ADARMA
TOGETHER WE'VE GOT THIS

AVIATION THREAT LANDSCAPE REPORT

Q3 2024

Contents

ADARMA
TOGETHER WE'VE GOT THIS

Cyber Threats Facing the Aviation Sector

The aviation industry is a cornerstone of global infrastructure, enabling the movement of millions of people, goods, and services across continents.

Its importance, however, also makes it a prime target for cyber threats. The latest Threat Landscape Report from Adarma underscores the persistent and evolving cyber threats facing this sector, with ransomware attacks the biggest threat followed by hacktivist attacks, phishing campaigns, and data breaches.

ADARMA
TOGETHER WE'VE GOT THIS

Ransomware Attacks

Below is a list, compiled by the Adarma Threat Intelligence Team of the most notable cyber-attacks targeting the aviation industry in Q2, 2024. By exploring these groups and their attacks we can better understand and predict what these threat actors will do next.

APRIL

MAY

01

Black Basta

On April 1, the Black Basta ransomware group targeted PDQ Airspares Limited, a UK-based supplier of consumables to the airline and MRO (Maintenance, Repair, and Overhaul) industry. While specific details of the impact were not disclosed, ransomware attacks typically involve operational disruptions and potential data exfiltration. BlackBasta is a relatively new but highly sophisticated ransomware group that emerged in early 2022. The group is known for using customised ransomware strains and advanced techniques to bypass security measures.

02

RansomHouse

On April 25, the RansomHouse group targeted Sterch-International S.R.O., a company in the aviation industry headquartered in the Czech Republic. The specifics of the data compromised, or the extent of the operational disruption were not detailed. Unlike traditional ransomware gangs that encrypt data and demand a ransom for decryption keys, RansomHouse focuses primarily on stealing sensitive data from organisations and threatening to publicly release it unless a ransom is paid. This tactic is part of a broader trend known as “double extortion.”

03

PLAY

On April 26, Precision Fluid Controls, a major player in the aerospace industry, suffered a ransomware attack carried out by the Play ransomware group. Sensitive data, including client documents, payroll details, and financial records were exposed. The Play group is notorious for their Linux-targeting ransomware based on the Babuk code, highlighting their focus on exploiting vulnerabilities in enterprise networks.

04

LockBit 3.0

In May, LockBit 3.0 claimed to have targeted TDT Aero, a Turkey-based aircraft line maintenance company. This attack underscores the persistent threat of ransomware to essential maintenance operations crucial for aviation safety. LockBit has been involved in numerous high-profile attacks, impacting organisations globally. The group’s success and growth have been attributed to their effective Ransomware-as-a-Service model and their ability to continually update and refine their ransomware.

Hacktivist Attacks

Hacktivism, driven by political motivations, poses a growing threat to the aviation sector, aiming to disrupt operations and draw attention to a particular ideology.

NoName057(16)

In May, the pro-Russian hacktivist group NoName057(16) launched distributed denial-of-service (DDoS) attacks against the websites of multiple European aviation organisations, including the European Business Aviation Association (Belgium), Apli Aviation, and Vulcanair (Italy).

The DDoS attacks disrupted online services, emphasising the hacktivist strategy of targeting web infrastructure. The group has implemented improved encryption mechanisms for their C2 servers, indicating their evolving sophistication.

Phishing Campaigns

ADARMA
TOGETHER WE'VE GOT THIS

Phishing continues to be an effective method for cybercriminals to gain initial access to systems, with recent campaigns showing increased complexity.

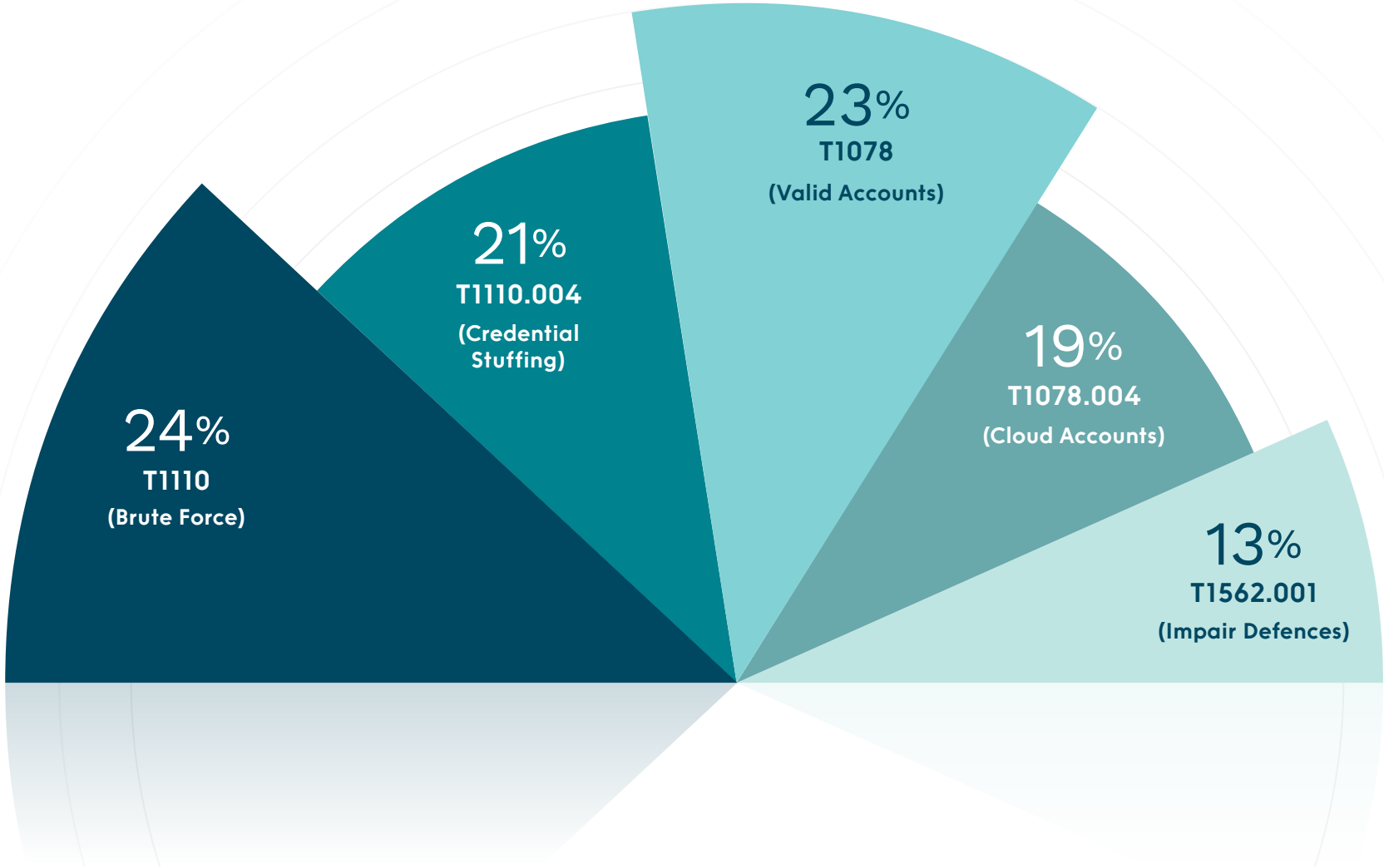
Sticky Werewolf

On June 6, a phishing campaign by Sticky Werewolf targeting the aviation sector was reported in the media. Having shifted from using malicious links to attachements, the group used phishing emails to deploy NetWire remote access trojan, in an attempt to compromise sensitive information.

The geopolitical context suggests potential connections to a pro-Ukrainian cyberespionage or hacktivist group, however this is unconfirmed.

Mitre ATT&CK Techniques

Top techniques identified in incidents concerning the Aviation sector that Adarma's internal SOC analysts addressed in Q2 of 2024.



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

> The top two techniques observed were related to internal account takeovers: Brute force and Valid Accounts. This emphasises the need for a strong password policy.
>
> Adarma Threat Team

T1110

Brute Force

Adversaries use brute force techniques to access accounts when passwords are unknown or when password hashes are obtained. They systematically guess passwords using repetitive methods, either by interacting with a service to validate credentials or offline against previously acquired data like password hashes.

T1110.004

Credential Stuffing

This is when adversaries exploit credentials from breach dumps of unrelated accounts to access target accounts through credential overlap. They can use this dumped information to compromise accounts by leveraging users' tendency to reuse passwords across personal and business accounts.

T1078

Valid Accounts

Adversaries abuse compromised account credentials to gain Initial Access, Persistence, Privilege Escalation, or Defense Evasion. These credentials can bypass system access controls, allowing persistent access to remote systems and services like VPNs, Outlook Web Access, and remote desktops. Additionally, compromised credentials can grant higher privileges or access to restricted network areas. Adversaries may also avoid using malware or tools to make detection more difficult.

T1078.004

Cloud Accounts

Valid cloud accounts can enable adversaries to achieve Initial Access, Persistence, Privilege Escalation, or Defense Evasion. These accounts, created by organisations for users, services, or administration, may exist solely in the cloud or be hybrid-joined with on-premises systems through syncing or federation with identity sources like Windows Active Directory.

T1562.001

Impair Defences

This is when an adversary modifies or disables security tools to avoid detection of their malware and activities. They may kill security software processes, alter or delete registry keys or configuration files to disrupt proper functioning or interfere with scanning and reporting. An adversary might also disable updates to prevent the latest security patches from being applied to the victim's systems.

Recommendations

The aviation industry must remain vigilant against a diverse array of cyber threats, from ransomware and hacktivism to sophisticated phishing campaigns.

Implementing robust cybersecurity measures, staying informed about emerging threats, and fostering a culture of security awareness are crucial steps in safeguarding critical infrastructure from cyber adversaries. By doing so, the aviation sector can mitigate risks and ensure the continuity and safety of its operations.

To learn how Adarma helped a leading airline mature its security operations to improve visibility and coverage, read the case study.

We Are Adarma

Adarma provides customised cybersecurity solutions to assist businesses in achieving future-ready cyber resilience. Our approach enables organisations to decrease cyber risks by implementing effective threat intelligence, exposure management, and detection and response capabilities.

We offer tailored threat intelligence, technological solutions, and strategic consultancy that cater to our customers' specific security requirements and business goals. Our expertise guarantees a balanced approach between security and operational efficiency, safeguarding our customers' most crucial infrastructure and data.

Discover our tailored services and find out why we are the preferred security partner for FTSE 350 firms and are recognised in the 2024 Gartner Market Guide for Co-Managed Security Monitoring Services.

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**.

You may also be interested in our "How to Design a Future-Ready Security Operations Centre (SOC)" report. This report lays out a detailed blueprint for building a SOC that tackles today's challenges while anticipating and preparing for tomorrow's threats.

Scan the QR code to find out more.

ADARMA
TOGETHER WE'VE GOT THIS

hello@adarma.com

www.adarma.com