SOCRadar®
Your Eyes Beyond

AVIATION INDUSTRY

Quarterly Incident Report (2024 Q1)

SOCRadar®
Your Eyes Beyond

Table of Contents

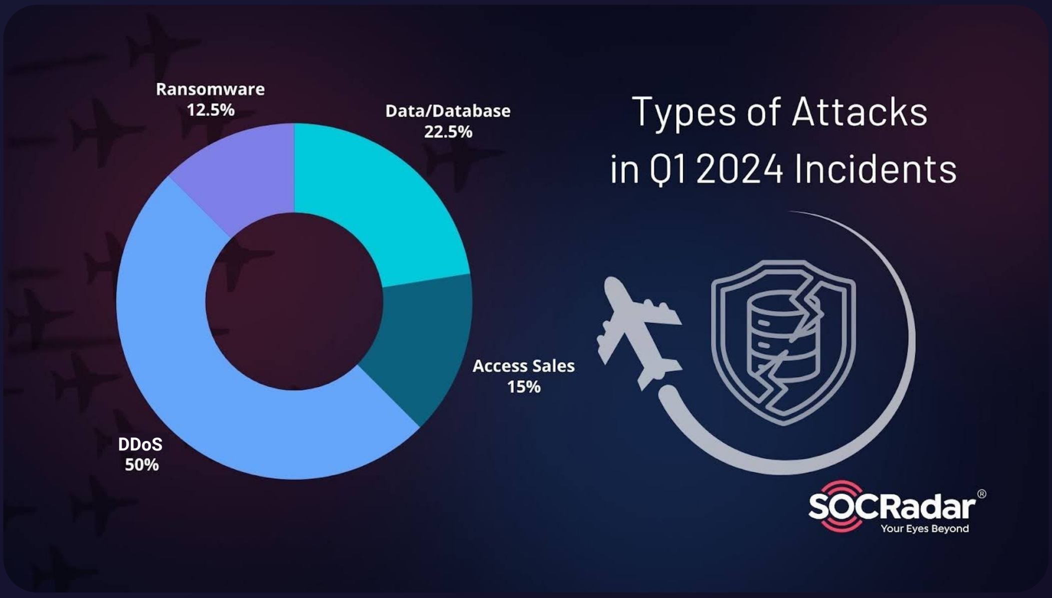
Executive Summary

In the first quarter of 2024, the aviation industry faced a multifaceted array of cybersecurity threats that highlighted its vulnerabilities and cybercriminals' persistent sophistication. This report delves into detailed incidents detected and analyzed through SOCRadar's comprehensive monitoring of hacker forums, Telegram channels, and dark web platforms.

Our findings underline the prevalent types of attacks and the significant focus on specific carriers and infrastructure, underscoring the pressing need for advanced security measures and proactive threat intelligence in the sector.

Cybersecurity Incident Statistics Analysis

The analysis of cybersecurity incidents in Q1 2024 reveals a disconcerting landscape of threats targeting the global aviation industry. We observed that:



Types of Attacks in Q1 2024 Incidents

- **Distributed Denial of Service (DDoS) Attacks:** Representing the most frequent type of incident, DDoS attacks constituted 50% of all reported cases. These attacks disrupt services and operations, causing significant downtime and financial losses.

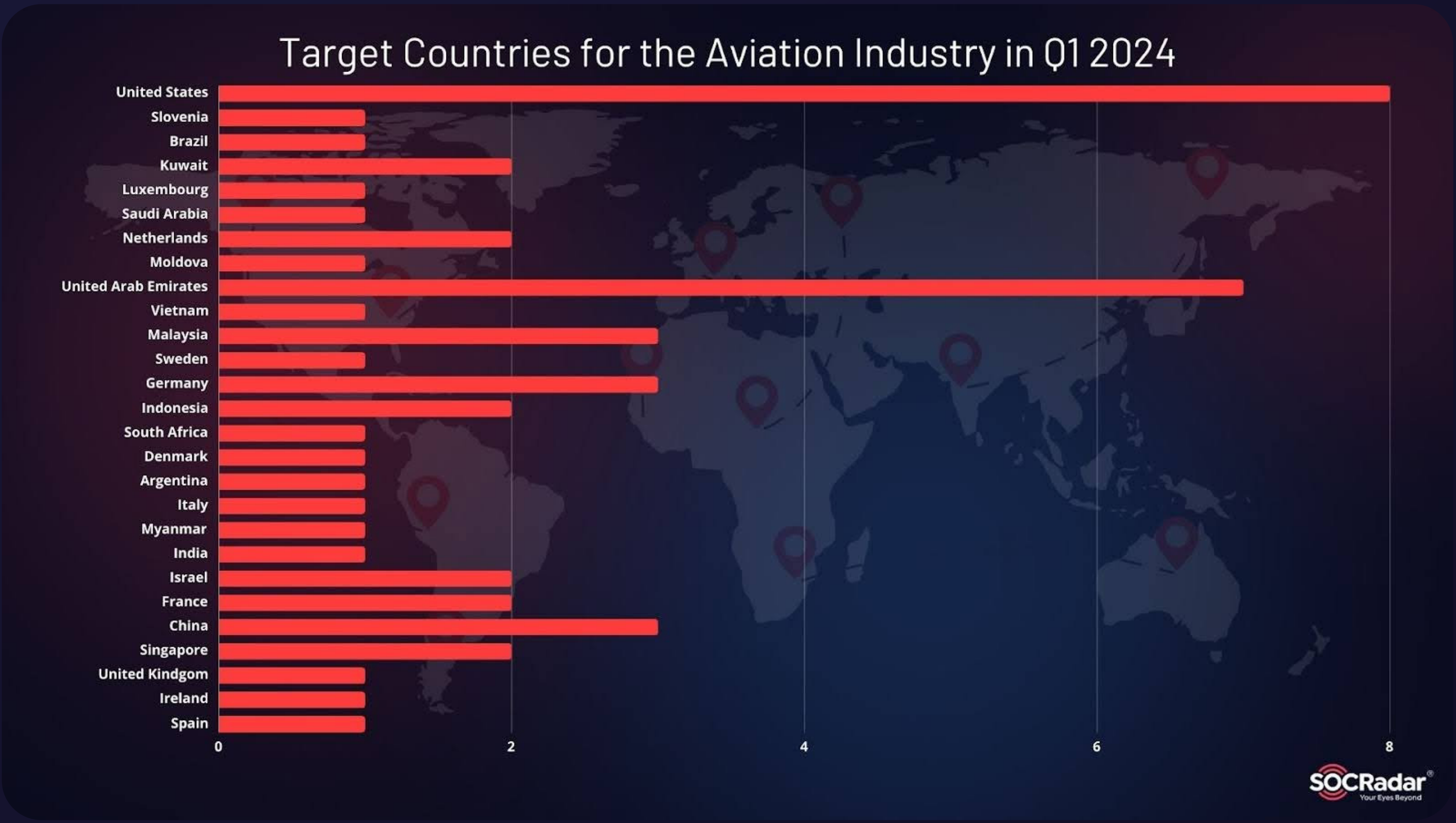
- **Data/Database Breaches:** Comprising 22.5% of the incidents, these breaches involved unauthorized access to sensitive data, affecting both operational security and consumer privacy.

- **Access Sales:** Amounting 15% of the total, this category highlights a troubling trend in the sale of initial access to systems, which can lead to further breaches and exploitation.

- **Ransomware Attacks:** Making up 12.5% of the incidents, these attacks continue to pose a severe threat by encrypting critical data and demanding ransom, reflecting cybercriminals' continued focus on monetizing their intrusions.

Analysis of Targeted Countries

In the first quarter of 2024, cyber threats to the aviation industry were distributed unevenly across various nations, each experiencing different levels of cyber risk. Here is a breakdown expressed as a percentage of total incidents, coupled with insights into possible motivations behind these attacks:



Target Countries for the Aviation Industry in Q1 2024

Highly Targeted Nations: The United States and the United Arab Emirates, with about 16% and 14% of incidents, respectively, are prominent targets. Their extensive air traffic, high economic stakes, and geopolitical significance make them attractive for both financially and politically motivated attacks. The high percentage reflects a mix of opportunistic breaches aimed at financial gain and strategic attacks possibly linked to Islamic-oriented or pro-Russian hacktivist threat actors.

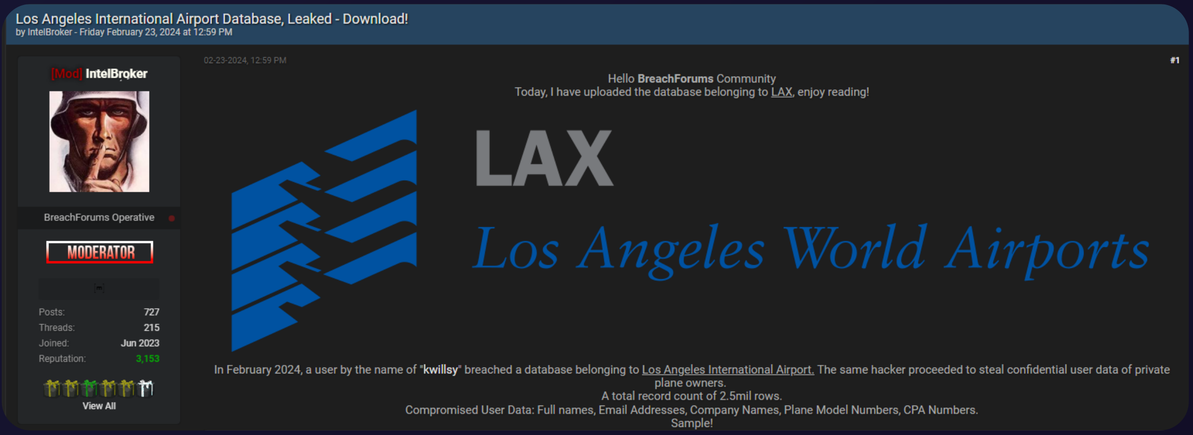
Moderately Targeted Nations: Germany, China, and Malaysia, each accounting for about 6% of the incidents, and Kuwait and the Netherlands at 4% each, also indicate targeted motives. Economic espionage and competitive intelligence gathering are likely incentives, especially in countries with advanced technological infrastructures and substantial commercial traffic.

Rarely Targeted Nations: Including countries like Brazil, Slovenia, and Luxembourg, each at about 2%, these incidents, though less frequent, might be exploratory in nature or tests for broader campaigns. The impact, even from single incidents, can be significant, suggesting that no nation is truly immune. The low frequency does not diminish the potential severity and disruptive capabilities of these attacks.

Data Breaches Account for 22.5% of Attack Types

Let's delve into the significant Data/Database claims detected by the SOCRadar Dark Web Team. This section explores various allegations and incidents involving data access and breaches within the aviation industry, as uncovered on dark web platforms.

Alleged Database Leak at Los Angeles International Airport Affects Private Plane Owners



Los Angeles International Airport Database, Leaked - Download!
by IntelBroker - Friday February 23, 2024 at 12:59 PM

[Mod] IntelBroker
BreachForums Operative
MODERATOR

Posts:	727
Threads:	215
Joined:	Jun 2023
Reputation:	3,153

View All

02-23-2024, 12:59 PM #1

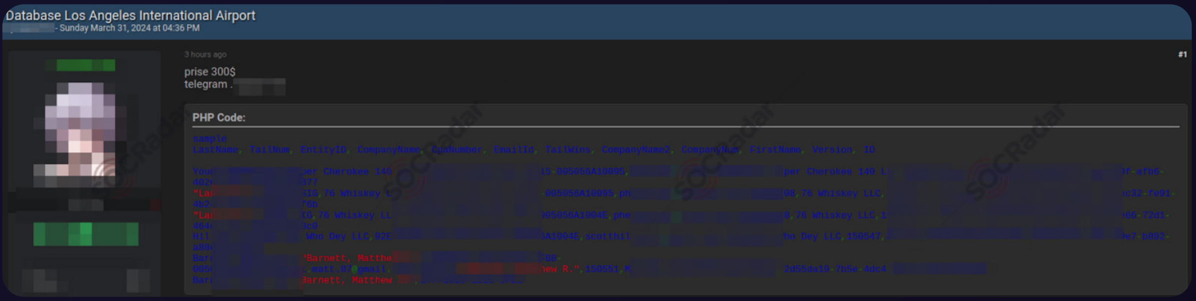
Hello **BreachForums** Community
Today, I have uploaded the database belonging to LAX, enjoy reading!

In February 2024, a user by the name of "**kwillsy**" breached a database belonging to Los Angeles International Airport. The same hacker proceeded to steal confidential user data of private plane owners.
A total record count of 2.5mil rows.
Compromised User Data: Full names, Email Addresses, Company Names, Plane Model Numbers, CPA Numbers.
Sample!

IntelBroker claiming to have leaked LAX data

On February 23, The SOCRadar Dark Web Team reported a post on a hacker forum where the notorious threat actor, **IntelBroker,** announced an alleged database leak concerning Los Angeles International Airport (LAX). According to IntelBroker, the leak occurred earlier in February 2024 and was orchestrated by a different threat actor, specifically targeting private plane owners.

The breach reportedly compromised about 2.5 million records. The stolen information includes full names, CPA numbers, email addresses, company names, plane model numbers, and tail numbers. This breach underscores the significant privacy risks facing the aviation sector.



Database Los Angeles International Airport
[redacted] - Sunday March 31, 2024 at 04:36 PM

3 hours ago #1

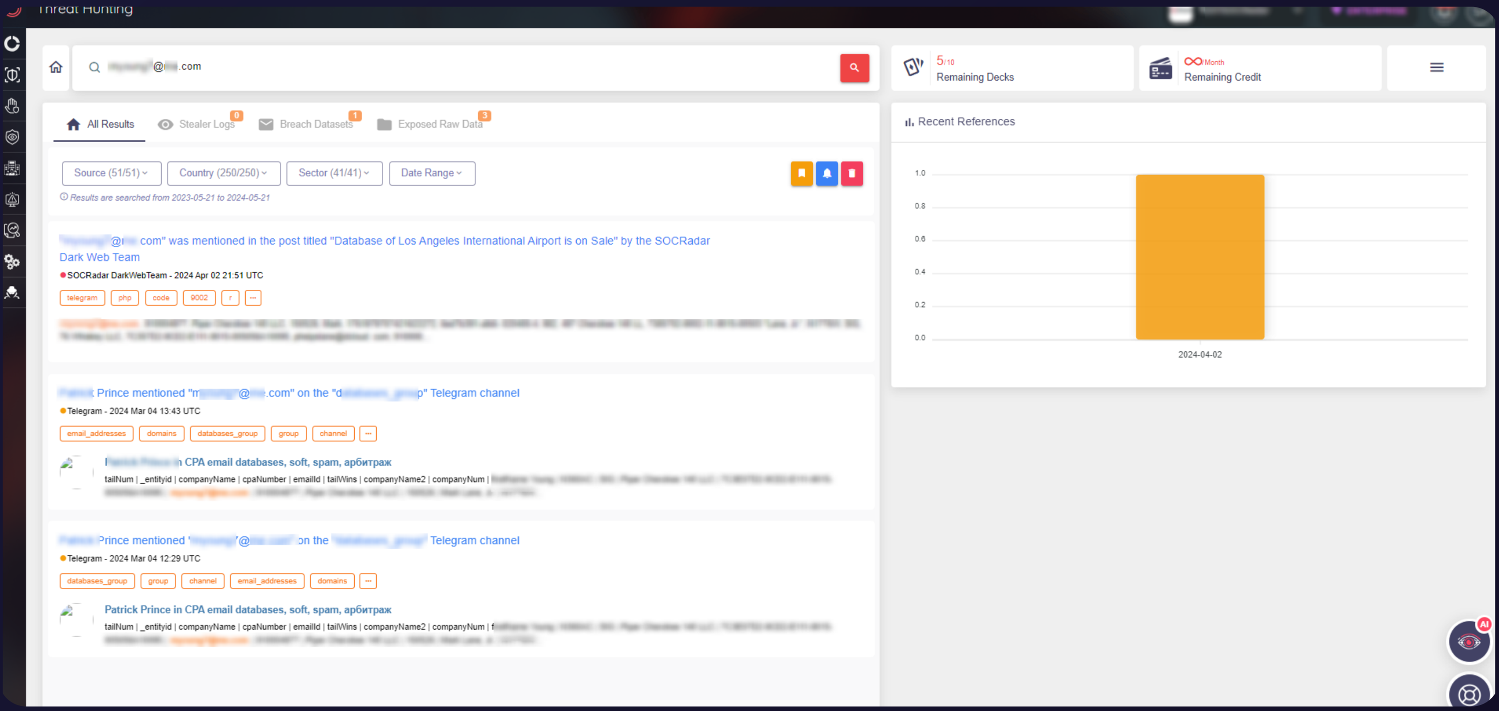
prise 300$
telegram . [redacted]

PHP Code:

```
sample
LastName, TailNum, EntityID, CompanyName, CpaNumber, EmailId, TailWins, CompanyName2, CompanyNum, FirstName, Version, ID
[redacted]
```

The post that shared on March 31

IntelBroker's claim garnered considerable attention across various platforms, including other dark web forums. Further complicating matters, the data was later republished and resold by other threat actors, treating it as a new breach. For instance, a post dated March 31 attempted to sell this data for $300.



[redacted]@[redacted].com

Results are searched from 2023-05-21 to 2024-05-21

"[redacted]@[redacted]com" was mentioned in the post titled "Database of Los Angeles International Airport is on Sale" by the SOCRadar Dark Web Team

● SOCRadar DarkWebTeam - 2024 Apr 02 21:51 UTC

telegram | php | code | 9002 | r | ···

[redacted]

[redacted] Prince mentioned "m[redacted]@[redacted].com" on the "d[redacted]p" Telegram channel

● Telegram - 2024 Mar 04 13:43 UTC

email_addresses | domains | databases_group | group | channel | ···

[redacted] CPA email databases, soft, spam, арбитраж

tailNum | _entityid | companyName | cpaNumber | emailId | tailWins | companyName2 | companyNum | [redacted]

[redacted] Prince mentioned "[redacted]@[redacted]" on the "[redacted]" Telegram channel

● Telegram - 2024 Mar 04 12:29 UTC

databases_group | group | channel | email_addresses | domains | ···

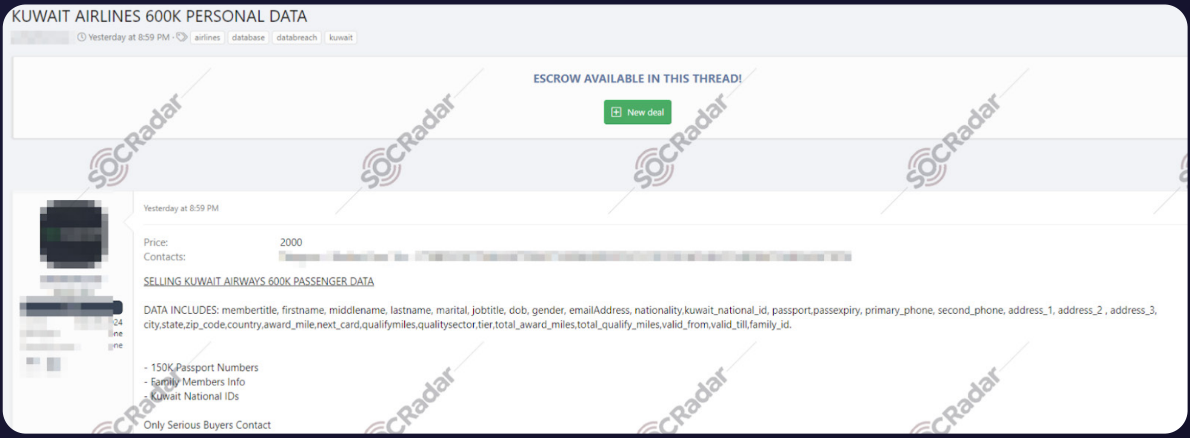
Patrick Prince in CPA email databases, soft, spam, арбитраж

tailNum | _entityid | companyName | cpaNumber | emailId | tailWins | companyName2 | companyNum | f[redacted]

Target Countries for the Aviation Industry in Q1 2024

Research conducted using the SOCRadar **Threat Hunting module,** with a sample email address from the leaked data, revealed that the information was also disseminated across Telegram channels. This incident highlights the aviation industry's growing appeal to cybercriminals and the ongoing challenges in protecting sensitive information.

Alleged Sale of Kuwait Airways Passenger Data Detected on Hacker Forum



KUWAIT AIRLINES 600K PERSONAL DATA

[redacted] Yesterday at 8:59 PM · airlines database databreach kuwait

ESCROW AVAILABLE IN THIS THREAD!

[redacted]

Yesterday at 8:59 PM

Price: 2000
Contacts: [redacted]

SELLING KUWAIT AIRWAYS 600K PASSENGER DATA

DATA INCLUDES: membertitle, firstname, middlename, lastname, marital, jobtitle, dob, gender, emailAddress, nationality,kuwait_national_id, passport,passexpiry, primary_phone, second_phone, address_1, address_2 , address_3, city,state,zip_code,country,award_mile,next_card,qualifymiles,qualitysector,tier,total_award_miles,total_qualify_miles,valid_from,valid_till,family_id.

- 150K Passport Numbers
- Family Members Info
- Kuwait National IDs

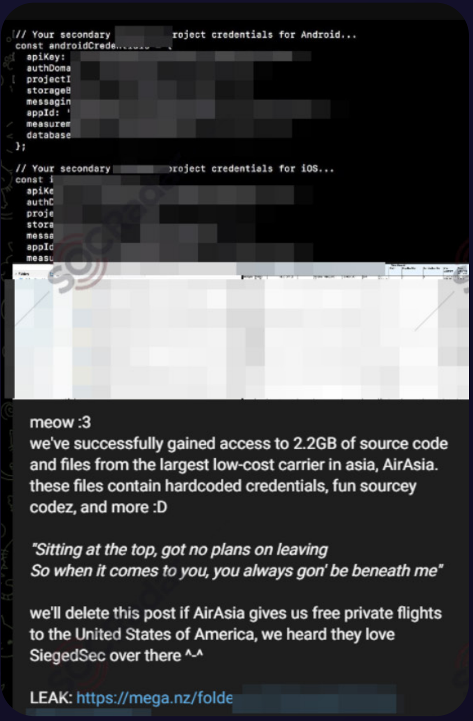
Only Serious Buyers Contact

Alleged Sale of Kuwait Airways' passenger data

On March 24, SOCRadar analysts detected a post on a popular Russian-speaking hacker forum, where a threat actor claimed to be selling a database of 600,000 Kuwait Airways passengers. The asking price for the data is set at $2,000. The claimed database purportedly contains extensive personal details including member titles, names, marital status, job titles, dates of birth, gender, email addresses, nationalities, Kuwait national IDs, passport numbers with expiry dates, phone numbers, addresses, and other sensitive information related to the airline's frequent flier program. Additionally, the database is said to include 150,000 passport numbers and detailed information on family members

SiegedSec Claims Breach of AirAsia Systems

On March 11, the hacktivist group SiegedSec announced via their Telegram channel that they had allegedly infiltrated AirAsia's systems and obtained 2.2 GB of data. The compromised data reportedly includes source code and hardcoded credentials. Alongside their claim, SiegedSec provided a link which allegedly contains the stolen files.



```
// Your secondary [redacted]roject credentials for Android...
const androidCrede[redacted]
  apiKey: [redacted]
  authDoma[redacted]
  projectI[redacted]
  storageB[redacted]
  messagin[redacted]
  appId: [redacted]
  measurem[redacted]
  database[redacted]
};

// Your secondary [redacted]roject credentials for iOS...
const i[redacted]
  apiKe[redacted]
  authD[redacted]
  proje[redacted]
  stora[redacted]
  messa[redacted]
  appId[redacted]
  measu[redacted]
```

[redacted]

meow :3
we've successfully gained access to 2.2GB of source code and files from the largest low-cost carrier in asia, AirAsia. these files contain hardcoded credentials, fun sourcey codez, and more :D

"Sitting at the top, got no plans on leaving
So when it comes to you, you always gon' be beneath me"

we'll delete this post if AirAsia gives us free private flights to the United States of America, we heard they love SiegedSec over there ^-^

LEAK: https://mega.nz/folde[redacted]

SiegedSec's statement

SiegedSec

Country of Origin: Unknown

SiegedSec is a Hacktivist group that has been actively targeting governmental organizations and leaking their sensitive data since April 2022.

-Ransomware Group-

Motivation: Hacktivisim

Target Countries: United States, Colombia, Mexico, India, Russia, China, Belgium, Italy, Taiwan

Target Sectors: Public Administration, Information, Finance, Professional Services, Manufacturing, Retail

Attack Type: XSS, SQL Injection, Use of Automated Tools, Exfiltration, Data Leak

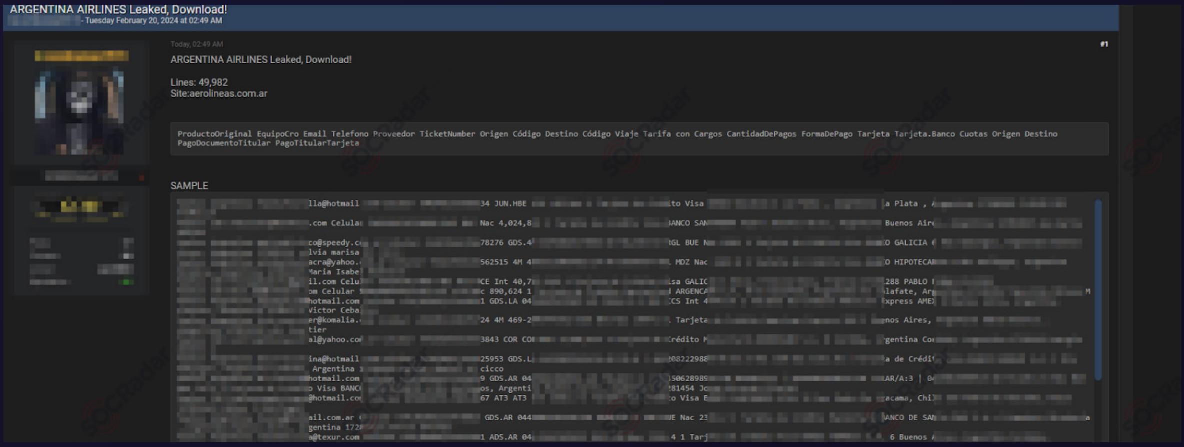
-TTPs-

Active Scanning:	T1595
Exploit Public-Facing Application:	T1190
Exfiltration Over Web Service:	T1567

SiegedSec's Threat Actor Profile Card

For further analysis and threat feed, check out our blog post about **SiegedSec.**

Customer Database of Aerolíneas Argentinas Allegedly Leaked



ARGENTINA AIRLINES Leaked, Download!
[redacted] - Tuesday February 20, 2024 at 02:49 AM

Today, 02:49 AM

#1

ARGENTINA AIRLINES Leaked, Download!

Lines: 49,982
Site:aerolineas.com.ar

```
ProductoOriginal EquipoCro Email Telefono Proveedor TicketNumber Origen Código Destino Código Viaje Tarifa con Cargos CantidadDePagos FormaDePago Tarjeta Tarjeta.Banco Cuotas Origen Destino
PagoDocumentoTitular PagoTitularTarjeta
```

SAMPLE

[redacted]

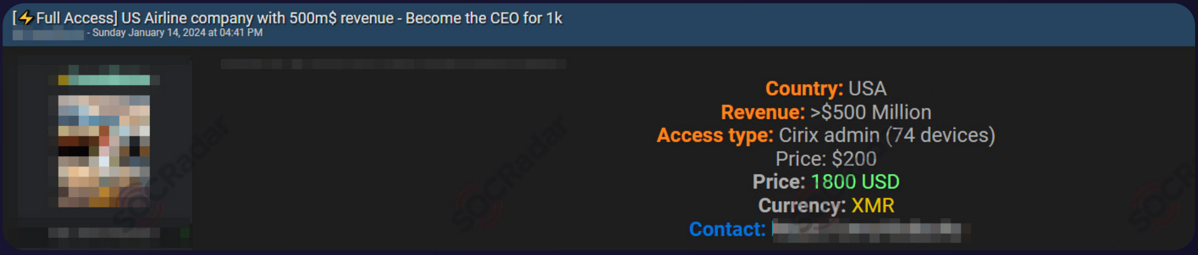
A screenshot from the hacker forum where the threat actor claims to have leaked a customer database from Aerolíneas Argentinas

On February 20, SOCRadar detected a post on a hacker forum claiming that a customer database of Aerolíneas Argentinas had been leaked. The threat actor's post titled "ARGENTINA AIRLINES Leaked, Download!" mentions the database containing 49,982 records from the site aerolineas.com.ar.

The data allegedly includes detailed customer information such as emails, phone numbers, ticket numbers, travel routes, payment details, and more.

Initial Access Sales on Dark Web

In recent investigations, a concerning trend has been observed within the aviation sector, highlighting an increase in the listings for unauthorized access to systems and databases on various hacker forums and Telegram channels. This growing threat poses a significant risk to the security of airlines, airports, and related infrastructure, underscoring the urgent need for heightened vigilance and enhanced protective measures throughout the industry.



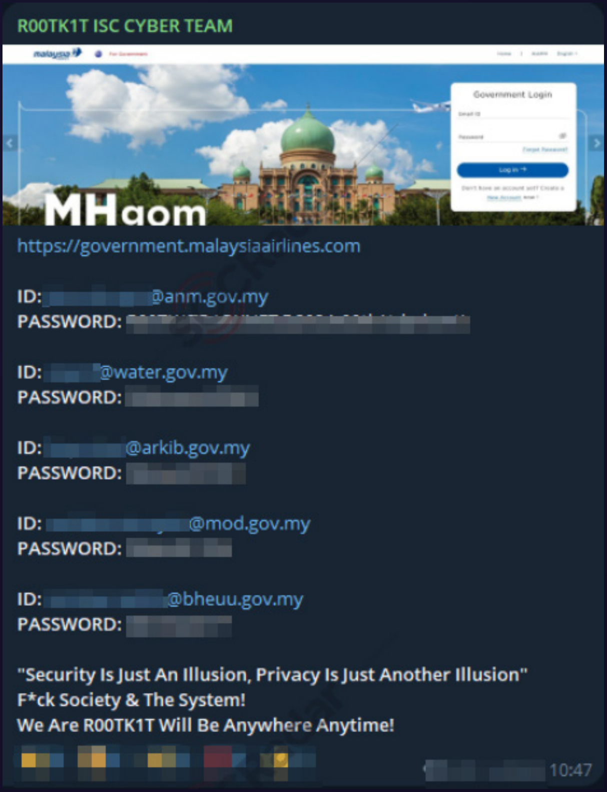
[⚡Full Access] US Airline company with 500m$ revenue - Become the CEO for 1k
[redacted] - Sunday January 14, 2024 at 04:41 PM

[redacted]

Country: USA
Revenue: >$500 Million
Access type: Cirix admin (74 devices)
Price: $200
Price: 1800 USD
Currency: XMR
Contact: [redacted]

The hacker forum post offered unauthorized Citrix access to an major American airline

On January 14, The SOCRadar Dark Web Team discovered a post on a hacker forum where a threat actor claimed to offer unauthorized Citrix access for sale. This access, allegedly linked to a major American airline with revenues over $500 million, reportedly includes administrative privileges on 74 devices, with an asking price of $1,800 USD. The specific airline was not named in the post.



R00TK1T ISC CYBER TEAM

https://government.malaysiaairlines.com

ID: [redacted]@anm.gov.my
PASSWORD: [redacted]

ID: [redacted]@water.gov.my
PASSWORD: [redacted]

ID: [redacted]@arkib.gov.my
PASSWORD: [redacted]

ID: [redacted]@mod.gov.my
PASSWORD: [redacted]

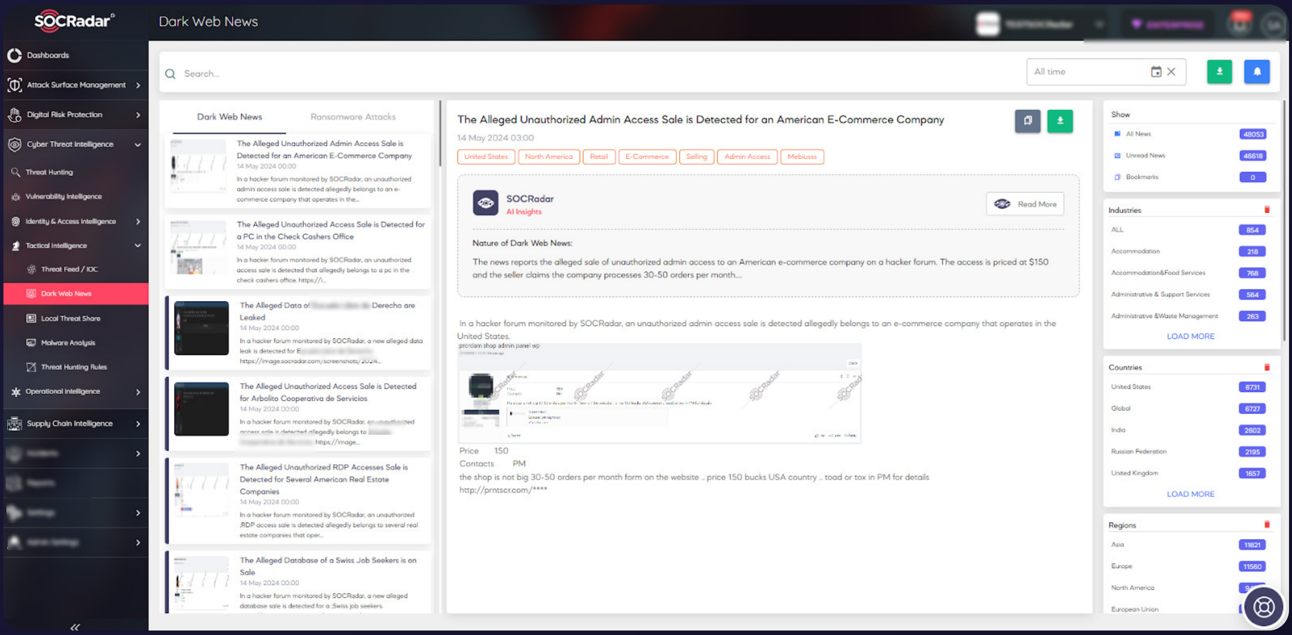
ID: [redacted]@bheuu.gov.my
PASSWORD: [redacted]

"Security Is Just An Illusion, Privacy Is Just Another Illusion"
F*ck Society & The System!
We Are R00TK1T Will Be Anywhere Anytime!

[redacted] 10:47

The Telegram post claimed unauthorized access to Malaysia Airlines email accounts

Further complicating the security landscape, another post was detected by The SOCRadar Dark Web Team on March 14. This time, the threat was found on a Telegram channel, where a threat group allegedly claimed to have obtained unauthorized access to email accounts associated with Malaysia Airlines. The compromised information is said to include sensitive login details for various Malaysian government email domains, along with their corresponding passwords.



The Alleged Unauthorized Admin Access Sale is Detected for an American E-Commerce Company
14 May 2024 00:00
In a hacker forum monitored by SOCRadar, an unauthorized admin access sale is detected allegedly belongs to an e-commerce company that operates in the...

The Alleged Unauthorized Access Sale is Detected for a PC in the Check Cashers Office
14 May 2024 00:00
In a hacker forum monitored by SOCRadar, an unauthorized access sale is detected that allegedly belongs to a pc in the check cashers office. https://i...

The Alleged Data of [redacted] Derecho are Leaked
14 May 2024 00:00
In a hacker forum monitored by SOCRadar, a new alleged data leak is detected for E[redacted]
https://image.socradar.com/screenshots/2024...

The Alleged Unauthorized Access Sale is Detected for Arbolito Cooperativa de Servicios
14 May 2024 00:00
In a hacker forum monitored by SOCRadar, [redacted] access sale is detected allegedly belongs to [redacted] https://image...

The Alleged Unauthorized RDP Accesses Sale is Detected for Several American Real Estate Companies
14 May 2024 00:00
In a hacker forum monitored by SOCRadar, an unauthorized ,RDP access sale is detected allegedly belongs to several real estate companies that oper...

The Alleged Database of a Swiss Job Seekers is on Sale
14 May 2024 00:00
In a hacker forum monitored by SOCRadar, a new alleged database sale is detected for a ;Swiss job seekers.

The Alleged Unauthorized Admin Access Sale is Detected for an American E-Commerce Company
14 May 2024 03:00
United States | North America | Retail | E-Commerce | Selling | Admin Access | Mebiusss

SOCRadar
AI Insights

Nature of Dark Web News:

The news reports the alleged sale of unauthorized admin access to an American e-commerce company on a hacker forum. The access is priced at $150 and the seller claims the company processes 30-50 orders per month....

In a hacker forum monitored by SOCRadar, an unauthorized admin access sale is detected allegedly belongs to an e-commerce company that operates in the United States.

prordam shop admin panel wp

Price 150
Contacts PM
the shop is not big 30-50 orders per month form on the website .. price 150 bucks USA country .. toad or tox in PM for details
http://prntscr.com/****

Show	
All News	48053
Unread News	46618
Bookmarks	0

Industries	
ALL	854
Accommodation	218
Accommodation&Food Services	768
Administrative & Support Services	564
Administrative &Waste Management	263

Countries	
United States	8731
Global	6727
India	2602
Russian Federation	2195
United Kingdom	1657

Regions	
Asia	11821
Europe	11560
North America	[illegible]
European Union	[illegible]

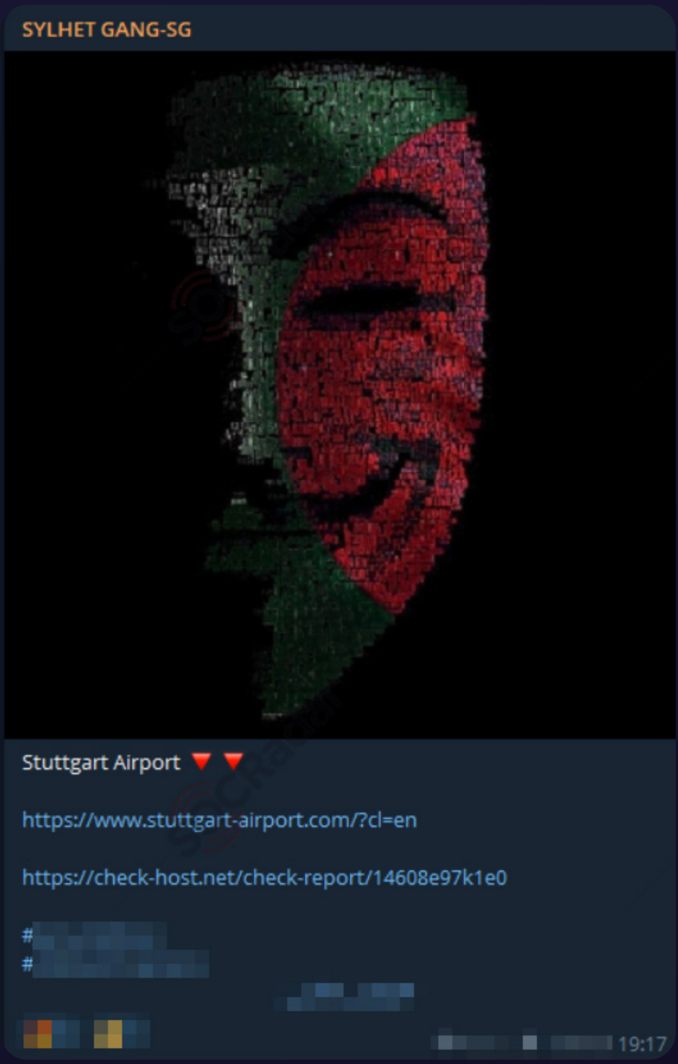
SOCRadar Dark Web News

SOCRadar's Dark Web News feature is a crucial tool for organizations looking to stay informed about the latest cybersecurity threats emerging from the dark web. This feature provides users with timely updates and detailed reports on hacker activities, discussions, and trends within deep and dark web forums, including channels on platforms like Telegram.

By leveraging this information, businesses can gain a deeper understanding of potential threats and adapt their security strategies accordingly. SOCRadar's Dark Web News acts not only as a surveillance tool but also as a strategic asset, helping companies anticipate and mitigate risks before they manifest into significant security breaches.

Cyber Attacks on Global Aviation Industry Linked to Political Motives

The aviation industry faces threats from cyber actors, driven by both financial and political motives. Among these, politically motivated actors are particularly active, employing tactics like DDoS and website defacement. These groups operate globally, utilizing platforms like Telegram to coordinate their attacks against the aviation sector.



SYLHET GANG-SG

Stuttgart Airport 🔻🔻

https://www.stuttgart-airport.com/?cl=en

https://check-host.net/check-report/14608e97k1e0

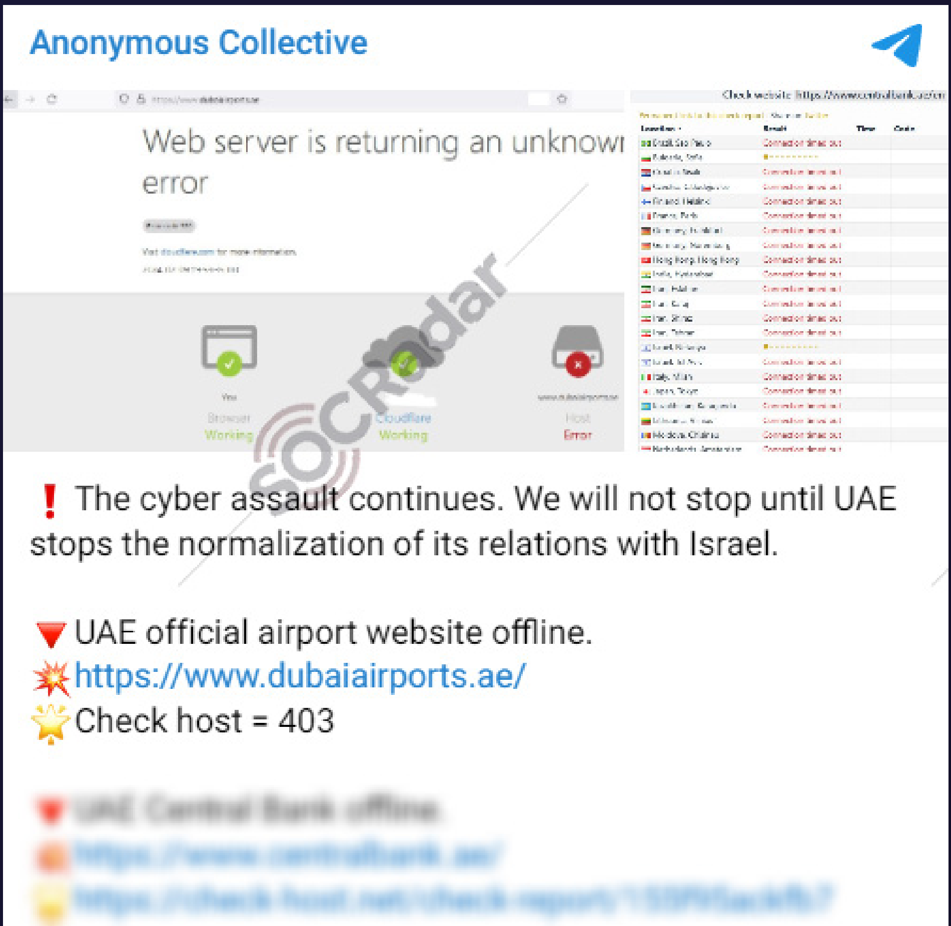
#[redacted]
#[redacted]

[redacted]

[redacted] 19:17

Announcement of Sylhet Gang - SG

According to SOCRadar's Dark Web News module, an Islamic-oriented Asian group known as Sylhet - Gang SG allegedly claimed to have disrupted the website of Stuttgart Airport in Germany with a DDoS attack on January 4. The group's claim was broadcast on its Telegram channel.



Anonymous Collective

Web server is returning an unknown error

❗ The cyber assault continues. We will not stop until UAE stops the normalization of its relations with Israel.

🔻UAE official airport website offline.
💥https://www.dubaiairports.ae/
🌟Check host = 403

[redacted]

Anonymous Collective's statement

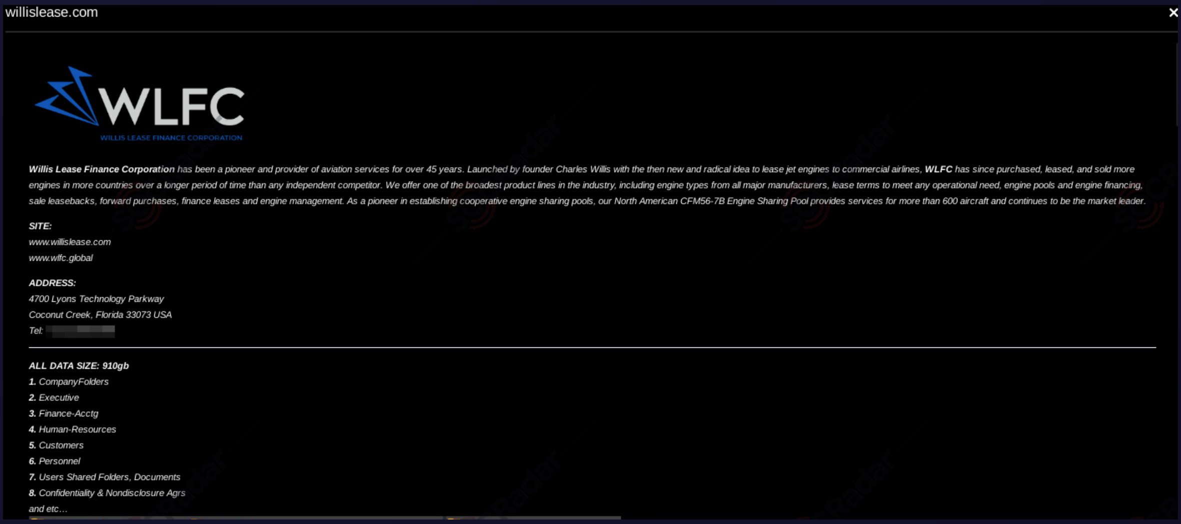
Similarly, on February 12, a group calling itself Anonymous Collective reportedly claimed to have targeted Dubai Airports in the United Arab Emirates with a DDoS attack. These claims were also made on their Telegram channel.

Threat Groups such as Sylhet Gang - SG and Anonymous Collective, particularly during the **Israel-Hamas conflict,** have been active as pro-Palestinian hacktivists, allegedly carrying out cyber attacks. The aviation industry remains a high-profile target amidst these geopolitical tensions.

SOCRadar's monitoring tools continue to track these and other cyber threats, providing insights from dark web forums, Telegram channels, and other platforms monitored by SOCRadar Dark Web Team.

Ransomware Attacks Persist in Aviation Industry

Recent findings from SOCRadar reveal that 12.52% of dark web incidents related to the aviation industry were ransomware attacks. Despite the FBI's ongoing Operation Cronos targeting the notorious LockBit ransomware group, LockBit remains active and prominent, continually updating its victim list. Notably, it ranks first among groups targeting the aviation sector.



Willis Lease Finance Corporation has been a pioneer and provider of aviation services for over 45 years. Launched by founder Charles Willis with the then new and radical idea to lease jet engines to commercial airlines, **WLFC** has since purchased, leased, and sold more engines in more countries over a longer period of time than any independent competitor. We offer one of the broadest product lines in the industry, including engine types from all major manufacturers, lease terms to meet any operational need, engine pools and engine financing, sale leasebacks, forward purchases, finance leases and engine management. As a pioneer in establishing cooperative engine sharing pools, our North American CFM56-7B Engine Sharing Pool provides services for more than 600 aircraft and continues to be the market leader.

SITE:
www.willislease.com
www.wlfc.global

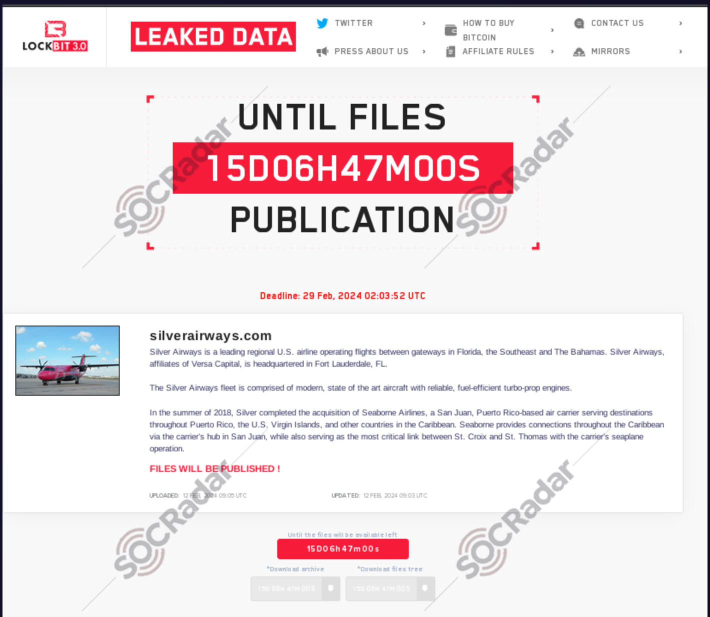
ADDRESS:
4700 Lyons Technology Parkway
Coconut Creek, Florida 33073 USA
Tel: [redacted]

ALL DATA SIZE: 910gb
1. CompanyFolders
2. Executive
3. Finance-Acctg
4. Human-Resources
5. Customers
6. Personnel
7. Users Shared Folders, Documents
8. Confidentiality & Nondisclosure Agrs
and etc...

Black Basta's announcement

Among other ransomware groups focusing on the aviation industry are Black Basta, BianLian, and Slug. On February 12, Black Basta claimed a significant breach by adding Willis Lease Finance Corporation to its victim roster, asserting infiltration into their systems.

Furthermore, on February 13, LockBit announced on their dark web platforms that they had successfully infiltrated the systems of Silver Airways.



UNTIL FILES
15D06H47M00S
PUBLICATION

Deadline: 29 Feb, 2024 02:03:52 UTC

silverairways.com

Silver Airways is a leading regional U.S. airline operating flights between gateways in Florida, the Southeast and The Bahamas. Silver Airways, affiliates of Versa Capital, is headquartered in Fort Lauderdale, FL.

The Silver Airways fleet is comprised of modern, state of the art aircraft with reliable, fuel-efficient turbo-prop engines.

In the summer of 2018, Silver completed the acquisition of Seaborne Airlines, a San Juan, Puerto Rico-based air carrier serving destinations throughout Puerto Rico, the U.S. Virgin Islands, and other countries in the Caribbean. Seaborne provides connections throughout the Caribbean via the carrier's hub in San Juan, while also serving as the most critical link between St. Croix and St. Thomas with the carrier's seaplane operation.

FILES WILL BE PUBLISHED !

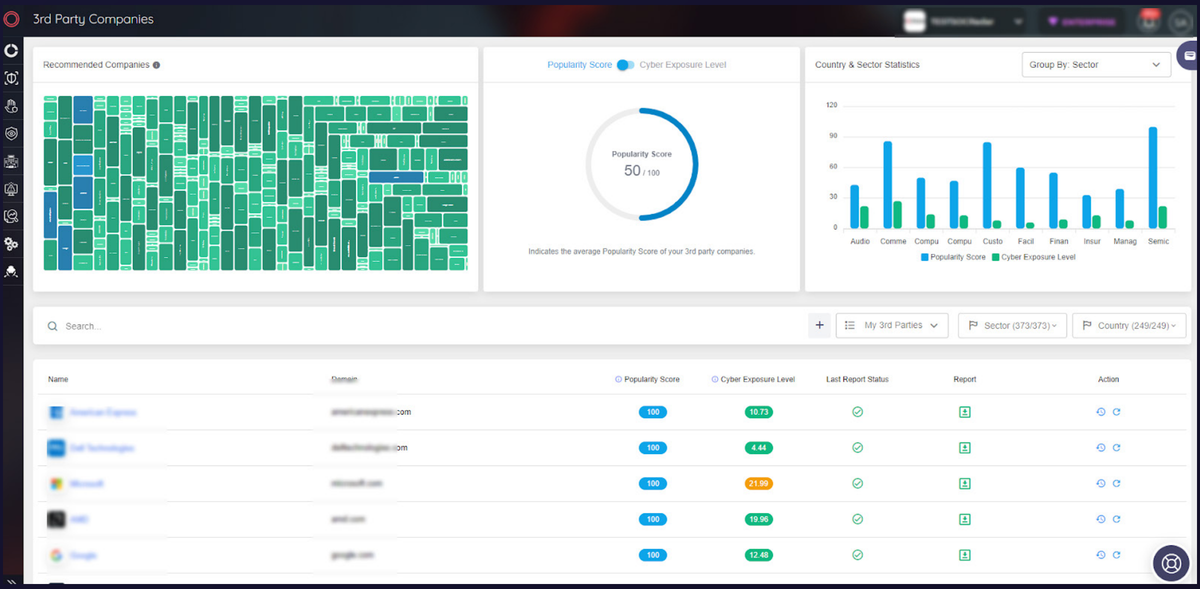
UPLOADED: 12 FEB, 2024 09:05 UTC
UPDATED: 12 FEB, 2024 09:03 UTC

Until the files will be available left
15D06h47m00s

LockBit's statement

Conclusion

The first quarter of 2024 has underscored the persistent and evolving threats facing the global aviation industry. From sophisticated DDoS attacks to intricate data breaches and ransomware infiltrations, cybercriminals continue to target critical infrastructure with increasing precision and malice. The incidents detailed in this report, ranging from the extensive data leak at Los Angeles International Airport to the sale of sensitive Kuwait Airways passenger information, highlight a crucial junction for cybersecurity within the sector.



Name	Domain	Popularity Score	Cyber Exposure Level	Last Report Status	Report	Action
[redacted]	[redacted].com	100	10.73	✓		
[redacted]	[redacted]om	100	4.44	✓		
[redacted]	[redacted]	100	21.99	✓		
[redacted]	[redacted]	100	19.96	✓		
[redacted]	[redacted]	100	12.48	✓		

SOCRadar Supply Chain Intelligence

To effectively address these challenges, the aviation industry must leverage advanced threat intelligence sources like SOCRadar's XTI platform. This platform provides an extended cyber threat intelligence solution, incorporating External Attack Surface Management (EASM) and Digital Risk Protection (DRP) to bolster defenses. Specifically, the Supply Chain Intelligence module offers real-time updates on vendors, which is crucial for managing and mitigating risks associated with third-party entities.

Who is SOCRadar®?

Your Eyes Beyond

SOCRadar provides Extended Threat Intelligence (XTI) that combines: **"Cyber Threat Intelligence, Brand Protection, External Attack Surface Management, and Dark Web Radar Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

Trusted by 21.000+ companies in 150+ countries

Dark Web Monitoring: SOCRadar's fusion of its unique Dark Web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep and Dark Web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

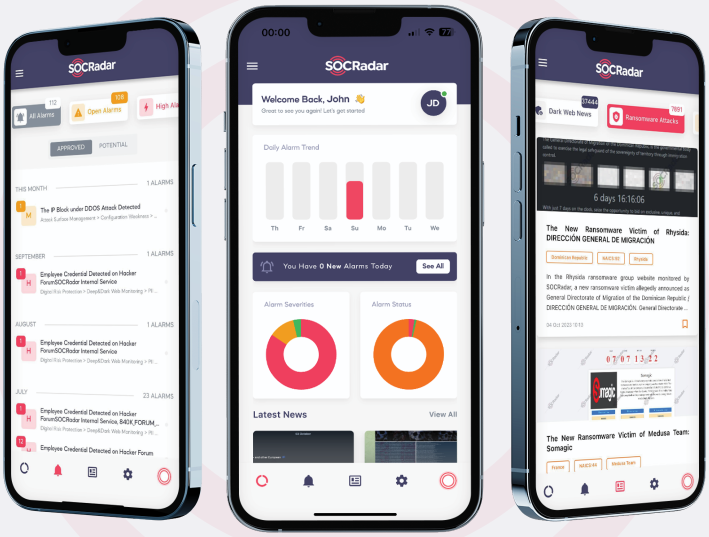
360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

GET ACCESS FOR FREE

MEET THE NEW MOBILE APP

Access threat intelligence, act on-the-go, and be instantly notified of new threats.View alerts, breaking Dark Web news, and new ransomware attacks

Download on the App Store



GET IT ON Google Play

Gartner Peer Insights™ 4.8/5 ★★★★★