On November 9, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google, Microsoft, 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
11 November 2022

In The News This Week

Department of Justice seized $3 billion in Bitcoin found in underground safe and popcorn tin after Silk Road fraud - The US Department of Justice has revealed a massive seizure of over 50,000 Bitcoin, the second biggest seizure the department has ever made. The DoJ said that Bitcoin was seized from James Zhong who pled guilty to committing wire fraud in September 2012 when he unlawfully obtained over 50,000 Bitcoin from the Silk Road dark web internet marketplace. Zhong pled guilty on Friday, November 4. The DoJ revealed it had seized 50,676.17851897 Bitcoin from devices at Zhong's home in November 2021, at which point the cache was valued at $3.36 billion. Today, thanks to falling prices, it's worth just under $1 billion. Read the rest of the article by Liam Tung here: ZDNet

Twitter's CISO Takes Off, Leaving Security an Open Question

Lea Kissner was one of three senior executives to quit this week, leaving many to wonder if the social media giant is ripe for a breach and FTC action. - Twitter CISO Lea Kissner has become the latest high-ranking executive to leave the company following Elon Musk's controversial $44 billion acquisition of the social media giant last month. In a tweet Thursday, Kissner said they had resigned from Twitter but did not offer any reason for the decision. "I've made the hard decision to leave Twitter," Kissner wrote. "I've had the opportunity to work with amazing people and I'm so proud of the privacy, security, and IT teams and the work we've done." - It's unclear who is now in charge of security at the tech behemoth, or how much manpower is devoted to it. In the less than two weeks since he took charge, Musk has laid off some 3,700 Twitter employees so far, or roughly half of its workforce. Kissner's resignation follows the reported resignations of two other high-ranking Twitter executives this week: chief compliance officer Marianne Fogarty and chief privacy officer Damien Kieran. Read the story by Jai Vijayan here: DarkReading

Hacker Rewarded $70,000 for Finding Way to Bypass Google Pixel Phones' Lock Screens

Google has resolved a high-severity security issue affecting all Pixel smartphones that could be trivially exploited to unlock the devices. - The vulnerability, tracked as CVE-2022-20465 and reported by security researcher David Schütz in June 2022, was remediated as part of the search giant's monthly Android update for November 2022. "The issue allowed an attacker with physical access to bypass the lock screen protections (fingerprint, PIN, etc.) and gain complete access to the user's device," Schütz, who was awarded $70,000 for the lock screen bypass, said in a write-up of the flaw...
Read the full story by Ravie Lakshmanan here: The Hacker News

Europe calls for joint cyber defense to ward off Russia

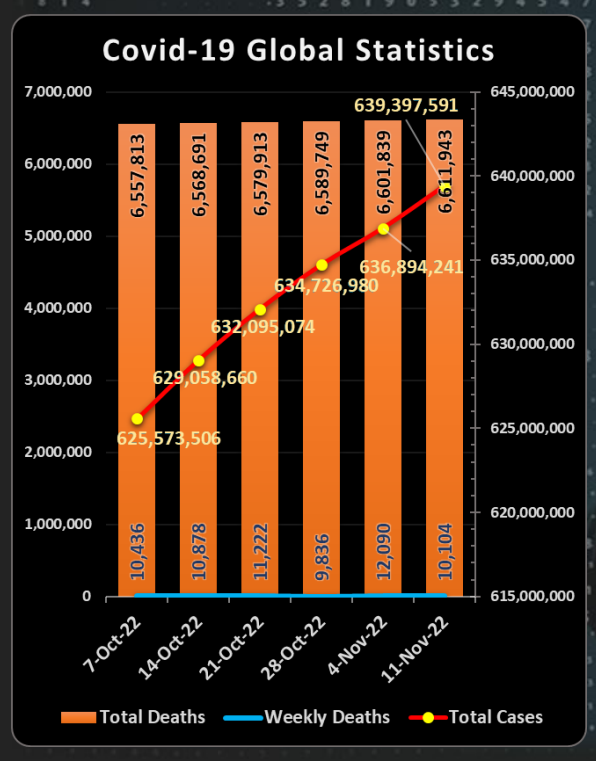
The European Commission on Thursday proposed a cyber defense policy in response to Europe's "deteriorating security environment" since Russia illegally invaded Ukraine earlier this year. The Commission, citing recent cyber attacks on energy networks, transportation infrastructure and space assets, called on member states to "significantly increase" investments in cybersecurity capabilities. It also aims to boost defense partnerships, threat-intel sharing, and cooperation between military, law enforcement, and private-industry infosec professionals. This will include establishing an EU Cyber Defense Coordination Centre, encouraging member states to more actively participate in Military Computer Emergency Response Teams (MICNET), while building a similar network for civilian cyber incident responders, according to a joint communication to the European Parliament and Council.. Read the story by Jessica Lyons Hardcastle here: The Register

Medibank refuses to pay ransom for hacked data as affected customer number doubles to 9.7m

Australia - Medibank says no ransom payment will be made to the criminal responsible for the recent data hack as the private health provider put a further head figure in data losses. The company believes the criminal accessed the name, date of birth, address, phone number and email address for about 9.7 million current and former customers and some of their authorised representatives. This figure, which has more than doubled since the last update from the company, represents around 5.1 million Medibank customers, around 2.8 million ahm customers and around 1.8 million international customers...
Read the full article by Samuel Yang here: ABC News

Outlook and Thunderbird accounts targeted with novel malware

Previously unknown StrelaStealer malware hunts for mail login data from popular email clients such as Outlook and Thunderbird. - The purpose-built malware researchers discovered in November 2022 targets explicitly mail login data, analysts from DCSO CyTec claim. Dubbed StrelaStealer, referencing Strela surface-to-air missile launcher, the malware might be a part of a larger targeted attack. "DCSO CyTec first discovered StrelaStealer in early November 2022 distributed via ISO files with what appears to be Spanish targets based on used lure documents. It is unclear at this point in time if StrelaStealer is part of a targeted attack," researchers said in a blog post. The newly detected malware operates as an infostealer. Threat actors often employ infostealers like Racoon Stealer to steal credit card data, crypto wallet credentials, browsing data, and other sensitive information. Usually, malware operators have a financial motive.
Read the full article by Vilius Petkauskas here: CyberNews, and more by Mihaela Marian at Heimdal Security



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

IS THE SATELLITE INDUSTRY READY FOR CYBERWARFARE?

With approximately 3,720 Low Earth Orbit (LEO), 134 Medium Earth Orbit (MEO), and 524 Geosynchronous Orbit (GEO) satellites orbiting our planet one could think of it as a satellite blanket covering the globe. Since the Russian invasion of the Ukraine in February, satellite imaging and communication was highlighted as both the West and the East started using satellites extensively as part of their defensive and offensive arsenals to gain an advantage in the conflict. The resulting shift towards satellites in the media also drew the attention of bad actors, state or criminal, to explore the possibilities of digitally compromising and laying claim to these satellites for sinister activities. This week Charlotte Van Camp of NSR posed the question? "IS THE SATELLITE INDUSTRY READY FOR CYBERWARFARE? - Below is an extract from Charlotte's article.

IS THE SATELLITE INDUSTRY READY FOR CYBERWARFARE?

Satellite cybersecurity is gaining more attention in the industry and among government officials, with raising concerns about a cyber warfare. The biggest space powers are taking the lead in satellite cybersecurity, while governments are publicly addressing how challenging it is to pinpoint security flaws, asking feedback and soliciting industry ideas to better defend satellites from cyber-attacks. The investments and initiatives that have been taken so far in the set-up of satellite cybersecurity have been a strong start. However, there remain security gaps in the defense against "new types of cyber-attacks" and security integration on different fronts.

NSR's Satellite and Space Cybersecurity Markets (Cyber) report forecasts cumulative cybersecurity revenues of $33.2B in the commercial segment and $5.9B from Government and Military over the next decade. Previously, NSR stated that SATCOM will generate 93% of all revenues due to the large volume of satellites in non-GEO. Nonetheless, high cybersecurity revenues for SATCOM does not address the growing threats in other applications across the satellite sector. There are many types of cyber-attacks that can target different satellite applications.

Assessing Risk, Probability, and Impact - For instance: a malware attack can be conducted on the ground segment but also on the satellite payload of any satellite that exposes some vulnerabilities. Similarly, data corruption attacks can occur on EO, SATCOM and Navigation satellites on the ground segment or the satellite link.

Historically, NSR has observed more eavesdropping, jamming, and spoofing attacks on satellites than other forms of attacks such as hardware backdoor, malware, or denial of service attacks on satellites. This is due to multiple reasons:

The attack surface used to be limited, with fewer players, fewer satellites, fewer satellite operators and technologies present in the satellite industry.

Nation state hackers mainly conducted cyber-attacks on satellites to spy on other nations and to intercept the spread of fake news.

For years, the satellite industry has been in a 'luxury' position to remain in the background and "out of sight" of attackers, who predominantly focused on other sectors such as banking, retail, healthcare, or government agencies.

In a nutshell, satellite cybersecurity does not look the same as it did twenty years ago, and threats continue to become more severe. The attack surface has been expanding together with the attackers' capabilities, and non-state hackers are now conducting cyber-attacks on satellites for personal and financial gain.

Satellite cybersecurity has also been put in the spotlight after the threats it exposed during the war in Ukraine, and cyber warfare has become a normal phenomenon where cyber-attacks are being conducted regularly to damage critical infrastructure and burden another nation's economy. Hence, what the satellite industry is fearing now can become a reality soon, i.e., ransomware and other forms of cyberattacks as we have seen across other industries coming to the space industry.

The probability and impact of an attack can differ depending on who is conducting the attack (non-state/ state hacker) and for what motive. For instance, the likelihood that state hackers will conduct eavesdropping attacks on other nations' satellites is high, because multiple governments have eavesdropping satellites. The impact of eavesdropping is "medium" because it will result in data theft but no physical damage to the satellite unless the eavesdropping satellite gets too close and potentially collides with the satellite it is spying on. Cyber-attacks on the supply chain are common in terrestrial networks and can have a very high impact if it leads to unauthorized access of the satellite. In this case, the operator is at high risk for loss of control over the spacecraft and the end user would be at risk for data theft and revenue losses.

For some types of these attacks, particularly those that the satellite industry experienced more often (spoofing, jamming, eavesdropping, replay) there already exist solutions such as anti-jamming capabilities that secure military operations. In addition, governments, especially those in the midst of a cyber warfare, are investing much in the development of cybersecurity standards.

Going Beyond Standards - Satellite operators will do what is within their control to protect the data and the satellite, often working with some of the leading cybersecurity vendors or purchasing customized security solutions. However, these anti-jamming capabilities, customized vendor solutions, and standards may not always suffice to defend against those attacks analyzed earlier. And beyond these methods that comply with government standards, some may argue that the responsibility shifts from satellite operators to the end user, who often have no or minimum methods to secure their data. This creates security gaps and "entry gates" for the attackers to do their work.

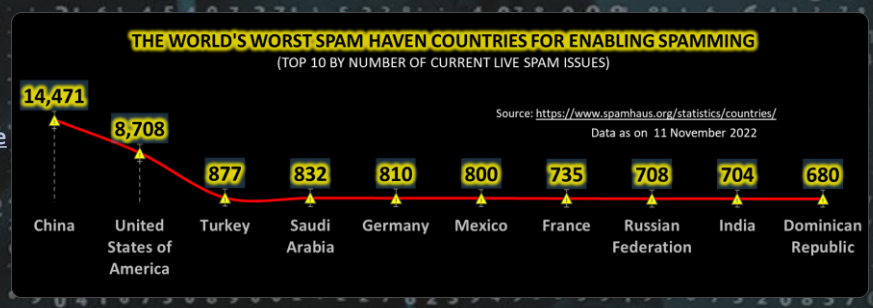
There are few companies who, prior to this recent cyber warfare, have invested in additional cybersecurity such as anti-jamming capabilities unless it is to serve government and military customers. SpaceX and OneWeb are developing more advanced cybersecurity features on their satellites. Xona Space Systems and Trustpoint are also aiming to enter the navigation market with more reliable anti spoof and anti-jam capabilities. But these are only a handful of players out of many companies that are equally at risk for cyber-threats. ..... That is all I have space for in this post, but please visit NSR to read the full article.

Other Resources: Reuters, CyberNews, VOX

Other Interesting News and Cyber Security bits:

- IBM - Cost of a data breach 2022 report.
- A million-dollar race to detect and respond
- This remarkable iPhone-powered headset gave me a glimpse into Apple's AR future
- 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