APT Groups that Target Aviaton Industry in Last 6 Month

Content

Executive Summary

This executive summary addresses the significance and impacts of cyberattacks targeting the aviation industry. In recent years, cyberattacks targeting the aviation sector have become a major threat for businesses. These attacks target critical infrastructure of airlines, including databases, reservation systems, flight systems, and even air traffic control systems.

The aviation industry is a sensitive target for cyberattacks. Protecting the critical infrastructure and data within the sector is of paramount importance for operational continuity and passenger safety. Cyberattacks can lead to serious consequences such as data theft, operational disruptions, flight cancellations, and even compromising flight safety.

In recent years, there has been an increase in the number of cyberattacks targeting the aviation sector. According to Eurocontrol reports, cyberattacks have occurred at least 530% more annually over the past four years. Notably, there is a significant concentration in attack types, accounting for 61% of cases. This situation necessitates comprehensive security measures.

Cyber attackers continuously aim to surpass security measures using evolving techniques and tactics. Behind these attacks lie various motivations, including financial gain, national security threats, espionage activities, or showcasing cyber attack capabilities.

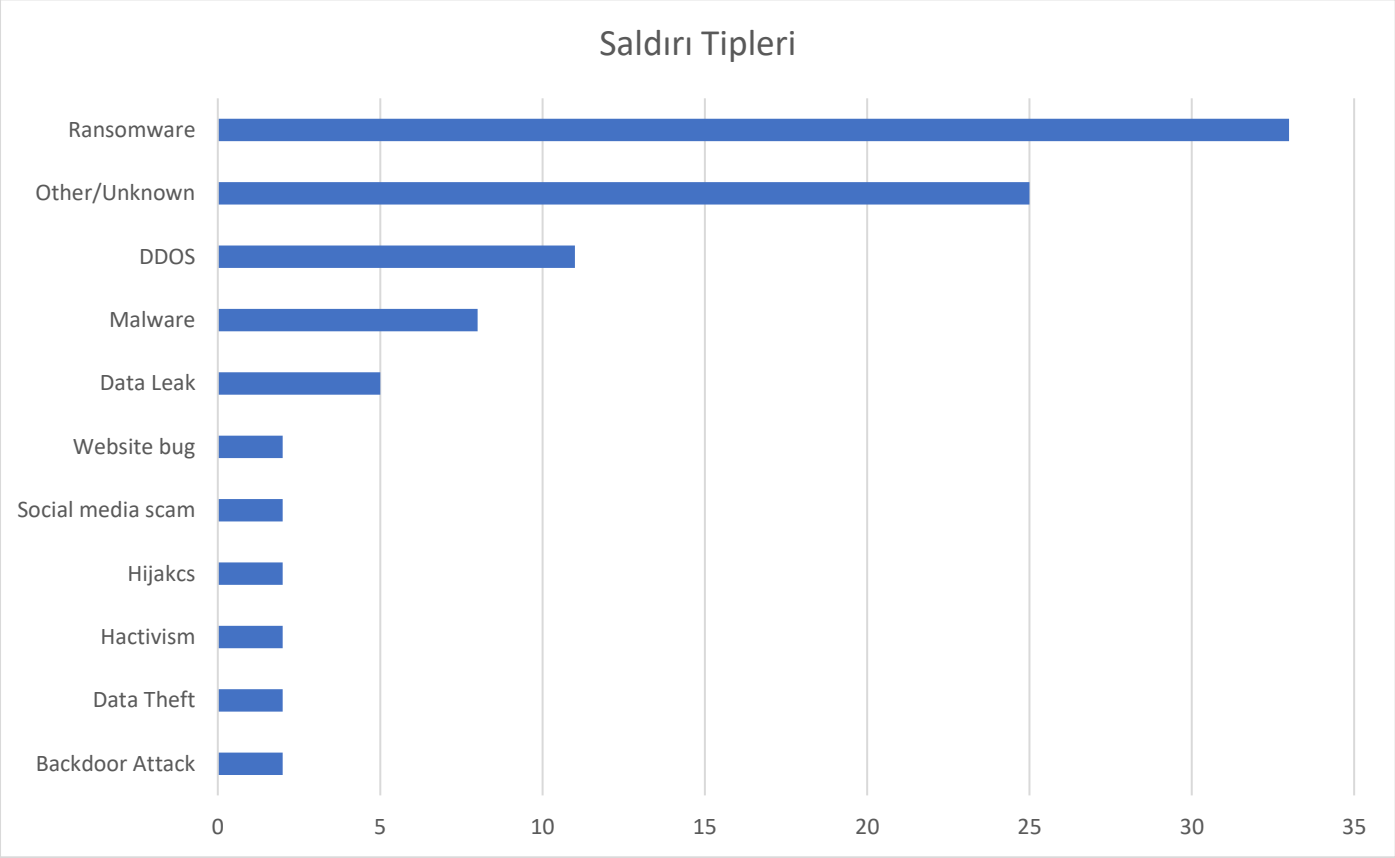
The aviation sector is a constantly evolving field in terms of cybersecurity. In order to mitigate future threats, the industry should regularly review security policies, invest in staff training, and closely monitor technological advancements.

This report aims to help executives in the aviation sector become aware of cybersecurity threats and take necessary measures to protect their companies.

Cyber Thread on Aviation Industry

In recent years, along with rapidly advancing technology, cyber attacks have become an increasingly serious threat. While these threats affect nearly every industry, sectors involving critical infrastructure and sensitive information, such as the aviation industry, are particularly targeted. The cyber attacks witnessed in the aviation sector over the past six months underscore the magnitude of this danger.

Over the past six months, cyber attacks in the aviation sector have become an increasingly concerning issue. The attacks, which have become more sophisticated and complex than previously thought, have tested the sector's defense mechanisms and intensified the focus on cybersecurity. These attacks can serve different purposes, such as leveraging air transportation for financial gain, posing a threat to national security, or causing reputational damage.



Grafik 1 Attack Types

The impacts of cyber attacks in the aviation sector can be quite severe. For instance, an attack on air traffic control systems could lead to disruptions in aircraft navigation, chaotic situations, and even potential accidents. The theft of customer information from airlines could result in identity theft and fraud. Additionally, cyber attacks on aircraft manufacturers or other aviation companies could have significant economic consequences, such as the theft of trade secrets and the loss of competitive advantage.

This report aims to examine the cyber attacks that have occurred in the aviation sector over the past six months, with the goal of understanding the magnitude of this threat and assessing the industry's future security measures. Additionally, we will delve into the motivations behind these attacks, the types of attacks observed, and the measures the sector is taking to combat these threats.

The aviation sector will continue to face an ongoing threat in terms of cybersecurity. However, research and technological advancements in this field can contribute to making the aviation industry more resilient against cyberattacks. This report aims to enhance awareness of cybersecurity within the aviation sector and strengthen preventive measures.

Incidents and Attacks in the First Half of the Year

Aer Lingus

In a ransomware attack, the data of 5,000 Aer Lingus personnel was compromised as attackers found a way to exploit the MOVEit Transfer software. The attack was attributed to a prolific Russian cybercriminal group known as Clop, recognized for targeting industrial entities with ransomware attacks and extortion tactics.

US Airlines

"The incident on January 10, 2023, saw attackers claiming that they could cancel and postpone flights belonging to US Airlines, along with the alleged capability to issue physical identity cards for airline personnel. They also claimed to have gained access to the No-Fly List.

Eurocontrol

European air traffic control confirmed that its website was under attack by pro-Russian hackers. Eurocontrol verified that its website had been 'under attack' since April 19, with the responsibility for the interruption claimed by 'pro-Russian hackers'

Scandinavian Airlines

Scandinavian airline reported falling victim to a cyberattack and urged its customers to refrain from using its application. As a result of the attacks on the company's website and application, it was announced that customer information had been compromised.

Colombia

On January 10, 2023, attackers claimed to have gained control over the No-Fly List, allowing them to cancel and delay flights belonging to US Airlines and even produce physical identity cards for airline personnel.

Safiran Airport

On June 18, 2023, a hacker group named 'Hooshyaran-e Vatan' claims to have breached the Safiran Airport Services database, alleging that a sample dataset containing various emails and invoices has been leaked.

Safiran Airport Services

British Air

On June 18, 2023, a hacker group known as 'Hooshyaran-e Vatan' claims to have leaked the database information of Safiran Airport Services. The alleged leaked sample dataset includes various emails and invoices..

.

Kenya Airport Authority Medusa Ransomware

In March 2023, the Medusa ransomware group targeted Kenya Airport company. Medusa Ransomware demanded a ransom of $500,000 in exchange for 514 GB of data. The alleged data includes crucial information such as employees' identification photos.

KAA

APT Groups Targeting the Aviation Sector in the Last 6 Months

As a result of assessments conducted by our team, it has been identified that certain APT groups have targeted the aviation sector since the beginning of this year. For the purpose of informing, the information related to these APT groups is provided below in the report.

Bitwise SPIDER

The Bitwise Spider APT group is an Advanced Persistent Threat entity that specifically targets countries with government institutions, large corporations, and critical infrastructures, notably in the defense, energy, communication, and technology sectors. Saldırılarda kullanılan zafiyetler ve saldırı teknikleri:

- Active Directory
- Shadow copy
- UAC Bypass
- ESXI

"Bitwise Spider employs sophisticated attack vectors to infiltrate target networks. These include phishing emails, exploiting vulnerabilities, malware injection, social engineering, and advanced process hijacking techniques.

The Bitwise Spider APT group utilizes customized malicious software tailored for espionage activities. These malicious tools are designed for covert operations and are often challenging to detect using conventional malware analysis methods. Bitwise Spider is known for developing two prominent malware families: LockBit Ransomware and StealBit InfoStealer Malware."

The Impact of the Bitwise Spider APT Group on Organizations:

1. Data Theft
2. Reputation Damage
3. Financial Losses
4. Decreased Competitive Advantage
5. Attack Costs

Berserk Bear

Berserk Bear, also known as Energetic Bear or Dragonfly, is an Advanced Persistent Threat (APT) group engaged in cyber espionage activities.

The focus of Berserk Bear's operations is organizations within the energy sector, particularly energy grids, oil and gas companies, and other critical infrastructure providers.

By gaining unauthorized access to these systems, the group aims to gather intelligence, disrupt operations, and establish control over significant resources.

Berserk Bear employs a variety of advanced techniques and tactics to reach its targets. These include **spear-phishing** campaigns where carefully crafted emails, often containing malicious attachments or links, are sent to specific individuals. The group also resorts to **watering hole** attacks, compromising legitimate websites frequently visited by their targeted organizations and utilizing malicious software or vulnerabilities.

Berserk Bear notably showcases the capability to exploit vulnerabilities in software and systems used in industrial control systems (ICS). Its ability to compromise critical infrastructure presents significant risks to the targeted organizations and the overall stability of affected sectors.

The group gained international attention for its role in affecting energy grids in Ukraine in 2015 and 2016, highlighting its capabilities and potential impact. While the energy sector remains a primary focus, Berserk Bear's attacks have also been observed on organizations in other sectors and countries, including the United States and Europe.

Due to the covert nature of its operations, detailed information about Berserk Bear is typically limited and closely guarded. Security researchers and government agencies continue to monitor its activities to understand and counter the threats posed by this persistent and highly capable APT group

MuddyWater

The MuddyWater APT group is an advanced persistent threat (APT) group that conducts attacks against various national and international targets.

First identified in 2017, this group is known for its active campaigns targeting public institutions, telecommunications companies, universities, and other sectors primarily in the Middle East and Asia."

MuddyWater's attacks typically involve advanced social engineering techniques, complex malware attacks, and targeted phishing campaigns. The group attempts to infiltrate target systems through messages that appear trustworthy, such as fake documents or Word and Excel files. In their attacks, they employ sophisticated privacy and evasion techniques to avoid detection.

The objectives of MuddyWater may include information gathering, espionage, data exfiltration, and gaining control over networks. Known as an adept actor capable of executing complex attacks, the group continuously refines its tactics and techniques.

The activities of the MuddyWater APT group are closely monitored and analyzed by information security experts and cybersecurity teams. This continuous tracking helps to gather insights into new attack trends and methods, enabling the development of defense strategies.

ALPHA SPIDER

The Alpha Spider APT group is an advanced persistent threat (APT) group known for conducting cyber attacks with a strong emphasis on maintaining secrecy.

Alpha Spider's attacks are typically directed towards strategic sectors such as government institutions, military organizations, energy companies, and financial institutions.

Employing sophisticated targeted attack techniques, this group attempts to infiltrate systems and aims to acquire sensitive data.

Alpha Spider is known for its cyber espionage activities, often aiming to achieve objectives such as information gathering, intellectual property theft, and leaking strategic information. The group employs advanced malware tools, exploits, and social engineering tactics in its cyber attacks. Additionally, it possesses the capability to remain undetected through advanced privacy and concealment techniques.

The Alpha Spider APT group consistently evolves and updates its attack tactics and techniques. Consequently, information security experts and cybersecurity teams continuously analyze their activities to stay abreast of their operations and update defense strategies.

Gaining further insights into the targets and attack methods of the Alpha Spider APT group is of great importance to strengthen defense mechanisms and implement more effective measures against their attacks.

ALPHA SPIDER

The Cosmic Wolf APT group is an advanced persistent threat (APT) group known for conducting cyber attacks. This group operates under the command of hackers and executes complex and sophisticated attacks against targets in various sectors.

Cosmic Wolf's targets typically encompass government agencies, military units, large corporations, and critical infrastructures, all of which hold strategic importance. The group may engage in attacks for financial gain, espionage, or political motives.

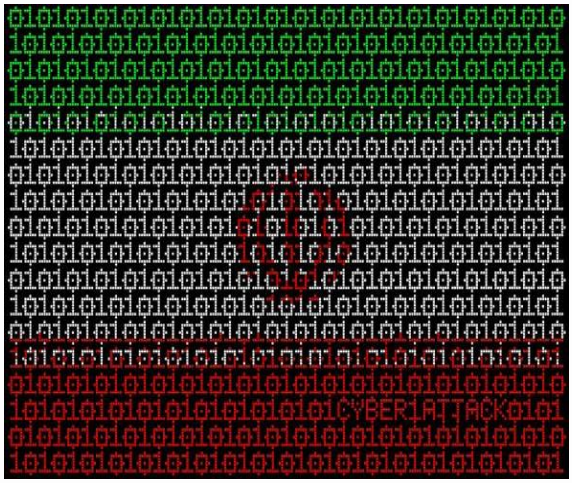
Cosmic Wolf employs advanced attack techniques to infiltrate target systems. The group undergoes an extensive intelligence gathering process to identify target organizations and uncover vulnerabilities. Subsequently, using specially crafted malicious software, exploits, and social engineering methods, they infiltrate the target systems.

Cosmic Wolf utilizes advanced obfuscation and camouflage techniques before and after attacks to hide traces within networks. This makes their detection challenging and tracking their activities, as well as thwarting their attacks, becomes more difficult.

This APT group continuously refines and updates their attack techniques, constantly renewing their efforts to surpass defense measures through advanced research and development. As a result, security experts and cybersecurity teams work tirelessly to monitor Cosmic Wolf's activities, detect their attacks, and update protection strategies.

Understanding the operations of the Cosmic Wolf APT group and bolstering defense measures are of paramount importance for targeted organizations. Collaborative efforts and information sharing within the security community play a vital role in accessing up-to-date information about the group and preventing their attacks.

APT39



APT39's focus on the telecommunications and travel industries involves creating additional access and vectors for the purpose of conducting monitoring, surveillance, or espionage operations against specific individuals. This group also gathers or facilitates the collection of private or customer data for commercial or operational purposes that serve strategic requirements related to national priorities.

Attack Lifecycle
APT39 employs various custom and publicly available malicious software and tools throughout all stages of the attack lifecycle.

APT39 is observed to take advantage of phishing emails with malicious attachments or hyperlinks, typically leading to a POWBAT infection. This group often registers domain addresses that appear to be legitimate web services and relevant to the targeted organizations, utilizing them for exploitation. Additionally, the group has routinely identified and exploited vulnerable web servers of targeted organizations to establish web shells like ANTAK and ASPXSPY, and has utilized compromised legitimate credentials to access externally facing Outlook Web Access (OWA) resources.

To establish a foothold in the target environment, APT39 leverages custom backdoors such as SEAWEED, CACHEMONEY, and a unique variant of POWBAT. During privilege escalation, observed tools include legitimate utilities like Windows Credential Editor and ProcDump, as well as freely available tools like Mimikatz and Ncrack. The group has employed custom scripts and specialized tools such as port scanners and freely available tools for command execution, like BLUETORCH.

APT39 facilitates lateral movement using numerous tools like Remote Desktop Protocol (RDP), Secure Shell (SSH), PsExec, RemCom, and xCmdSvc. Specialized tools like REDTRIP, PINKTRIP, and BLUETRIP have also been used to create SOCKS5 proxies between infected host systems. In addition to using RDP for lateral movement, APT39 has employed this protocol to maintain persistence in a victim environment. To conclude their tasks, APT39 often archives stolen data using compression tools like WinRAR or 7-Zip.

ECHO

CYBER THREAT INTELLIGENCE