SPACE CYBERSECURITY WEEKLY WATCH

Weeks 51 & 52

December 12 – December 31, 2023

Timeframe : Weekly

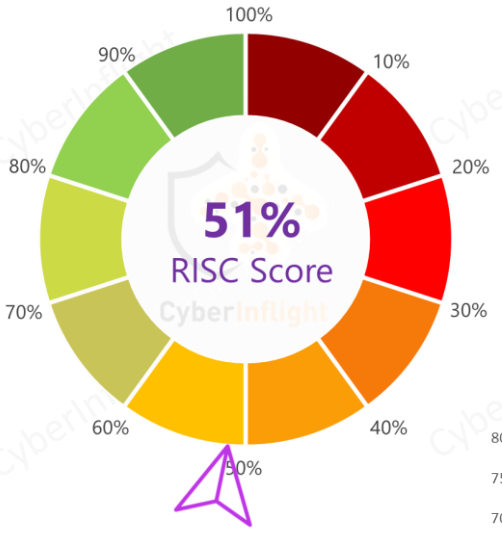
# of articles identified : 42

Est. time to read : 1h45 min

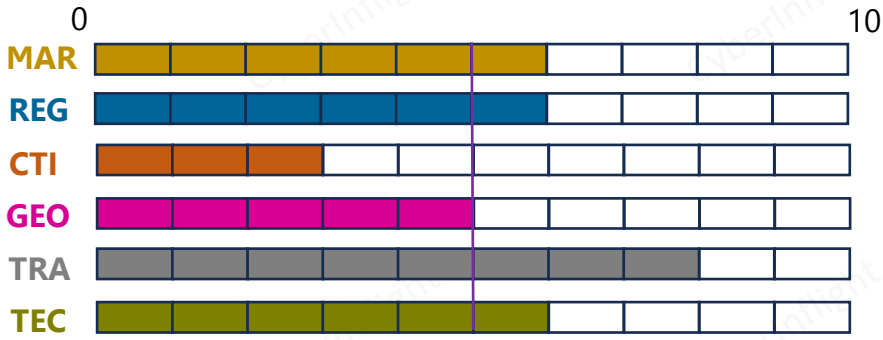
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

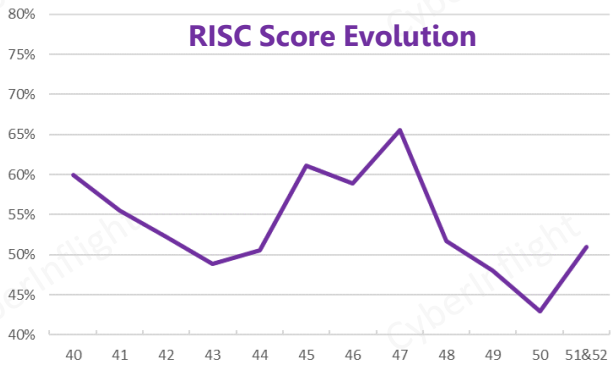
MARKET & COMPETITION
REGULATION
THREAT INTELLIGENCE
GEOPOLITIC
TRAINING & EDUCATION
TECHNOLOGY
IMPORTANT NEWS

Overview & RISC Score



Increase from last week (from 43% to 51%)





There was a peak on W47, with a RISC Score of 66%, the highest of the year. The lowest of the year was W50, with a RISC Score of 43%

The RISC Score for this watch is 51%. During this end-of-year period, NASA released its Cybersecurity Guide for Space Industry. On the market front, CYSEC won the ESA PUSH contract to accelerate the adoption of cybersecurity in the space industry. This watch features more threat intel news than average. Among others, the Israeli space agency was attacked on December 25, 2023 by the KETAPANG GREY HAT TEAM. A summary of BlackBerry Research & Intelligence Team research on threat actor AeroBlade was also published. Also during this period, the USSF announced a new component dedicated to SPACECOM. On the technology front, scientists in Russia and China have established quantum communication encrypted with the help of secure keys transmitted by China's quantum satellite. Finally, the ESA Academy has opened registration for its 2024 edition of the Cybersecurity Training Course, which will take place in April.

MARKET & COMPETITION

Result of the ESA PUSH contract won by CYSEC to accelerate the adoption of cybersecurity in the space industry

PUSH enables companies to offer their innovative space-related products and services to other European companies within the NewSpace ecosystem. ESA Commercialisation Gateway provides funding to facilitate the adoption of these services to future customers. **#PUSH #CYSEC**

Link: https://www.linkedin.com/posts/cysecsystems_cybersecurity-space-activity-7142801927536332801-uhhP?utm_source=share&utm_medium=member_desktop

REGULATION

NASA launches cybersecurity guide for space industry

NASA has published its first Space Security Best Practices Guide, a 57-page document the agency said would help enhance cybersecurity for future space missions. **#NASA #Cybersecurityguide**

Link: https://swehb.nasa.gov/display/SWEHBVD/7.22+-+Space+Security%3A+Best+Practices+Guide

THREAT INTELLIGENCE

Briefing 16: Analyzing Tactics, Techniques and Procedures Used by Cyber Threat Actors to Access US Space Industry

This article proposes a resume of BlackBerry Research & Intelligence Team research. The team revealed that they had been tracking a long-term cyber campaign targeting the U.S. aerospace sector. The threat actor, tracked as AeroBlade, conducted multiple spearphishing campaigns targeting the same aerospace organization from September 2022 – July 2023.

#USSpaceIndustry #Cyberattack

Link: https://www.kratosdefense.com/constellations/articles/analyzing-tactics-techniques-and-procedures-used-by-cyber-threat-actors-to-access-us-space-industry

South Korea's spy satellite vulnerable to North's jamming, cyberattacks

This article proposes a resume of North Korea's capabilities that can disrupt the operations of South Korea's satellites. The North has tested their efficacy several times, disrupting communications and suspending air and sea traffic in the South. **#NorthKorea #AntiSatellite**

Link: https://www.koreatimes.co.kr/www/nation/2023/12/205_362116.html

China to lock down GPS data for security concerns

China has recently taken a stringent approach towards applications seeking Global Positioning System (GPS) access. Concerned about the potential leakage of sensitive information to foreign servers, the Chinese government perceives the risk of misuse for activities such as profiling, tracking, surveillance, and causing unnecessary battery drain. **#China #GPS**

Link: https://www.cybersecurity-insiders.com/china-to-lock-down-gps-data-for-security-concerns/

ANONYMOUS RUSSIA targets the website of European Space Agency

The post states that the website of the European Space Agency (ESA) has been targeted by a group called ANONYMOUS RUSSIA. The proof of downtime for the website is provided through a link. The post was published on Telegram and belongs to the category of a DDoS attack. The victims of this attack are the European Space Agency, specifically their website esarth.esa.int. **#AnonymousRussia #ESA**

Link: https://t.me/anon_ita/1705

Iata reports rise in jamming aircraft navigation systems

Airlines have reported a spate of "spoofing or jamming" the Global Navigation Satellite Systems (GNSS) on aircraft in the past two years, according to Iata. **#Jamming #AircraftNavigationSystems**

Link: https://travelweekly.co.uk/news/air/iata-reports-rise-in-jamming-aircraft-navigation-systems

Inside the Growing Threat of GPS Spoofing

A GNSS (Global Navigation Satellite System) industry specialist explains recent consumer views related to spoofing attacks and why they are a significant threat for automakers. **#Spoofing #GPS**

Link: https://www.ainonline.com/industry-news/inside-growing-threat-gps-spoofing

The Alarming Surge of GNSS Jamming That's Threatening Flight Safety

GNSS (jamming (and spoofing) is becoming a massive threat to flight safety, especially now that we're fully transitioning to Performance Based Navigation (PBN) procedures across the globe. EUROCONTROL reported a 2000% increase in GNSS interference incidents in 2019, and almost 40% of European air traffic operates through regions that are regularly affected by GNSS (jamming and spoofing. **#GNSS #Jamming**

Link: https://pilotsofredwebby.com/2023/12/19/the-alarming-surge-of-gnss-jamming-that-threatening-flight-safety/

Data loss prevention isn't rocket science, but NASA hasn't made it work in Microsoft 365

NASA's Office of Inspector General has run its eye over the aerospace agency's privacy regime and found plenty to like – but improvements are needed. In an audit published on December 19th, the OIG found NASA lacks the data to track and monitor PII leaks and gives recommendations. **#NASA #OfficeofInspectorGeneral**

Link: https://www.theregister.com/2023/12/21/nasa_osg_privacy_review/?utm_source=dlvr.it&utm_medium=linkedin

Satellite or Earth? or Both: RSCC's Alexey Volin spoke about diversity in TV broadcasting at the Telefamily Days conference

According to Alexey Volin, since the beginning of 2023, Director General of Russian Satellite Communications Company RSCC has repelled about 15 thousand attempts to interrupt TV broadcasting on Russian spacecraft. It strives to prevent interference every day. **#RSSC #Jamming**

Link: https://spacewatch.global/2023/12/satellite-or-earth-or-both-rscc-s-alexey-volin-spoke-about-diversity-in-tv-broadcasting-at-the-telefamily-days-conference/

THREAT INTELLIGENCE

KETAPANG GREY HAT TEAM targets Israel Space Agency website

KETAPANG GREY HAT TEAM, a threat actor, has targeted the website of the Israel Space Agency. The proof of downtime is provided through a link to a website that shows the reported downtime of the targeted website. The post was published on December 25, 2023, on the Telegram network by the KETAPANG GREY HAT TEAM. The category of the attack is a DDoS attack, and the victims include the Israel Space Agency, with their website space.gov.il/en being targeted. **#IsraelSpaceAgency #DDoS**

Link: https://t.me/KetapangGreyHatTeamV2/920

GEOPOLITIC

USSF Creates New Component for SPACECOM

The name—U.S. Space Forces – Space—may seem a little redundant, but the newest Space Force component will have an outsized role in how the Space Force coordinates with U.S. Space Command. Chief of Space Operations Gen. B. Chance Saltzman revealed the new command Dec. 12 at a conference in Orlando. **#USSF #SPACECOM**

Link: https://www.airandspaceforces.com/space-force-new-component-spacecom/

TRAINING & EDUCATION

Apply now for the 2024 edition of ESA Academy's Cybersecurity Training Course
ESA Academy is looking for 30 highly motivated Bachelor and Master students to attend the Cybersecurity Training Course 2024. The training course is going to be held from 8 to 12 April 2024 at the ESA Education Training and Learning Facility in ESEC-Galaxia, Belgium. **#EASAcademy #ESEC-Galaxia**
Link:
https://www.esa.int/Education/ESA_Academy/Apply_now_for_the_2024_edition_of_ESA_Academy_s_Cybersecurity_Training_Course

TECHNOLOGY

Space Development Agency looking into alternatives for GPS

The Space Development Agency is working with the Army to provide alternative positioning, navigation and timing (PNT) capabilities that are not dependent on GPS through its Proliferated Warfighter Space Architecture, SDA Director Derek Tournear said. **#SpaceDevelopmentAgency #GPS**

Link: https://federalnewsnetwork.com/space-operations/2023/12/space-development-agency-looking-into-alternatives-for-gps/

Axiom Space Partners with Kepler Space and Skyloom to Operationalize the World's 1st Orbital Data Center

The Houston-based company Axiom Space has entered agreements with Kepler Communications US Inc. and Skyloom Global Corp. to integrate and demonstrate high data rate Optical Intersatellite Links (OISLs) on the first module of Axiom Space's commercial space station – Axiom Station. In parallel, the Axiom Space team is building the world's first scalable, cloud technology-enabled, commercial orbital data center to be hosted on Axiom Station.

#AxiomSpacePartners #KeplerSpace

Link: https://www.axiomspace.com/news/orbital-data-center

Successful Space Demonstration of QRNG-PQC Module with Squareroot8

NuSpace and Squareroot8 Technologies have successfully demonstrated a light-weight prototype of Post-Quantum Cryptography (PQC) key exchange between a nano-satellite, NuCraft, and a Singapore Ground Station using keys generated by an on-board Quantum Random Number Generator (QRNG) chipset. **#PQC #NuSpace #Squareroot8**

Link: https://www.nuspace.sg/successful-space-demonstration-of-qrng-pqc-module-with-squareroot8/

Introducing NANOlink Security: elevating communication with enhanced security

On December 2024NANOlink-S announced the release communication subsystem NANOlink-S. NANOlink-S, as its name suggest, is based on SkyLabs' flagship and flight proven NANOlink architecture, but further extended with an unmatched communication security feature using 256-bit cryptography. **#SkyLab #NANOlink-Security**

Link: https://www.skylabs.si/introducing-nanolink-security-elevating-communication-with-enhanced-security/

Benefits of modernized GNSS signals for timing applications in communications networks

This article gives an overview of the benefits of modern GNSS signals for modern terrestrial applications.

#GNSSsignals #Timingapplications

Link: https://electronics.ua.com/news/7956-benefits-of-modernized-gnss-signals-for-timing-applications-in-communications-networks

GPS anti-jamming system to be installed on South Korean helicopters

Israel Aerospace Industries (IAI) has signed a contract with Korea Aerospace Industries (KAI) to provide its ADIA GPS anti-jamming systems for the Light Armed Helicopter (LAH) 2nd Phase Production, the company announced in a statement.

#Korea #AntiJamming

Link: https://militaryembedded.com/radar-rwr/signal-processing/gps-anti-jamming-system-to-be-installed-on-south-korean-helicopters

China and Russia test 'hack-proof' quantum communication link for Brics countries

Scientists in Russia and China have established quantum communication encrypted with the help of secure keys transmitted by China's quantum satellite, showing that a BRICS quantum communication network may be technically feasible. **#Quantum #Encryption**

Link: https://www.scmp.com/news/china/science/article/3246752/china-and-russia-test-hack-proof-quantum-communication-link-brics-countries?module=inline&pgtype=article