ADARMA
TOGETHER WE'VE GOT THIS

# AVIATION THREAT LANDSCAPE REPORT

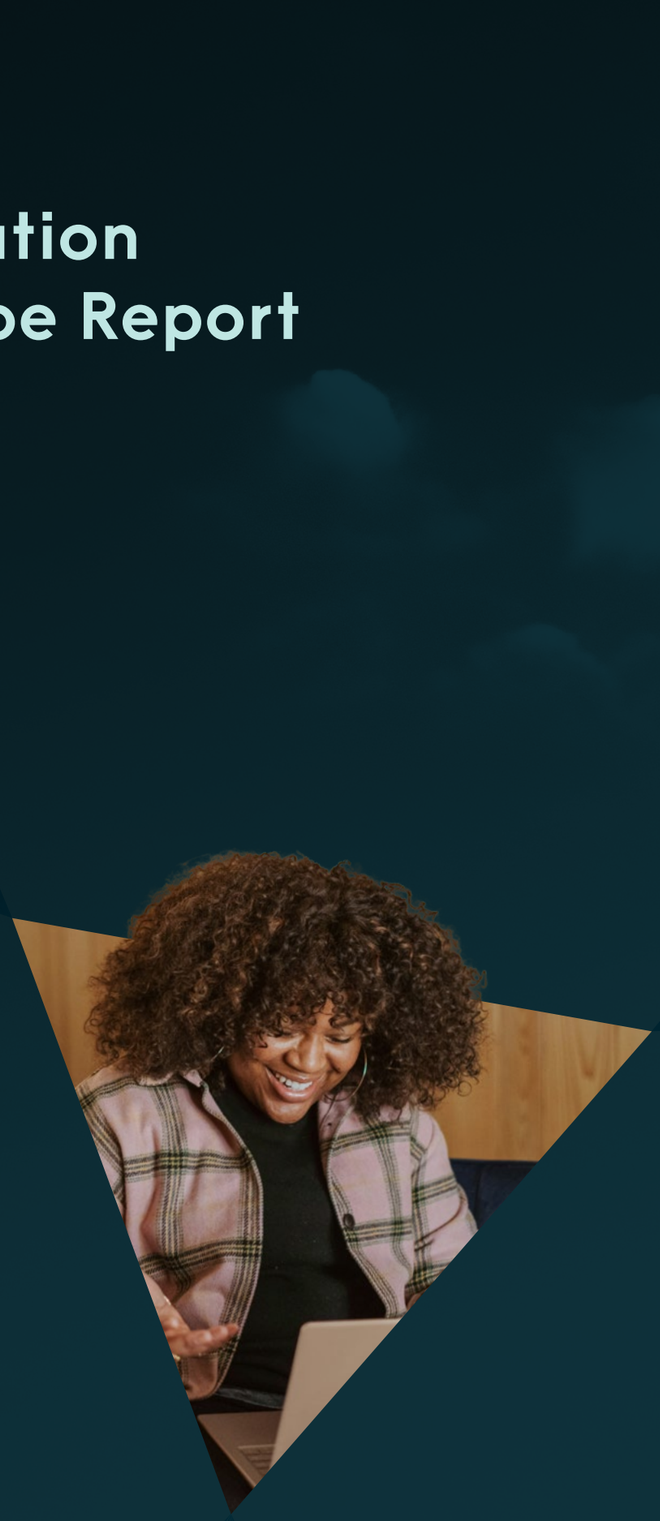
Q4 2024

# Contents

# Adarma Q4 Aviation Threat Landscape Report

## Purpose

**Adarma's latest Aviation Threat Landscape Report provides a comprehensive look at the major cyber threats that impacted the aviation industry in Q3 2024. Drawing on intelligence gathered by Adarma's Threat Intelligence Team from both internal and external sources, this report presents the most critical findings for the sector during this period. It also features insights from our partner, Recorded Future. While the primary focus is on cyber activity from July 1 to September 30 2024, we have included relevant information from outside this timeframe where applicable.**



## Insights from Adarma

As one of the most technologically advanced and globally interconnected industries, aviation remains a prime target for cybercriminals. From flight operations and booking systems to air traffic control and in-flight entertainment, aviation operates within a vast, complex network of interconnected systems, making it particularly vulnerable. This interdependency means that a single vulnerability in any part of the network can cascade into widespread operational disruptions, making cybersecurity a critical concern for the industry.

Moreover, the sector's handling of vast amounts of personal and financial data, including passenger names, payment information, and passport details, makes it a lucrative target for cybercriminals. Adding another layer of risk is the sector's rapid adoption of new digital solutions to improve operational efficiency and enhance passenger experiences, in a highly competitive market.

Based on the findings of our Threat Team, ransomware continues to dominate the aviation threat landscape, followed closely by Advanced Persistent Threat (APT) groups, underscoring the need for heightened vigilance and robust cybersecurity measures.

The following is a summary of the most active adversaries, their attack techniques, and major cyber-attacks in the aviation industry in Q3 2024. By analysing these threat actors and their methods, we can gain insights into their future strategies and improve defence mechanisms against their activities. Understanding the patterns of these cybercriminals helps organisations anticipate and mitigate potential risks in the aviation sector.

ADARMA
TOGETHER WE'VE GOT THIS

# Notable Ransomware Attacks in Q3

**Below is a list, compiled by the Adarma Threat Intelligence Team, of the most notable cyber-attacks targeting the aviation industry in Q3 2024. By exploring these groups and their attacks, we can better understand and predict what these threat actors will do next.**

JULY

01

## Akira

In July, Akira ransomware caused a complete shutdown of Split Saint Jerome Airport's IT infrastructure, leading to flight cancellations and diversions. The airport's operations were severely impacted due to the loss of IT support, forcing check-ins to be performed manually. This follows a similar attack in June, when Akira ransomware targeted LATAM Airlines Group, the largest airline in Latin America. Attackers reportedly gained access to LATAM's network through the Secure Shell (SSH) protocol, potentially by exploiting CVE-2023-27532, a vulnerability in Veeam Backup & Replication. After exfiltrating critical data, Akira used a combination of legitimate tools and Living-off-the-Land Binaries and Scripts (LOLBAS), marking a trend of Akira ransomware targeting Critical National Infrastructure (CNI).

AUGUST

02

## Helldown

On August 22 2024, Barry Avenue Plating (BAP), an aviation and aerospace component manufacturer, discovered a data breach. The Helldown ransomware group claimed responsibility, stating they had accessed sensitive information, including non-disclosure agreements, employee records, financial data, and personally identifiable information. The attack is suspected to have exploited vulnerabilities like phishing, unpatched software, or supply chain weaknesses, though the full scope of the breach is still under investigation.

SEPTEMBER

03

## Fancy Bear

In September, Deutsche Flugsicherung (DFS), the German state-owned company responsible for the country's air traffic control, confirmed that it had been breached. The attack affected the company's administrative IT infrastructure but did not impact air traffic control operations. While those responsible for the attack have not been identified, it is suspected that APT28, also known as Fancy Bear, may be behind the attack. The full scope of the breach is still under investigation, and it remains unclear whether any data was compromised. APT28 is a cyber-espionage group believed to be linked to Russia's military intelligence agency, the GRU.

### APT Activities

In Q3 2024, MuddyWater, specifically targeted the aviation sector as part of its intensified cyber-espionage activities, focusing on high-value sectors in the Middle East. The Iranian-linked group leveraged spear-phishing campaigns that deployed the custom BugSleep malware via legitimate Remote Monitoring and Management (RMM) tools, such as Atera and ScreenConnect, to infiltrate networks. This approach has allowed MuddyWater to establish persistent access, giving them the capability to monitor and control compromised airline systems. These attacks, which also impacted other sectors, demonstrate MuddyWater's strategic expansion to critical infrastructure, reflecting its alignment with Iran's geopolitical interests.

# Threat Actor Profiles

**Listed below are the three most active threat actors targeting the aviation sector during Q3 2024.**

## BlackSuit

A relatively new ransomware group, Blacksuit, first emerged in May 2023. According to Cybersecurity and Infrastructure Security Agency (CISA), BlackSuit ransomware is the evolution of the ransomware previously identified as Royal ransomware, which was used from approximately September 2022 through June 2023. BlackSuit shares numerous coding similarities with Royal ransomware and has exhibited improved capabilities.

BlackSuit's attacks have spread across numerous critical infrastructure sectors, including, but not limited to, commercial facilities, healthcare and public health, government facilities, and critical manufacturing.

The group conducts data exfiltration and extortion before encryption and then publishes victim data to a leak site if a ransom is not paid. Phishing emails are among the most successful vectors for initial access by BlackSuit threat actors. After gaining access to victims' networks, BlackSuit actors disable antivirus software and exfiltrate large amounts of data before ultimately deploying the ransomware and encrypting the systems. In Q3, the group have been one of the most active ongoing threats throughout 2024.

## Helldown

Helldown is a relatively new and advanced ransomware group that employs a double extortion technique. They not only encrypt victims' data but also threaten to leak it on the dark web if the ransom isn't paid. Since the group's emergence in early 2023, Helldown has rapidly become a significant threat in the cybercrime world. The group is suspected to be linked to a cybercriminal organisation based in Eastern Europe, known for developing and deploying sophisticated malware.

## Akira

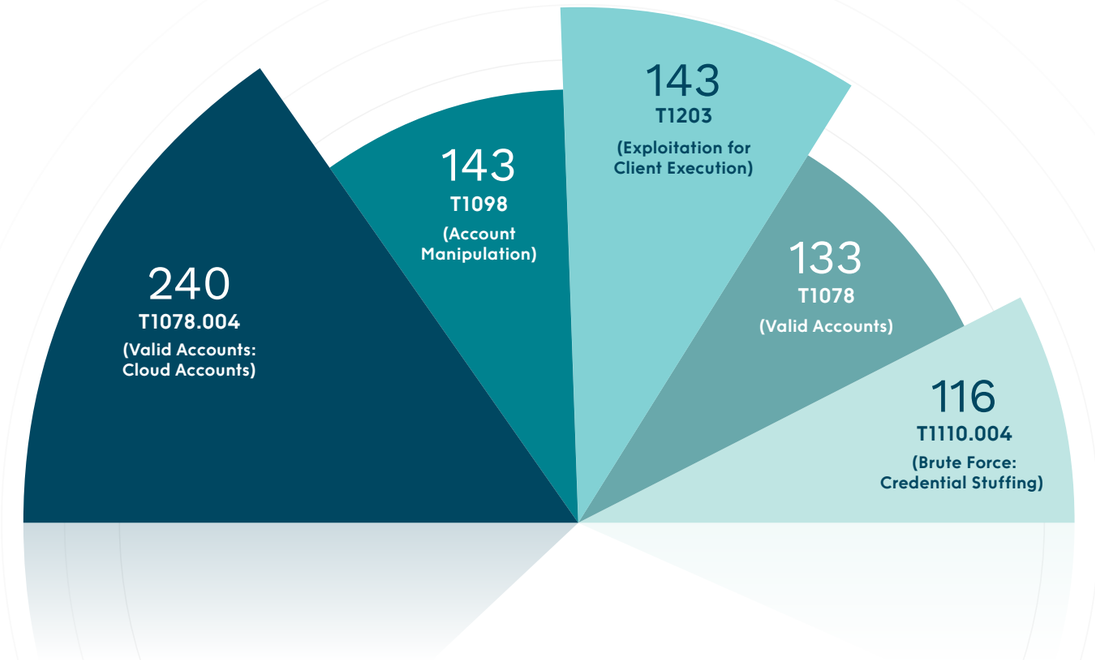
Akira is swiftly becoming one of the fastest-growing ransomware families, largely due to its use of double extortion tactics and its ransomware-as-a-service (RaaS) distribution model. First detected in March 2023, Akira ransomware is linked to the RaaS group known as Storm-1567, also referred to as Punk Spider or Gold Sahara. This group is responsible for both the development and management of Akira ransomware, as well as overseeing its dedicated leak sites. The group typically uses a double-extortion method, exfiltrating critical data before deploying ransomware to cripple the victim's systems. As of January 1 2024, Akira ransomware had affected over 250 organisations and amassed approximately £34.44 million in ransom payments.


> **"In response to the ongoing threat from ransomware, the Adarma Threat Team has produced several Emerging Threat Hunting packs aimed to help our customers detect suspicious or malicious activity within their networks. These packs have related to prominent ransomware groups Blacksuit, RansomHub, Qilin and Akira, and have contained several threat hunts based on the group activities and MITRE ATT&CK TTPs."**
>
> Adarma Threat Intelligence Team

ADARMA
TOGETHER WE'VE GOT THIS

# Mitre ATT&CK Techniques

**Top attack techniques discovered by Adarma's internal SOC analysts while responding to incidents targeting the aviation industry in Q3 2024.**




**T1078.004**

## Valid Accounts: Cloud Accounts

Attackers may use compromised cloud accounts, such as those for cloud services or Software-as-a-Service applications, to gain unauthorised access to a victim's infrastructure. Once attackers have access to cloud credentials, they can exploit these accounts to move laterally, escalate privileges, exfiltrate data, or conduct other malicious activities within the compromised cloud environment.



**T1098**

## Account Manipulation

Adversaries may manipulate accounts, such as changing permissions or modifying credentials, to maintain access or gain further privileges within a compromised environment. Attackers may create new accounts, modify existing ones, or change security groups to enable persistence, elevate privileges, or conduct lateral movement. This technique is particularly dangerous because it allows attackers to blend in with legitimate users, making detection more difficult.



**T1203**

## Exploitation for Client Execution

This involves attackers exploiting software vulnerabilities in client applications to run malicious code. These vulnerabilities often exist due to insecure coding. Attackers may target browsers (via drive-by downloads or spearphishing links), office applications (through phishing with malicious documents), and third-party software like Adobe Reader or Flash. Successful exploitation can grant attackers remote access or control over a system, often without user action required. This technique is widely used to compromise endpoint systems in corporate environments.

**T1078**

## Valid Accounts

This refers to attackers using stolen or compromised credentials to access systems and bypass normal authentication controls. These credentials could belong to users, administrators, or service accounts, allowing the attacker to blend in with legitimate users and evade detection. This technique enables attackers to perform lateral movement, escalate privileges, or maintain persistent access within a network.

**T1110.004**

## Brute Force: Credential Stuffing

Adversaries attempt to exploit credentials obtained from breach dumps to access target accounts through credential reuse. Users often use the same passwords across different personal and business accounts, making this tactic effective. Credential stuffing involves using these username and password combinations to try and gain access, but it carries risks such as triggering account lockouts or numerous authentication failures, depending on the organisation's policies.

For further detailed information about these techniques, please refer to the Mitre ATT&CK website (https://attack.mitre.org/).

# Our Services

## Threat Intelligence Platform Managment

Adarma's Threat Specialists can set up, configure, and maintain a threat intelligence platform tailored to your business needs. This platform enables the storage of reports, incident details, and indicators of compromise (IOCs) while integrating intelligence feeds into your SIEM, EDR, firewall, web proxy, or phishing protection solutions. By creating associations between threat actor groups, malware types, and related IOCs, the platform streamlines investigations and prioritises detection efforts.

## Security Threat Modelling

Our services include security threat modelling that adheres to industry standards. We can assess threats for applications, platforms, or entire organisations, helping our customers in identifying potential vulnerabilities and risks that could affect their systems and solutions.

## Quarterly Threat Briefings

To support your long-term strategic planning, our Threat Intelligence team provide quarterly threat briefings. These briefings focus on trends based on industry sector, geographical location, and other customer-specific considerations, providing senior stakeholders with the insights they need for effective planning, budgeting, and risk management.

## Monthly Operational Briefings

To deliver actionable intelligence that informs short-term tactical decision-making and resource allocation, we provide monthly operational threat briefings. Our Threat Intelligence team monitors data sources, threat feeds, dark web tools, and information-sharing platforms to deliver detailed breakdowns of current and emerging security threats to your business.

## Threat Hunting Expertise

Adarma's Threat Team comprises specialists and analysts experienced in threat hunting across SIEM and EDR platforms. We conduct custom behavioural threat hunts, tailored to your organisation's unique security concerns. These hunts uncover previously undetected malicious activity, logging issues, compliance problems, and offer recommendations to enhance your security posture.

# How Adarma Can Help

**We are Adarma, the UK's leading Security Operations specialist for modern global enterprises.**

We protect organisations in the FTSE 350, including those in Critical National Infrastructure and other regulated sectors. We offer effective threat detection and incident response, acting as an extension of your team to enhance your security posture and optimise security investments for maximum risk reduction.

Our security operations platform, Socket, along with our engineering expertise, provides co-managed security monitoring and consulting services, integrated with top enterprise security providers like Splunk, Google, and Microsoft. Our mission is to make cyber resilience a reality for organisations worldwide.

## Get in touch

If you would like to speak to an Adarma consultant about any issues or approaches raised in this paper, please email **hello@adarma.com**.

ADARMA

TOGETHER WE'VE GOT THIS

**hello@adarma.com**

**www.adarma.com**