSO, EU DisinfoLab

Other Interesting News and Cyber Security bits:

- UAE Central Bank establishes cybersecurity center
- US offers $10 million reward for information on DarkSide leaders, $5 million for affiliates
- How To Make A Raspberry Pi Zero Wi-Fi Security Camera, Also Accessible Over The Internet



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