

Cyber Threats Targeting Aviation and Aerospace in 2026

 blog.polyswarm.io/turbulence-ahead-cyber-threats-targeting-aviation-and-aerospace-in-2026

The Hivemind



Verticals Targeted: Aviation, Aerospace

Regions Targeted: US, Global

Related Threat Actors: Scattered Spider, Refined Kitten, Wicked Panda, Fancy Bear

Related Families: Qilin, LockBit, Cl0p

Executive Summary

Cyber risk in the aviation and aerospace sector is evolving toward ransomware, identity-based intrusion, platform-level disruption, and potential impacts to navigation and satellite-dependent services. Recent reporting on airport disruption in April 2026, combined with the confirmed 2025 Collins Aerospace/MUSE ransomware incident, shows how cyber incidents can rapidly affect passenger processing, baggage handling, scheduling, and broader aviation continuity.

Key Takeaways

- Shared airport IT platforms remain a major single point of failure, as demonstrated by the confirmed 2025 Collins Aerospace/MUSE incident and later 2026 reporting on European airport disruption.
- Ransomware and data extortion groups continue to target airports, airlines, aerospace suppliers, and supporting vendors.
- Identity-based intrusion, including Scattered Spider-style help desk social engineering, is a growing aviation-sector risk.
- GNSS interference, satellite dependencies, and connected airport operational systems expand the threat surface beyond conventional IT.

Threat Overview

The aviation and aerospace sector presents a uniquely attractive target set because it combines time-sensitive operations, public visibility, valuable passenger and corporate data, regulated safety environments, and complex third-party dependencies. Airlines, airports, aerospace manufacturers, ground handlers, maintenance providers, reservation platforms, and aviation IT vendors operate as a tightly connected ecosystem. A cyber incident affecting one of these nodes can produce disruption far beyond the initially compromised entity.

The strongest recent example of this systemic risk remains the September 2025 [cyberattack](#) affecting Collins Aerospace's MUSE passenger-processing platform. The attack reportedly disrupted check-in, baggage processing, and boarding at multiple European airports, including major hubs such as Heathrow, Brussels, Berlin, and Dublin, with manual operations required during recovery. It was later disclosed that the Collins Aerospace event involved ransomware.

April 2026 reporting indicated a separate wave of cyber-related aviation IT disruption across European airports between April 4 and April 6, with travel-sector sources reporting delays, cancellations, manual fallback operations, and cascading operational impacts at airports not directly affected. However, technical attribution and root-cause confirmation remain limited in the public record, so this should be framed as reported disruption rather than a fully confirmed vendor-attributed incident.

Ransomware and Threat Actors Targeting Aviation and Aerospace

Qilin

Qilin is included as a malware family of interest due to 2026 airport-specific activity. Tulsa Airports Improvement Trust disclosed that an unauthorized third party accessed and acquired files from its systems between January 17 and January 20, 2026. Ransomware tracking and media reporting later linked the Tulsa International Airport incident to Qilin, with the group allegedly posting stolen documents on its leak site. Public airport disclosure confirms unauthorized access and file acquisition, while the Qilin attribution comes from ransomware leak-site tracking and third-party reporting.

LockBit

LockBit remains relevant to aerospace and aviation-adjacent organizations because of its history of targeting large enterprises and critical suppliers. The group's model combines affiliate-driven ransomware deployment, data theft, and extortion pressure. For aviation and aerospace entities, LockBit-style operations are most concerning where they affect suppliers, manufacturers, or operational support providers whose outages could disrupt downstream airline or airport functions.

CI0p

CI0p is best viewed as a supply chain and data-extortion threat rather than a confirmed aviation-specific ransomware operator. However, the group's campaigns against widely used enterprise software and file transfer platforms make it relevant to aviation and aerospace because the sector depends on shared vendors, managed service providers, and cross-organization data exchange. A CI0p-style compromise can expose sensitive passenger, employee, supplier, or engineering data without necessarily causing immediate operational disruption.

Scattered Spider

Scattered Spider is a threat actor of interest. The FBI warned in 2025 that the group had expanded its targeting to the airline sector. The group is known for identity-centric intrusion, help desk social engineering, MFA manipulation, SIM swapping, and impersonation of employees or contractors. This is particularly dangerous in aviation environments because airlines and airports rely on distributed workforces, contractors, third-party IT providers, and shared identity workflows.

Refined Kitten

Refined Kitten is a strong inclusion for aerospace targeting. MITRE [identifies](#) the group as having particular interest in aviation and energy. Its relevance is primarily espionage and potential pre-positioning rather than financially motivated extortion. For aerospace manufacturers, aviation suppliers, and defense-adjacent entities, the group's operations raise concerns around credential theft, reconnaissance, and long-term access to strategically valuable systems.

Wicked Panda

Wicked Panda is relevant to aerospace due to prior targeting of strategic industries, including defense and aerospace, for intellectual property and sensitive technical data. With this threat actor, the primary risk is not immediate passenger disruption but long-term theft of aircraft design data, avionics research, propulsion information, manufacturing processes, and supplier intelligence.

Fancy Bear

Fancy Bear is relevant to aviation and aerospace through its broader targeting of defense, government, and strategic infrastructure. Aerospace organizations supporting military aviation, satellite programs, or defense procurement are higher-value targets for intelligence collection. Fancy Bear is more likely to focus on espionage, credential theft, and strategic access rather than commercial airport disruption.

Other Aviation Sector Risks

Aviation Supply Chain and Shared Platform Risk

Aviation's reliance on shared IT platforms creates systemic exposure. Passenger-processing systems, reservation systems, flight planning tools, maintenance software, baggage systems, crew scheduling tools, and Electronic Flight Bag applications all represent potential aggregation points. If attackers manage to compromise a widely used platform, the effect can extend across multiple airlines and airports simultaneously.

Airport Operational Technology and Ground Systems

Airports depend on connected systems for baggage handling, fueling, gate operations, access control, building management, and ground support coordination. These systems may not be part of flight safety-critical avionics, but their disruption can still delay departures, strand passengers, and force manual operations.

GNSS Spoofing and Jamming

GNSS interference should be included as an aviation risk, but it should be framed carefully as navigation interference and hybrid operational risk rather than standard network intrusion.

Satellite and Space-Based Dependencies

Aerospace and aviation depend on satellite-enabled navigation, communications, weather data, and tracking. Threats to ground stations, satellite communications links, telemetry integrity, and signal reliability can create upstream disruption. This is especially relevant for aerospace, military aviation, remote routes, and regions affected by geopolitical conflict.

Emerging Threat Vectors

The most important emerging vectors likely to be exploited when targeting aviation and aerospace entities include identity compromise, shared-platform compromise, aviation SaaS exposure, GNSS interference, satellite dependency risk, and attacks against smaller airports with weaker security maturity. Smaller and regional airports may be especially exposed because they often rely on third-party service providers and may lack the internal security staffing of major international hubs.

Related Incidents in 2026

In January 2026, Tulsa Airports Improvement Trust [confirmed](#) unauthorized access and file acquisition from its systems. Qilin later claimed the airport attack on its leak site, and third-party reporting stated that leaked material included financial records, internal emails, employee identification data, and other sensitive documents. While this did not lead to a major operational disruption, it resulted in data theft and extortion.

In April 2026, travel-sector reporting [described](#) a suspected cyber-related disruption affecting European airport IT systems, with impacts to check-in, boarding, baggage handling, and flight schedules. At this time, no further information has been provided on the nature of the incident.

Potential Operational Impact

Cyber incidents in aviation can produce immediate passenger-facing disruption even when flight safety systems are not directly affected. Impacts may include delayed check-in, manual boarding, baggage processing failures, flight cancellations, missed connections, aircraft and crew displacement, customer service overload, and degraded airport throughput.

For aerospace manufacturers and suppliers, the impact profile differs. Espionage or ransomware can expose intellectual property, engineering files, procurement data, supplier contracts, export-controlled information, and sensitive defense-adjacent materials. A breach in this part of the ecosystem may not ground flights immediately, but it can create long-term strategic, regulatory, and competitive consequences.

Analyst Commentary

The aviation and aerospace sector should be treated as a system-of-systems cyber target. The most serious risk is not only that one airline, airport, or supplier is breached, but that compromise of a shared service provider or identity layer can cascade across multiple organizations. The 2025 Collins Aerospace/MUSE ransomware incident remains the strongest verified example of this risk, while 2026 reporting indicates continued pressure on airports and aviation IT environments.

PolySwarm supports aviation and aerospace defenders by enabling artifact analysis across a marketplace of specialized security engines, with verdicts and metadata aggregated into a unified [PolyScore](#). This multi-engine model can increase the likelihood of identifying malicious or anomalous artifacts that may be missed by single-engine workflows, supporting faster triage in sectors where operational continuity is critical.

IOCs

PolySwarm has multiple malware samples associated with the malware families and threat actors profiled above. Below is a selection of hashes of samples from those families and threat actor groups.

Qilin

41870d512f107c019caf0dcf3b36f38667e5979c74d7f8d3f526758f18bffb38
db7d2cf9e276307fd8b2ee68ff9ac1d500d9aa7fd305e23ed0fe188a7b5b54b9
cd9ccee24d80862dfbed92a5730cbeebe5c376b1e60d6214016f31d402a45f
87c818abe58388b4ad7180640ff08d8ac988ea74eb7f540367f756c0e7f0780a
360fe852aa900333145f95e64a956c294950754e590772bb45071f871a464b2d
ac1e24738db284fdc36fe5c6b1e7cfab1c773a4f60f178d4bfa45df487b599fe
4eac69e5cb9e4101d1eb76ec1e8cea128d3e10d577e28d7e954f72ba477214b8
0652209388559ab60da3fa56985bc5596d8b6fb785bc456d64943ab9b9a065f4
3db4e6a271465643e669753592044b879bf107c1e200091295cff928ce1171b4
61d29bf4b6c7fc706839bcb13583410c46c838707424380aae7496e35889b687
fb28c7291d212097db6e82a5c11e2306d364569fdaf095a9abbf5a681462064a
dbcad7f3121dd0ccbcac1315337b25789fa86ca976472bea0531762d87b801a3
e2bb66a2c06d0a681f03723d8918a5ba9efeb63f7576ea325fcae6f8261c5768
79143992c007f9c791bf656fb91377423441a18793ab0ad9e0f8986c891ade90
005a02b2294d897d9cfe1f4a517e083267a7c82e00063e4c51a14b53d774b760

LockBit

911a7c16d81af4714ff2239028a7c5c65bce541175e77004a763854b207ec34e
E85d5b739c510bb3db9de81c11f09ad3eb6806e3362a9abc59ab75c679f8a1c4

e45df726061253ad13fcf8fed548b4f2d5d1dde8d98ac65f2478c1352bf67f03
58ba719453346a433d974976f39e06a5f103684959f1228466ba02ba9ef4182a
49c30eab089183dc0644b3836e924c3f4f42a80a3ed9c0ffb7705254354566dd
a5bfb7a7bfaf645edc78e30796d38508603ae1ea7aa76484138433badcdab329
7be35e662568c8bf8ba478f5e3cd547caf161dc0a433c87615fcdae6cc24594e
2ae19c0f05abacc036f400c290018fda40ae7f72043af705f3b25f31a491b4be
a1aad716ef61cc29379a4fd096f891f86b3aa8c4aea038a09b59e61cc1d36302
c32710f593c26bb8055c4bd3b087165e636ad99fca78c5178e5ab5ad40198e47
08eb5e4b21105373f07c76622ffd0f5d9b7e42f5b6035206f1d399431b7be6e8
f9fb816a81b732b0631d9c1bed2958edc47ca52160c0bb03db352872bbd6cbd9
1129a6c4350a0f452c9a441ec7b847bdbad252f4aacdcc85145473cbcd3fcc52
baf54c7af3955552a324b4ffc16872a1cebc498a46c9cfb82b24bbd412e0aa6f
a003915423021c94c18ded624ac1a1dd393c0e8e94cf962999613ad638d7ed32

CI0p

3d6717c50b86bfae23cc7f9dd6296208ca7046fbe119ee1f7020429711113540
fb9cb023e9e209b51dc8128036564a70e7015d03247ef4a49525c2fc902e4808
96bb4ec6c820e485782bd206975a66a11f40dd7424abd9bace54760cbda0ae93
a72a4536965ef12690a1d791690987f80889f03477065ea186e175321fbb02f4
7f584c5a711783f013836667e061bec12602c34f4d6d4ff72ef1e57320b01b8a
38346fe148f72fe5cdcea735fa40c99870b734d25169a460a9f78fa905b73eb6

b2908b7c6c0e950baf208c0e93158accfb7df7ead1fd59e72d5b1b575b2d0b10
069f77bb5c4242ada7a7db8580c9cbac5007e1f830e093587a98ce3fc74933d2
7911fa708d34f53db5dcd693f8d3ea03a259b3ea32f8008567f382294849722f
edc07fa1b6e33c5092fcd48bb7150e0a013b7d9765024c77352528a6607d3048
5a4164420db1e1bb6803981aada44b4e728914f7356d90ca91dd13cfdb097900
fd4e0420035dbe31c1bf803ae5f4d5edb4fcfadcc6b28e7c6f28d37eb33088ee
0e8c37c81a4fed100a275d65c1a5865719e089d4fc483bbc0092637ed7865539
7c7666ae9155977d16fe18f3df1980826ae5faa6901debcde51ce28bfec41d45
18033a3e5dddb1c155f5c68d5ccbb49e0072cef92f21104536b6d20040540660

Refined Kitten

e7bea41981fbfa81186eba50b182e656bed66acb1103df1b85324b5a40567dae
84b24f76f9fafcda438d8971ebbe68354e3f83f871faa5d20e896b9ac66198b0
e0927806ab5820d9cf1f11d3d45ba7ddef51b91a474da7d9a47c327e1241367d
0f1d2eebcd34d77a6e4938578c7ab6b95c243e87dd20f09adedf40b8ed258e70
ea463dd003087dded83ab8483d43a6062bda20f934bd0291ee0ead0ff5c0f479
561d5036a1ecb3f12f2a0e9a439106b794993273f5775fe801717cd13ceb7631
5782bce800d721b1380f87727da4d767c31c70b981a936b0ab2106219a91165e
55a72b15f478b8c3092a454b3664424b765b469a4340621b5593411d76d4fe88
21e3dba05111c86468bd060a51e6884c0954940d7b2d8f0ca3f72687e2d5fbac
6d39974e149162e28e9df6bf6e3c5c9ba75e6bcdcd0a681c774e6075616ce98c
5288353d7946566a1247f78239a98b2c859071c1547ce3f6db88ebae43db5f40
e1763c22d4a4bad7987552d0327c83c850358f207c7b22d3af67a6af887a9870
220aaec1aece8a619ea3798e047310b0e19832a7af7ee5378df9c8202c68e5f1
3b39884710c182ebffa7e351f84ceabb248ccb79fb1b0fbb610bd4c1927f759d
2cccf76afa98629ec5b4cc7c765c6d2bce22a40b94ce4191f3acd50e55866d60

Wicked Panda

0a2ca20652027178598b2cf0fe9791a39044b21e0b855389dd24c5d01ac2a76c
ae7a9c4c75bc015e4bebf976b0a0ffcdab21b2c8310e13feac5130405110638a
192b4baaa7d371ab45808b3a4370354a8ff4fa2ffadf3dc09089b28bf9a0c8fc

5911cf1a1649b3896a4a2aa74f5beb90217ef8be26be2195fde06008ce1dfc3c
fbd088f45e58e8193632ecf549249846a1897241230301a4c70a9bc292726960
99863ac3695a51fc26856d9ccc8de7289587a71ec00e784b60450f48cef59eb3
3667880449ea6b1ed82f364bbd77229ea77a46f28ff954e51ede66bcb56644ad
891142b3eab667b9e61686d3a3ba5b6fc546bc35755c573efec6b5bb32715270
881881f8da61ecfe9660b559b6906f09ec57f756d132f3f994950e2bfaa12a68
169870cac2f7e9f89b1cde8e94ea85f9b8f79f6b0de73923b7e6cd2e818e31ed
ba5309cd129544429e238a2df5fa5e0af9f6b30d8c279f4203c2762db97dede0
0108607ba7cdd48e24b2023e19102189371b754dd5e633fa735101c1fd0e1139
d7235ba21f30973b8c5b83bd6d2cb929377fcbe61d66b2d7582e30eeaf71aa0f
13ae70e513ddb90182ad119b2d80d0c77d11cae73c79223b91bd4cb6d7e11010
572b37a5c1a2a6e53bbaa92433fbc529c6c7f8b2dec43e778e9c59e3ebce0b1c

Fancy Bear

f65f27e8541da17f46ea61fb5896287d7f16684824eb8df6bb966479efceffc5
55f11d7e93fda96f6ab7e5fa3a654896f70493a5957ebe3f319363422345c362
f380fc4b89b61107c1c37df6b06e712fe52b5f74059dd53eb8734d50c9773a9a
1334f20e9559777fba749918a72bf174f0ab2437059161027d2f29949e9845e5
b185639e6221d0a3b6e7f463ef44e82b53ad1db7f66f9ccc20108879832e88ba
c4eefd90983b213bc59a8009efa87e791007f17d5aeb10e904bd070487e2c509
0b1e1ed4fa71ee0fc200af56438171bec5a1ace82e8efb2c2cff469f9599ac07
73fb1d086265a23aa055a4715d5a48a3d6f5cc49d226e1471aca9d8871dc4a4f
64f7ca593ec7e151ca657b7d024b4d4036cb25df7acc7b998f8fe75c90bd6823
d96762faa2323ba1e43e794ccf3ac2ba6674fa235d50bb4260766a2ea3156e0c
eab1cf3c1312de58cdaefa14621658ec55f5b6887413112ec198b77a0b66d00e
e3bba315a700fa7d10f86aa47db3346c799c0b0786717e8b73512d5439125b1d
900fe9269c7ca2feb0b073a2c1184bca984b25c457477be4c340120e760002de
1979530e00102fd69aa217aeda725571e91d99a04610187d367760f2c04c86ec
ebceaeb9388afab081280f7707fcac8f7ff82d00ede3c189414ba61d6bf94116

Don't have a PolySwarm account? Go [here](#) to sign up for a free Community plan or subscribe.

Contact us at hivemind@polyswarm.io | Check out our [blog](#) | [Subscribe](#) to our reports.

Topics: [Threat Bulletin](#), [aviation ransomware](#), [aviation supply chain attack](#), [aviation cybersecurity](#), [aerospace cybersecurity](#), [airline cyber threats](#), [identity-based cyber attack](#), [GNSS spoofing](#), [aviation](#), [airport cyberattack](#)