On August 17, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google products and active exploitation of vulnerabilities affecting Zimbra products.
CIS Security Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
19 Aug 22	599,124,439	6,466,793

Deaths this week: 17,660

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
19 August 2022

In The News This Week

U.K. Water Supplier Hit with Clop Ransomware Attack

A U.K. water supplier suffered a disruption in its corporate IT systems Monday as a result of a cyber-attack but claims that its water supply was not affected. Meanwhile, the alleged attack perpetrator—the Clop ransomware group—claimed the attack was on another, larger water utility, which for its part indignantly called the claim a "cyber hoax." South Staffordshire PLC, the parent company of South Staffs Water and Cambridge Water, confirmed on Monday that it was the victim of a cyber-attack that did not affect its "ability to supply safe water" to all of its customers, it said in a statement Monday. The company provides water to about 1.6 million consumers daily. *Victim Misidentified* - The Clop ransomware gang took responsibility for an attack on a U.K. water supplier on its dark web site, but said the victim was Thames Water and not South Staffordshire, according to a report posted on BleepingComputer. Thames Water is the United Kingdom's largest water supplier, serving 15 million customers in Greater London and other areas on the river that runs through the city. Thames Water quickly took to its website to let all of its customers know that any media report claiming it suffered a cyber-attack was completely bogus. In its post, the Clop gang claimed it accessed the company's SCADA systems... Read the rest of the post by Elizabeth Montalbano here: ThreatPost

Iran-linked hacking group is targeting Israeli shipping, US cybersecurity firm says

A hacking group that appears to be linked to Iran has been targeting Israeli shipping in recent years, as the shadow war between Israel and Iran began to play out at sea after mainly being waged on land and in the air, a leading US cybersecurity firm said Wednesday. The hacking group focused on collecting intelligence from Israeli entities and has also targeted Israeli government, energy and health care organizations, said the Virginia-based cybersecurity firm Mandiant. The cybersecurity group warned that intelligence and data the hackers obtained could be leveraged for nefarious activities, such as becoming fodder for damaging leaks or guiding direct military action. It wasn't clear how successful the hackers had been in their attacks.. Read the article by Luke Tress here: TOI

"Star De-Linked": SpaceX Offers Job To 'Bad*** Engineer' Who Hacked Starlink Satellite Network With A Homemade Device

A Belgian security researcher successfully hacked Elon Musk's Starlink satellite dishes with the help of a homemade circuit board that cost about $25 to create, according to various media reports. Lennert Wouters gave a presentation titled "Glitched on Earth by humans" at the annual Black Hat Security Conference on August 10, where he described the vulnerabilities that enabled him to break into Starlink satellite terminals and write his custom code. "The widespread availability of Starlink User Terminals (UT) exposes them to hardware hackers and opens the door for an attacker to freely explore the network," Wouters said in a press release. .... Wouters first analyzed the Starlink dish to develop a layout for the modchip that would fit over the existing Starlink board. He connected the modchip, which included a Raspberry Pi microcontroller, flash storage, electronic switches, and a voltage regulator, to the existing Starlink printed circuit board (PCB) and wired it together. .... Wouters carried out the hack as a part of a program run by SpaceX that rewards researchers for spotting flaws in the Starlink service. On August 10, SpaceX praised Wouters for the discovery and announced that it had released a software update. Read the article by Ashish Dangwal here: EurAsian Times

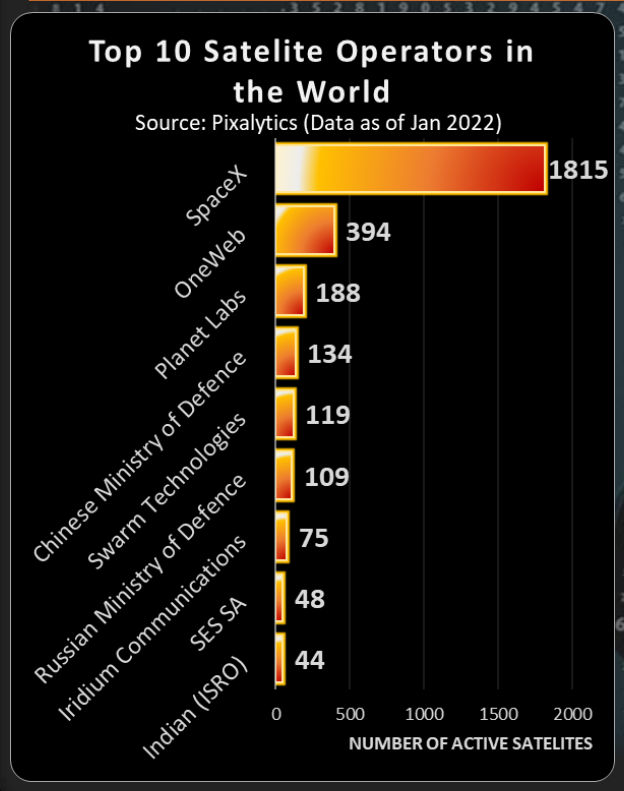
China unleashes secret attack on Russia as Xi begins to abandon Putin in huge U-turn

CHINESE hackers with links to the Communist Party are suspected of carrying out numerous cyberattacks on Russian defence industries. The news will come as a devastating blow to Vladimir Putin, who has viewed Beijing as a staunch ally in his fight against NATO and the West. Prior to launching his invasion of Ukraine, the Russian president visited Beijing to meet with President Xi Jinping. At a subsequent press conference, the two leaders professed a "friendship without limits" and declared there were "no forbidden areas" of cooperation. However, it appears that Beijing has only been paying lip service to its commitment to stand by Putin. New reports suggest that China has been secretly stealing sensitive data from Russian defence enterprises. Kaspersky Labs, a Russian cybersecurity company, claimed that China's TA428 government-connected hacking group was behind numerous attacks on Russia's military-industrial complex. .... The hackers successfully compromised the networks of dozens of targets, sometimes even taking control of their entire IT infrastructure by hijacking systems used to manage security solutions.
Read the rest of the article by John Varga here: Daily Express

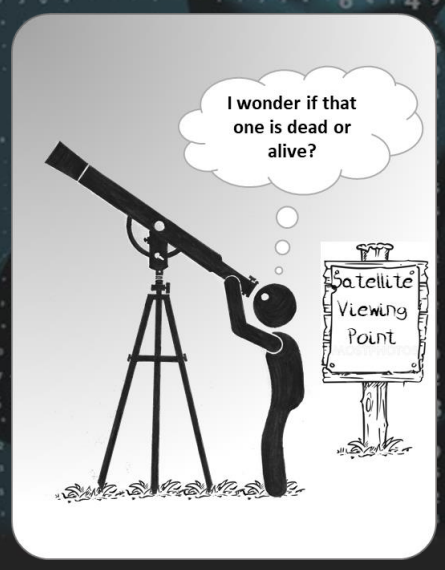
Ukraine nuclear power company says Russia attacked website

Ukraine's state nuclear power company Energoatom said Russian-based hackers launched a major three-hour attack on its website but had not caused significant problems. "The Russian group 'People's Cyber Army' carried out a cyber attack using 7.25 million bot users, who simulated hundreds of millions of views of the company's main page," Energoatom said in a statement on Tuesday. "[This] did not significantly affect operations of the Energoatom website." The Russian "popular cyberarmy" group used bots to attack the website for three hours, Energoatom said, but the assault "did not have a considerable impact on the work of the Energoatom website". A Telegram channel called "popular cyberarmy" in Russian around midday called on its followers to attack the Ukrainian nuclear operator's website. But by Tuesday evening, it had announced a "change" in plans, redirecting supporters to a new target – the Ukrainian Institute of National Remembrance, whose website was sluggish. Read the full the story here: Aljazeera

SatelliteXplorer ← Click Here To Explore Active Satellites Orbiting Earth



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



Satellite Swarms/Constellations

The ongoing Russian invasion of Ukraine that started in February this year highlighted a number of global security concerns. One concern, in particular, is an Internet blackout, whether instigated by State Actors or hackers, that could hamper meaningful assistance to those in distress. Global communication and the Internet are almost synonymous in the modern digital era, and the world's growing dependence on the availability of an Internet connection is a massive concern. This is where satellite swarms or constellations are coming in as a viable alternative or complement to the current dominant terrestrial broadband networks.
What is a satellite constellation? - A satellite constellation is a group of artificial satellites working together as a system. Unlike a single satellite, a constellation can provide permanent global or near-global coverage, such that at any time everywhere on Earth at least one satellite is visible. Satellites are typically placed in sets of complementary orbital planes and connect to globally distributed ground stations. They may also use inter-satellite communication. Most traditional communications satellite constellations are geosynchronous (GEO), which means they are parked in an orbit above the equator at an altitude synchronized with the rotation of the earth below. These GEO constellations however were marred with performance issues and high cost which meant a slow uptake of the technology. But, thanks to a new wave of non-geosynchronous-orbit (NGSO) satellite constellations the bandwidth and latency issues associated with traditional geosynchronous-equatorial-orbit (GEO) satellite connectivity, seem to be a thing of the past, and all at a reasonable cost. The race is on to populate the space above our stratosphere with "swarms" of satellites. According to the United Nations Office of Outer Space Affairs (UNOOSA), which keeps track of these things, Elon Musk's Starlink company is way ahead of the competition with the last count of around 2642 active satellites in orbit, and 952, of these, were launched in 2022 alone. The UK's OneWeb is currently the next biggest operator with 445 active satellites which marks an increase of 51 since January as shown in the statistics elsewhere in this bulletin. As I said, the race is on, and the number of satellites is increasing rapidly. Amazon is also getting into the game as they signed a massive rocket deal in April this year with 3 firms, including Bezos' Blue Origin, to launch internet satellites. They plan to build a network of 3,236 satellites in low Earth orbit (LEO), to provide high-speed internet to anywhere in the world.

With that being said I wanted to find out more about the leader of the pack and found a recent CNET article by Ry Crist that dive a little bit into what Starlink is all about. Below is a short extract of the article but feel free to visit the CNET page to read more.

Starlink Explained: Everything to Know About Elon Musk's Satellite Internet Venture

The billionaire SpaceX CEO is launching satellites into orbit and promising to deliver high-speed broadband internet to as many people as possible. After years of development within SpaceX, Starlink picked up the pace in 2021. In January, after three years' worth of successful launches, the project had surpassed 1,000 satellites delivered into orbit. One year and dozens of successful launches later, Starlink now boasts well over 2,000 functional satellites orbiting overhead. Starlink says that it now offers service in 32 countries around the world.

Starlink isn't without its controversies. Members of the scientific community have raised concerns about the impact of Starlink's low-earth orbit satellites on night sky visibility. Meanwhile, satellite internet competitors including Viasat, HughesNet and Amazon's Project Kuiper have taken notice of Starlink's momentum, too, prompting regulatory jousting and attempts to slow Musk down. Most recently, Dish has taken issue with Starlink and its claims that 5G expansions in the 12GHz band would interfere with its satellite signals. This August, nearly two years after Starlink secured nearly $885.5 million in grant funds from the Federal Communications Commission, the FCC decided to reverse that decision and cancel Starlink's subsidies, claiming that the service "failed to meet program requirements."

Technically a division within SpaceX, Starlink is also the name of the spaceflight company's growing network, or "constellation" of orbital satellites. In the years since, SpaceX has deployed thousands of Starlink satellites into the constellation across dozens of successful launches, the most recent of which took place on Aug. 9 and delivered another 52 satellites into low-Earth orbit.

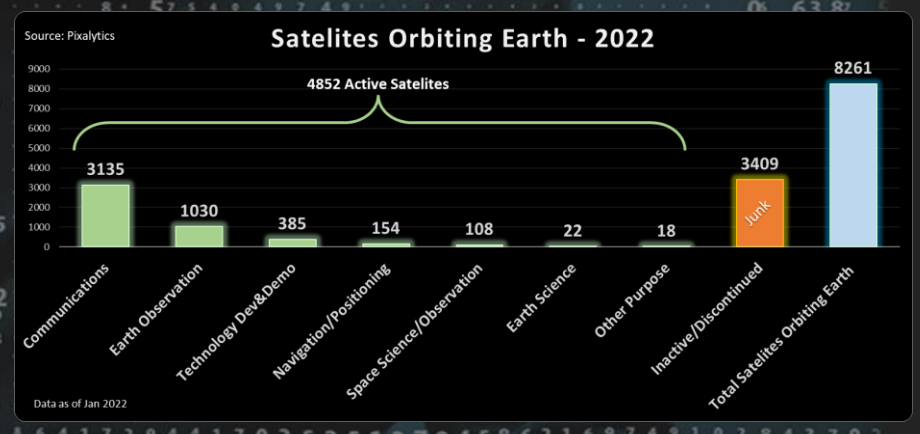
And those satellites can connect my home to the internet? - That's the idea, yes. Just like existing providers of satellite internet like HughesNet or Viasat, Starlink wants to sell internet access -- particularly to people in rural areas and other parts of the world who don't already have access to high-speed broadband. "Starlink is ideally suited for areas of the globe where connectivity has typically been a challenge," the Starlink website reads. "Unbounded by traditional ground infrastructure, Starlink can deliver high-speed broadband internet to locations where access has been unreliable or completely unavailable."
All you need to do to make the connection is set up a small satellite dish at your home to receive the signal and pass the bandwidth on to your router. The company offers a number of mounting options for rooftops, yards and the exterior of your home. There's even a Starlink app for Android and iOS that uses augmented reality to help customers pick the best location and position for their receivers. Starlink's service is only available in select regions in the US, Canada and abroad at this point, but the service now boasts more than 100,000 satellite terminals shipped to customers, and the coverage map will continue to grow as more satellites make their way into the constellation. Eventually, Starlink hopes to blanket the entire planet in a usable, high-speed Wi-Fi signal, including for moving vehicles and in-flight Wi-Fi.

How fast is Starlink's internet service? - According to Ookla, Starlink offered download speeds exceeding 100Mbps. Musk tweeted last year that as the network grows, he expects speeds to exceed 300Mbps soon.... Read the rest od the CNET article here.

Resources: Pixalytics, SpaceX Handily Fought Off Russian Starlink Jamming Attempts, McKinsey&Company, UNOOSA, Union of Concerned Scientists (UCS),

Other Interesting News and Cyber Security bits:

- Hackers are finding ways around multi-factor authentication. Here's what to watch for
- Scareware 101: How to spot this dangerous cyberattack and protect yourself
- NASA enters contract for computing processor that will change space exploration
- SANS Daily Network Security Podcast (Storm cast)



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