Characterizing Cyber Attacks against the Aerospace Sector Using CVE Data

CVE	References
CVE-2017-11774 CVE-2018-20250 CVE-2017-0213 [APT 33]	https://www.kratosdefense.com/constellations/articles/peach-sandstorm-group-targets-space-sector-in-new-espionage-campaign https://www.microsoft.com/en-us/security/blog/2020/06/18/inside-microsoft-threat-protection-mapping-attack-chains-from-cloud-to-endpoint/ https://attack.mitre.org/groups/G0064/ https://www.security.com/threat-intelligence/elfin-apt33-espionage
CVE-2022-47966 CVE-2022-26134 CVE-2022-42475	https://www.microsoft.com/en-us/security/blog/2023/09/14/peach-sandstorm-password-spray-campaigns-enable-intelligence-collection-at-high-value-targets/ https://www.kratosdefense.com/constellations/articles/aerospace-industry-targeted-by-multiple-cyber-espionage-campaigns https://www.cybersecuritydive.com/news/aviation-organization-apt-cve-duo/693117/ https://www.kratosdefense.com/constellations/articles/cisa-identifies-2-critical-vulnerabilities-used-to-exploit-aerospace-sector https://therecord.media/aerospace-company-hacked-cisa-fbi-cybercom-alert https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-250a https://www.tenable.com/blog/aa23-250a-multiple-nation-state-threat-actors-exploit-cve-2022-47966-and-cve-2022-42475 https://www.cybercom.mil/Media/News/Article/3518476/cnmf-and-partners-illuminate-multiple-nation-state-exploitation-efforts/ https://therecord.media/aerospace-company-hacked-cisa-fbi-cybercom-alert https://duo.com/decipher/apt-exploited-known-zoho-fortinet-flaws-to-hit-aeronautical-entity https://www.darkreading.com/vulnerabilities-threats/iranian-apt-hits-us-aviation-org-via-manageengine-fortinet-bugs
CVE-2021-21551	https://web-assets.esetstatic.com/wls/2022/11/eset_apt_activity_report_t22022.pdf https://www.welivesecurity.com/2022/09/30/amazon-themed-campaigns-lazarus-netherlands-belgium/ https://www.virusbulletin.com/uploads/pdf/conference/vb2022/VB2022-Kalnai-Havranek.pdf https://www.welivesecurity.com/2022/09/30/amazon-themed-campaigns-lazarus-netherlands-belgium/ https://www.welivesecurity.com/2023/02/23/winordll64-backdoor-vast-lazarus-arsenal/ https://www.welivesecurity.com/2022/09/30/eset-research-uncovers-new-lazarus-campaigns-week-security-tony-anscombe/
CVE-2015-5122	https://unit42.paloaltonetworks.com/watering-hole-attack-on-aerospace-firm-exploits-cve-2015-5122-to-install-isspace-backdoor/ https://app.box.com/s/8izjpumhif40wt5jzbe6yej6j1sewt0b
CVE-2013-0634	https://www.cyberdefensemagazine.com/adobe-0-days-exploited-for-ieee-aerospace-spearphishing-attacks/
CVE-2017-0199	https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-north-star-a-job-offer-thats-too-good-to-be-true/

CVE-2013-5065 CVE-2013-3346 CVE-2012-1723 CVE-2013-2729 CVE-2009-3129 CVE-2012-4681 [Turla?]	https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/ https://securelist.com/the-epic-turla-operation/65545/ https://www.trendmicro.com/en_us/research/23/i/examining-the-activities-of-the-turla-group.html https://www.kaspersky.com/blog/epic-turla-catching-the-reptiles-tail/14991/
CVE-2015-3113	https://cloud.google.com/blog/topics/threat-intelligence/operation-clandestine-wolf-adobe-flash-zero-day/
CVE-2022-2462 CVE-2022-27924 CVE-2022-27925 CVE-2022-37042 CVE-2022-30333	https://go.recordedfuture.com/hubfs/reports/cta-2023-0808.pdf https://www.cisa.gov/sites/default/files/publications/MAR-10398871.r1.v2.WHITE.pdf
CVE-2017-0213	https://global.ptsecurity.com/analytics/pt-esc-threat-intelligence/space-pirates-a-look-into-the-group-s-unconventional-techniques-new-attack-vectors-and-tools
CVE-2014-0322	https://orkl.eu/libraryEntry/df52f8ef-acc4-4b3a-b95f-eaca5766f94d https://app.box.com/s/yh95vh5l17z2vcffwjvg3v05fzn0pzp1
CVE-2017-11292	https://orkl.eu/libraryEntry/9fc18b9e-a55f-47e0-9075-689e88ae1544 https://www.proofpoint.com/us/threat-insight/post/apt28-racing-exploit-cve-2017-11292-flash-vulnerability-patches-are-deployed
CVE-2012-0158	https://cloud.google.com/security/resources/insights/apt-groups https://www.proofpoint.com/us/threat-insight/post/APT-targets-russia-belarus-zerot-plugx
CVE-2015-6585 CVE-2015-8651 CVE-2016-0034 CVE-2016-1019 CVE-2016-4117	https://www.cisa.gov/news-events/alerts/2017/06/13/hidden-cobra-north-koreas-ddos-botnet-infrastructure https://orkl.eu/libraryEntry/41c27ecb-213c-47f0-9e4b-b6893a434949
CVE-2014-0322 CVE-2012-4792 CVE-2012-1889 CVE-2013-3893	https://blogs.cisco.com/security/talos/threat-spotlight-group-72 https://attack.mitre.org/groups/G0001/ https://securityaffairs.com/25002/hacking/elderwood-platform-still-active.html
CVE-2014-6324 CVE-2017-0213 CVE-2019-0604 CVE-2021-26855 CVE-2021-26857 CVE-2021-26858 CVE-2021-27065 CVE-2018-0798	https://www.secureworks.com/research/bronze-union https://attack.mitre.org/groups/G0027/
CVE-2009-3129 CVE-2010-3333 CVE-2011-3544 CVE-2012-0158 CVE-2012-1856 CVE-2014-1761 CVE-2017-11882 CVE-2018-0802	https://orkl.eu/libraryEntry/f09a0ea2-066d-4992-9586-97ae27f2447d 2022 Cyber Threat Handbook [5]
CVE-2015-8651	https://orkl.eu/libraryEntry/f09a0ea2-066d-4992-9586-97ae27f2447d

CVE-2016-1019 CVE-2016-4119	2022 Cyber Threat Handbook [5]
CVE-2009-3129 CVE-2012-1723 CVE-2012-4681 CVE-2013-2729 CVE-2013-3346 CVE-2013-5065	https://orkl.eu/libraryEntry/f09a0ea2-066d-4992-9586-97ae27f2447d 2022 Cyber Threat Handbook [5]
CVE-2017-11882	https://orkl.eu/libraryEntry/f09a0ea2-066d-4992-9586-97ae27f2447d 2022 Cyber Threat Handbook [5]
CVE-2010-0249 CVE-2011-0609 CVE-2011-0611 CVE-2011-2110 CVE-2012-0779 CVE-2012-1535 CVE-2012-1875 CVE-2012-1889 CVE-2012-4792 CVE-2013-1347 CVE-2013-1493 CVE-2013-3893 CVE-2014-0322 CVE-2018-0802	https://orkl.eu/libraryEntry/f09a0ea2-066d-4992-9586-97ae27f2447d 2022 Cyber Threat Handbook [5]
CVE-2012-0158 CVE-2012-1723 CVE-2012-1856 CVE-2013-0422	https://orkl.eu/libraryEntry/f09a0ea2-066d-4992-9586-97ae27f2447d 2022 Cyber Threat Handbook [5]
CVE-2014-6352 CVE-2017-0199 CVE-2017-11882 CVE-2017-8759	https://orkl.eu/libraryEntry/f09a0ea2-066d-4992-9586-97ae27f2447d 2022 Cyber Threat Handbook [5]
CVE-2016-0034 CVE-2017-7269	https://orkl.eu/libraryEntry/f09a0ea2-066d-4992-9586-97ae27f2447d 2022 Cyber Threat Handbook [5]
CVE-2013-0808 CVE-2013-4979 CVE-2014-8439 CVE-2015-2387 CVE-2015-2419 CVE-2015-2545 CVE-2015-3105 CVE-2015-5119 CVE-2015-5122 CVE-2015-7645 CVE-2016-1019 CVE-2016-4117 CVE-2017-0199 CVE-2018-0802 CVE-2018-4878	https://orkl.eu/libraryEntry/f09a0ea2-066d-4992-9586-97ae27f2447d 2022 Cyber Threat Handbook [5]
CVE-2017-0199 CVE-2017-11882	https://orkl.eu/libraryEntry/f09a0ea2-066d-4992-9586-97ae27f2447d 2022 Cyber Threat Handbook [5]

CVE-2020-0688	
CVE-2020-1472	https://orkl.eu/libraryEntry/f09a0ea2-066d-4992-9586-97ae27f2447d 2022 Cyber Threat Handbook [5]
CVE-2010-3333 CVE-2012-0158 CVE-2013-1347 CVE-2013-3897 CVE-2013-3906 CVE-2014-0515 CVE-2014-1761 CVE-2014-1776 CVE-2014-4076 CVE-2015-1641 CVE-2015-1642 CVE-2015-1701 CVE-2015-2387 CVE-2015-2424 CVE-2015-2590 CVE-2015-3043 CVE-2015-4902 CVE-2015-5119 CVE-2015-7645 CVE-2016-7255 CVE-2016-7855 CVE-2017-0144 CVE-2017-0262 CVE-2017-0263 CVE-2020-0688 CVE-2020-17144	https://orkl.eu/libraryEntry/f09a0ea2-066d-4992-9586-97ae27f2447d 2022 Cyber Threat Handbook [5]
CVE-2017-0199	https://orkl.eu/libraryEntry/f09a0ea2-066d-4992-9586-97ae27f2447d 2022 Cyber Threat Handbook [5]
CVE-2023-46604 CVE-2023-42793 CVE-2023-3519 CVE-2023-35078 CVE-2023-34362 CVE-2023-33246 CVE-2023-32784 CVE-2023-32315 CVE-2023-3079 CVE-2023-28771 CVE-2023-33010 CVE-2023-2868 CVE-2023-27997 CVE-2023-25690 CVE-2023-21932 CVE-2023-0669 CVE-2022-47966 CVE-2022-41352 CVE-2022-27925 CVE-2022-30190	https://www.kratosdefense.com/constellations/articles/andariel-emerges-as-a-persistent-cyber-threat-to-aerospace-and-defense-entities https://media.defense.gov/2024/Jul/25/2003510137/-1/-1/0/Joint-CSA-North-Korea-Cyber-Espionage-Advance-Military-Nuclear-Programs.PDF https://cyberscoop.com/north-korea-hacking-indictment-fbi-apt-45/ https://www.microsoft.com/en-us/security/blog/2023/10/18/multiple-north-korean-threat-actors-exploiting-the-teamcity-cve-2023-42793-vulnerability/ https://cyberscoop.com/north-korean-hacking-group-makes-waves-to-gain-mandiant-fbi-spotlight/ https://breakingdefense.com/2024/07/us-south-korean-warn-north-korean-hacking-group-andariel-targets-defense-aerospace-firms/ https://www.state.gov/rewards-for-justice-reward-offer-for-information-on-north-korean-malicious-cyber-actor-targeting-u-s-critical-infrastructure/ https://www.darkreading.com/cyberattacks-data-breaches/feds-warn-of-north-korean-cyberattacks-on-us-critical-infrastructure https://asec.ahnlab.com/en/82971/ https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-207a

CVE-2022-25064 CVE-2022-24990 CVE-2021-45837 CVE-2022-24785 CVE-2022-24665 CVE-2022-24664 CVE-2022-24663 CVE-2022-22965 CVE-2022-22947 CVE-2022-22005 CVE-2022-21882 CVE-2021-44228 CVE-2021-44142 CVE-2021-43226 CEV-2021-43207 CVE-2021-36955 CVE-2021-41773 CVE-2021-40684 CVE-2021-3018 CVE-2021-20038 CVE-2021-20028 CVE-2019-15637 CVE-2019-7609 CVE-2019-0708 CVE-2017-4946 CVE-2021-44228 Andariel	https://www.microsoft.com/en-us/security/blog/2024/07/25/onyx-sleet-uses-array-of-malware-to-gather-intelligence-for-north-korea/ https://www.darkreading.com/cyberattacks-data-breaches/feds-warn-of-north-korean-cyberattacks-on-us-critical-infrastructure
CVE-2011-0611	Backdoor.Barkiofork Targets Aerospace and Defense Industry [9] https://www.securityweek.com/symantec-uncovers-attacks-targeting-defense-aerospace-execs/ https://gadgetsnow.indiatimes.com/tech-news/new-phishing-malware-targets-aerospace-defence-industries/articleshow/18305721.cms
CVE-2014-0322	The Black Vine cyberespionage group [11] https://app.tidalcyber.com/references/0b7745ce-04c0-41d9-a440-df9084a45d09?tab=1
CVE-2011-0611 CVE-2012-0158 CVE-2009-0927 CVE-2010-3333 CVE-2012-0754	https://orkl.eu/libraryEntry/33c58668-0d51-4a9b-abc7-43a89484d4e9
CVE-2023-46604 CVE-2023-22515 CVE-2023-27350 CVE-2023-42793 CVE-2021-44228	https://www.microsoft.com/en-us/security/blog/2024/07/25/onyx-sleet-uses-array-of-malware-to-gather-intelligence-for-north-korea/ https://www.microsoft.com/en-us/security/blog/2023/10/18/multiple-north-korean-threat-actors-exploiting-the-teamcity-cve-2023-42793-vulnerability/
CVE-2024-21887 CVE-2023-46805	https://www.volexity.com/blog/2024/01/15/ivanti-connect-secure-vpn-exploitation-goes-global/ https://cloud.google.com/blog/topics/threat-intelligence/suspected-apt-targets-ivanti-zero-day/

	https://www.securityweek.com/ivanti-epmm-vulnerability-targeted-in-attacks-as-exploitation-of-vpn-flaws-increases/
CVE-2012-0158	https://blogs.blackberry.com/en/2015/05/spear-a-threat-actor-resurfaces https://blogs.blackberry.com/en/2016/01/puttering-into-the-future
CVE-2015-5119	https://cloud.google.com/blog/topics/threat-intelligence/demonstrating-hustle/
CVE-2023-34048 CVE-2022-41328 CVE-2022-22948 CVE-2023-20867 CVE-2022-42475 CVE-2023-20867	https://cloud.google.com/blog/topics/threat-intelligence/uncovering-unc3886-espionage-operations https://cloud.google.com/blog/topics/threat-intelligence/chinese-vmware-exploitation-since-2021/
CVE-2022-41352	https://cloud.google.com/blog/topics/threat-intelligence/cyber-threats-targeting-brazil
CVE-2018-4878 CVE-2018-0802 CVE-2017-0199 CVE-2015-2387 CVE-2015-2545 CVE-2015-7645 CVE-2016-4117 CVE-2013-4979 CVE-2015-5122 CVE-2014-8439 CVE-2016-1019 CVE-2015-5119 CVE-2015-2419 CVE-2015-3105 CVE-2015-3043	https://cloud.google.com/blog/topics/threat-intelligence/apt37-overlooked-north-korean-actor https://services.google.com/fh/files/misc/apt37-reaper-the-overlooked-north-korean-actor.pdf
CVE-2014-6332	https://cloud.google.com/blog/topics/threat-intelligence/threat-actors-leverage-eternalblue-exploit-deliver-non-wannacry-payloads
CVE-2023-2868	https://cloud.google.com/blog/topics/threat-intelligence/unc4841-post-barracuda-zero-day-remediation
CVE-2021-22893 CVE-2021-20021 CVE-2021-20023	https://cloud.google.com/blog/topics/threat-intelligence/suspected-apt-actors-leverage-bypass-techniques-pulse-secure-zero-day
CVE-2016-4117 CVE-2018-4878 CVE-2017-0199 CVE-2020-1380 CVE-2020-26411 CVE-2021-26411 CVE-2018-0802 CVE-2016-0147 CVE-2024-38178 CVE-2013-0808	APT group: Reaper, APT 37, Ricochet Chollima, ScarCruft[23] https://blog.talosintelligence.com/korea-in-crosshairs/ https://attack.mitre.org/groups/G0067/
CVE-2018-13379	https://www.sentinelone.com/blog/the-good-the-bad-and-the-ugly-in-cybersecurity-week-46-6/ https://www.sentinelone.com/labs/log4j2-in-the-wild-iranian-aligned-threat-actor-tunnelvision-actively-exploiting-vmware-horizon/

CVE-2022-41328 CVE-2022-22948 CVE-2023-20867 CVE-2022-42475	https://www.sentinelone.com/blog/the-good-the-bad-and-the-ugly-in-cybersecurity-week-25-5/ https://cloud.google.com/blog/topics/threat-intelligence/uncovering-unc3886-espionage-operations https://www.cybersecuritydive.com/news/aviation-organization-apt-cve-duo/693117/
CVE-2017-0213	https://www.ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/space-pirates-tools-and-connections/ https://www.bleepingcomputer.com/news/security/chinese-space-pirates-are-hacking-russian-aerospace-firms/
CVE-2017-0199	https://www.sentinelone.com/blog/the-blindingcan-rat-and-malicious-north-korean-activity/ https://www.cisa.gov/news-events/analysis-reports/ar20-232a
CVE-2021-26606	https://www.virusbulletin.com/conference/vb2023/abstracts/lazarus-campaigns-and-backdoors-2022-2023/
CVE-2017-8570	https://www.virusbulletin.com/virusbulletin/2019/01/vb2018-paper-inside-formbook-infostealer/
CVE-2024-24919	https://cybersixgill.com/news/articles/cve-2024-24919-vulnerability
CVE-2010-3333 CVE-2012-0158 CVE-2009-3129	https://www.darkreading.com/cyberattacks-data-breaches/-red-october-attacks-the-new-face-of-cyberespionage
CVE-2017-0213	https://cloud.google.com/blog/topics/threat-intelligence/overruled-containing-a-potentially-destructive-adversary/ https://www.darkreading.com/vulnerabilities-threats/attackers-continue-to-exploit-outlook-home-page-flaw
CVE-2021-27101 CVE-2021-27102 CVE-2021-27103 CVE-2021-27104	https://unit42.paloaltonetworks.com/clop-ransomware/ https://cloud.google.com/blog/topics/threat-intelligence/accellion-fta-exploited-for-data-theft-and-extortion https://www.mcafee.com/blogs/other-blogs/mcafee-labs/clop-ransomware/
CVE-2011-2462 CVE-2013-3163 CVE-2014-0322	https://blog.talosintelligence.com/threat-spotlight-group-72-opening/ https://blogs.cisco.com/security/talos/opening-zxshell?dtid=osscdc000283
CVE-2014-0322 CVE-2012-4792 CVE-2012-1889 CVE-2013-3893	https://blogs.cisco.com/security/talos/threat-spotlight-group-72
CVE-2012-1723 CVE-2013-1347 CVE-2013-1690	https://blogs.cisco.com/security/watering-hole-attacks-target-energy-sector?dtid=osscdc000283
CVE-2023-23397 CVE-2023-38831	https://thehackernews.com/2024/02/cybersecurity-agencies-warn-ubiquiti.html https://www.ic3.gov/CSA/2024/240227.pdf https://www.proofpoint.com/us/blog/threat-insight/ta422s-dedicated-exploitation-loop-same-week-after-week
CVE-2023-35082	https://thehackernews.com/2024/01/us-cybersecurity-agency-warns-of.html
CVE-2022-0609	https://thehackernews.com/2022/03/north-korean-hackers-exploited-chrome.html https://blog.google/threat-analysis-group/countering-threats-north-korea/

CVE-2024-38193	https://securityaffairs.com/167246/apt/microsoft-zero-day-cve-2024-38193-lazarus.html
CVE-2011-3544 CVE-2010-0738	https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage https://securityaffairs.com/39154/cyber-crime/panda-emissary-apt.html
CVE-2013-0633 CVE-2013-0634	https://securityaffairs.com/12294/cyber-crime/adobe-0-days-exploited-for-ieee-aerospace-spearphishing-attacks.html
CVE-2022-41128 CVE-2024-38178	https://securityaffairs.com/169983/apt/north-korea-apt37-ie-zero-day.html
CVE-2023-4966	https://securityaffairs.com/154115/cyber-crime/lockbit-ransomware-leaked-boeing-data.html
CVE-2017-11882 CVE-2018-0802	https://securityaffairs.com/89788/malware/cloud-atlas-recent-activity.html
CVE-2013-3918 CVE-2012-0159 CVE-2013-3894 CVE-2010-2568 CVE-2012-1723 CVE-2012-4681	https://securityaffairs.com/33637/cyber-crime/the-equation-group-atp.html https://www.infosecinstitute.com/resources/threat-intelligence/equation-group-apt-tao-nsa-two-hacking-arsenals-similar/ Equation Group: Questions and Answers Version: 1.5, February 2015, Kaspersky Lab [41]
CVE-2016-9923	https://www.proofpoint.com/us/threat-insight/post/remote-video-conferencing-themes-credential-theft-and-malware-threats

There have been some vulnerabilities in different component of the space, such as ground systems as shown below [1,2,3]. However, the table above focuses on CVEs that have been used as part of a campaign targeting the aerospace sector.

References

1. Tieby, N., Khoury, J. and Bou-Harb, E., 2024, June. Characterizing and analyzing leo satellite cyber landscape: A starlink case study. In *ICC 2024-IEEE International Conference on Communications* (pp. 1352-1357). IEEE.

2. Yu, L., Hao, J., Ma, J., Sun, Y., Zhao, Y. and Luo, B., 2024, December. A Comprehensive Analysis of Security Vulnerabilities and Attacks in Satellite Modems. In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security* (pp. 3287-3301).

3. Bailey, B. (2018) *Reducing the Software Risk in Ground Systems*, *Ground System Architectures Workshop Tutorial I*. Available at: https://ntrs.nasa.gov/api/citations/20180001541/downloads/20180001541.pdf (Accessed: 14 January 2025).
4. https://www.resecurity.com/blog/article/the-aviation-and-aerospace-sectors-face-skyrocketing-cyber-threats

5. https://www.thalesgroup.com/en/worldwide/security/press_release/thales-presents-2022-thales-cyberthreat-handbook

6. https://www.kratosdefense.com/search?q=Aerospace [Threat Briefing 10, Threat Briefing 20, Threat Briefing 24, Threat Briefing 4, Threat Briefing 13]

7. https://www.kratosdefense.com/constellations/articles/threat-briefing-4-hacktivists-carry-out-cyber-attacks-on-aerospace-firms-in-russia-ukraine-war

8. Cybersecurity Alerts and Advisories [Keyword: Aerospace]: https://www.cisa.gov/news-events/cybersecurity-advisories?search_api_fulltext=AEROSPACE&sort_by=field_release_date&url=
9. https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=73a35ea9-1a0f-4bff-b4b2-1567d7749ec7&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
10. Unmasking Threats Impacting the Aerospace and Defense Industry - https://intel471.com/resources/whitepapers/unmasking-threats-impacting-aerospace-and-defense-industry
11. https://scadahacker.com/library/Documents/Cyber_Events/Symantec%20-%20Security%20Response%20-%20Black%20Vine%20Cyberespionage%20Group.pdf
12. https://securelist.com/internet-exposed-gnss-receivers-in-2024/114548/
13. https://vx-underground.org/Papers/Malware%20Defense/Malware%20Analysis
14. https://orkl.eu/search?orkl_library%5BsortBy%5D=orkl_library%3Ats_creation_date%3Adesc&orkl_library%5Bquery%5D=AEROSPACE%20cve
15. https://www.microsoft.com/en-us/security/blog/?s=aerospace
16. https://www.trendmicro.com/en_us/research.html?
17. https://www.trendmicro.com/en_us/research/17/g/spam-remote-access-trojan-adwind-jrat.html
18. https://aerospace.org/publications-resources
19. https://cloud.google.com/blog/search/?query=AEROSPACE&language=en&category=article&paginate=25&order=newest&hl=en
20. https://www.cybersecurity-review.com/?s=aerospace
21. https://blogs.blackberry.com/en/search#q=AEROSPACE%20CVE&t=Blogs&sort=date%20descending
22. https://www.volexity.com/?s=aerospace
23. https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Reaper%2C%20APT%2037%2C%20Ricochet%20Chollima%2C%20ScarCruft&n=1
24. https://www.sentinelone.com/?s=aerospace
25. https://www.virusbulletin.com/index.php/global-search-results/?search_paths%5B%5D=&query=AEROSPACE&submit=Search%21
26. https://asec.ahnlab.com/en/?s=aerospace
27. https://www.nccgroup.com/us/search/?q=aerospace&p=1#search
28. https://www.resecurity.com/blog/article/the-aviation-and-aerospace-sectors-face-skyrocketing-cyber-threats

29. https://www.picussecurity.com/hs-search-results?term=aerospace&type=BLOG_POST&offset=0
30. https://www.darkreading.com/search?q=aerospace
31. https://www.welivesecurity.com/en/search/?term=aerospace+CVE
32. https://www.paloaltonetworks.com/search#q=AEROSPACE%20CVE&sort=relevancy
33. https://unit42.paloaltonetworks.com/curious-serpens-falsefont-backdoor/
34. https://unit42.paloaltonetworks.com/threat-actor-groups-tracked-by-palo-alto-networks-unit-42/
35. https://apt.etda.or.th/cgi-bin/listgroups.cgi?c=&v=&s=Aerospace&m=&x=
36. https://search.cisco.com/search?query=aerospace%20cve&locale=enUS&bizcontext=blogs&cat=&mode=text&clktyp=button&autosuggest=false&istadisplayed=false&tareqid=&categoryvalue=
37. https://www.mandiant.com/search?search=aerospace
38. https://cse.google.com/cse?q=aerospace&cx=partner-pub-7983783048239650%3A3179771210#gsc.tab=0&gsc.q=aerospace%20cve&gsc.sort=
39. https://securityaffairs.com/?s=aerospace+CVE
40. https://social.cyware.com/search?search=aerospace%20cve
41. https://web.archive.org/web/20150216212508/http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2015/02/Equation_group_questions_and_answers.pdf
42. https://social.cyware.com/search?search=aerospace&search_type=ALERTS
43. https://www.proofpoint.com/us/search?content[query]=AEROSPACE%20CVE