ECHO
CYBER THREAT INTELLIGENCE

SECTORAL REPORT 2024

ATTACKS ON THE AVIATION SECTOR IN THE FIRST HALF OF THE YEAR

@echocti

@echocti

echocti.com

Content

Executive Summary

This executive summary addresses the importance and impact of cyber-attacks targeting the aviation industry. In recent years, cyber-attacks in the aviation industry have become a major threat to businesses. These attacks target critical infrastructure such as airline databases, reservation systems, flight systems and even air traffic control systems.

The aviation sector is a sensitive target against cyber attacks. Protection of critical infrastructures and data in the sector is of great importance for operational continuity and passenger safety. Cyber attacks can lead to serious consequences such as data theft, operational disruptions, flight cancellations and even compromising flight safety.

Cyber attackers aim to overcome security measures by using constantly evolving techniques and tactics. There are different motivations behind the attacks, such as financial gain, national security threat, espionage activities or demonstration of cyber attack capabilities.

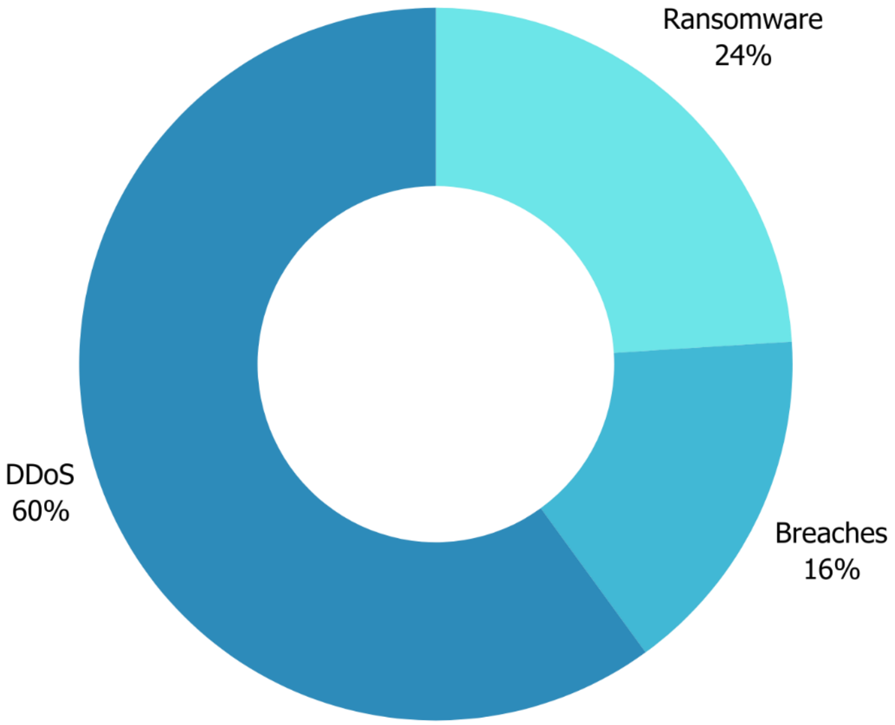


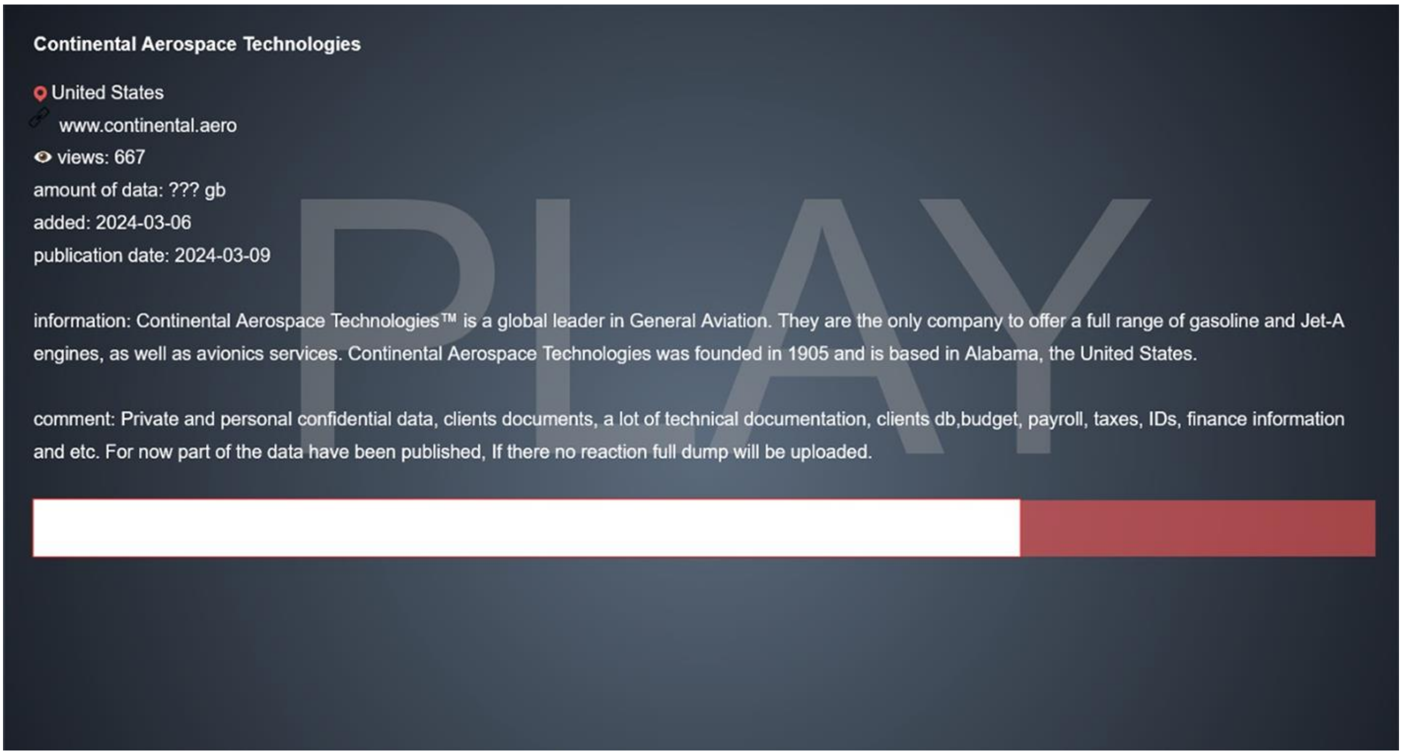
Figure 1 Types of Attacks on the Aviation Sector

The aviation industry is an area that needs to be constantly updated on cyber security. In order to prevent future threats, the sector should constantly review its security policies, invest in personnel training and closely follow technological developments.

This report aims to help managers in the aviation industry raise awareness of cyber attack threats and protect their companies by taking the necessary precautions.

Ransomware Attack

Continental Aerospace Technologies Became Victim of PLAY Ransomware



Continental Aerospace Technologies

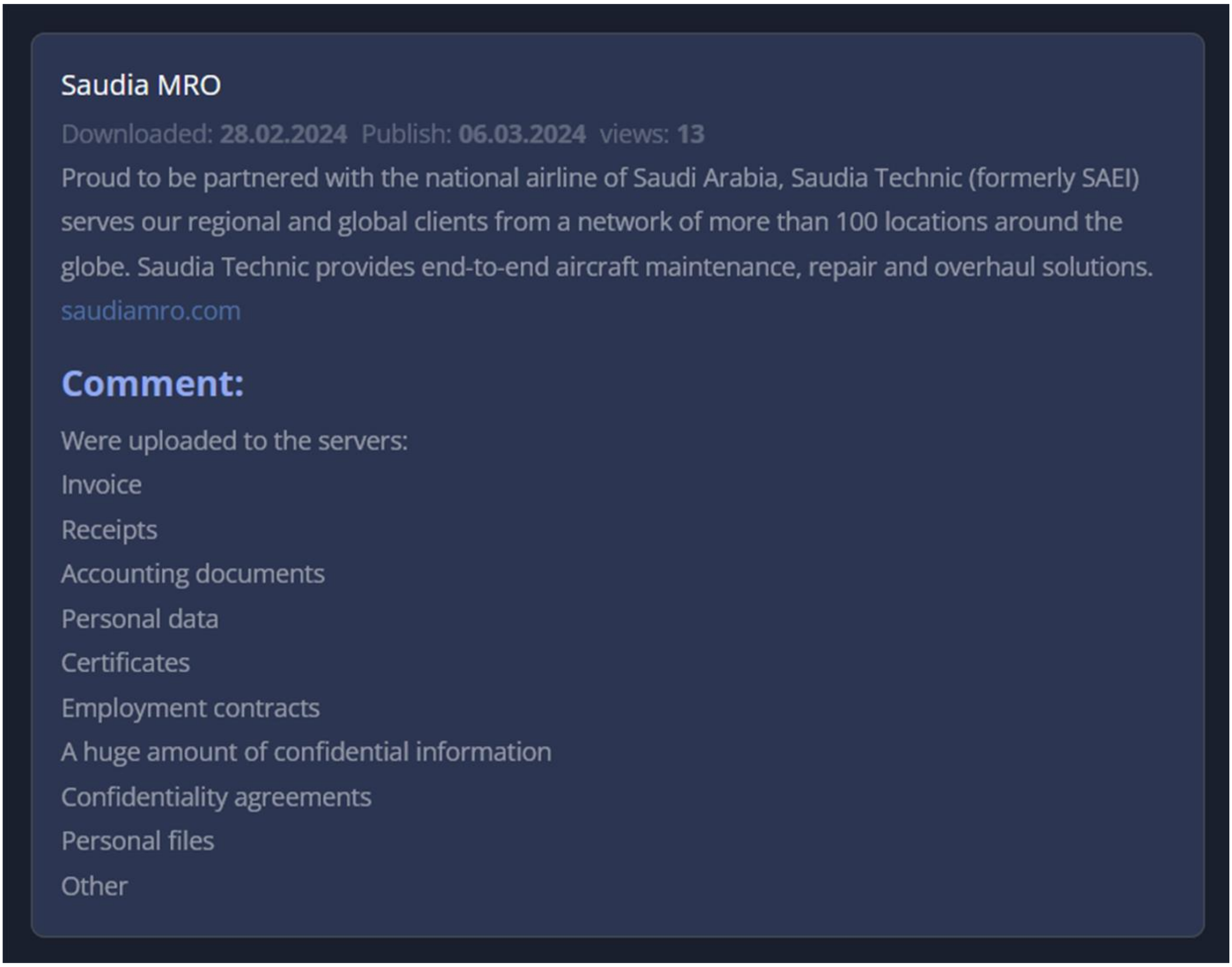
United States
www.continental.aero
views: 667
amount of data: ??? gb
added: 2024-03-06
publication date: 2024-03-09

information: Continental Aerospace Technologies™ is a global leader in General Aviation. They are the only company to offer a full range of gasoline and Jet-A engines, as well as avionics services. Continental Aerospace Technologies was founded in 1905 and is based in Alabama, the United States.

comment: Private and personal confidential data, clients documents, a lot of technical documentation, clients db,budget, payroll, taxes, IDs, finance information and etc. For now part of the data have been published, If there no reaction full dump will be uploaded.

Continental Aerospace Technologies, an Alabama-based aircraft engine manufacturer, has suffered a cyber attack attributed to PLAY ransomware. PLAY ransomware is a sophisticated malware that encrypts files and makes them inaccessible until a ransom is paid. These attacks pose a major threat to the aerospace sector, with attackers often exploiting vulnerabilities for financial gain. It is believed that the network of Continental Aerospace Technologies, the victim of the attack, was infiltrated through phishing emails, compromised software or exploiting vulnerabilities. The attackers demanded a payment from the organisation to obtain the decryption key by paying a ransom. This attack has the potential to halt production processes, jeopardise intellectual property and impact operational efficiency. Continental Aerospace Technologies collaborated with cybersecurity experts and law enforcement to investigate the incident, analyse the attack and take measures against future attacks. This attack emphasises the importance of security assessments and measures in the aviation industry.

Saudia MRO 8BASE Victim of Ransomware



Saudia MRO

Downloaded: **28.02.2024** Publish: **06.03.2024** views: **13**

Proud to be partnered with the national airline of Saudi Arabia, Saudia Technic (formerly SAEI) serves our regional and global clients from a network of more than 100 locations around the globe. Saudia Technic provides end-to-end aircraft maintenance, repair and overhaul solutions.

saudiamro.com

Comment:

Were uploaded to the servers:

Invoice

Receipts

Accounting documents

Personal data

Certificates

Employment contracts

A huge amount of confidential information

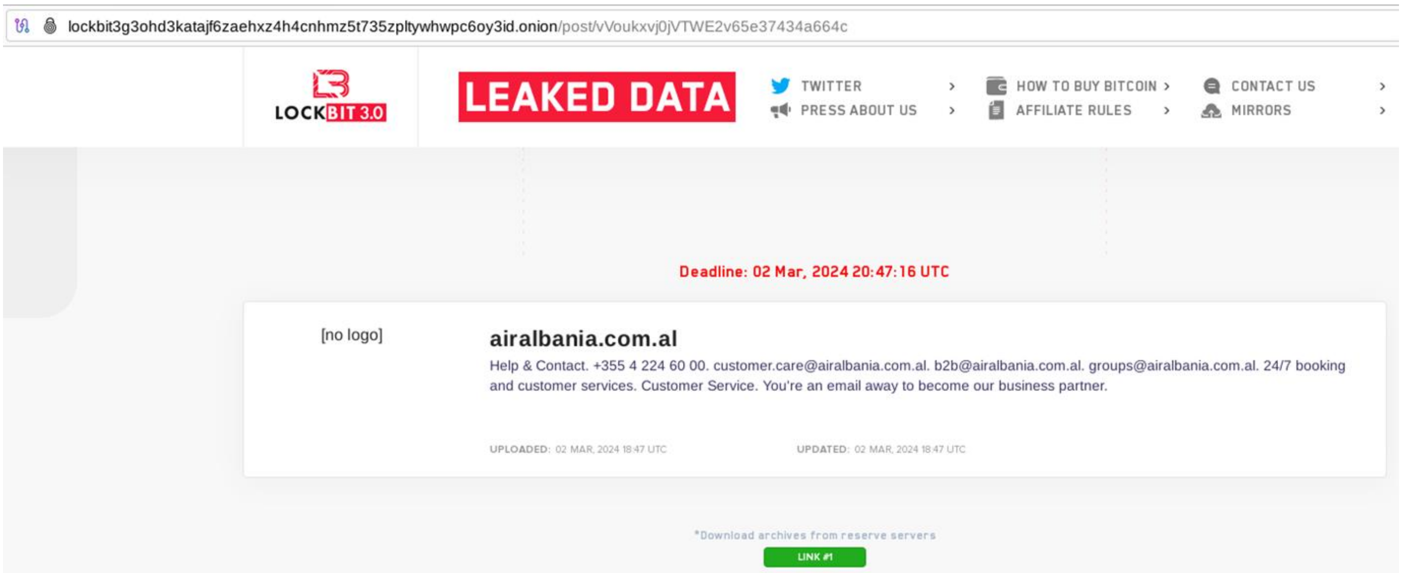
Confidentiality agreements

Personal files

Other

On 28 February 2024, Saudia Technic, the MRO division of Saudi Arabian Airlines, was the target of a serious cyber attack by the 8BASE ransomware gang. This attack highlighted vulnerabilities in aviation infrastructure and raised concerns over aircraft maintenance and operational safety. 8BASE is a sophisticated ransomware that blocks access to files until a ransom is paid. Ransomware attacks target organisations across a range of sectors for financial gain, and according to Boeing research, these attacks have increased by 600%. The attack on Saudia Technic is believed to have involved the distribution of 8BASE ransomware via phishing emails to the organisation's network. As a result of this attack, critical maintenance and operational databases, documents and communication channels were compromised, causing disruptions to Saudi Arabian Airlines services. The attack caused significant disruption to aircraft maintenance programmes, operational planning and communication systems, and caused financial and reputational damage. This incident highlights the critical importance of cyber security in the aviation industry.

Air Albania Attacked by LockBit Ransomware Group



lockbit3g3ohd3katajf6zaehxz4h4cnhmz5t735zpltywhwpc6oy3id.onion/post/vVoukxvj0jVTWE2v65e37434a664c

Deadline: 02 Mar, 2024 20:47:16 UTC

[no logo]

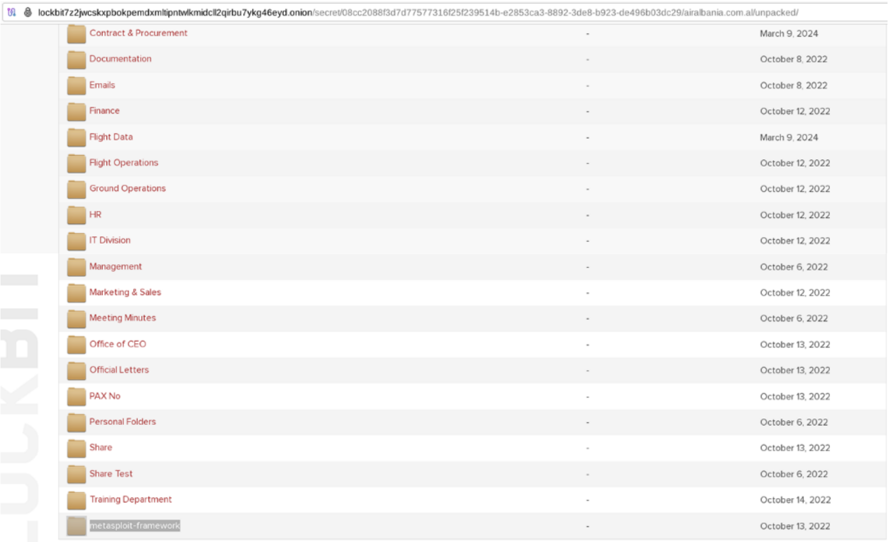
airalbania.com.al

Help & Contact. +355 4 224 60 00. customer.care@airalbania.com.al. b2b@airalbania.com.al. groups@airalbania.com.al. 24/7 booking and customer services. Customer Service. You're an email away to become our business partner.

UPLOADED: 02 MAR, 2024 18:47 UTC

UPDATED: 02 MAR, 2024 18:47 UTC

*Download archives from reserve servers

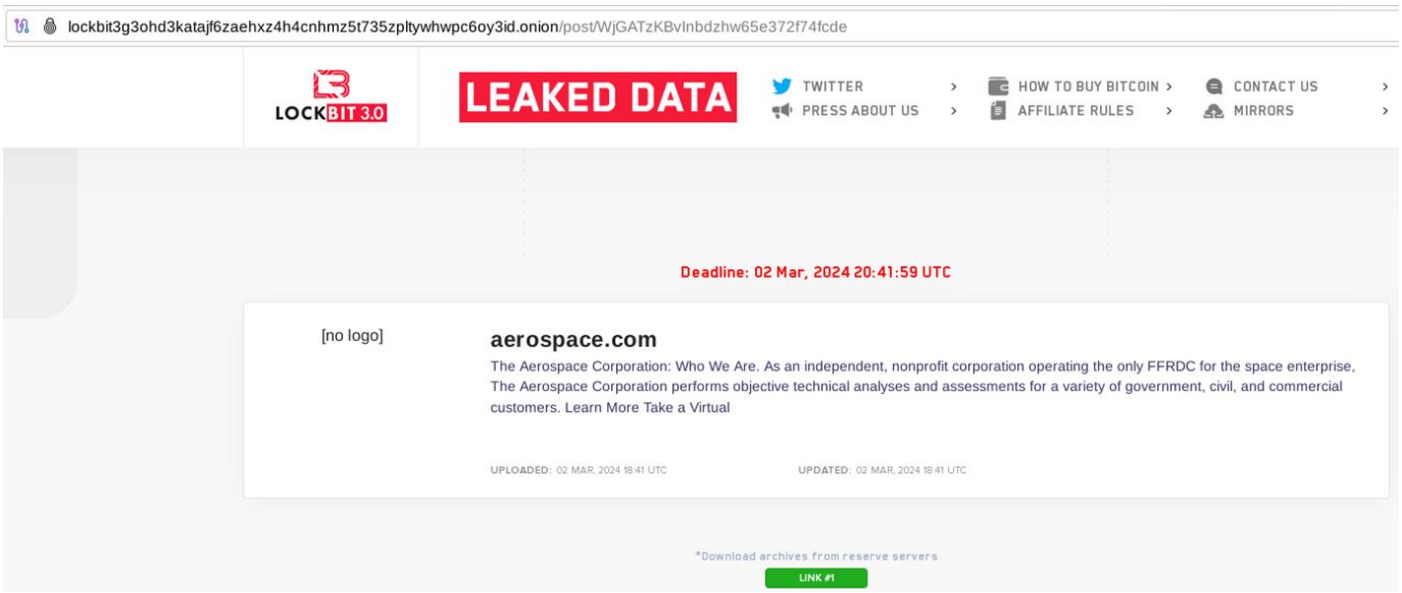


lockbit7z2jwcskxpbokpemdxmltipntwlkmidcll2qirbu7ykg46eyd.onion/secret/08cc2088f3d7d77577316f25f239514b-e2853ca3-8892-3de8-b923-de496b03dc29/airalbania.com.al/unpacked/

Contract & Procurement	-	March 9, 2024
Documentation	-	October 8, 2022
Emails	-	October 8, 2022
Finance	-	October 12, 2022
Flight Data	-	March 9, 2024
Flight Operations	-	October 12, 2022
Ground Operations	-	October 12, 2022
HR	-	October 12, 2022
IT Division	-	October 12, 2022
Management	-	October 6, 2022
Marketing & Sales	-	October 12, 2022
Meeting Minutes	-	October 6, 2022
Office of CEO	-	October 13, 2022
Official Letters	-	October 13, 2022
PAX No	-	October 13, 2022
Personal Folders	-	October 6, 2022
Share	-	October 13, 2022
Share Test	-	October 6, 2022
Training Department	-	October 14, 2022
metasploit-framework	-	October 13, 2022

Albania's flag carrier airline Air Albania has been targeted by the LockBit ransomware group. The Albanian government has increasingly faced cyberattacks organised by Iranian-backed threat actors in recent months. Relations between Albania and Iran are strained and have been exacerbated by allegations that Albania has provided sanctuary to members of the Iranian People's Mujahedeen of Iran (MEK). The LockBit ransomware gang frequently targets the aviation sector. They have attacked major airlines such as Bangkok Airways, E.M.I.T Aviation Consulting and Kuwait Airways. While it is not known exactly how Air Albania was compromised, the LockBit gang pointed to a Metasploit Framework folder in the leaked data set. From this, it can be inferred that the threat actors used the framework to exfiltrate data from several employees and existing file shares.

Aerospace Hit by LockBit Ransomware Attack



lockbit3g3ohd3katajf6zaehxz4h4cnhmz5t735zpltywhwpc6oy3id.onion/post/WjGATzKBvlnbdzhw65e372f74fcde

Deadline: 02 Mar, 2024 20:41:59 UTC

[no logo]

aerospace.com

The Aerospace Corporation: Who We Are. As an independent, nonprofit corporation operating the only FFRDC for the space enterprise, The Aerospace Corporation performs objective technical analyses and assessments for a variety of government, civil, and commercial customers. Learn More Take a Virtual

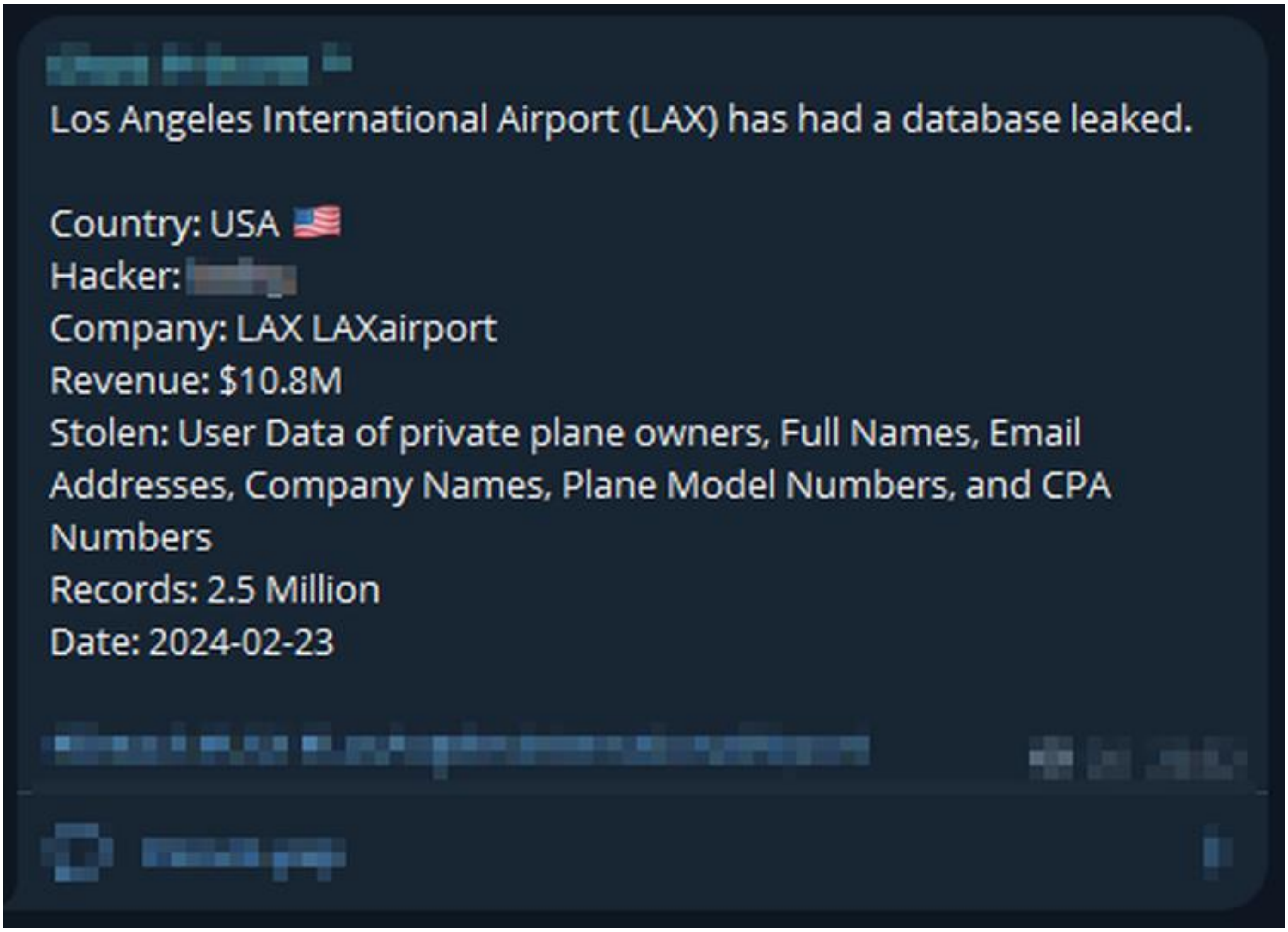
UPLOADED: 02 MAR, 2024 18:41 UTC UPDATED: 02 MAR, 2024 18:41 UTC

*Download archives from reserve servers

India's Aerospace Laboratories (NAL), a major aerospace research company, was attacked by the notorious ransomware group LockBit. LockBit added NAL to its dark web leak site, threatening to publish the organisation's data. According to the leaked information, LockBit published eight allegedly stolen documents, including confidential letters and an employee's passport. As NAL's website is down, neither the company nor the Indian cyber agency CERT-In has yet to make an official statement on the matter. Last month, LockBit targeted the US branch of the Industrial and Commercial Bank of China (ICBC), disrupting transactions in the US Treasury market, and the bank reportedly paid a ransom. LockBit's business model is known as "ransomware-as-a-service", selling its malware to other hackers.

Data Leaks

Ghost Princess Cyber Threat Group Targets US Aviation Sector



[redacted]

Los Angeles International Airport (LAX) has had a database leaked.

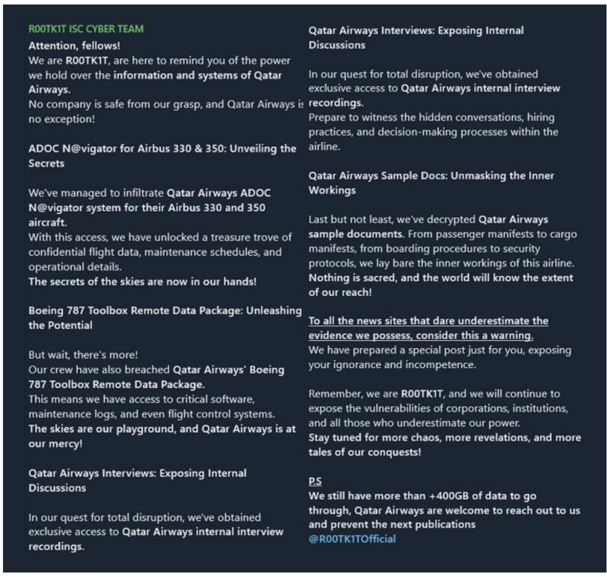
Country: USA 🇺🇸
Hacker: [redacted]
Company: LAX LAXairport
Revenue: $10.8M
Stolen: User Data of private plane owners, Full Names, Email Addresses, Company Names, Plane Model Numbers, and CPA Numbers
Records: 2.5 Million
Date: 2024-02-23

[redacted]

The attack was shared by the hacktivist group Ghost Princess on their secret Telegram channel.

Threat actor Ghost Princess claimed that they targeted Los Angeles International Airport (LAX), the international airport located in Los Angeles, California, USA. Threat actors claim that they leaked the database as a result of their cyber attack. When the claim is examined, it is claimed that there is a leak involving 2.5 million users of "Los Angeles International Airport (LAX)", and that the leak includes "User Data, Full Names, E-mail Addresses, Company Names, Aircraft Model Numbers and CPA Numbers of private aircraft owners"

Qatar Airways Data Allegedly Leaked by R00TK1T ISC Cyber Team



R00TK1T ISC CYBER TEAM

Attention, fellows!
We are **R00TK1T**, are here to remind you of the power we hold over the **information and systems of Qatar Airways.**
No company is safe from our grasp, and Qatar Airways is no exception!

ADOC N@vigator for Airbus 330 & 350: Unveiling the Secrets

We've managed to infiltrate **Qatar Airways ADOC N@vigator system for their Airbus 330 and 350 aircraft.**
With this access, we have unlocked a treasure trove of confidential flight data, maintenance schedules, and operational details.
The secrets of the skies are now in our hands!

Boeing 787 Toolbox Remote Data Package: Unleashing the Potential

But wait, there's more!
Our crew have also breached **Qatar Airways' Boeing 787 Toolbox Remote Data Package.**
This means we have access to critical software, maintenance logs, and even flight control systems.
The skies are our playground, and Qatar Airways is at our mercy!

Qatar Airways Interviews: Exposing Internal Discussions

In our quest for total disruption, we've obtained exclusive access to **Qatar Airways internal interview recordings.**

Qatar Airways Interviews: Exposing Internal Discussions

In our quest for total disruption, we've obtained exclusive access to **Qatar Airways internal interview recordings.**
Prepare to witness the hidden conversations, hiring practices, and decision-making processes within the airline.

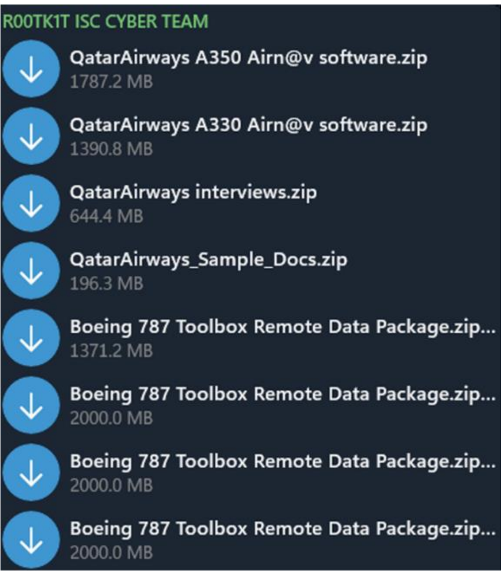
Qatar Airways Sample Docs: Unmasking the Inner Workings

Last but not least, we've decrypted **Qatar Airways sample documents.** From passenger manifests to cargo manifests, from boarding procedures to security protocols, we lay bare the inner workings of this airline.
Nothing is sacred, and the world will know the extent of our reach!

To all the news sites that dare underestimate the evidence we possess, consider this a warning.
We have prepared a special post just for you, exposing your ignorance and incompetence.

Remember, we are **R00TK1T**, and we will continue to expose the vulnerabilities of corporations, institutions, and all those who underestimate our power.
Stay tuned for more chaos, more revelations, and more tales of our conquests!

P.S
We still have more than +400GB of data to go through, Qatar Airways are welcome to reach out to us and prevent the next publications
@R00TK1TOfficial



R00TK1T ISC CYBER TEAM

QatarAirways A350 Airn@v software.zip
1787.2 MB

QatarAirways A330 Airn@v software.zip
1390.8 MB

QatarAirways interviews.zip
644.4 MB

QatarAirways_Sample_Docs.zip
196.3 MB

Boeing 787 Toolbox Remote Data Package.zip...
1371.2 MB

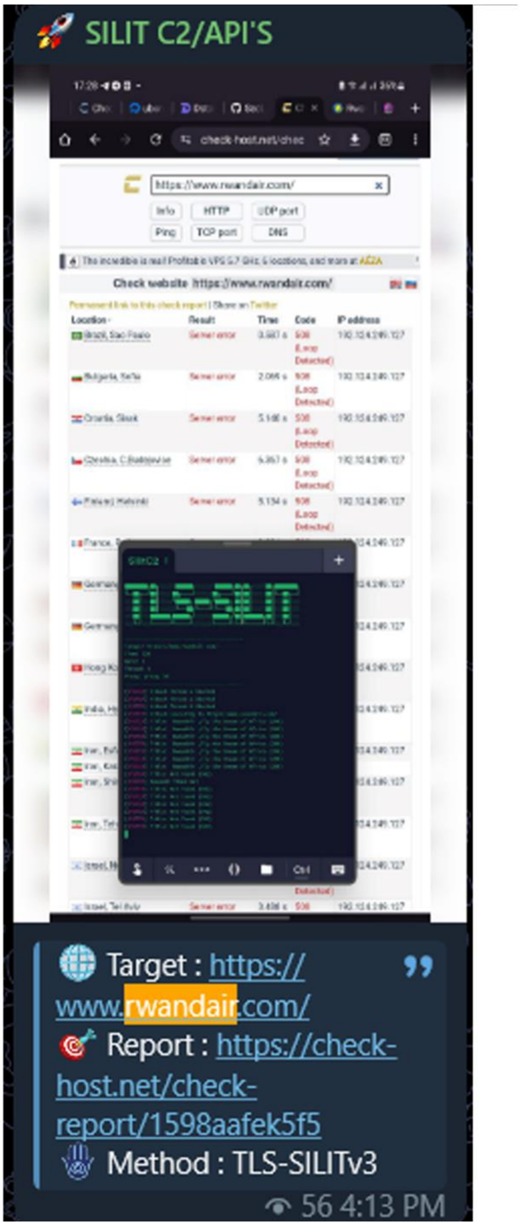
Boeing 787 Toolbox Remote Data Package.zip...
2000.0 MB

Boeing 787 Toolbox Remote Data Package.zip...
2000.0 MB

Boeing 787 Toolbox Remote Data Package.zip...
2000.0 MB

On 29 December 2023, a group of threat actors named "R00TK1T ISC Cyber Team" claimed to have carried out a successful attack on Qatar Airways. First, the group announced that they had compromised the ADOC Navigator system for Airbus A330 and A350 aircraft. This breach provided access to flight data, maintenance schedules and operational details. The attackers also said they had infiltrated the Boeing 787 Toolbox Remote Data Pack, taking control of the aircraft's systems. Within the breach, they claimed to have exposed Qatar Airways' internal negotiations, hiring practices and decision-making processes. The breach also exposed passenger manifests, cargo manifests, boarding procedures and security protocols. The threat actors offered Qatar Airways an opportunity to negotiate and prevent further data leaks by alerting news sites and stating that they had more than 400 GB of data. The attack shows that there are bolder and more aggressors aiming to target the aviation industry, and the industry needs to be more vigilant against these threats.

SilitNetwork Targets RwandAir Ltd



SILIT C2/API'S

17:28

check-host.net/chec

https://www.rwandair.com/

Info | HTTP | UDP port

Ping | TCP port | DNS

The incredible is real! Profitable VPS 5.7 GHz, 6 locations, and more at AÉZA

Check website https://www.rwandair.com/

Permanent link to this check report | Share on Twitter

Location	Result	Time	Code	IP address
Brazil, Sao Paulo	Server error	3.887 s	508 (Loop Detected)	192.124.249.127
Bulgaria, Sofia	Server error	2.066 s	508 (Loop Detected)	192.124.249.127
Croatia, Sisak	Server error	5.148 s	508 (Loop Detected)	192.124.249.127
Czechia, C.Budejovice	Server error	6.367 s	508 (Loop Detected)	192.124.249.127
Finland, Helsinki	Server error	5.134 s	508 (Loop Detected)	192.124.249.127
France, [illegible]	[illegible]	[illegible]	[illegible]	192.124.249.127
Germany, [illegible]	[illegible]	[illegible]	[illegible]	192.124.249.127
Germany, [illegible]	[illegible]	[illegible]	[illegible]	192.124.249.127
Hong Kong, [illegible]	[illegible]	[illegible]	[illegible]	192.124.249.127
India, [illegible]	[illegible]	[illegible]	[illegible]	192.124.249.127
Iran, [illegible]	[illegible]	[illegible]	[illegible]	192.124.249.127
Iran, [illegible]	[illegible]	[illegible]	[illegible]	192.124.249.127
Iran, [illegible]	[illegible]	[illegible]	[illegible]	192.124.249.127
Iran, [illegible]	[illegible]	[illegible]	[illegible]	192.124.249.127
Israel, [illegible]	[illegible]	[illegible]	[illegible]	192.124.249.127
Israel, Tel Aviv	Server error	3.486 s	508	192.124.249.127

SilitC2

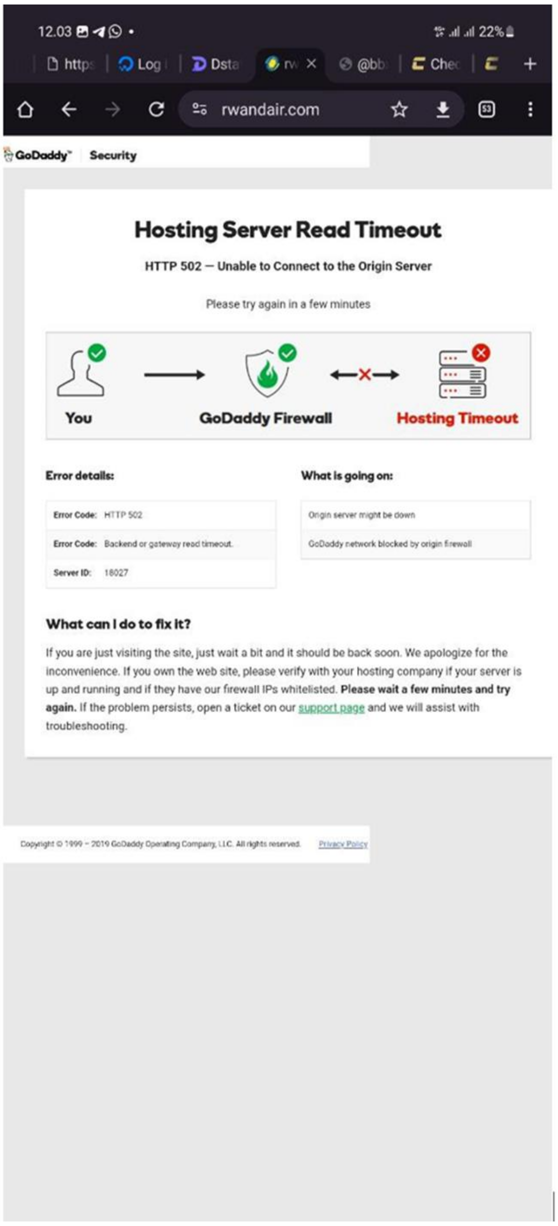
```
TLS-SILIT
```

Target : https://www.rwandair.com/

Report : https://check-host.net/check-report/1598aafek5f5

Method : TLS-SILITv3

56 4:13 PM



12.03 22%

rwandair.com

GoDaddy Security

Hosting Server Read Timeout

HTTP 502 — Unable to Connect to the Origin Server

Please try again in a few minutes

Error details:

Error Code: HTTP 502

Error Code: Backend or gateway read timeout.

Server ID: 18027

What is going on:

Origin server might be down

GoDaddy network blocked by origin firewall

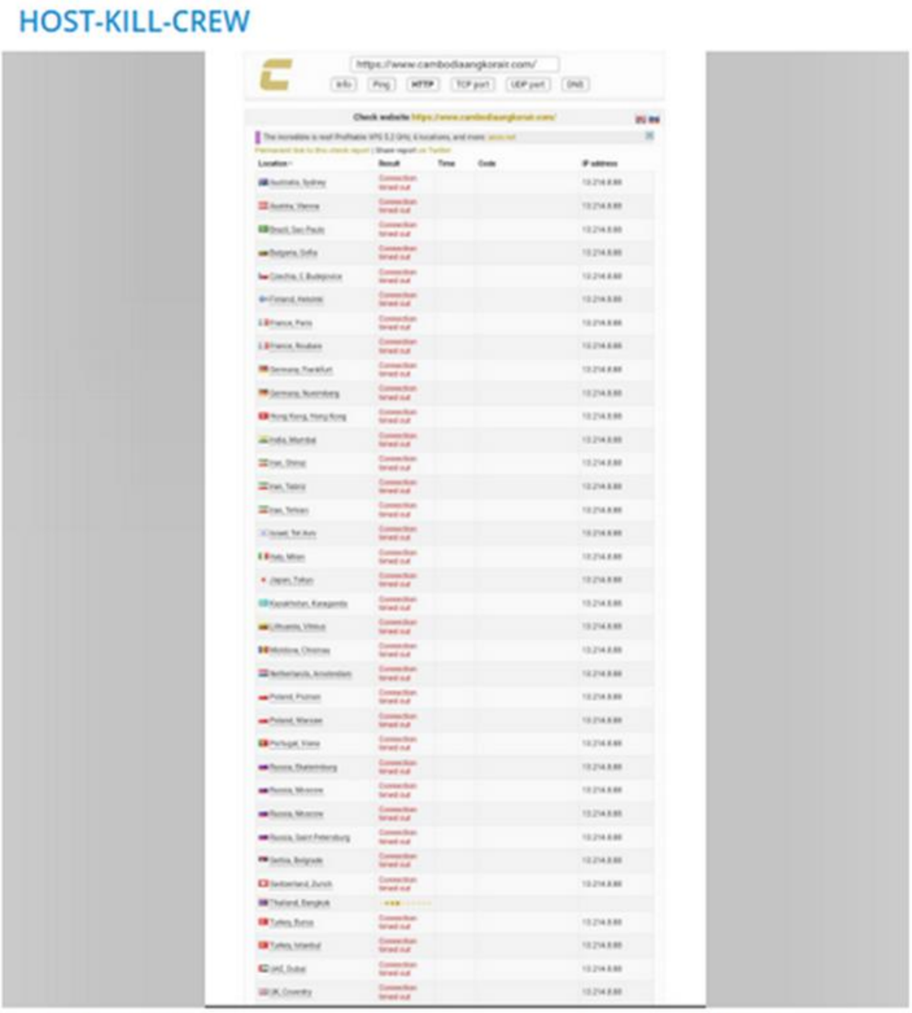
What can I do to fix it?

If you are just visiting the site, just wait a bit and it should be back soon. We apologize for the inconvenience. If you own the web site, please verify with your hosting company if your server is up and running and if they have our firewall IPs whitelisted. **Please wait a few minutes and try again.** If the problem persists, open a ticket on our support page and we will assist with troubleshooting.

Copyright © 1999 – 2019 GoDaddy Operating Company, LLC. All rights reserved. Privacy Policy

On 16 February 2024, the hacking group SilitNetwork carried out a cyber attack against Rwanda's national airline RwandAir Ltd. This incident highlights the vulnerability of the aviation sector and the potential impact on airline operations and passenger data security. The SilitNetwork is known as a group that operates in cyber-attacks against high-profile targets, often for financial gain, political motivations or to showcase their hacking capabilities. The attack on RwandAir Ltd was an effort to target the airline's digital infrastructure, with hackers gaining unauthorised access using sophisticated methods. The motivations behind this attack are speculative, but could include the theft of sensitive passenger information, disruption of airline operations, or even extortion attempts. The attack has the potential to impact airline operations as well as compromise the confidentiality and integrity of passenger data. RwandAir is cooperating with cyber security organisations to investigate the attack and take security measures. This attack once again demonstrates the importance of strong cyber security measures in the aviation industry.

'Host Kill Crew Hackers' Target Cambodia Angkor Air



HOST-KILL-CREW

https://www.cambodiaangkorair.com/

Check website: https://www.cambodiaangkorair.com/

[illegible]

Permanent link to this check report | Share report on Twitter

Location	Result	Time	Code	IP address
Australia, Sydney	Connection timed out			13.214.8.88
Austria, Vienna	Connection timed out			13.214.8.88
Brazil, Sao Paulo	Connection timed out			13.214.8.88
Bulgaria, Sofia	Connection timed out			13.214.8.88
Czechia, C. Budejovice	Connection timed out			13.214.8.88
Finland, Helsinki	Connection timed out			13.214.8.88
France, Paris	Connection timed out			13.214.8.88
France, Roubaix	Connection timed out			13.214.8.88
Germany, Frankfurt	Connection timed out			13.214.8.88
Germany, Nuremberg	Connection timed out			13.214.8.88
Hong Kong, Hong Kong	Connection timed out			13.214.8.88
India, Mumbai	Connection timed out			13.214.8.88
Iran, Shiraz	Connection timed out			13.214.8.88
Iran, Tabriz	Connection timed out			13.214.8.88
Iran, Tehran	Connection timed out			13.214.8.88
Israel, Tel Aviv	Connection timed out			13.214.8.88
Italy, Milan	Connection timed out			13.214.8.88
Japan, Tokyo	Connection timed out			13.214.8.88
Kazakhstan, Karaganda	Connection timed out			13.214.8.88
Lithuania, Vilnius	Connection timed out			13.214.8.88
Moldova, Chisinau	Connection timed out			13.214.8.88
Netherlands, Amsterdam	Connection timed out			13.214.8.88
Poland, Poznan	Connection timed out			13.214.8.88
Poland, Warsaw	Connection timed out			13.214.8.88
Portugal, Viana	Connection timed out			13.214.8.88
Russia, Ekaterinburg	Connection timed out			13.214.8.88
Russia, Moscow	Connection timed out			13.214.8.88
Russia, Moscow	Connection timed out			13.214.8.88
Russia, Saint Petersburg	Connection timed out			13.214.8.88
Serbia, Belgrade	Connection timed out			13.214.8.88
Switzerland, Zurich	Connection timed out			13.214.8.88
Thailand, Bangkok	●●●······			
Turkey, Bursa	Connection timed out			13.214.8.88
Turkey, Istanbul	Connection timed out			13.214.8.88
UAE, Dubai	Connection timed out			13.214.8.88
UK, Coventry	Connection timed out			13.214.8.88

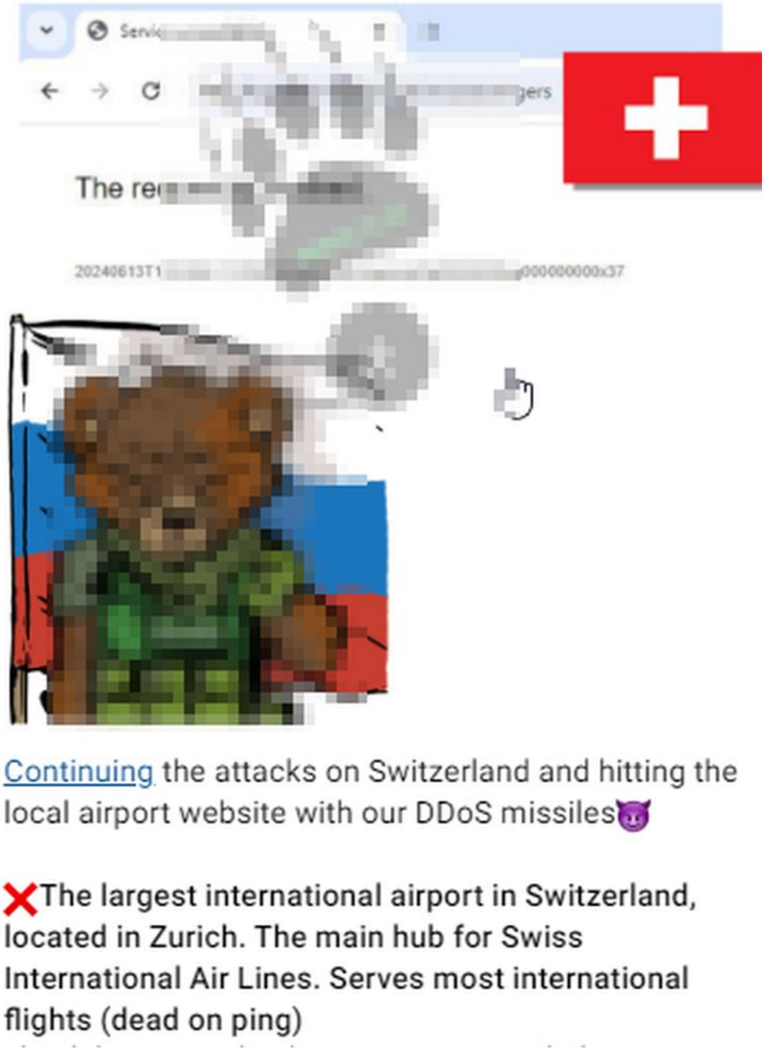
Cambodia Angkor air flight website down By Host-Kill-Crew

URL:https://www.cambodiaangkorair.com
CHECK-HOST🎯:https://check-host.net/check-report/fd66ffbk858

A lesser-known hacker group calling themselves Host Kill Crew has claimed responsibility for the Cambodian Angkor Air cyberattack. The group posted details of the attack on their Telegram channel, claiming a DDOS (Distributed Denial of Service attack) and halting online services for a time.

DDoS Attack

Threat Actor NoName057(16) Targets Critical European Airports

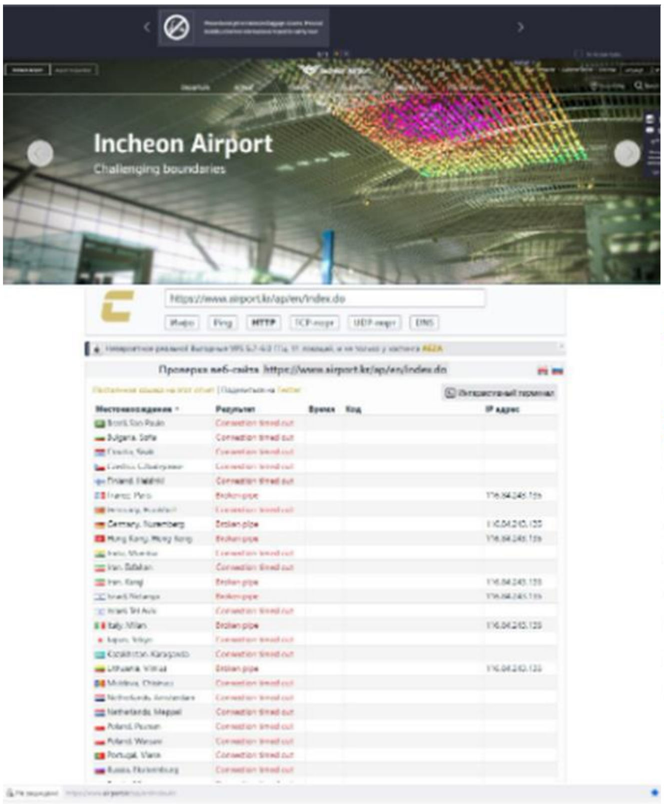


Continuing the attacks on Switzerland and hitting the local airport website with our DDoS missiles😈

❌The largest international airport in Switzerland, located in Zurich. The main hub for Swiss International Air Lines. Serves most international flights (dead on ping)

The attack was posted by the hacktivist group NoName057(16) on secret Telegram channels. The Russian threat actor "NoName057(16)" claims to be targeting Switzerland's largest international airport, Flughafen Zürich in Zurich, which serves most international flights. The attack method is a Distributed Denial-of-Service (DDoS) attack, which is a very common technique among threat actors.

Threat Actor HackNet Targeted Incheon Airport, One of South Korea's Largest Airport Operators, Together with Other Actor



https://www.airport.kr/ap/en/index.do

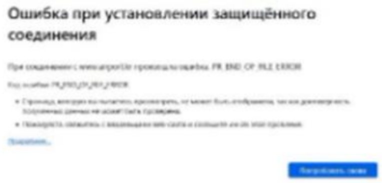
Инфо | Ping | HTTP | TCP-порт | UDP-порт | DNS

Проверка веб-сайта https://www.airport.kr/ap/en/index.do

Постоянная ссылка на этот отчёт | Поделиться в Twitter

Интерактивный терминал

Местонахождение	Результат	Время	Код	IP адрес
Brazil, Sao Paulo	Connection timed out			
Bulgaria, Sofia	Connection timed out			
[illegible]	Connection timed out			
Czechia, C.Budejovice	Connection timed out			
Finland, Helsinki	Connection timed out			
France, Paris	Broken pipe			116.84.245.135
Hungary, [illegible]	Connection timed out			
Germany, Nuremberg	Broken pipe			116.84.245.135
Hong Kong, Hong Kong	Broken pipe			116.84.245.135
India, Mumbai	Connection timed out			
Iran, Esfahan	Connection timed out			
Iran, Karaj	Broken pipe			116.84.245.135
Israel, Netanya	Broken pipe			116.84.245.135
Israel, Tel Aviv	Connection timed out			
Italy, Milan	Broken pipe			116.84.245.135
Japan, Tokyo	Connection timed out			
Kazakhstan, Karaganda	Connection timed out			
Lithuania, Vilnius	Broken pipe			116.84.245.135
Moldova, Chisinau	Connection timed out			
Netherlands, Amsterdam	Connection timed out			
Netherlands, Meppel	Connection timed out			
Poland, Poznan	Connection timed out			
Poland, Warsaw	Connection timed out			
Portugal, Viana	Connection timed out			
Russia, Ekaterinburg	Connection timed out			



Ошибка при установлении защищённого соединения

При соединении с www.airport.kr произошла ошибка. PR_END_OF_FILE_ERROR

Код ошибки: PR_END_OF_FILE_ERROR

- Страница, которую вы пытаетесь просмотреть, не может быть отображена, так как достоверность полученных данных не может быть проверена.
- Пожалуйста, свяжитесь с владельцами веб-сайта и сообщите им об этой проблеме.

Подробнее…

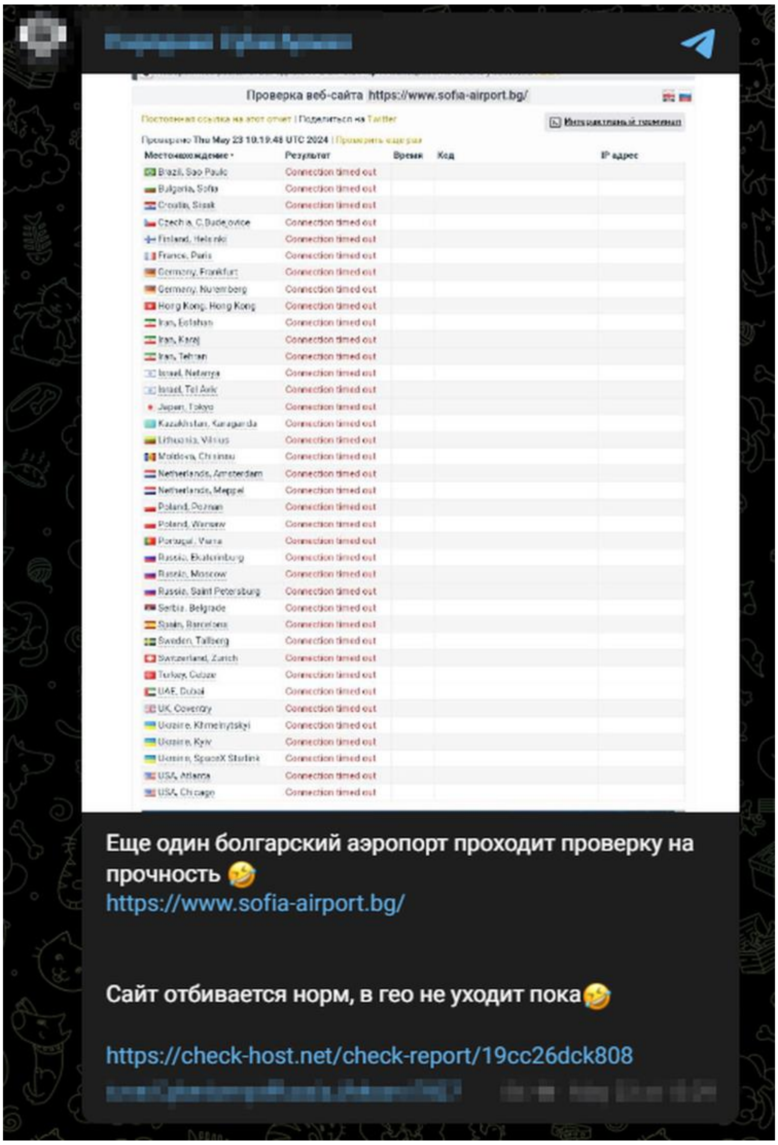
А мы присоединяемся к нашим друзьям NoName057(16) и НароднаяCyberАрмия и начинаем атаки на Южною Корею

❌ Международный аэропорт Инчхон — это международный аэропорт, расположенный в городе-метрополии Инчхон, в семидесяти километрах от столицы Республики Корея — города Сеула. Он является крупнейшим авиационным узлом страны и одним из крупнейших аэропортов мира по показателям объёма международных авиаперевозок и количества операций взлётов и посадок воздушных судов.

The attack was shared by the hacktivist group **"HackNet "** via secret Telegram channels.

The Russian threat actor **"HackNet"**, along with other Russian threat actors **"NoName057(16) "** and **"НароднаяCyberАрмия"**, claim to be targeting Incheon Airport, one of the largest airport operators in South Korea. As an attack method, they stated that they used Distributed Denial-of-Service (DDoS) attack, which is a very common technique among threat actors.

Threat Actor Народная CyberАрмия Claims to Target Bulgarian Aviation Sector



[redacted]

Проверка веб-сайта https://www.sofia-airport.bg/

Постоянная ссылка на этот отчет | Поделиться на Twitter

Интерактивный терминал

Проверено Thu May 23 10:19:48 UTC 2024 | Проверить еще раз

Местонахождение ▾	Результат	Время	Код	IP адрес
Brazil, Sao Paulo	Connection timed out			
Bulgaria, Sofia	Connection timed out			
Croatia, Sisak	Connection timed out			
Czechia, C.Budejovice	Connection timed out			
Finland, Helsinki	Connection timed out			
France, Paris	Connection timed out			
Germany, Frankfurt	Connection timed out			
Germany, Nuremberg	Connection timed out			
Hong Kong, Hong Kong	Connection timed out			
Iran, Esfahan	Connection timed out			
Iran, Karaj	Connection timed out			
Iran, Tehran	Connection timed out			
Israel, Netanya	Connection timed out			
Israel, Tel Aviv	Connection timed out			
Japan, Tokyo	Connection timed out			
Kazakhstan, Karaganda	Connection timed out			
Lithuania, Vilnius	Connection timed out			
Moldova, Chisinau	Connection timed out			
Netherlands, Amsterdam	Connection timed out			
Netherlands, Meppel	Connection timed out			
Poland, Poznan	Connection timed out			
Poland, Warsaw	Connection timed out			
Portugal, Viana	Connection timed out			
Russia, Ekaterinburg	Connection timed out			
Russia, Moscow	Connection timed out			
Russia, Saint Petersburg	Connection timed out			
Serbia, Belgrade	Connection timed out			
Spain, Barcelona	Connection timed out			
Sweden, Tallberg	Connection timed out			
Switzerland, Zurich	Connection timed out			
Turkey, Gebze	Connection timed out			
UAE, Dubai	Connection timed out			
UK, Coventry	Connection timed out			
Ukraine, Khmelnytskyi	Connection timed out			
Ukraine, Kyiv	Connection timed out			
Ukraine, SpaceX Starlink	Connection timed out			
USA, Atlanta	Connection timed out			
USA, Chicago	Connection timed out			

Еще один болгарский аэропорт проходит проверку на прочность 🤣
https://www.sofia-airport.bg/

Сайт отбивается норм, в гео не уходит пока🤣

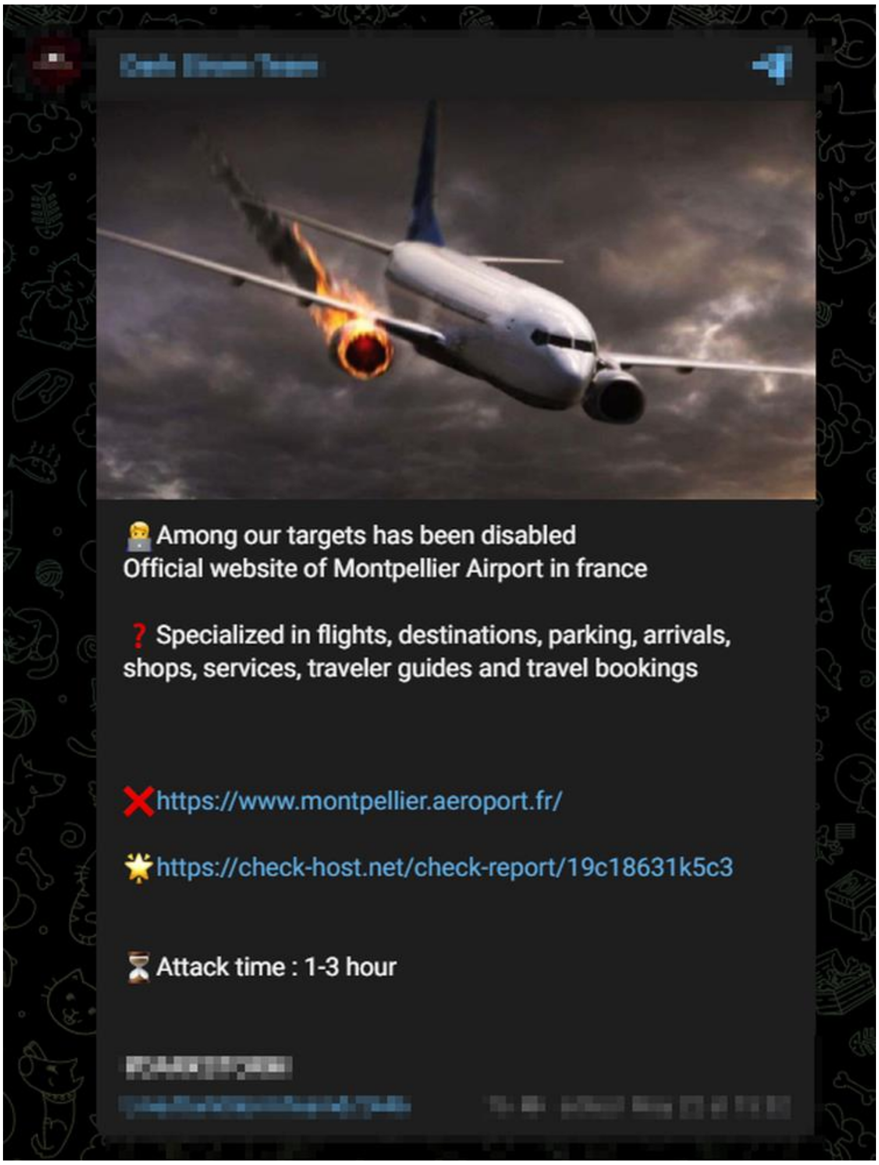
https://check-host.net/check-report/19cc26dck808

[redacted]

The attack was posted by the hacktivist group "Народная CyberАрмия" in secret Telegram channels.

The Russian threat actor "Народная CyberАрмия" claims to be targeting "Sofia Airport", a Bulgarian aviation company. The threat actors stated that they used a Distributed Denial-of-Service (DDoS) attack, which is a very common technique among threat actors.

Threat Actor Dark Strom Team Targets France Aviation Sector



[redacted]

👨‍💻Among our targets has been disabled
Official website of Montpellier Airport in france

❓Specialized in flights, destinations, parking, arrivals, shops, services, traveler guides and travel bookings

❌https://www.montpellier.aeroport.fr/

🌟https://check-host.net/check-report/19c18631k5c3

⏳Attack time : 1-3 hour

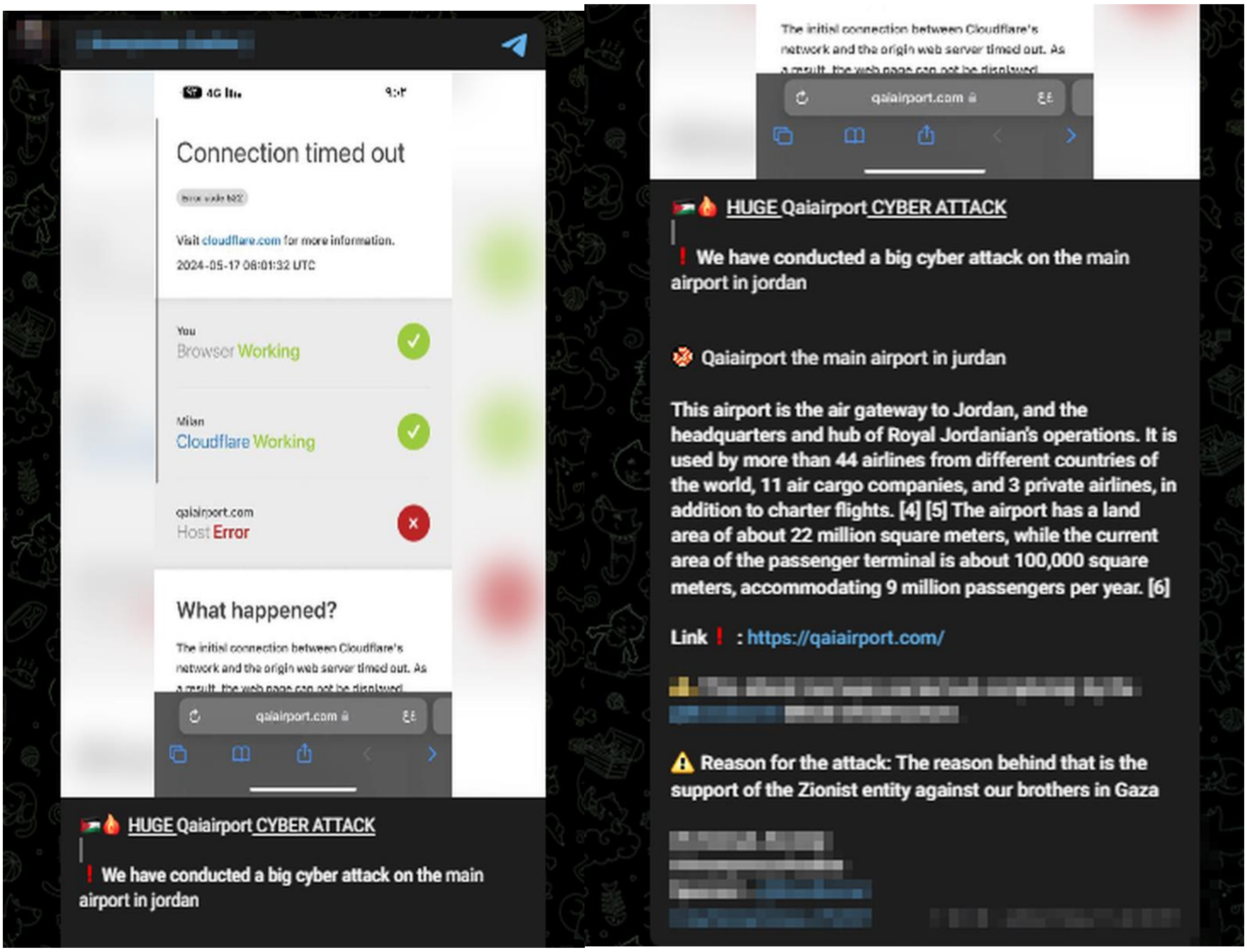
[redacted]

[redacted] [redacted]

The attack was shared by the hacktivist group "Dark Strom Team" via secret Telegram channels.

The Russian threat actor "Dark Strom Team" claims that they are targeting "Aéroport Montpellier Méditerranée", which serves the French aviation industry. Threat actors stated that they used Distributed Denial-of-Service (DDoS) attack, which is a very common technique among threat actors.

Threat Actor Anonymous Arabia Targets Jordanian Aviation Sector



[redacted]

4G 9:07

Connection timed out

Error code 522

Visit cloudflare.com for more information.

2024-05-17 08:01:32 UTC

You
Browser Working ✓

Milan
Cloudflare Working ✓

qaiairport.com
Host Error ✕

What happened?

The initial connection between Cloudflare's network and the origin web server timed out. As a result, the web page can not be displayed.

qaiairport.com

HUGE Qaiairport CYBER ATTACK

❗ We have conducted a big cyber attack on the main airport in jordan

The initial connection between Cloudflare's network and the origin web server timed out. As a result, the web page can not be displayed.

qaiairport.com

HUGE Qaiairport CYBER ATTACK

❗ We have conducted a big cyber attack on the main airport in jordan

Qaiairport the main airport in jurdan

This airport is the air gateway to Jordan, and the headquarters and hub of Royal Jordanian's operations. It is used by more than 44 airlines from different countries of the world, 11 air cargo companies, and 3 private airlines, in addition to charter flights. [4] [5] The airport has a land area of about 22 million square meters, while the current area of the passenger terminal is about 100,000 square meters, accommodating 9 million passengers per year. [6]

Link ❗ : https://qaiairport.com/

[redacted]

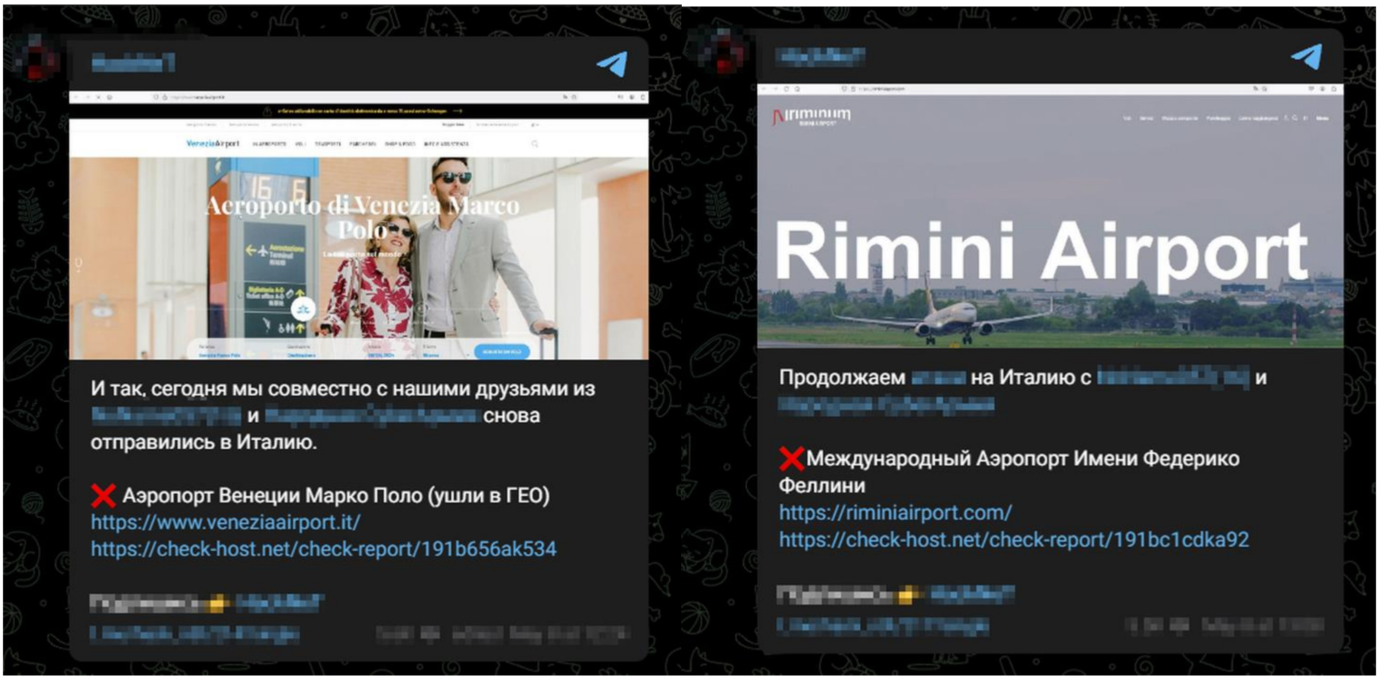
⚠ Reason for the attack: The reason behind that is the support of the Zionist entity against our brothers in Gaza

[redacted]

The attack was shared by the hacktivist group "Anonymous Arabia" via secret Telegram channels.

The threat actor claims that "Anonymous Arabia" and "Criminal_Society" are jointly targeting "Qaiairport" airport, which serves the Jordanian aviation industry. The threat actors stated that they used Distributed Denial-of-Service (DDoS) attack, which is a very common technique among threat actors.

HackNeT Italy Targets Aviation Sector



[redacted]

И так, сегодня мы совместно с нашими друзьями из [redacted] и [redacted] снова отправились в Италию.

❌ Аэропорт Венеции Марко Поло (ушли в ГЕО)
https://www.veneziaairport.it/
https://check-host.net/check-report/191b656ak534

[redacted]

[redacted]

Продолжаем [redacted] на Италию с [redacted] и [redacted]

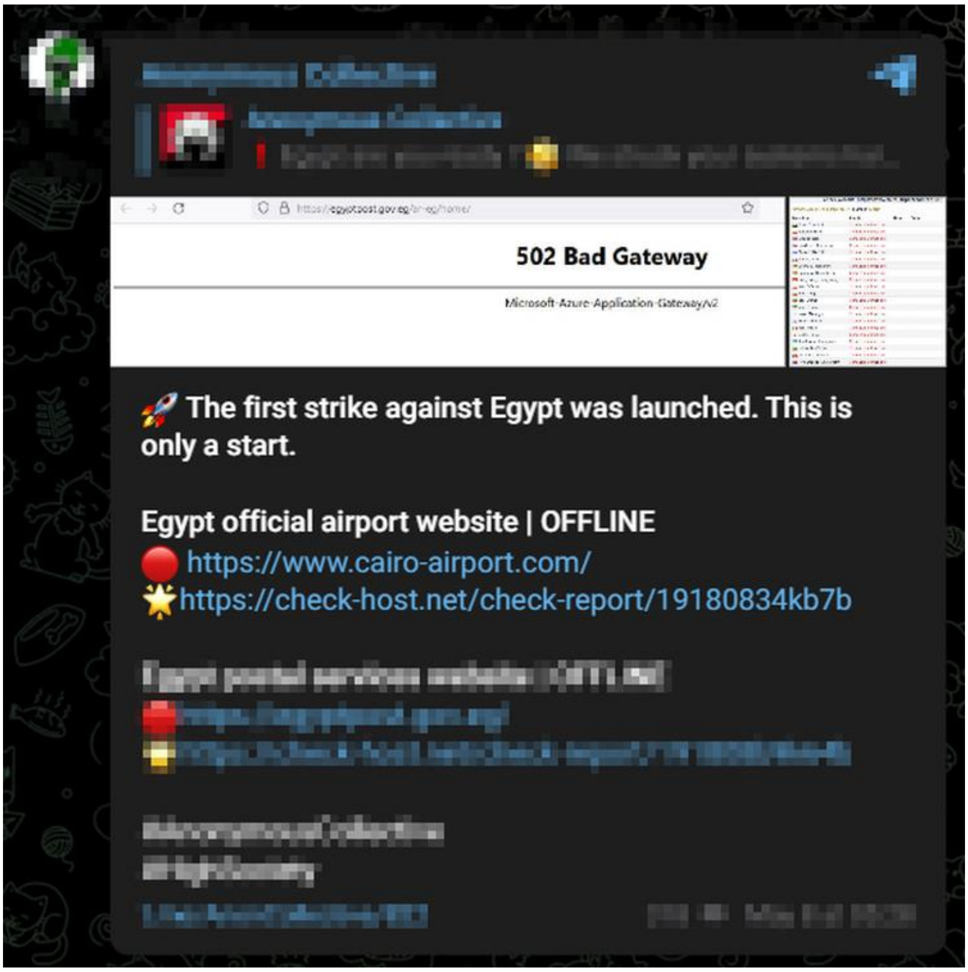
❌Международный Аэропорт Имени Федерико Феллини
https://riminiairport.com/
https://check-host.net/check-report/191bc1cdka92

[redacted]

The attack was shared by the hacktivist group HackNeT via secret Telegram channels.

Russian threat actors "HackNeT" "NoName057(16)" and "Народная CyberАрмия" jointly claimed to have targeted "Venice Marco Polo Airport", the fifth busiest airport in Italy, and "Federico Fellini International Airport" in Rimini, Italy. The threat actors stated that they used Distributed Denial-of-Service (DDoS) attack, which is a very common technique among threat actors.

Anonymous Collective Cyber Threat Group Targets Egyptian Aviation Sector



[redacted]

[redacted]

https://egyptpost.gov.eg/ar-eg/home/

502 Bad Gateway

Microsoft-Azure-Application-Gateway/v2

🚀 The first strike against Egypt was launched. This is only a start.

Egypt official airport website | OFFLINE
🔴 https://www.cairo-airport.com/
🌟https://check-host.net/check-report/19180834kb7b

[redacted]

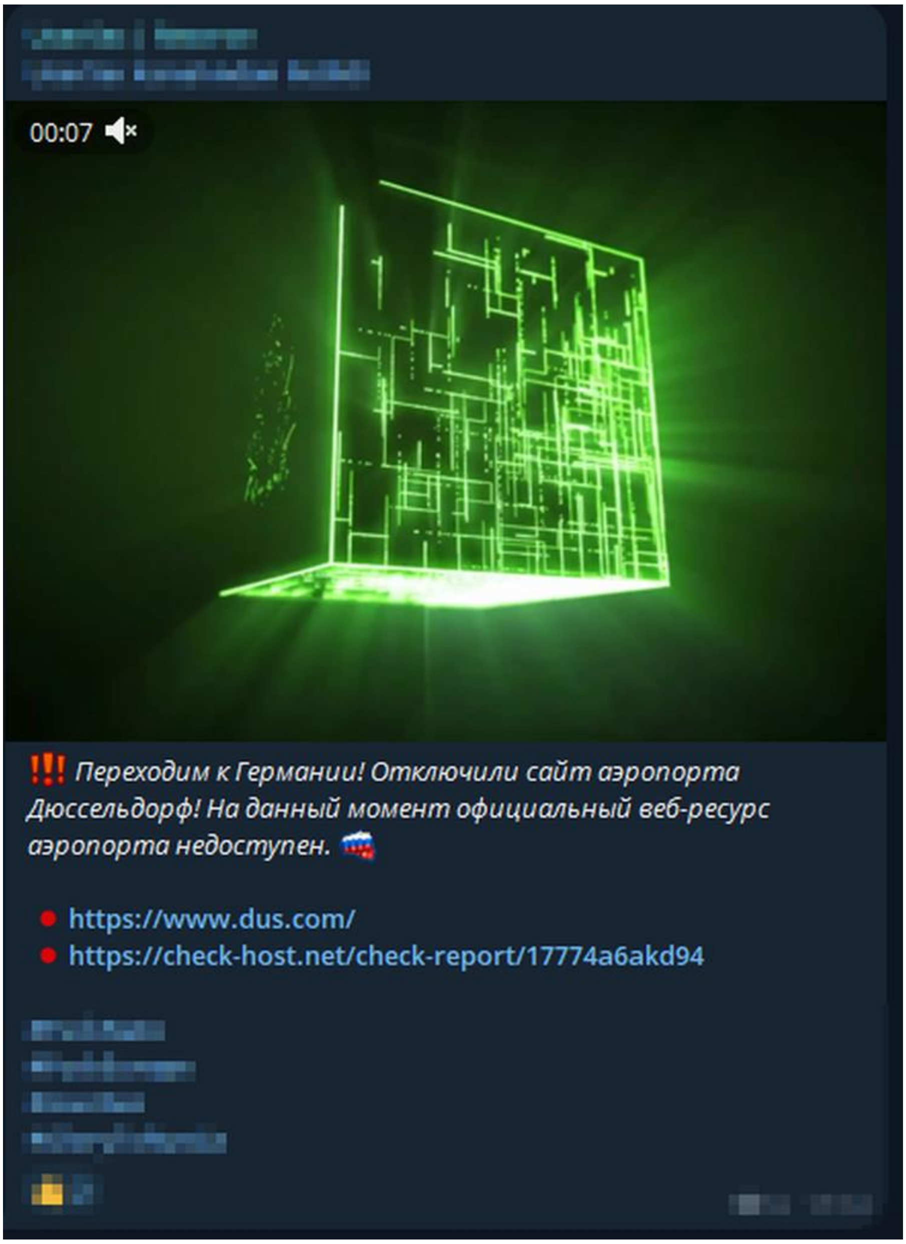
[redacted]

[redacted]

The attack was shared by the hacktivist group Anonymous Collective via secret Telegram channels.

The threat actor, in partnership with "Anonymous Collective" and "HighSociety", claimed that they targeted "Cairo International Airport", which serves in the Egyptian aviation sector. The threat actors stated that they used Distributed Denial-of-Service (DDoS) attack, which is a very common technique among threat actors.

Cyber Threat Group UserSec Targets German Aviation Industry



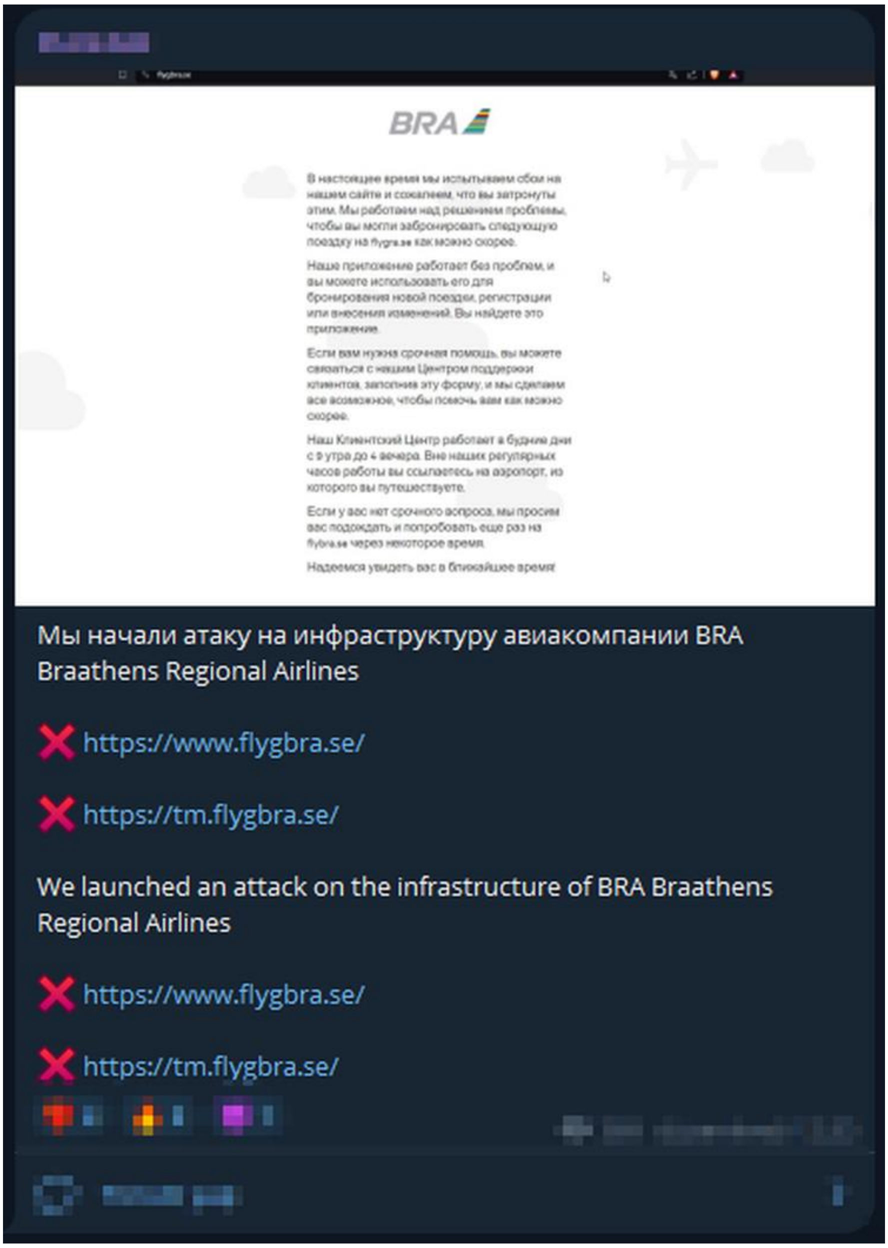
!!! *Переходим к Германии! Отключили сайт аэропорта Дюссельдорф! На данный момент официальный веб-ресурс аэропорта недоступен.*

- ● https://www.dus.com/
- ● https://check-host.net/check-report/17774a6akd94

The related attack post was made by the hacktivist group UserSec on secret Telegram channels.

UserSec, a Russian threat actor, hacked "Düsseldorf Airport", which serves the German aviation industry. claimed that they were targeting. The threat actors stated that they used Distributed Denial-of-Service (DDoS) attack, which is a very common technique among threat actors.

PHOENIX Claims to Target Swedish Aviation Sector



[redacted]

BRA

В настоящее время мы испытываем сбои на нашем сайте и сожалеем, что вы затронуты этим. Мы работаем над решением проблемы, чтобы вы могли забронировать следующую поездку на flygbra.se как можно скорее.

Наше приложение работает без проблем, и вы можете использовать его для бронирования новой поездки, регистрации или внесения изменений. Вы найдете это приложение.

Если вам нужна срочная помощь, вы можете связаться с нашим Центром поддержки клиентов, заполнив эту форму, и мы сделаем все возможное, чтобы помочь вам как можно скорее.

Наш Клиентский Центр работает в будние дни с 9 утра до 4 вечера. Вне наших регулярных часов работы вы ссылаетесь на аэропорт, из которого вы путешествуете.

Если у вас нет срочного вопроса, мы просим вас подождать и попробовать еще раз на flygbra.se через некоторое время.

Надеемся увидеть вас в ближайшее время!

Мы начали атаку на инфраструктуру авиакомпании BRA Braathens Regional Airlines

❌ https://www.flygbra.se/

❌ https://tm.flygbra.se/

We launched an attack on the infrastructure of BRA Braathens Regional Airlines

❌ https://www.flygbra.se/

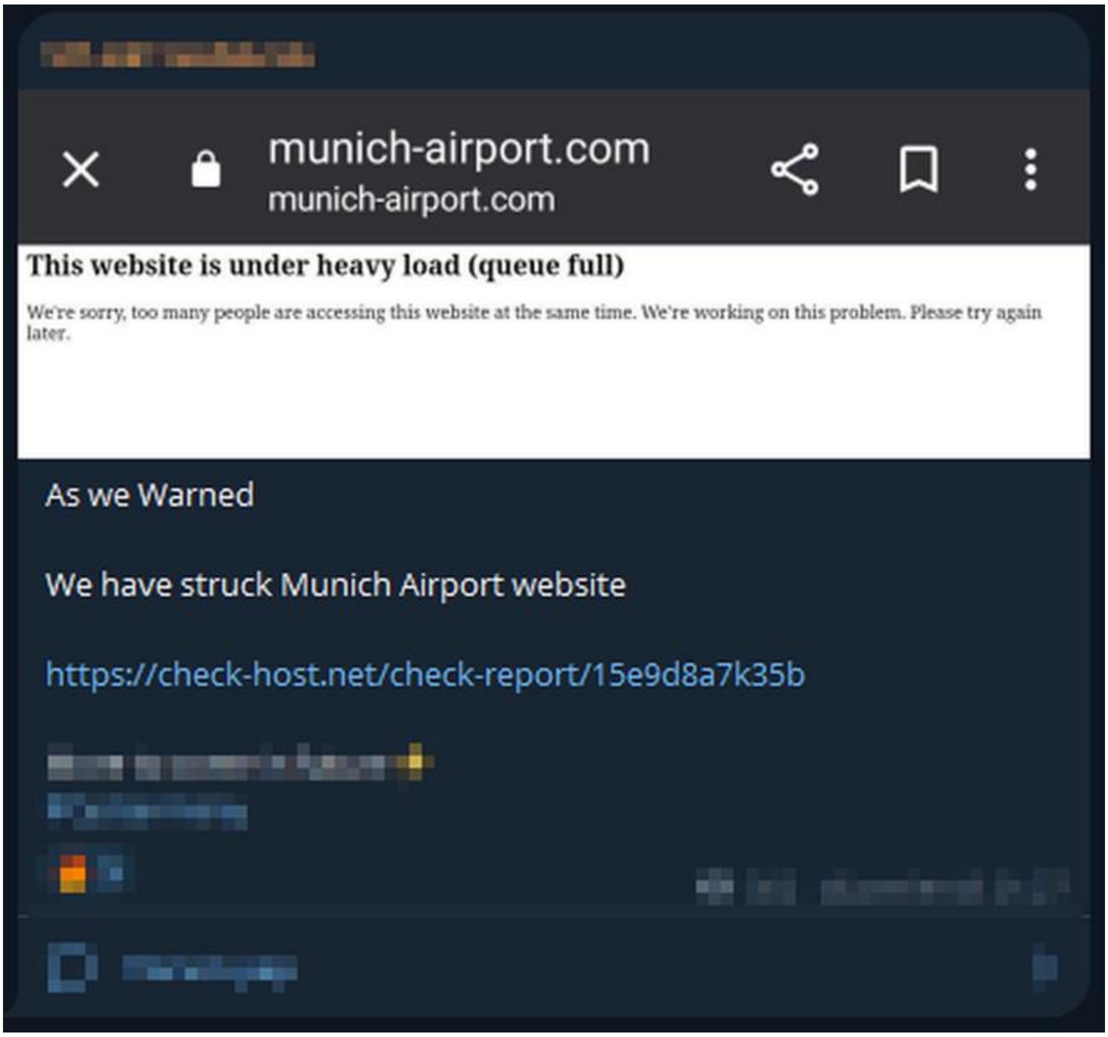
❌ https://tm.flygbra.se/

[redacted]

The attack was posted by the hacktivist group PHOENIX on their secret Telegram channel.

The threat actor "PHOENIX" claimed to be targeting "BRA Braathens Regional Airlines", often abbreviated as BRA, a Swedish regional airline based in Stockholm. The threat actors stated that they used a Distributed Denial-of-Service (DDoS) attack, which is a very common technique among threat actors.

SYLHET GANG-SG Cyber Threat Group Targets German Aviation Sector



[redacted]

munich-airport.com
munich-airport.com

This website is under heavy load (queue full)

We're sorry, too many people are accessing this website at the same time. We're working on this problem. Please try again later.

As we Warned

We have struck Munich Airport website

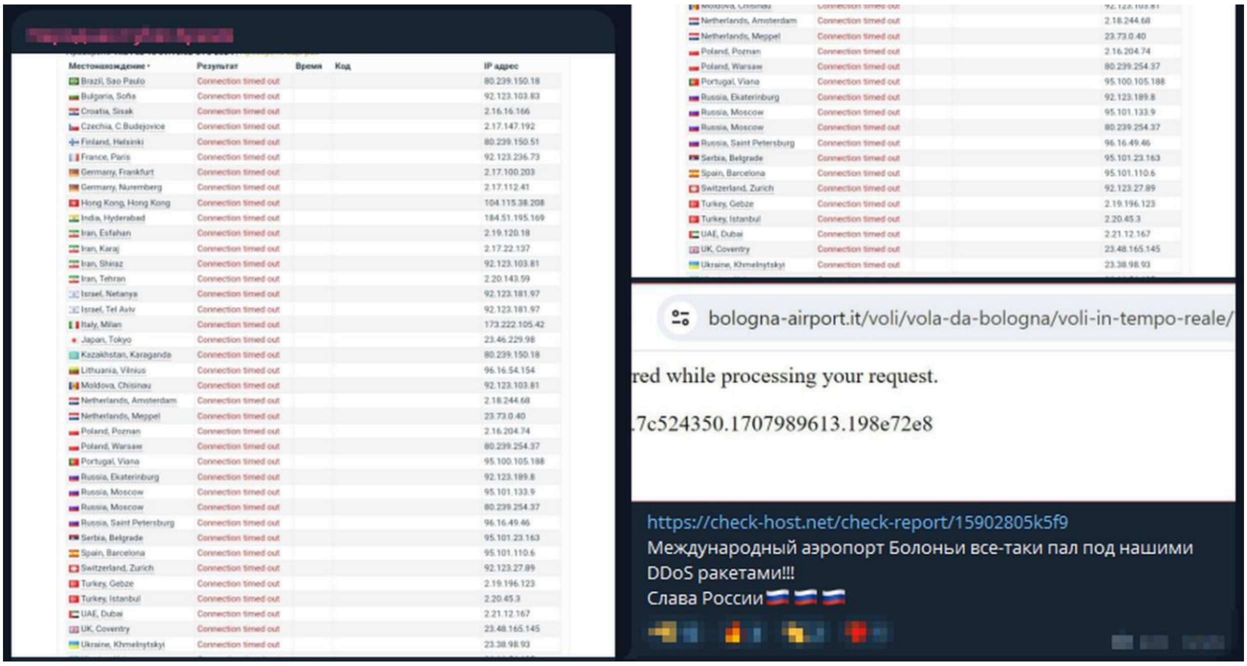
https://check-host.net/check-report/15e9d8a7k35b

[redacted]

The attack was shared by the hacktivist group SYLHET GANG-SG on their secret Telegram channel.

The threat actor SYLHET GANG-SG claimed to be targeting Munich Franz Josef Strauss Airport, the international airport serving Munich, the centre of the German state of Bavaria. Threat actors stated that they used Distributed Denial-of-Service (DDoS) attack, which is a very common technique among threat actors.

CyberArmyofRussia_Reborn Targets Italian Aviation Sector



[redacted]

Местонахождение ▾	Результат	Время	Код	IP адрес
Brazil, Sao Paulo	Connection timed out			80.239.150.18
Bulgaria, Sofia	Connection timed out			92.123.103.83
Croatia, Sisak	Connection timed out			2.16.16.166
Czechia, C.Budejovice	Connection timed out			2.17.147.192
Finland, Helsinki	Connection timed out			80.239.150.51
France, Paris	Connection timed out			92.123.236.73
Germany, Frankfurt	Connection timed out			2.17.100.203
Germany, Nuremberg	Connection timed out			2.17.112.41
Hong Kong, Hong Kong	Connection timed out			104.115.38.208
India, Hyderabad	Connection timed out			184.51.195.169
Iran, Esfahan	Connection timed out			2.19.120.18
Iran, Karaj	Connection timed out			2.17.22.137
Iran, Shiraz	Connection timed out			92.123.103.81
Iran, Tehran	Connection timed out			2.20.143.59
Israel, Netanya	Connection timed out			92.123.181.97
Israel, Tel Aviv	Connection timed out			92.123.181.97
Italy, Milan	Connection timed out			173.222.105.42
Japan, Tokyo	Connection timed out			23.46.229.98
Kazakhstan, Karaganda	Connection timed out			80.239.150.18
Lithuania, Vilnius	Connection timed out			96.16.54.154
Moldova, Chisinau	Connection timed out			92.123.103.81
Netherlands, Amsterdam	Connection timed out			2.18.244.68
Netherlands, Meppel	Connection timed out			23.73.0.40
Poland, Poznan	Connection timed out			2.16.204.74
Poland, Warsaw	Connection timed out			80.239.254.37
Portugal, Viana	Connection timed out			95.100.105.188
Russia, Ekaterinburg	Connection timed out			92.123.189.8
Russia, Moscow	Connection timed out			95.101.133.9
Russia, Moscow	Connection timed out			80.239.254.37
Russia, Saint Petersburg	Connection timed out			96.16.49.46
Serbia, Belgrade	Connection timed out			95.101.23.163
Spain, Barcelona	Connection timed out			95.101.110.6
Switzerland, Zurich	Connection timed out			92.123.27.89
Turkey, Gebze	Connection timed out			2.19.196.123
Turkey, Istanbul	Connection timed out			2.20.45.3
UAE, Dubai	Connection timed out			2.21.12.167
UK, Coventry	Connection timed out			23.48.165.145
Ukraine, Khmelnytskyi	Connection timed out			23.38.98.93

Moldova, Chisinau	Connection timed out			92.123.103.81
Netherlands, Amsterdam	Connection timed out			2.18.244.68
Netherlands, Meppel	Connection timed out			23.73.0.40
Poland, Poznan	Connection timed out			2.16.204.74
Poland, Warsaw	Connection timed out			80.239.254.37
Portugal, Viana	Connection timed out			95.100.105.188
Russia, Ekaterinburg	Connection timed out			92.123.189.8
Russia, Moscow	Connection timed out			95.101.133.9
Russia, Moscow	Connection timed out			80.239.254.37
Russia, Saint Petersburg	Connection timed out			96.16.49.46
Serbia, Belgrade	Connection timed out			95.101.23.163
Spain, Barcelona	Connection timed out			95.101.110.6
Switzerland, Zurich	Connection timed out			92.123.27.89
Turkey, Gebze	Connection timed out			2.19.196.123
Turkey, Istanbul	Connection timed out			2.20.45.3
UAE, Dubai	Connection timed out			2.21.12.167
UK, Coventry	Connection timed out			23.48.165.145
Ukraine, Khmelnytskyi	Connection timed out			23.38.98.93

bologna-airport.it/voli/vola-da-bologna/voli-in-tempo-reale/

red while processing your request.

.7c524350.1707989613.198e72e8

https://check-host.net/check-report/15902805k5f9

Международный аэропорт Болоньи все-таки пал под нашими DDoS ракетами!!!

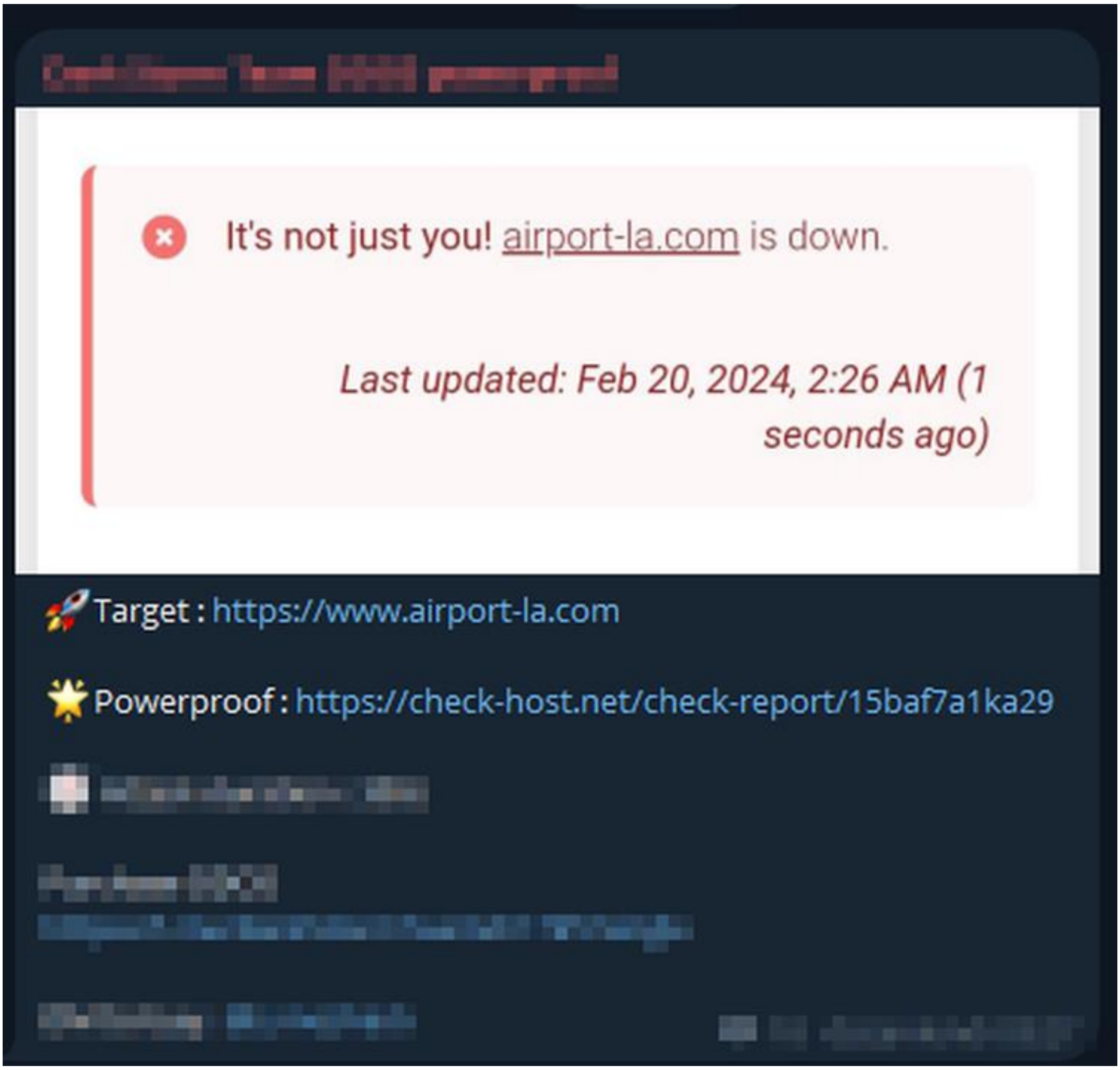
Слава России🇷🇺🇷🇺🇷🇺

[redacted]

The attack post was made by the hacktivist group CyberArmyofRussia_Reborn, also known as Народная CyberАрмия, via secret Telegram channels.

The Russian threat actor "CyberArmyofRussia_Reborn" claimed that they targeted the international airport "Bologna Guglielmo Marconi Airport" in Bologna, Italy. Threat actors stated that they used Distributed Denial-of-Service (DDoS) attack, which is a very common technique among threat actors.

Dark Storm Team Targets US Aviation Industry



[redacted]

It's not just you! airport-la.com is down.

Last updated: Feb 20, 2024, 2:26 AM (1 seconds ago)

🚀Target : https://www.airport-la.com

🌟Powerproof : https://check-host.net/check-report/15baf7a1ka29

[redacted]

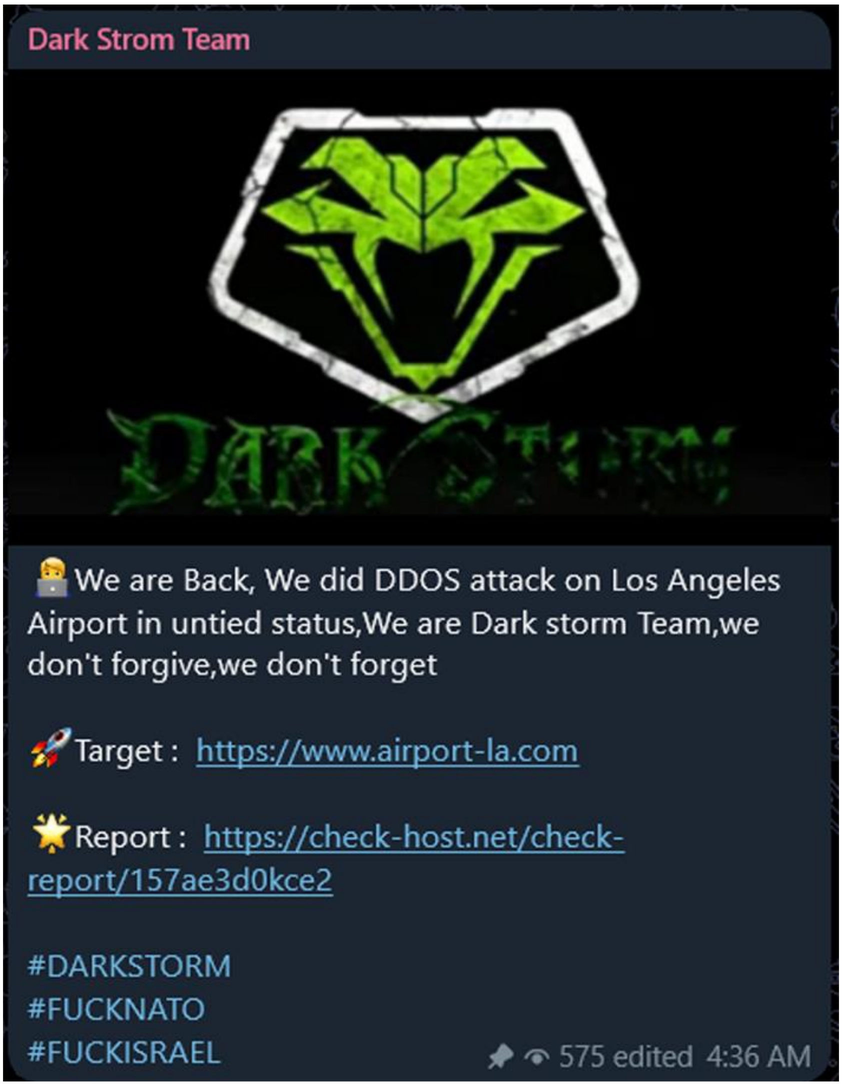
[redacted]

[redacted]

The attack was shared by the hacktivist group Dark Storm Team on their secret Telegram channel.

The threat actor Dark Storm Team claimed that they targeted "airport-la.com", the international airport located in Los Angeles, California, USA. The threat actors stated that they used a Distributed Denial-of-Service (DDoS) attack, which is a very common technique among threat actors.

Dark Strom Team Performed DDOS Attack on Los Angeles Airport



Dark Strom Team

🧑‍💻We are Back, We did DDOS attack on Los Angeles Airport in untied status,We are Dark storm Team,we don't forgive,we don't forget

🚀Target : https://www.airport-la.com

🌟Report : https://check-host.net/check-report/157ae3d0kce2

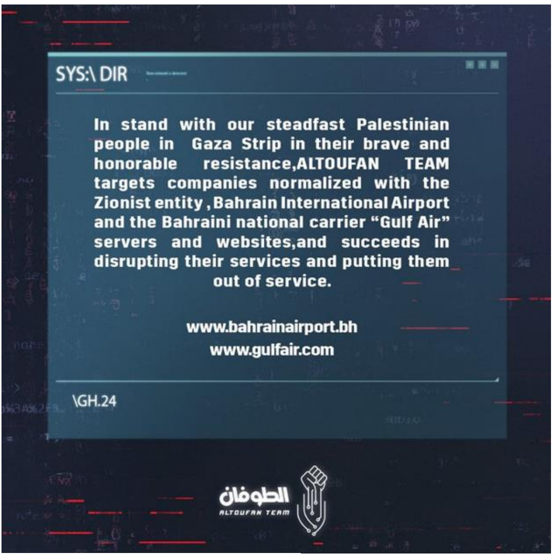
#DARKSTORM
#FUCKNATO
#FUCKISRAEL

575 edited 4:36 AM

On 12 February 2024, Los Angeles International Airport (LAX) was affected by a DDoS attack by the Dark Strom Team. This attack demonstrated the vulnerability of aviation infrastructure to cyberattacks. Dark Strom Team is a notorious hacking group and is known for DDoS attacks. In the attack on LAX, network traffic to online platforms increased. This increase caused the airport website to temporarily shut down and passengers and staff were unable to use online services. The motivation for the attack is still a matter of speculation, but the impact was great. Airport authorities experienced difficulties with updates, which exacerbated the inconvenience caused by the cyber attack. The airport's cyber security team responded quickly to the attack and took measures. This incident led to a review of the airport's cyber security infrastructure. An investigation has been launched to identify the source of the attack and LAX is collaborating with law enforcement and cybersecurity firms. This attack highlights the importance of implementing cybersecurity measures at airports and demonstrates the need to improve incident response planning to ensure uninterrupted service.

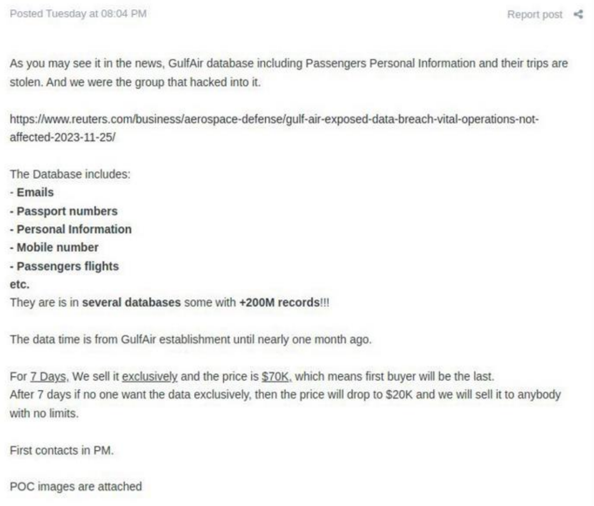
Gulf Air Subjected to Cyber Attack

GULF AIR
طيران الخليج
على طيران الخليج الاستعداد للطوفان القادم!!
Gulf Air must prepare for the coming flood !!
الطوفان
ALTOUFAN TEAM



In stand with our steadfast Palestinian people in Gaza Strip in their brave and honorable resistance,ALTOUFAN TEAM targets companies normalized with the Zionist entity ,Bahrain International Airport and the Bahraini national carrier "Gulf Air" servers and websites,and succeeds in disrupting their services and putting them out of service.

www.bahrainairport.bh
www.gulfair.com



As you may see it in the news, GulfAir database including Passengers Personal Information and their trips are stolen. And we were the group that hacked into it.

https://www.reuters.com/business/aerospace-defense/gulf-air-exposed-data-breach-vital-operations-not-affected-2023-11-25/

The Database includes:
- **Emails**
- **Passport numbers**
- **Personal Information**
- **Mobile number**
- **Passengers flights**
etc.
They are is in **several databases** some with **+200M records**!!!

The data time is from GulfAir establishment until nearly one month ago.

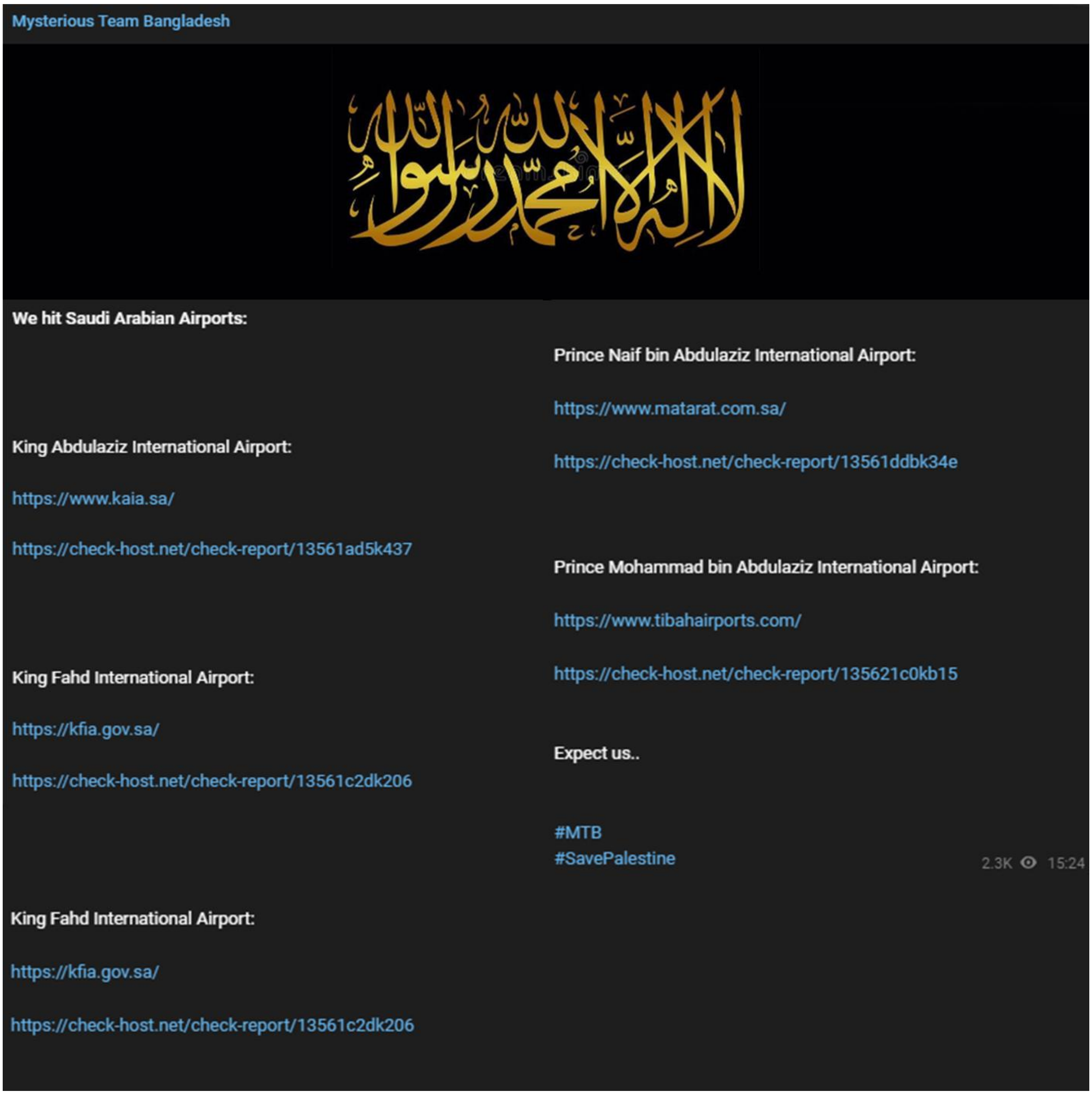
For 7 Days, We sell it exclusively and the price is $70K, which means first buyer will be the last.
After 7 days if no one want the data exclusively, then the price will drop to $20K and we will sell it to anybody with no limits.

First contacts in PM.

POC images are attached

ALTOUFAN TEAM, a threat-actor group, has announced their intention to carry out a Distributed Denial of Service (DDoS) attack on Gulf Air, Bahrain's national airline. The group associates its actions with support for the Palestinian cause. ALTOUFAN TEAM also announced a successful DDoS attack against Gulf Air and Bahrain International Airport. These attacks caused disruptions to Gulf Air's online services and operational difficulties. On the same day, Bahrain Airport's online portal also became temporarily inaccessible due to a DDoS attack. Gulf Air announced that its data had been breached, but the Bahrain news agency stated that the airline's operations were not affected. It was reported that the company's e-mail system and customer database may have been compromised as a result of ALTOUFAN TEAM's attack. Contingency plans were put in place to contain the attack.

Mysterious Team Bangladesh Targeted Saudi Arabia Airport Website



Mysterious Team Bangladesh

We hit Saudi Arabian Airports:

King Abdulaziz International Airport:

https://www.kaia.sa/

https://check-host.net/check-report/13561ad5k437

King Fahd International Airport:

https://kfia.gov.sa/

https://check-host.net/check-report/13561c2dk206

King Fahd International Airport:

https://kfia.gov.sa/

https://check-host.net/check-report/13561c2dk206

Prince Naif bin Abdulaziz International Airport:

https://www.matarat.com.sa/

https://check-host.net/check-report/13561ddbk34e

Prince Mohammad bin Abdulaziz International Airport:

https://www.tibahairports.com/

https://check-host.net/check-report/135621c0kb15

Expect us..

#MTB
#SavePalestine

2.3K 15:24

On 19 November 2023, a group calling itself "Mysterious Team Bangladesh" (MTB) launched a Distributed Denial of Service (DDoS) attack on several major airports in Saudi Arabia. The affected airports included King Abdulaziz International Airport, King Fahd International Airport, Prince Naif bin Abdulaziz International Airport and Prince Mohammed bin Abdulaziz International Airport.

It is not yet clear why MTB organised the attack and its true intentions. MTB's use of the hashtag #SavePalestine suggests that it may have ideological or political motivations related to the Gaza conflict. However, more research is needed to find out the real intentions behind the attack and the broader geopolitical connections. Their last message ended with the phrase "Wait for us..." and included the hashtags #MTB and #SavePalestine.

ECHO

CYBER THREAT INTELLIGENCE