Supporting
European
Aviation

EUROCONTROL

# Cyber-security in aviation

## EUROCONTROL/EATM-CERT services

Patrick MANA
EATM-CERT Manager

FOUNDING MEMBER SESAR JOINT UNDERTAKING

NETWORK MANAGER

# EUROCONTROL


EUROCONTROL is an inter-governmental, pan-European, civil-military organisation dedicated to supporting European aviation.

# **EUROCONTROL** HISTORY

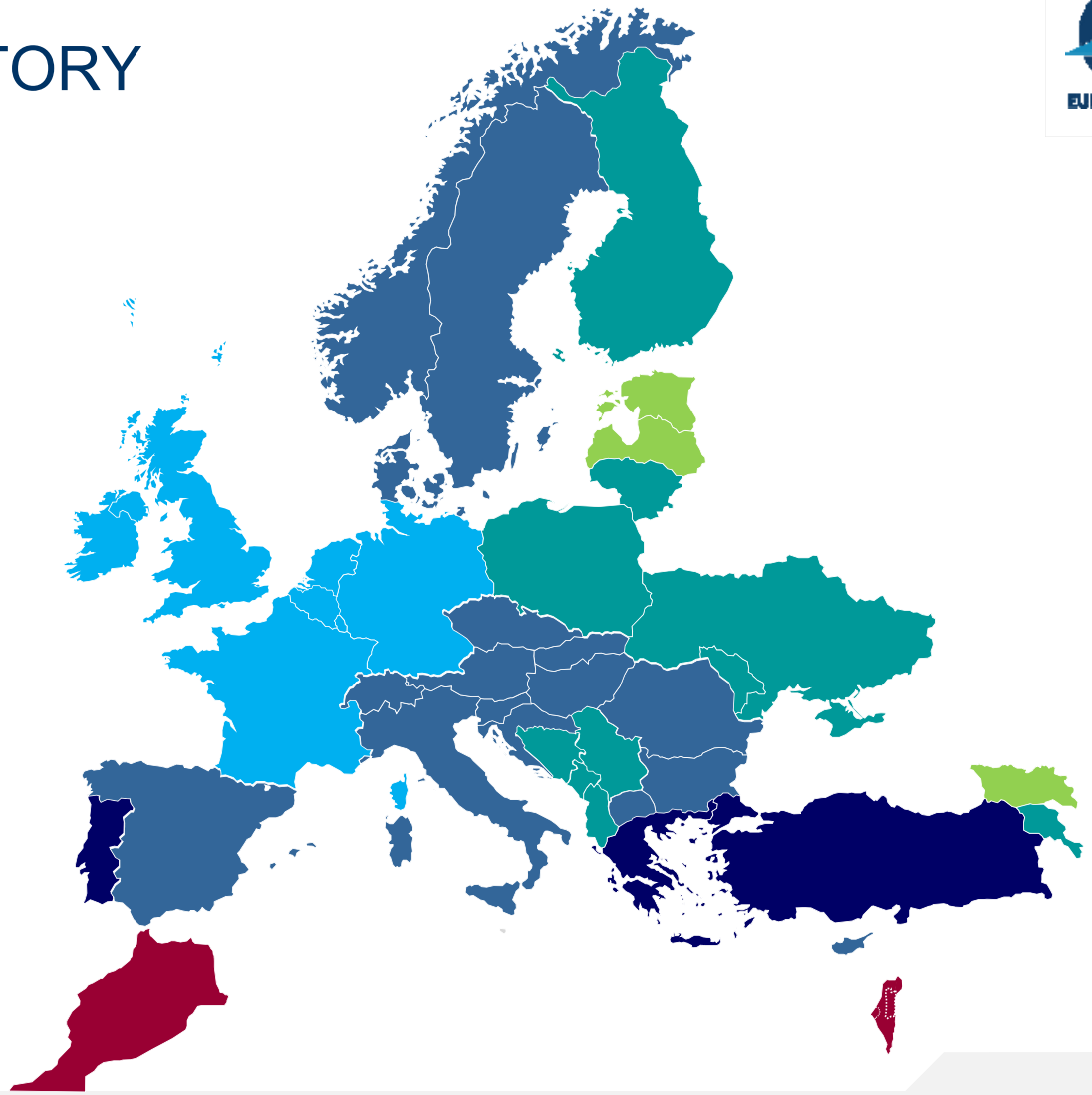
1960s

1980s

1990s

2000s

2010s



41 Member States &
the European Union

2 ‘Comprehensive Agreement’
States: Morocco & Israel

# Building the Single European Sky !

Provide air traffic services in upper airspace of Benelux & North west of Germany

Manage the pan-European network

R&D => Deployment


Products

Collect route and terminal charges

Leonardo Company / Kopter Group

2D 6H 58 S

Secret data link: Hidden

Password: Hidden

Kopter Group (Leonardo) have been hacked and data locked and stolen. They do not write to us so we will publish all data in 72 hours. Some example files have been uploaded for proof: 2019-12-17_Statement_of_Accounts_-_Sales_Contracts.xlsx Avionic_Elec_Detailed_Plan.xlsm Projekt LINDEN - Linden_Finance Q&A_05122019_V1.xlsx Projekt LINDEN - Linden_Finance Q&A_05122019.xlsx Projekt LINDEN - Linden_Finance Q&A_06122019_CTI.xlsx Projekt LINDEN - Linden Tax 191205_QA List Tax.xlsx All data release in final upload.

## Manufacturing giant Aebi Schmidt hit by ransomware

Zack Whittaker @zackwhittaker / 11:04 PM GMT+2 • April 23, 2019


EUROCONTROL

## Boeing Hit by Cyberattack, Says Jetliner Production Not Affected

Aircraft production and deliveries aren't affected, the airplane manufacturer said.

Bloomberg
MAR 29, 2018

4 DEC 2020 NEWS

## Aerospace Giant Embraer Downed by Suspected Ransomware

## Airbus hit by series of cyber attacks on suppliers

Issued on: 26/09/2019 - 09:26

FRANCE 24

Saturday, 12 December 2020 08:38

## Tech Giant GE Discloses Data Breach After Service Provider Hack

By Sergiu Gatlan

March 23, 2020 05:47 PM 0

## Dassault subsidiary in US hit by Windows Ragnar Locker ransomware Featured


AIRLINE NEWS

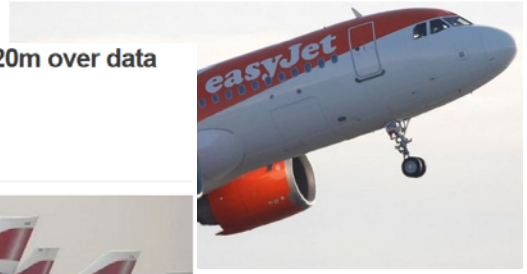
## Israeli Flight Attendant Sold Access to Private Passenger Information and Airline Systems in Major Security Breach

7TH JUNE 2020

## EasyJet admits data of nine million hacked

By Jane Wakefield
Technology reporter

19 May




## British Airways fined £20m over data breach

16 October 2020 | Technology


SFO CONNECT

SFO

Home | About SFO | Badging & Security | Forms | Businesses

Home / About / SFO News / NOTICE OF DATA BREACH: March 2020

## NOTICE OF DATA BREACH: March 2020

Click Here for Notice

April 7, 2020

TO: All Airport Commission Employees

FROM: Airport ITT

SUBJECT: Notice of Data Breach

EUROCONTROL

## Source: Hacker holding Cleveland Hopkins International Airport systems hostage demands ransom via Bitcoin

By Paul Orlousky | April 25, 2019 at 4:20 PM EDT - Updated April 26 at 10:46 AM

## European Airport Systems Infected With Monero-Mining Malware

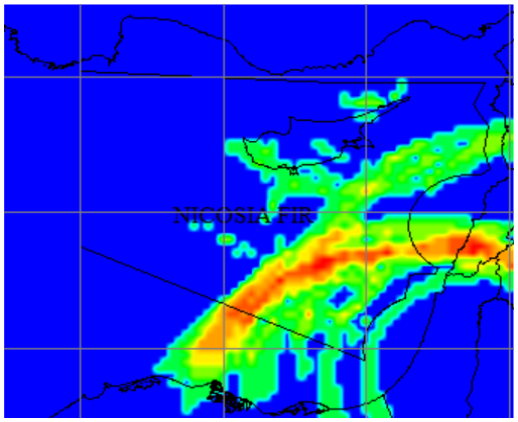
By Sergiu Gatlan

October 17, 2019 | 11:47 AM | 0

LILY HAY NEWMAN SECURITY 07.27.2020 07:53 PM

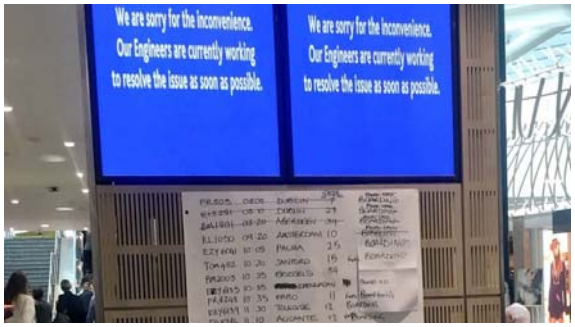
# A Cyberattack on Garmin Disrupted More Than Workouts

A ransomware hit and subsequent outage caused problems in the company's aviation services, including flight planning and mapping.




# Man hijacks Portland airport monitor to play video games, until PDX officials declare 'game over'

Posted Jan 16, 2020





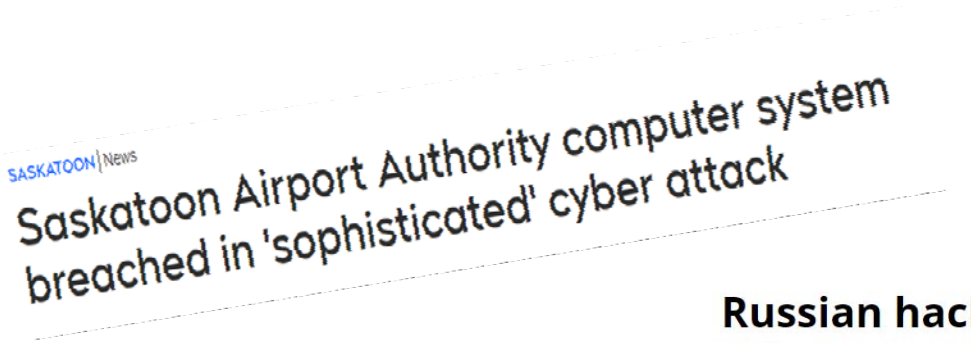
# Airline forced to cancel flights in Alaska after cyberattack

By Associated Press

December 23, 2019 | 12:16pm


# Bradley International Airport website hit by DDoS cyber attack; no data breach has been reported

Updated: Mar. 29, 2022, 5:34 p.m. | Published: Mar. 29, 2022, 3:40 p.m.



SASKATOON | News

# Saskatoon Airport Authority computer system breached in 'sophisticated' cyber attack

## Oiltanking and Wisag: Hacker attacks on German companies

2/1/2022, 4:53:54 PM

The attacks from the network are not decreasing: Now it hits an airport service provider and an oil logistician - this apparently can no longer fill tankers.

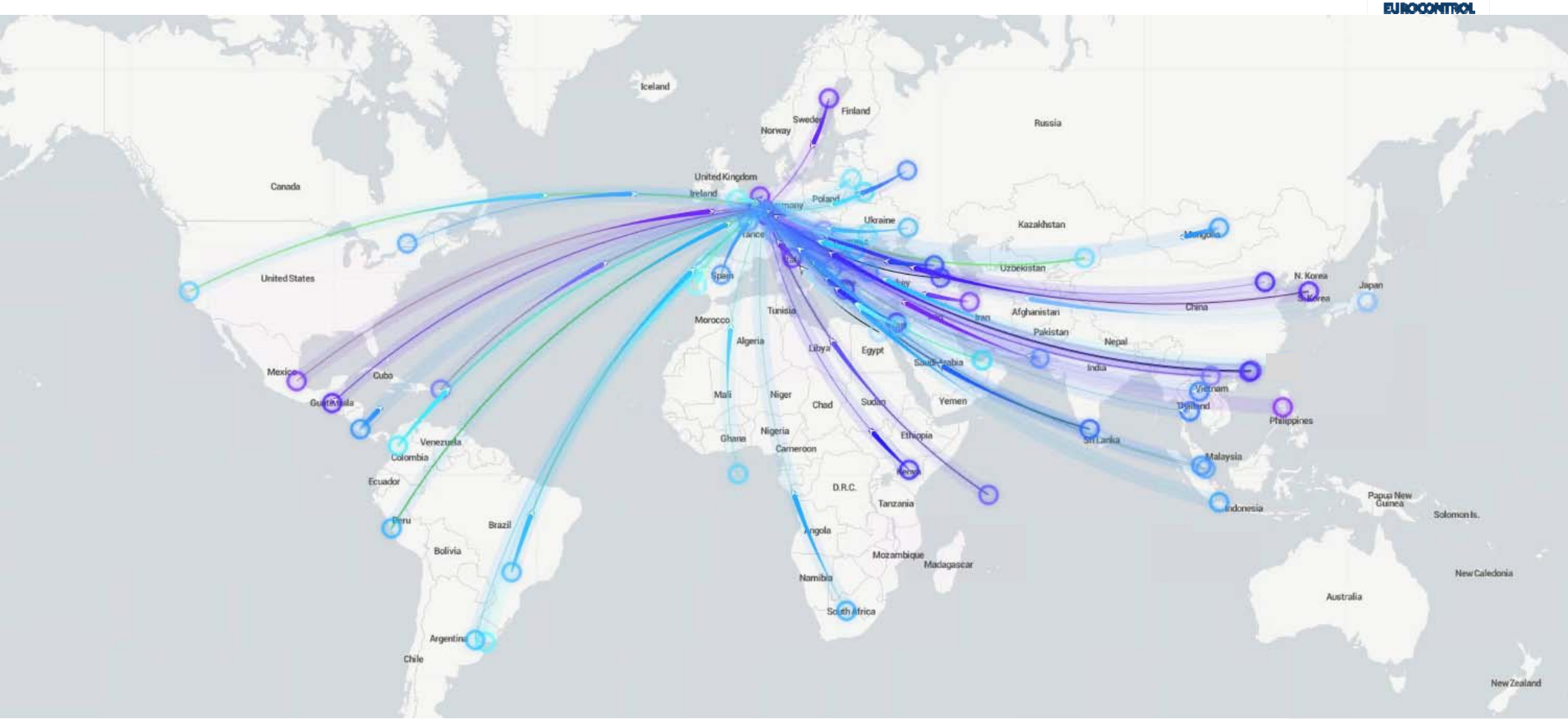
## Russian hackers target Czech websites in a series of cyberattacks

Czech railroads, regional airports, and a public administration portal have been facing cyberattacks from a pro-Russian hacker group Killnet.

Written by ČTK

Published on 20.04.2022 15:07 (updated on 21.04.2022)

Reading time: 4 minutes


Iceland
Finland
Sweden
Norway
Russia
Canada
United Kingdom
Ireland
Poland
Ukraine
Kazakhstan
Mongolia
United States
Uzbekistan
N. Korea
S. Korea
Japan
China
Afghanistan
Pakistan
Nepal
India
Morocco
Tunisia
Algeria
Libya
Egypt
Saudi Arabia
Iran
Mexico
Cuba
Guatemala
Mali
Niger
Chad
Sudan
Yemen
Vietnam
Thailand
Philippines
Venezuela
Colombia
Ecuador
Ghana
Nigeria
Cameroon
Ethiopia
Sri Lanka
Malaysia
Kenya
D.R.C.
Tanzania
Indonesia
Papua New Guinea
Solomon Is.
Peru
Brazil
Bolivia
Angola
Mozambique
Madagascar
Namibia
New Caledonia
Australia
South Africa
Argentina
Chile
New Zealand

Swissport
@swissportNews

⚠️ A part of #Swissport's IT infrastructure was subject to a ransomware attack. The attack has been largely contained, and we are working actively to fully resolve the issue as quickly as possible. Swissport regrets any impact the incidence has had on our service delivery.

# Lockbit ransomware colpisce la compagnia Aerea Hi Fly

Pubblicato il 15 Febbraio 2022
By **Redazione**

# Bangkok Airways hit by LockBit ransomware attack, loses lotsa data after refusing to pay

Partial credit card numbers appear and, worse still, passengers' meal preferences

Tue 31 Aug

Laura Dobberstein

16

Bangkok Airways has revealed it was the victim of a cyberattack from ransomware group LockBit on August 23rd, resulting in the publishing of stolen data.

Bangkok Airways' announcement about the matter came last Thursday, a day after LockBit posted a message on its dark web portal threatening the airline to pay a ransom or suffer a data leak.

The airline was given five days to sort payment, but instead of coughing up it disclosed the breach. LockBit responded by publishing the lot. Competing claims about the resulting data dump rate it at 103GB and over 200GB.

# Israeli Defense Company E.M.I.T. Aviation Consulting Targeted by LockBit 2.0 Ransomware

October 4, 2021 CIM Team

E.M.I.T. Aviation Consulting Ltd, an Israeli aerospace and defense company, was targeted by the LockBit 2.0 ransomware gang. Cyber attackers claim to have stolen information from the firm and threaten to release it on the gang's dark web leak site if the firm does not pay a ransom.

E.M.I.T. Aviation Consulting Ltd came into existence in 1986. The firm has designed and assembled complete aircraft, tactical and sub-tactical UAV systems, and portable integrated reconnaissance systems.

According to the threat intelligence firm Cyble, the ransomware gang has stolen databases containing over 6TB of data and is asking a $50M ransom:

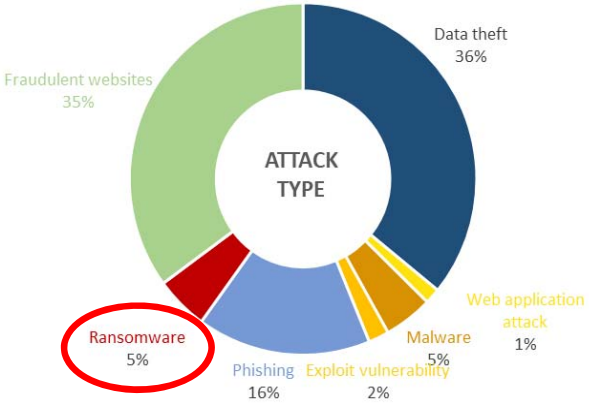
# L'École Nationale de l'Aviation Civile frappée avec le ransomware Hive

**L'ENAC a été frappée, durant le week-end du 12 mars, par une cyberattaque impliquant le ransomware Hive. Ses activités sont fortement perturbées. Une rançon de 1,2 million de dollars est demandée.**

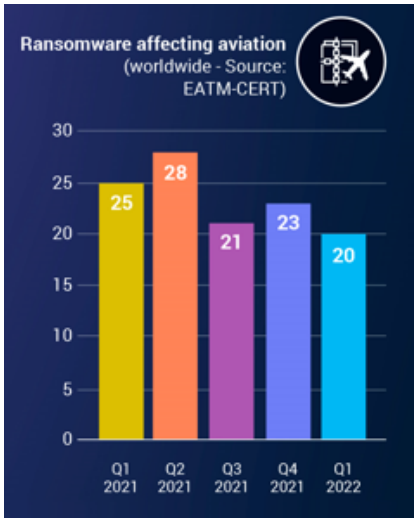
# Ransomware in aviation (global)

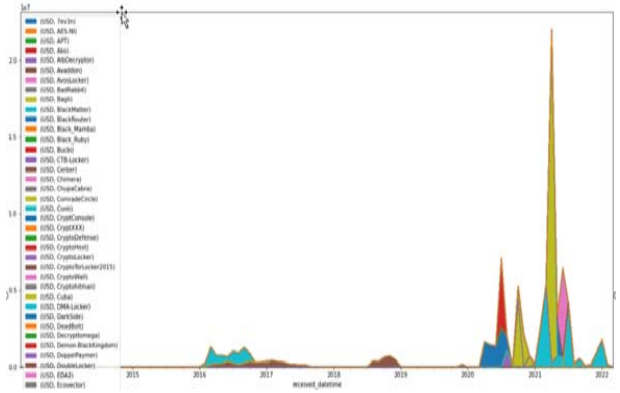
2020
One/week

2021
2,5/week




Out of 1.260 events

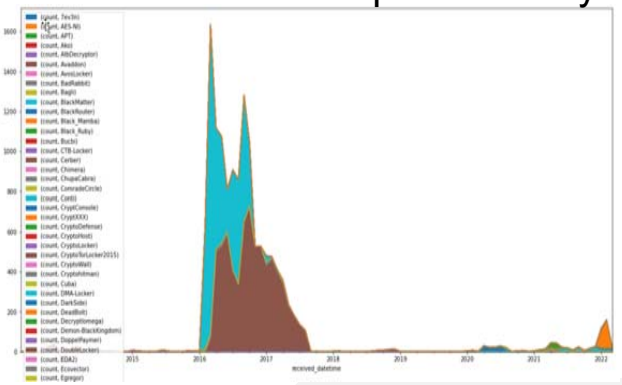


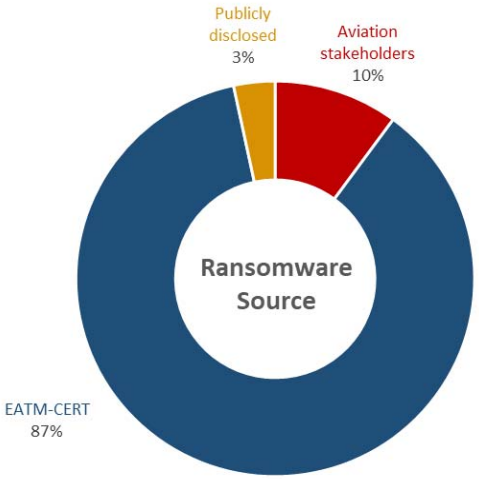
Amount of money earned monthly

All sectors

Number of ransoms paid monthly



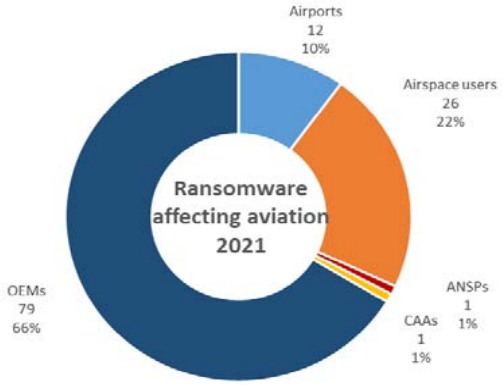
# Ransomware in aviation

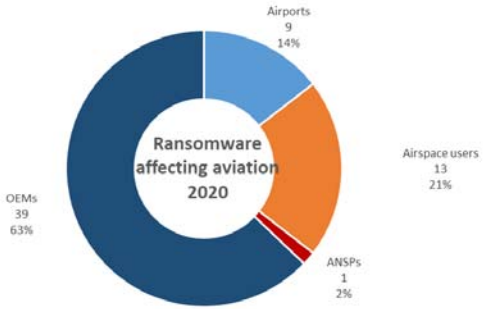



Aviation worldwide:

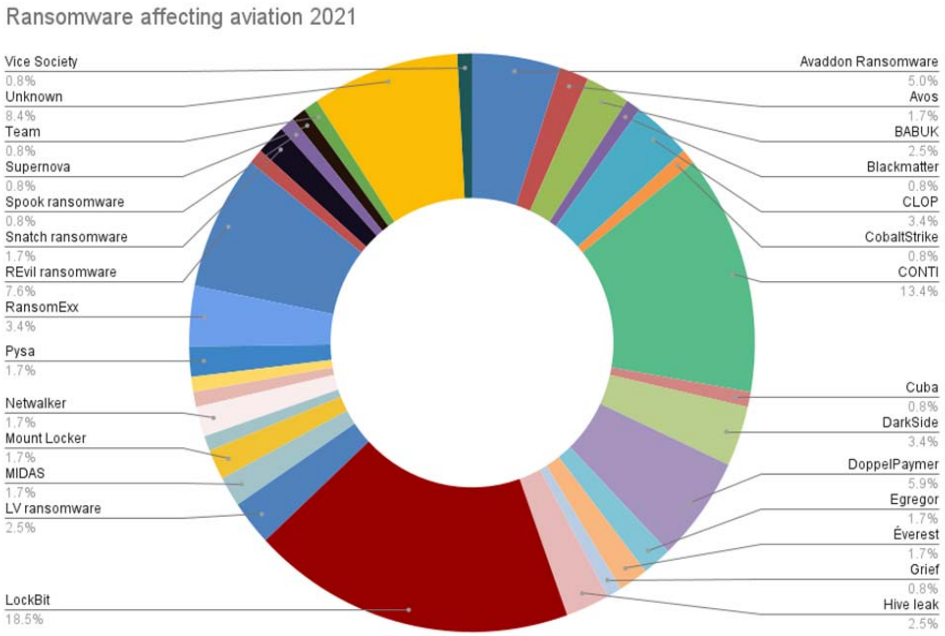
2021: 2,5 ransomware/week

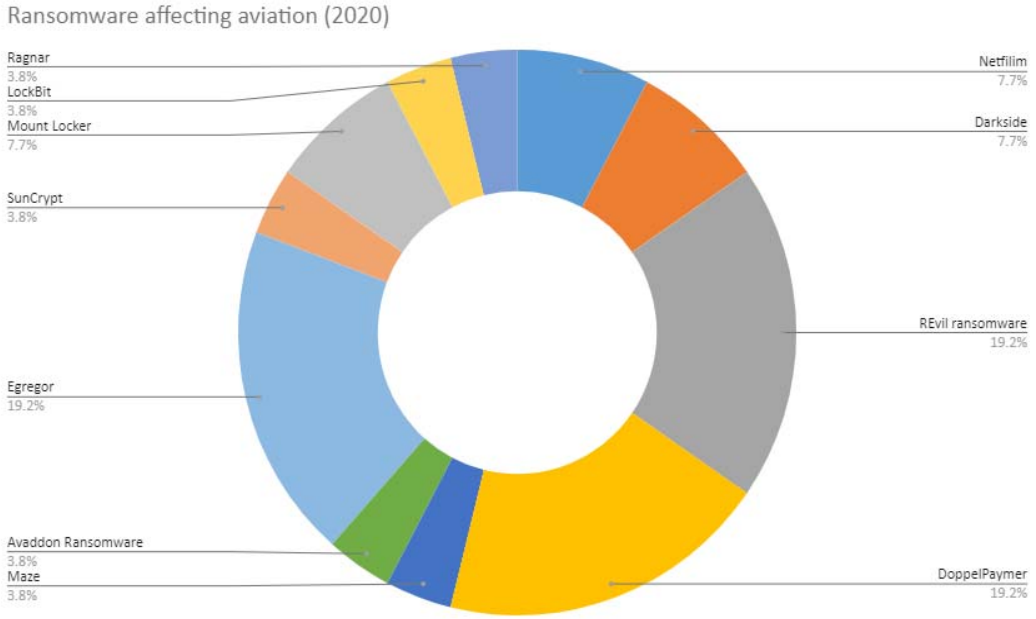
2020: 1 ransomware/week



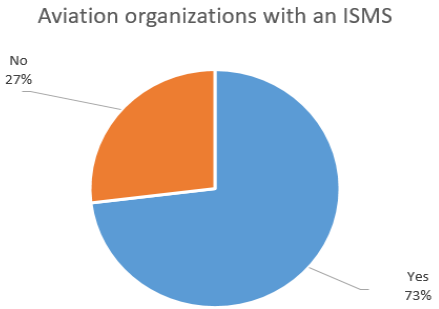



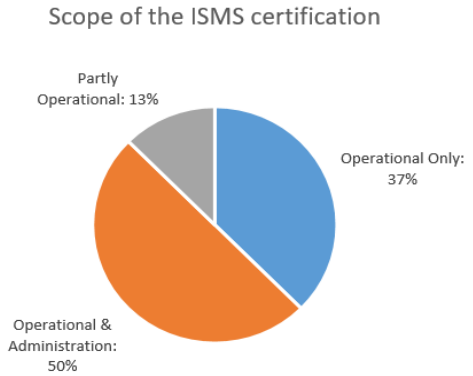
# Ransomware in aviation

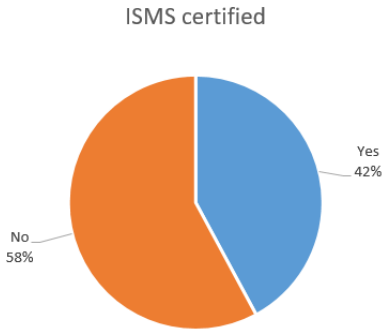


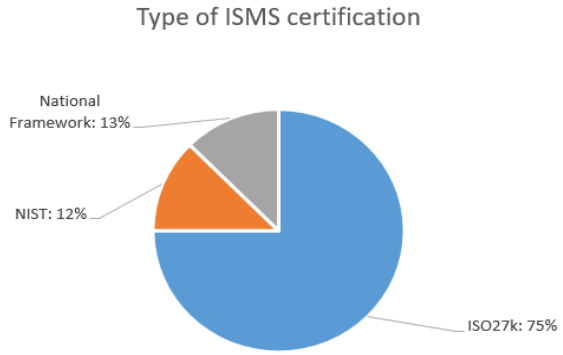



# ISMS implementation

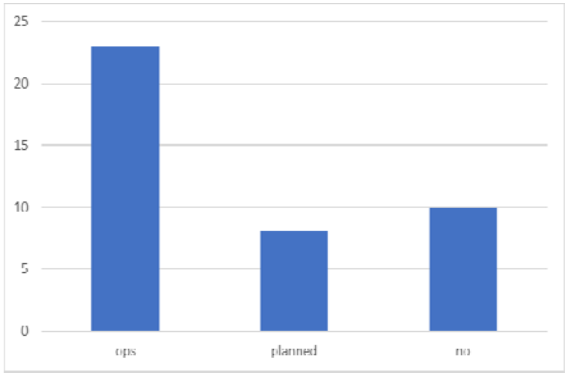


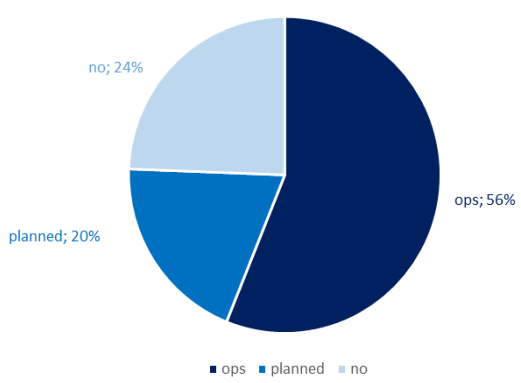



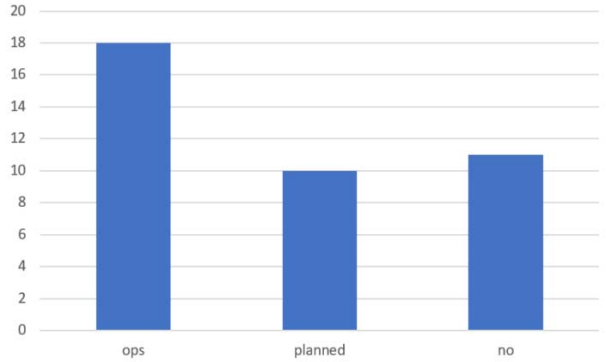



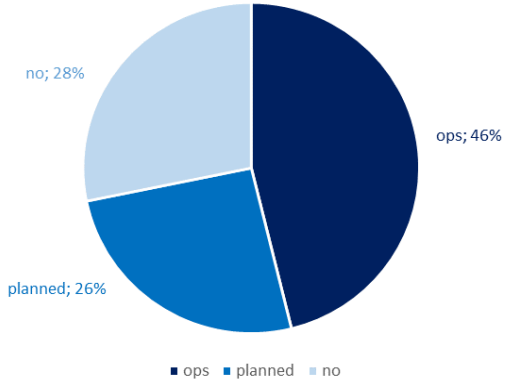
# SOC implementation



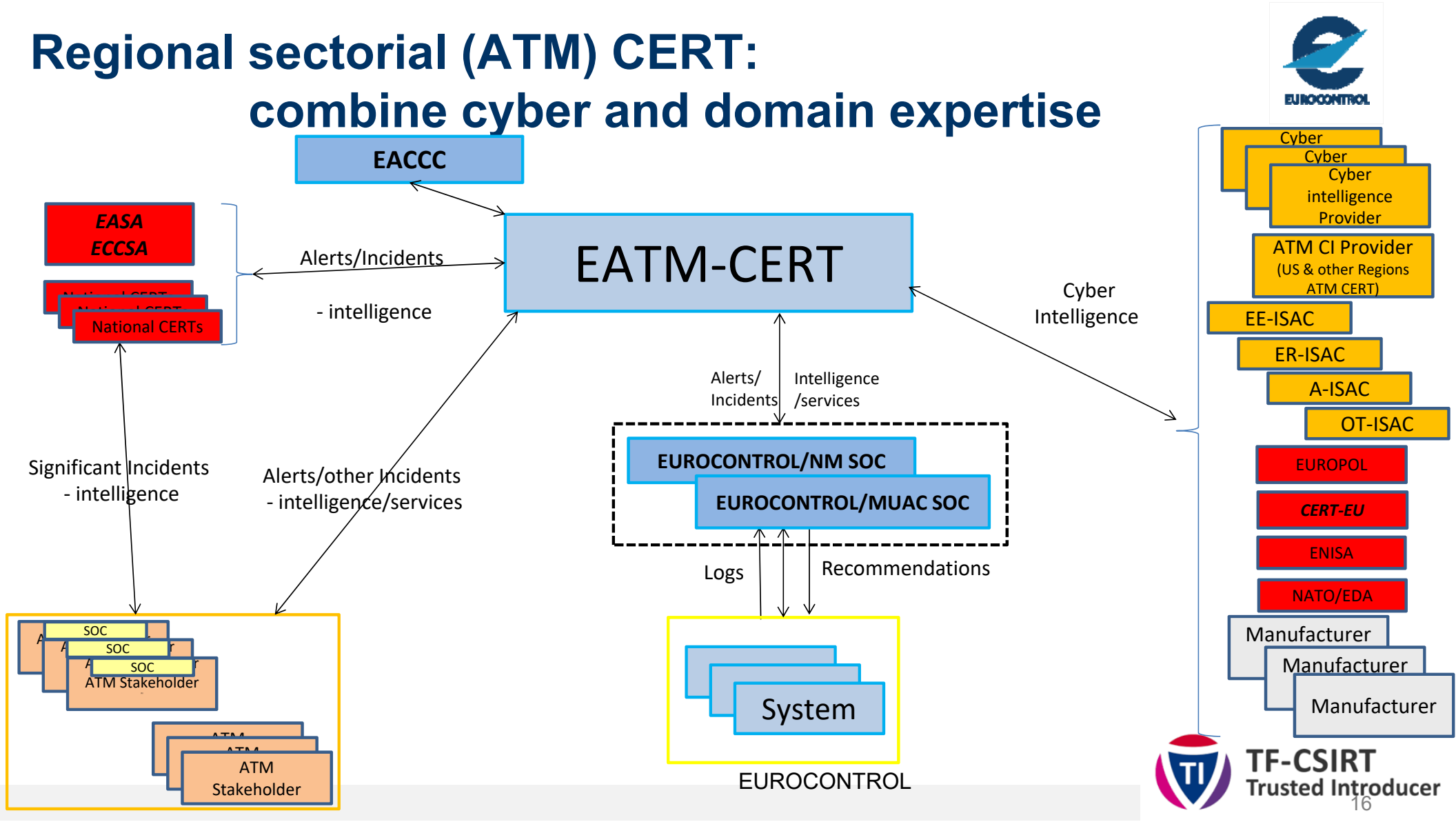

European ANSPs in 2021




European ANSPs in 2020

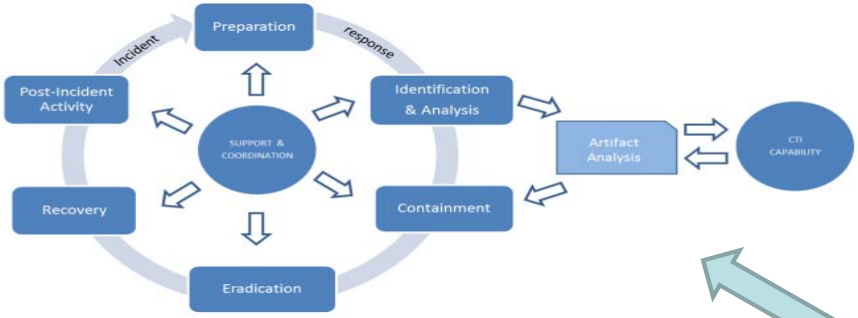
# Regional sectorial (ATM) CERT: combine cyber and domain expertise



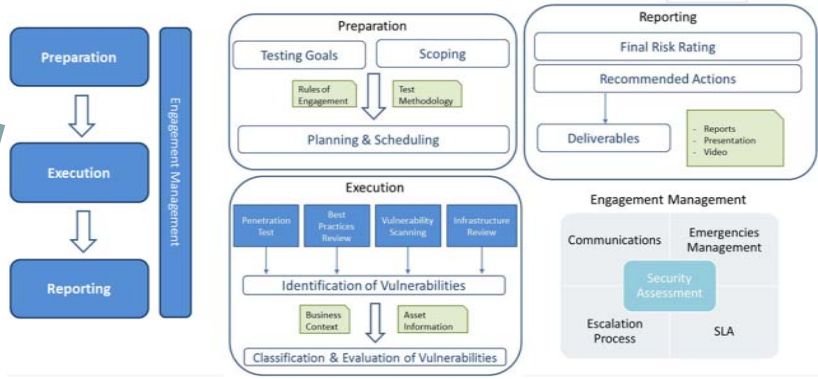

TF-CSIRT
Trusted Introducer

# EATM-CERT: catalogue of services

## Incident Response

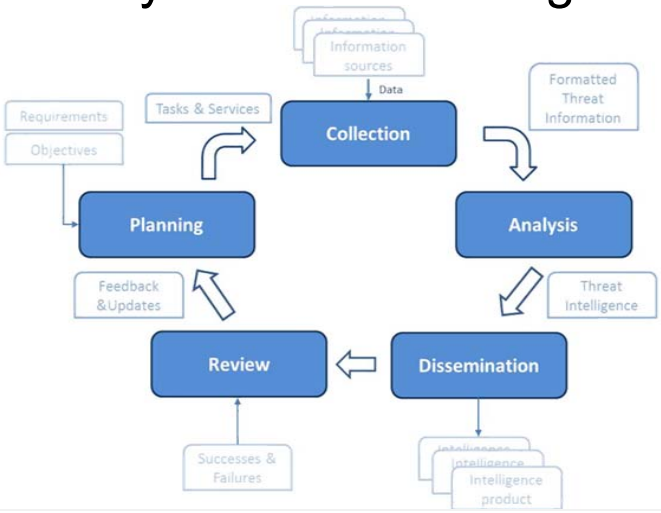



## Security Assessment





## Cyber Threat Intelligence




## Alerts & Warnings

# EATM-CERT services

1. Penetration test (EUROCONTROL services & products + Aviation stakeholders)
2. Bank transfer scams via email
3. Credentials leaks detection
4. Sensitive document leaks detection
5. Cyber Threat Intelligence (CTI) and feeds for aviation
6. Quarterly cyber threat landscape report for senior management
7. Annual report “cyber in aviation”
8. Support to incident response / Artefacts analysis
9. TLP:WHITE CTI tools – raising awareness
   - Cyber events map, tweeter
10. Vulnerability scanning of Aviation Stakeholders
11. IOC Scanner
12. Training exercises (table-top & technical) - EACCC-CYBER22
13. Phishing awareness campaigns

Soon

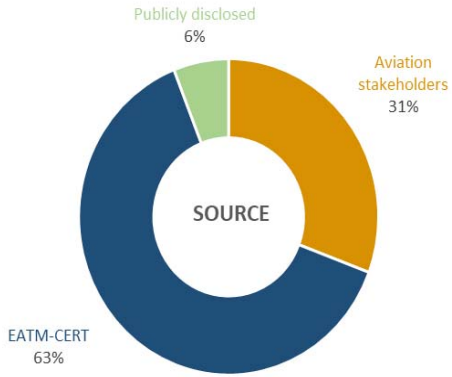
1. Test of Anti-DDOS solutions


EUROCONTROL

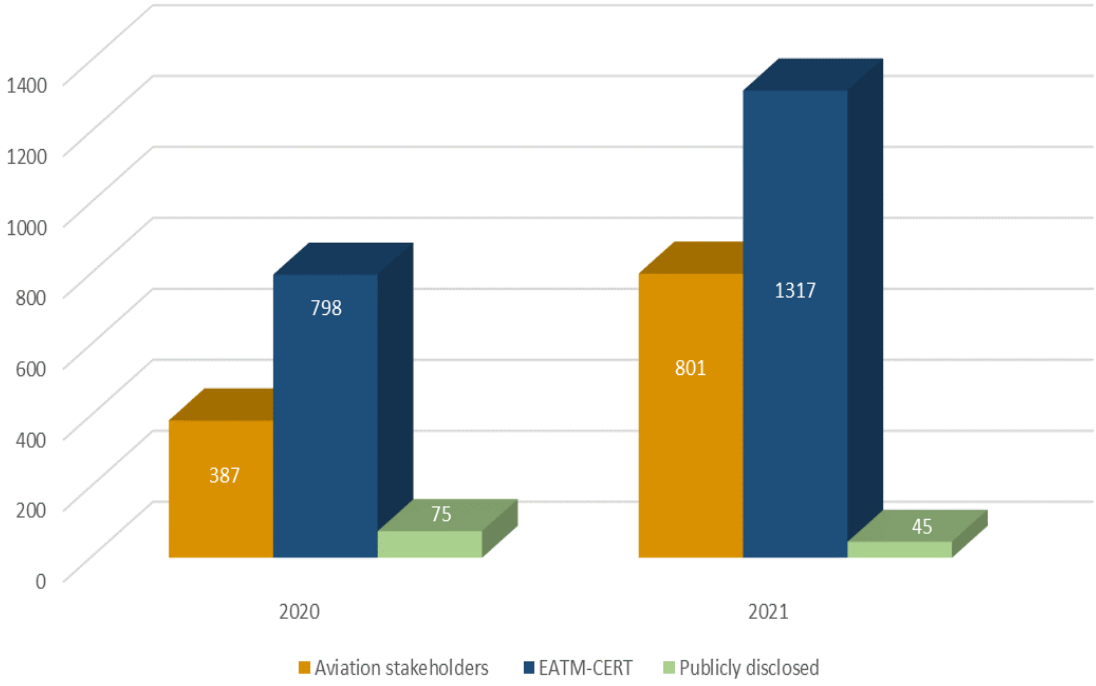
Report is
TLP:GREEN

# Source of events

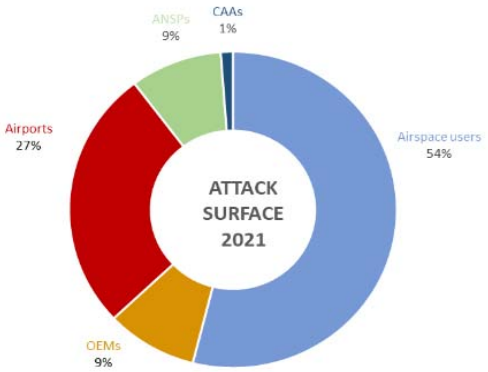

Source of events in 2021

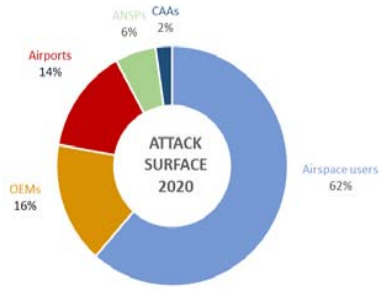


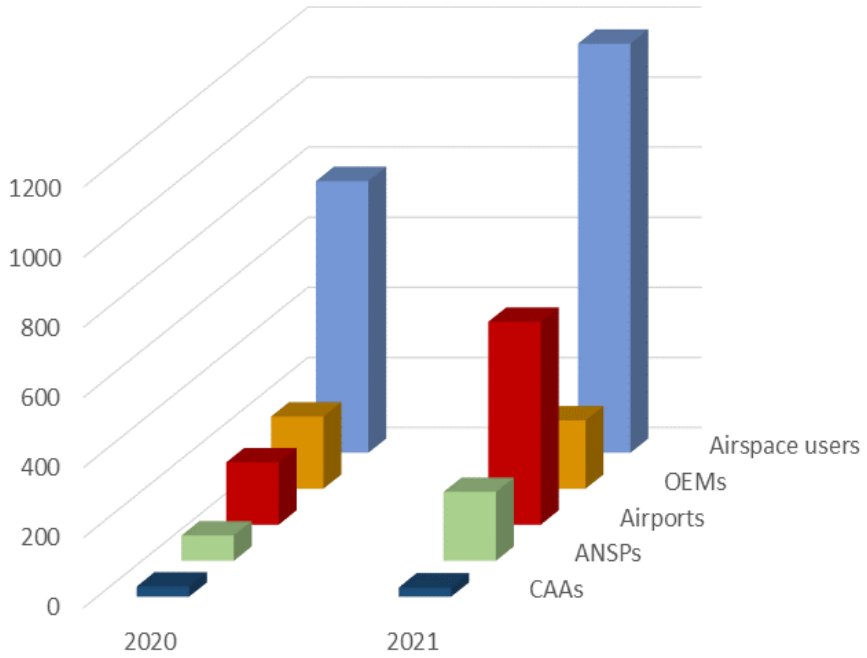

Source of events in 2020



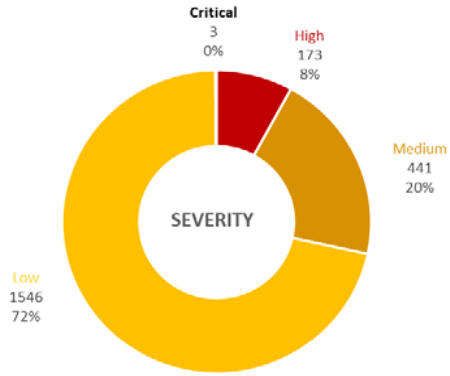
# Aviation threat landscape



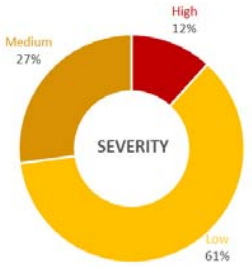



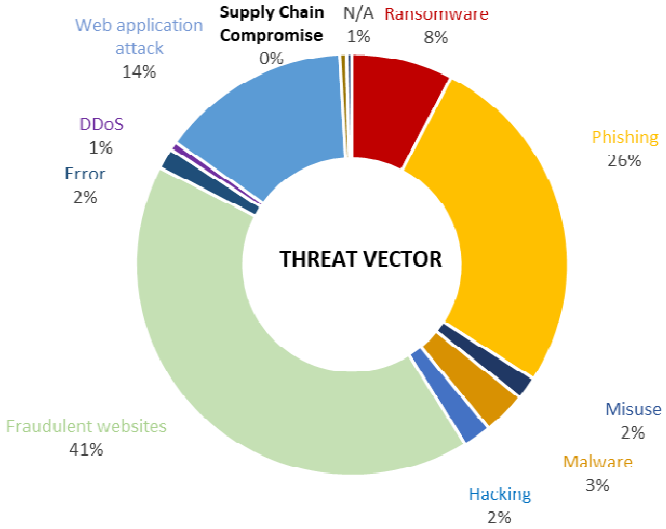

2021



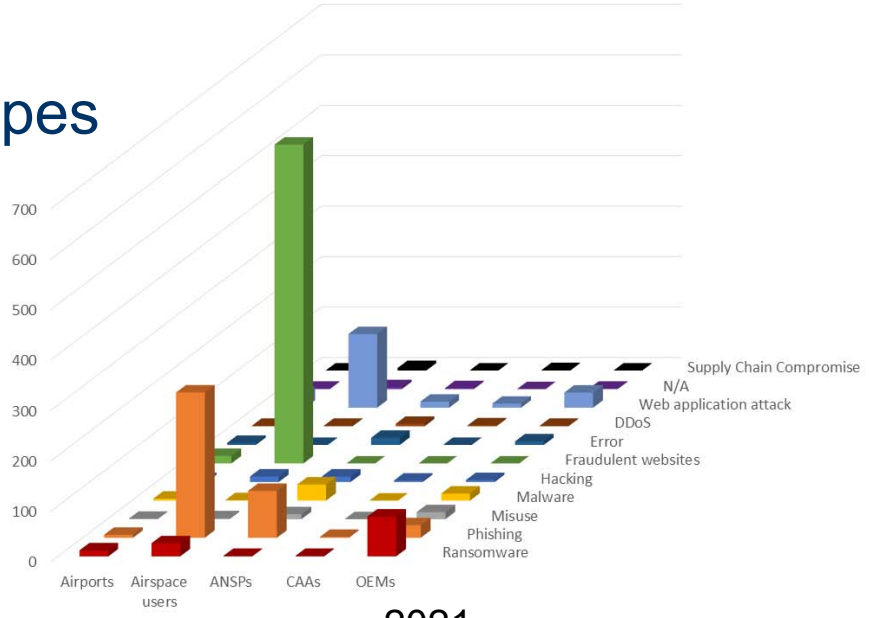

2020



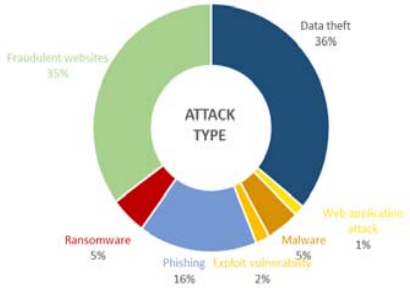
# Aviation – attack types



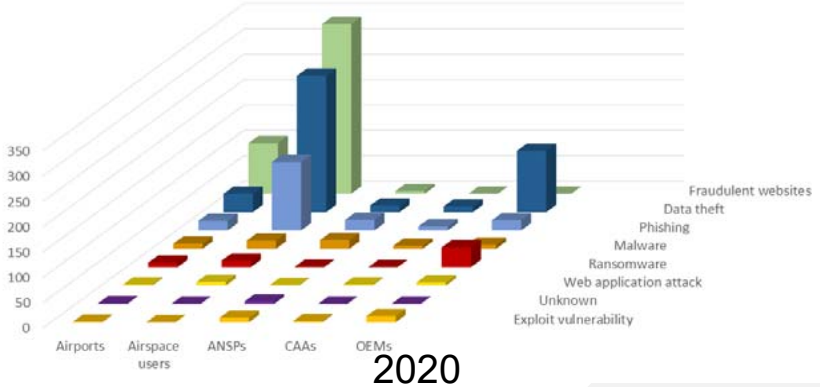

2021




2021



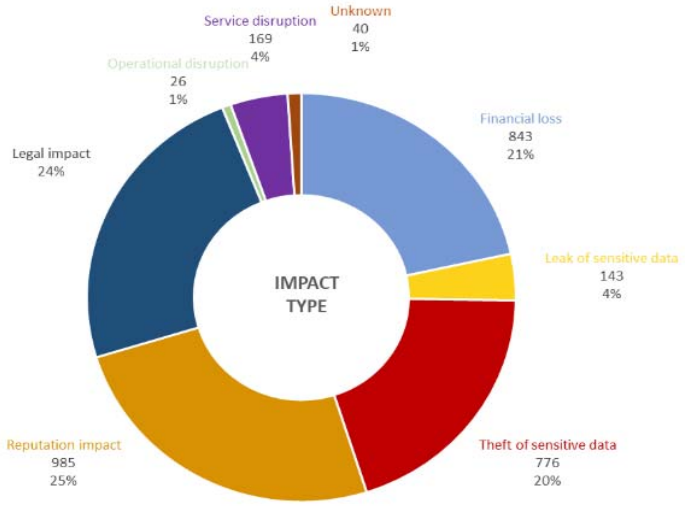

2020

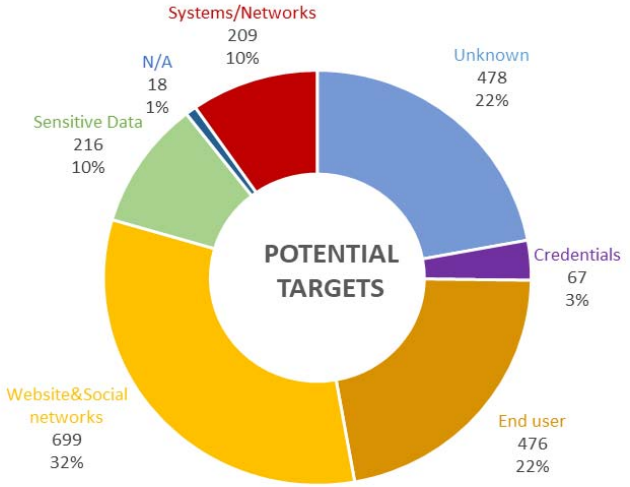



2020

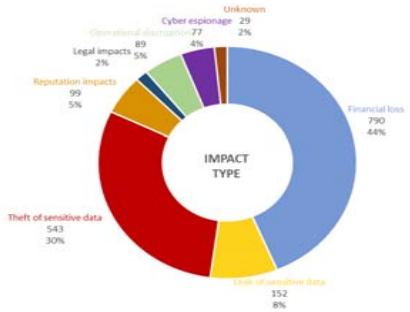
# Overview

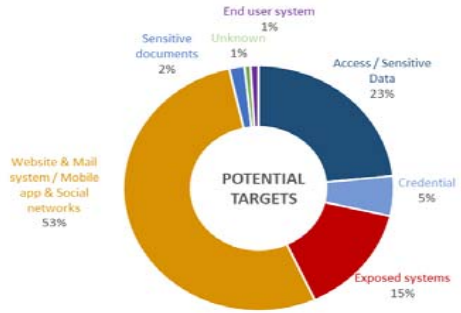
2021

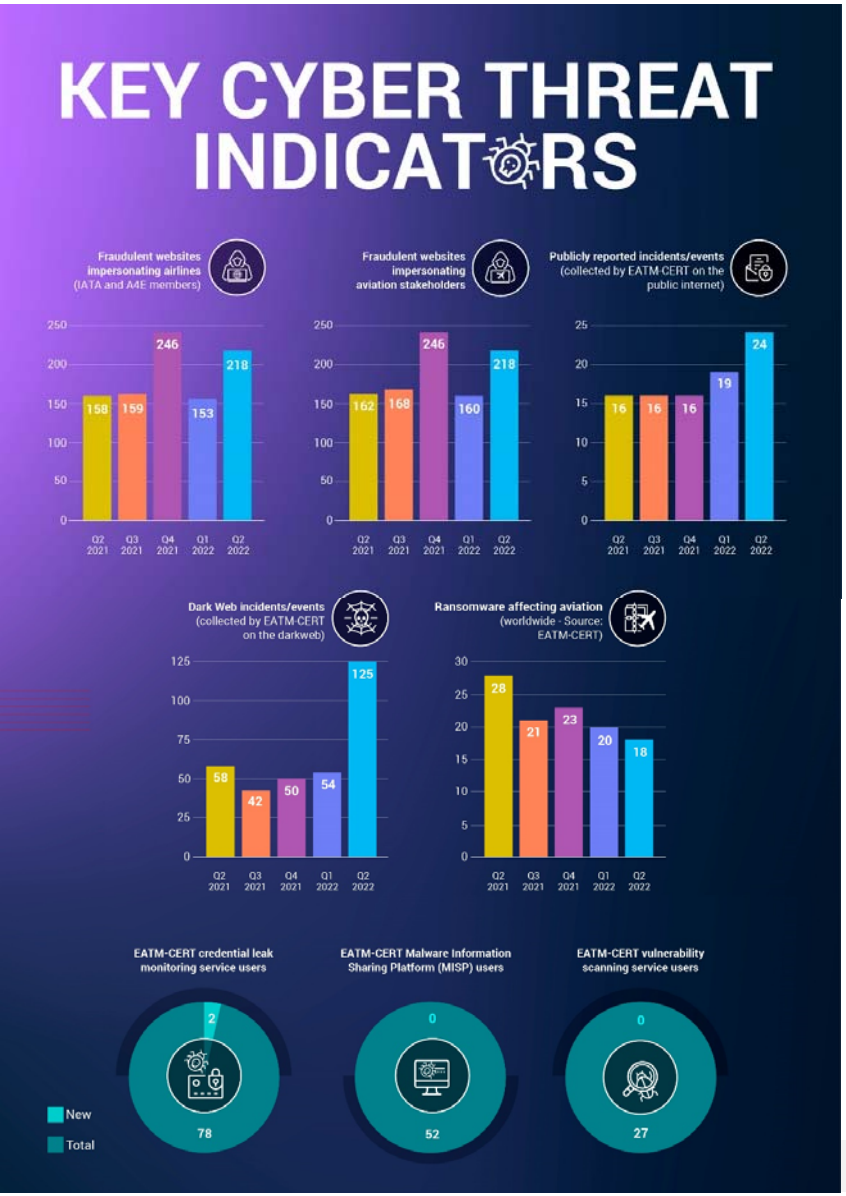


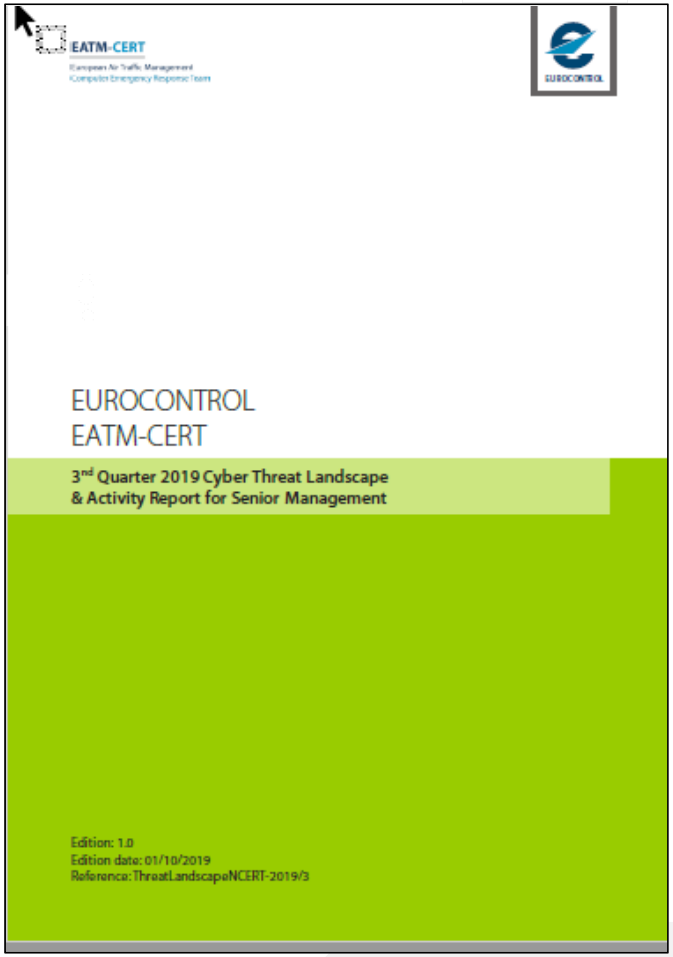




2020

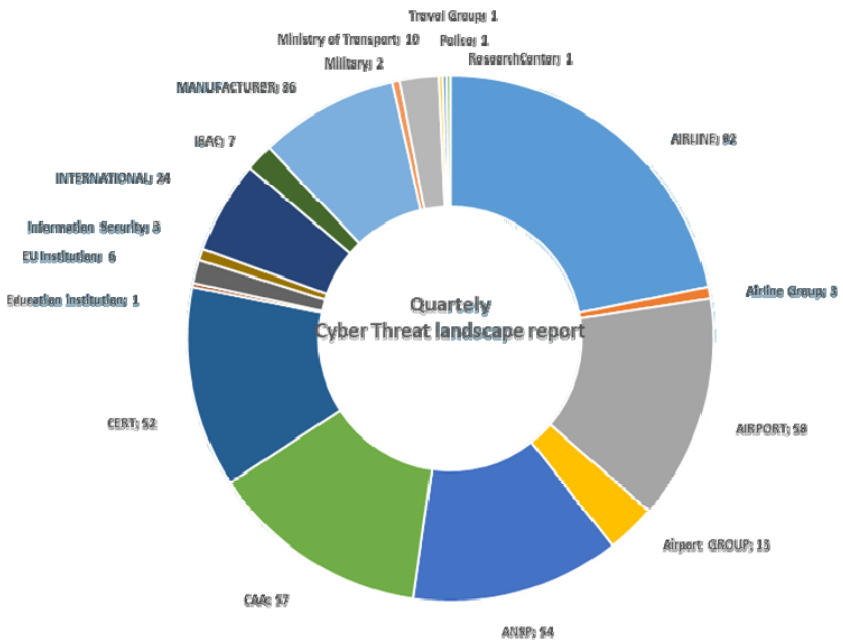



KEY CYBER THREAT INDICATORS
Fraudulent websites impersonating airlines (IATA and A4E members)
Fraudulent websites impersonating aviation stakeholders
Publicly reported incidents/events (collected by EATM-CERT on the public internet)
Q2 2021
Q3 2021
Q4 2021
Q1 2022
Q2 2022
158
159
246
153
218
162
168
246
160
218
16
16
16
19
24
Dark Web incidents/events (collected by EATM-CERT on the darkweb)
Ransomware affecting aviation (worldwide - Source: EATM-CERT)
58
42
50
54
125
28
21
23
20
18
EATM-CERT credential leak monitoring service users
EATM-CERT Malware Information Sharing Platform (MISP) users
EATM-CERT vulnerability scanning service users
2
78
0
52
0
27
New
Total

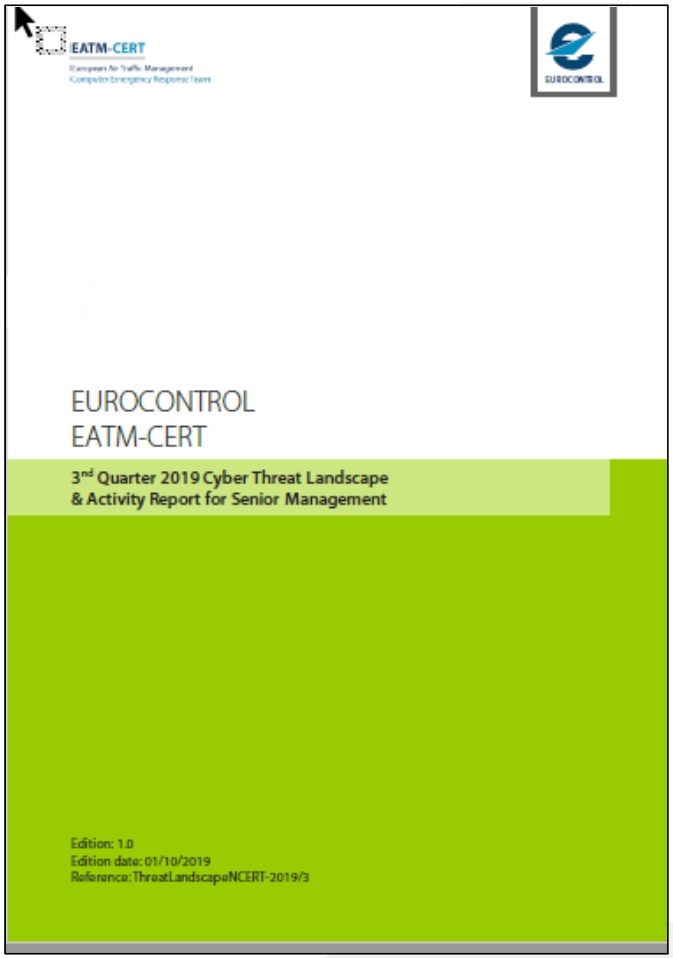

EATM-CERT
EUROCONTROL
EATM-CERT
3nd Quarter 2019 Cyber Threat Landscape
& Activity Report for Senior Management
Edition: 1.0
Edition date: 01/10/2019
Reference: ThreatLandscapeNCERT-2019/3

# Quarterly cyber threat landscape report




421 organisations

1,223 individuals



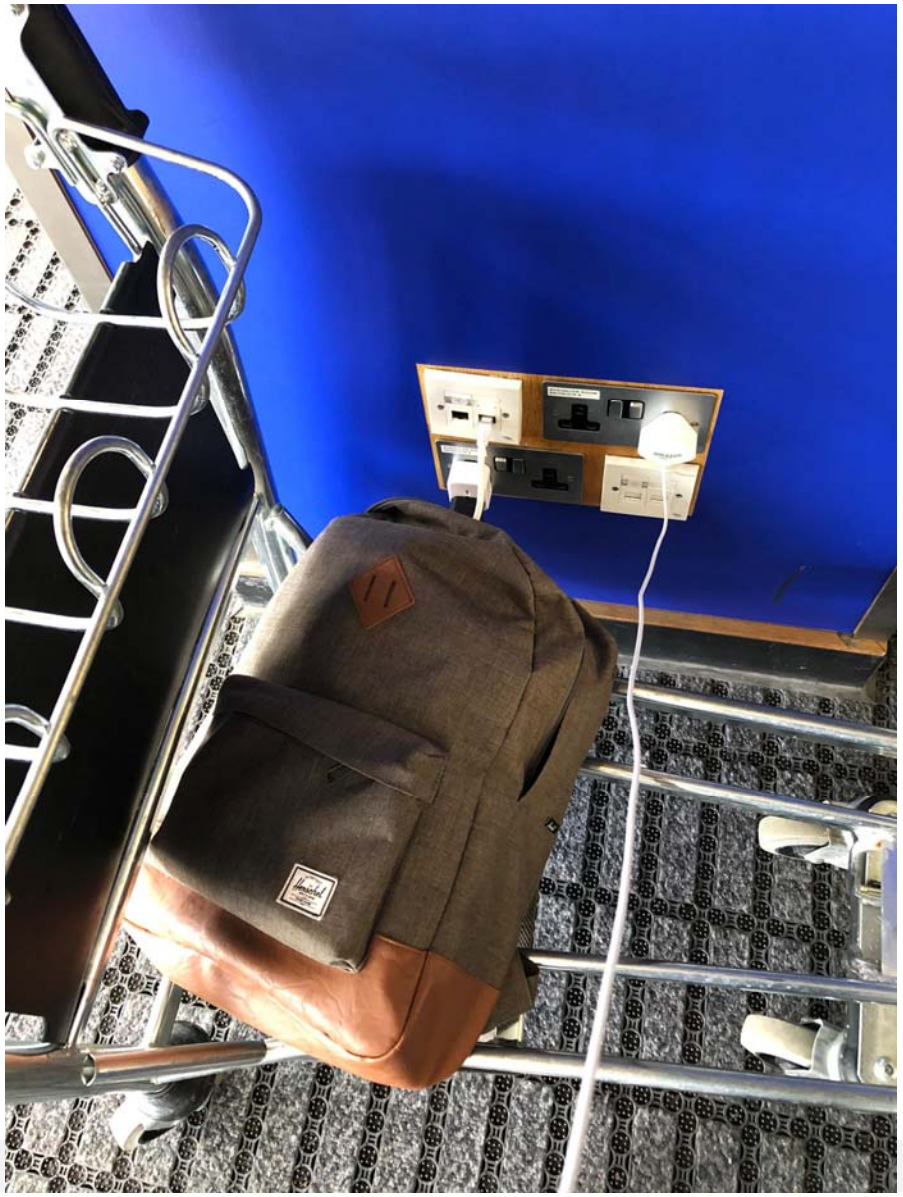
# Penetration test

# Service of pentest on aviation systems

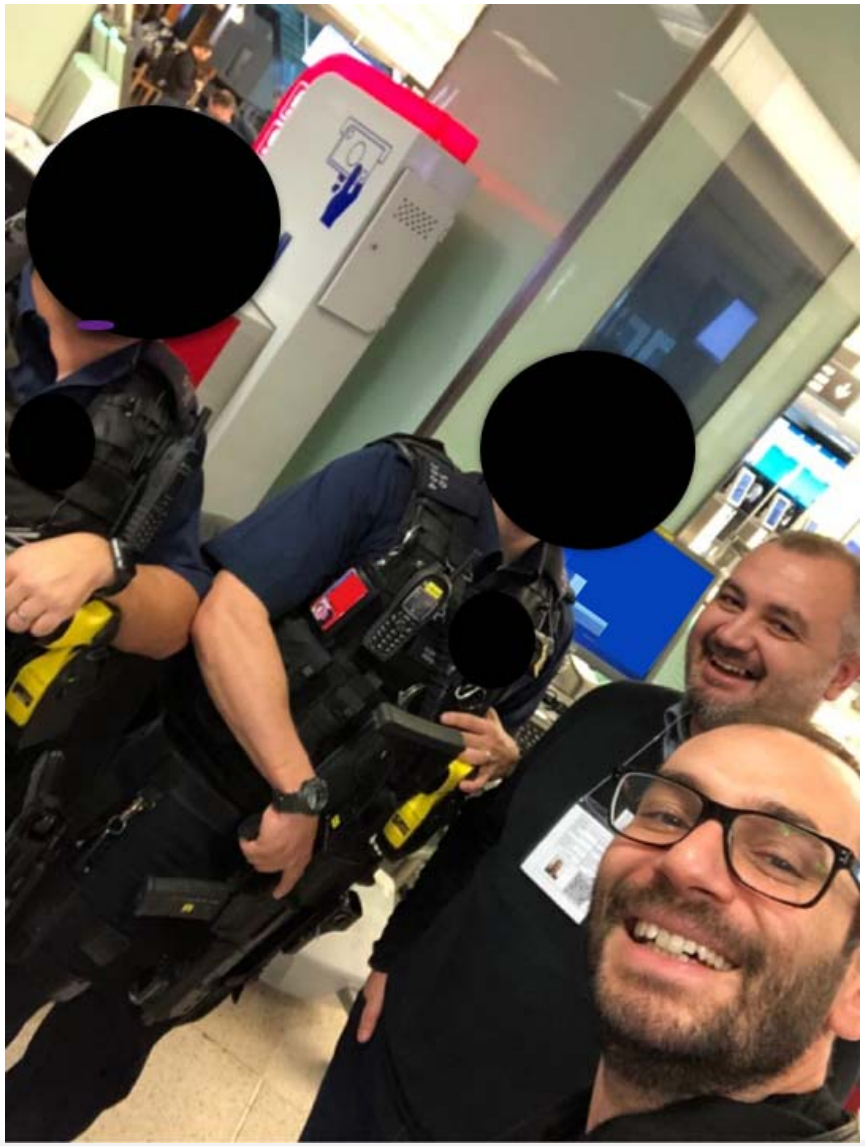
- Able to conduct max 8 to 12 pentests on stakeholders systems
  - Free of charge for Aviation stakeholders of EUROCONTROL Member States
  - Collaborative

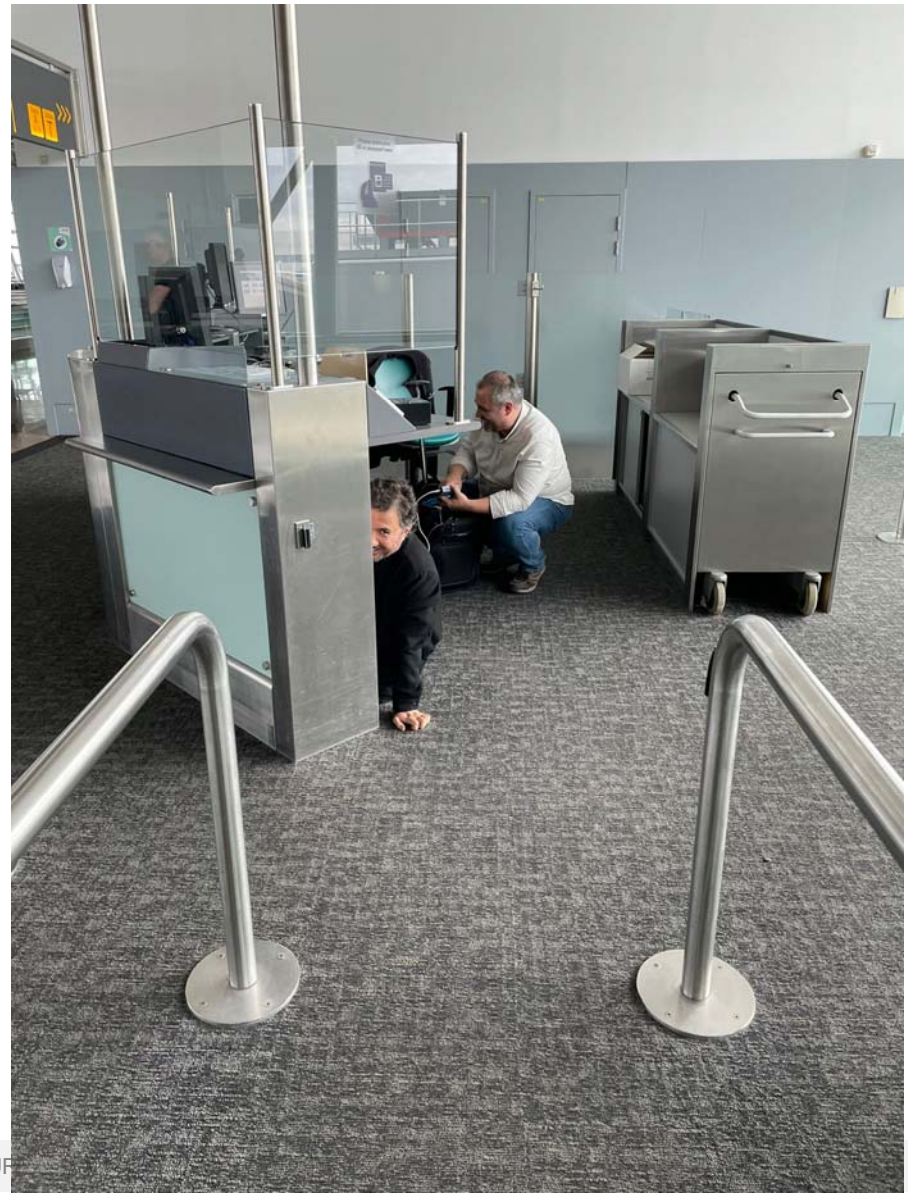
  - 3 steps:
    1. Scoping document: collaborative definition of scope, objectives, scenarios, schedule
    2. One-week pentest on-site. No risk of operational impact. Joint activity.
       COVID-19: need to adapt to local restrictions
    3. Final report subject to review-approval

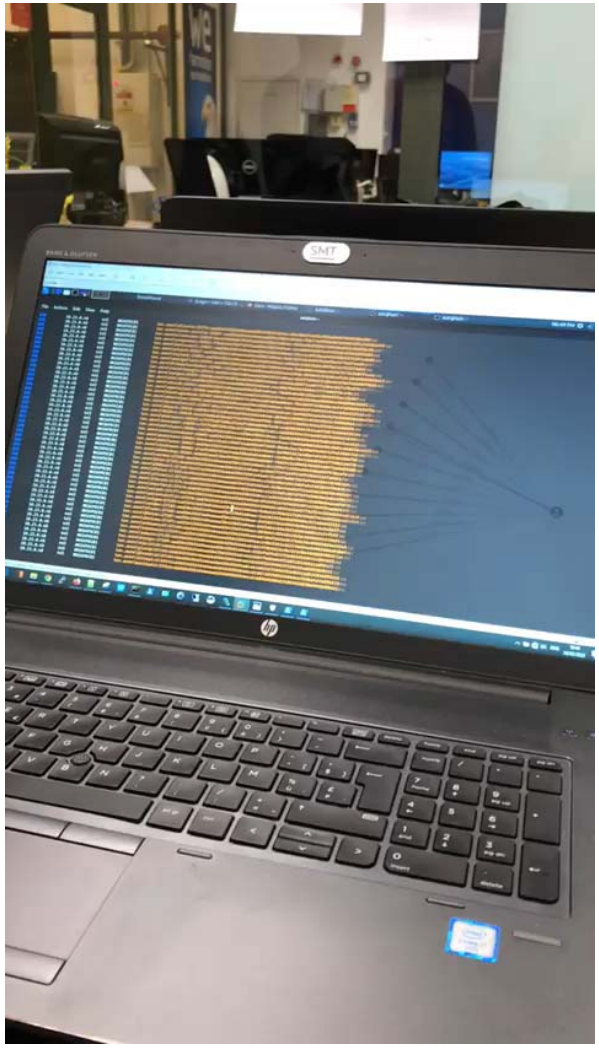
  - 2 categories of findings:
    - Local: only for stakeholder
    - Generic: de-identified and shared with aviation community on a need to know basis

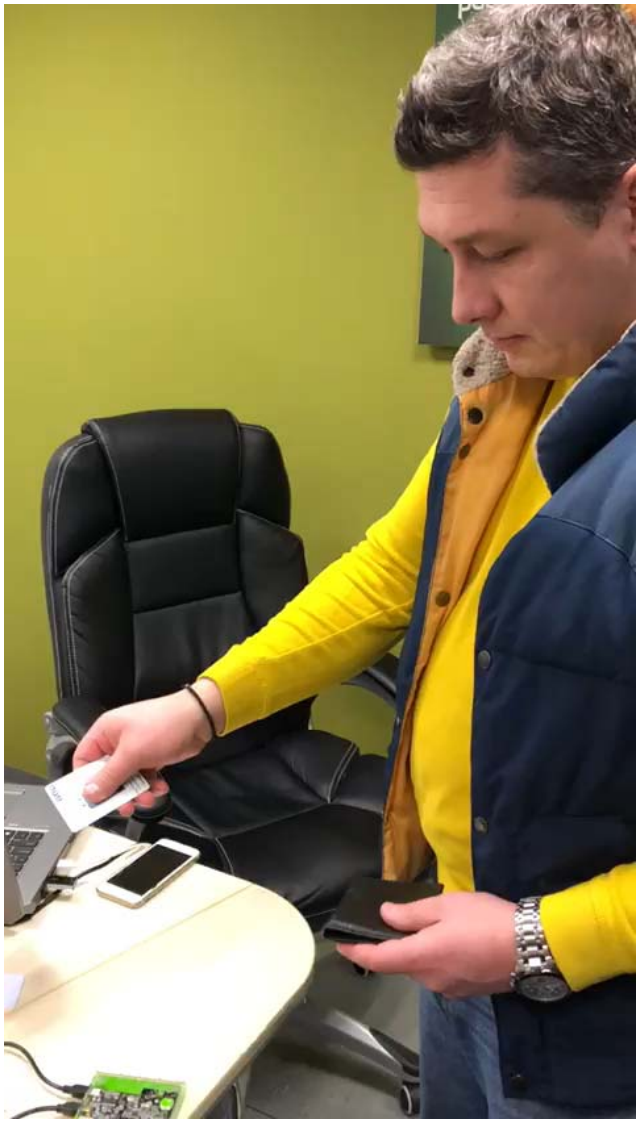


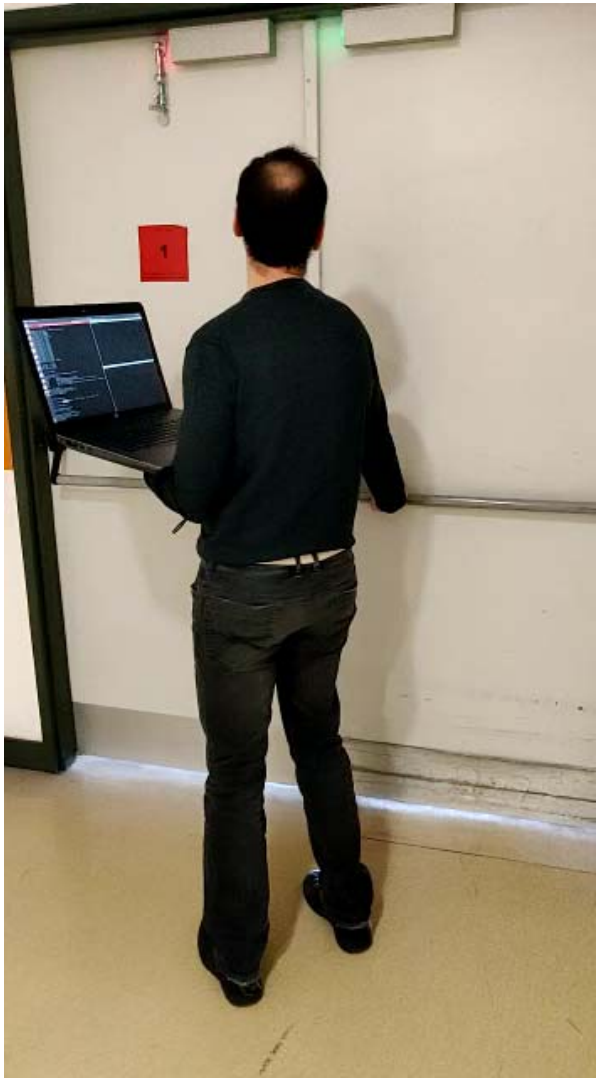

amazon

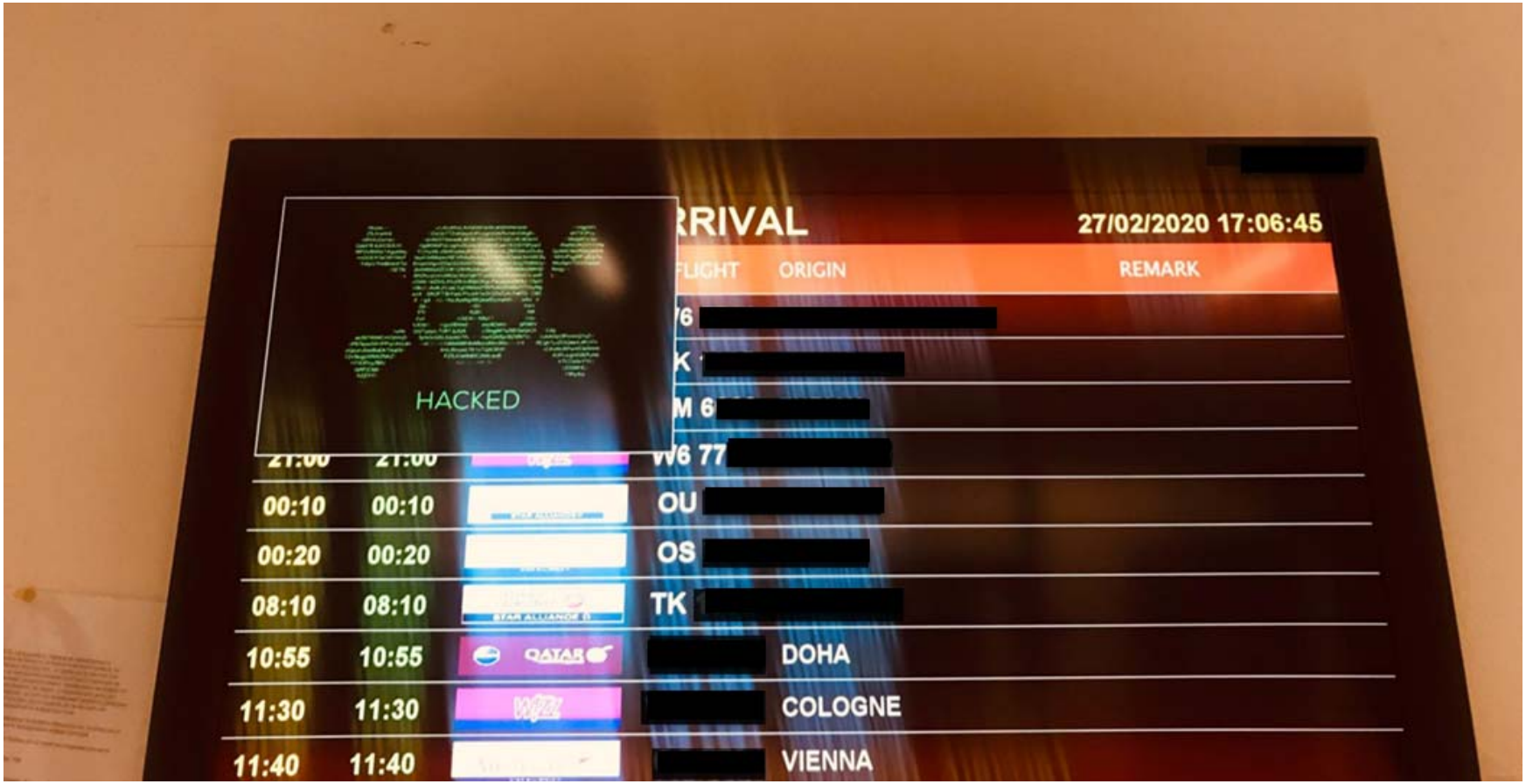




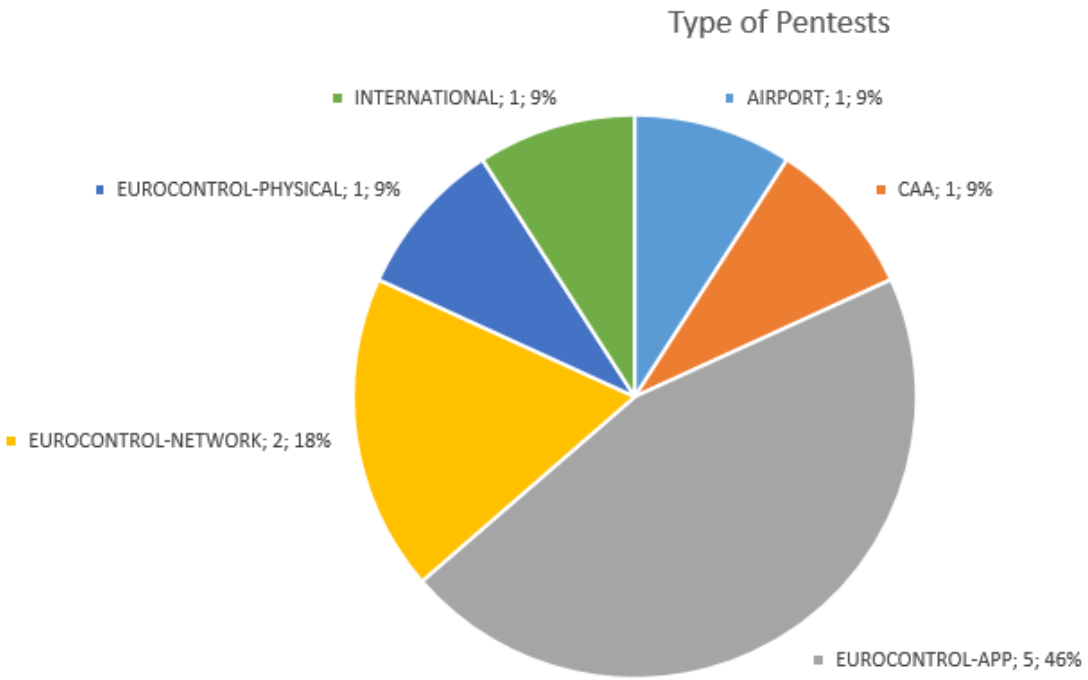


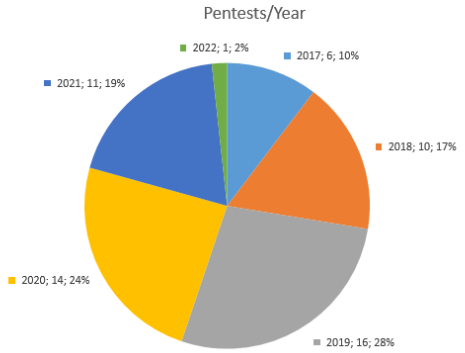





RRIVAL
27/02/2020 17:06:45
FLIGHT
ORIGIN
REMARK
HACKED
00:10 00:10
00:20 00:20
08:10 08:10
10:55 10:55
DOHA
11:30 11:30
COLOGNE
11:40 11:40
VIENNA

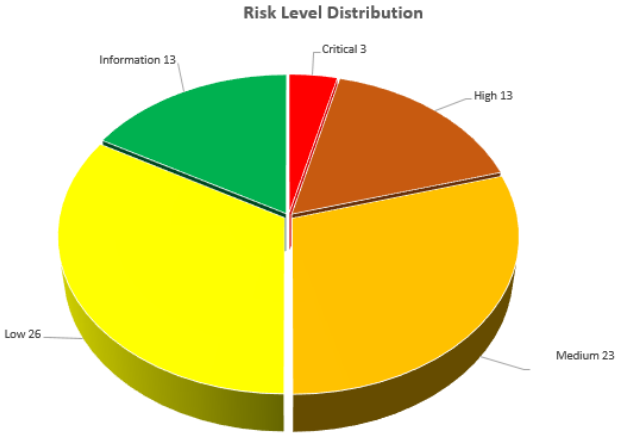
# Pentests 2021 - Constituents

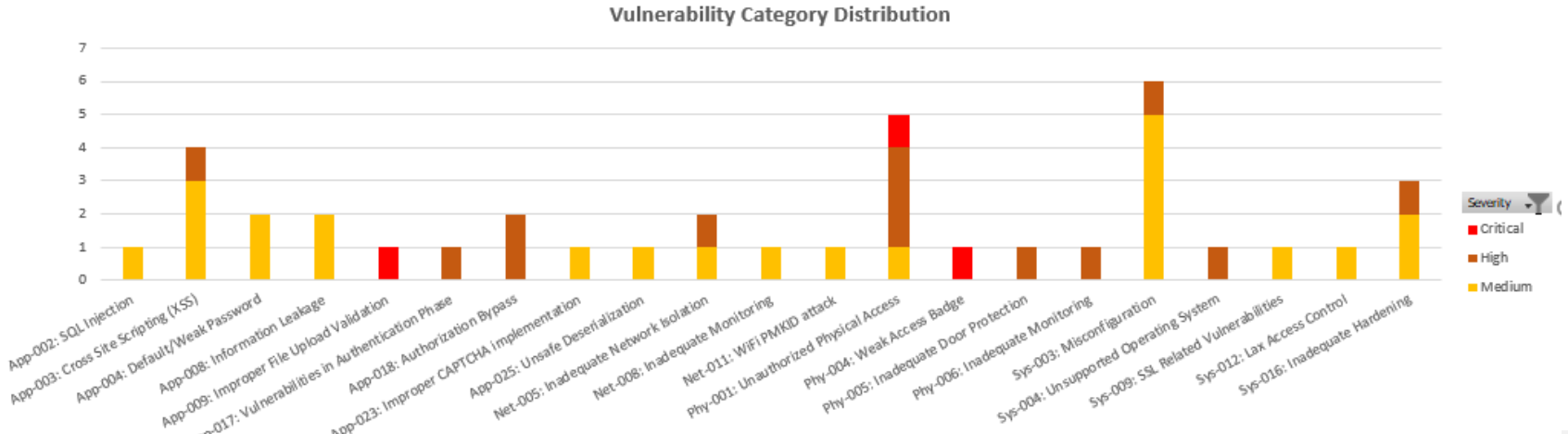



TOTAL=11 Pentests

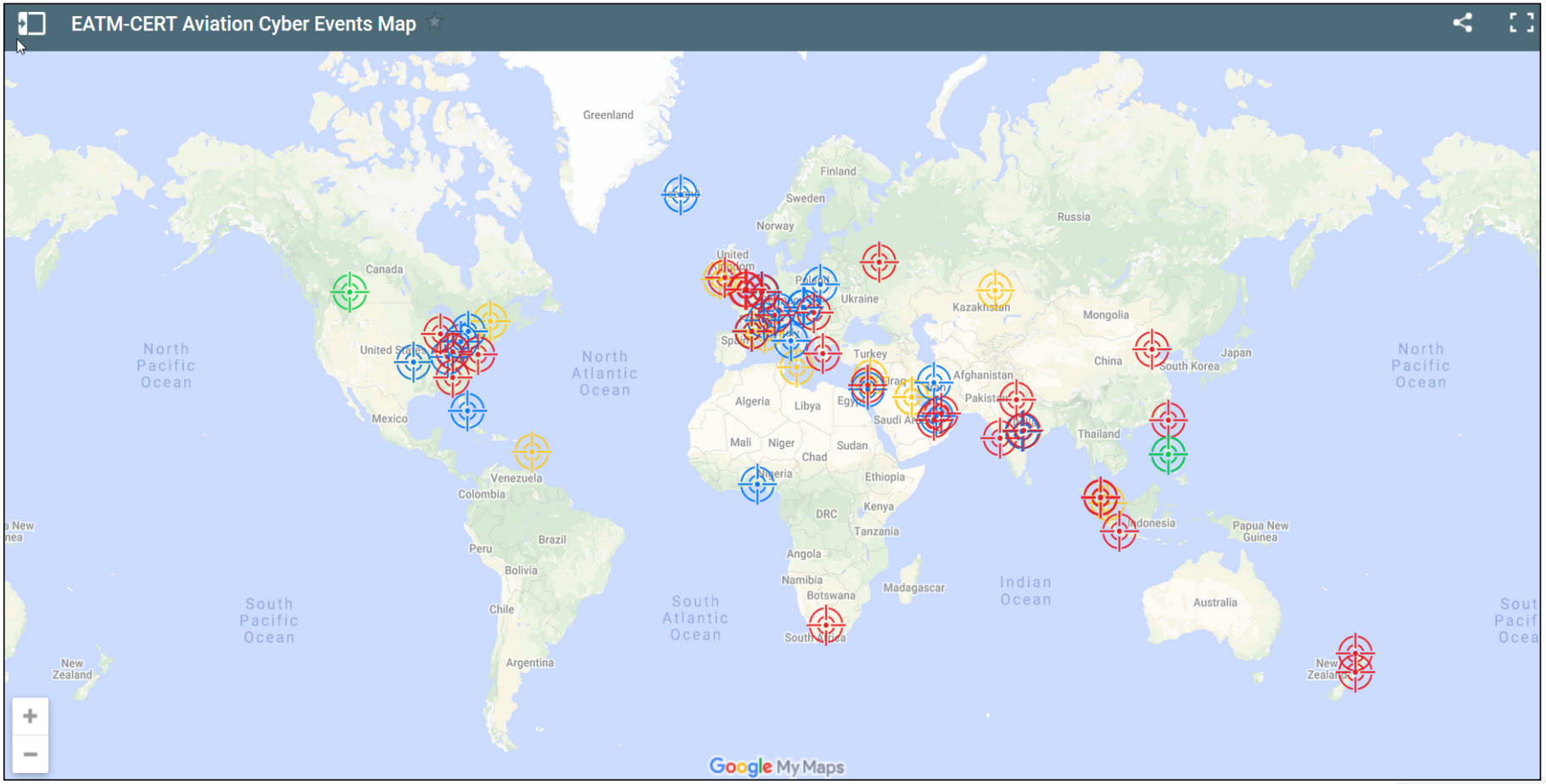
# Pentests 2021 - Findings

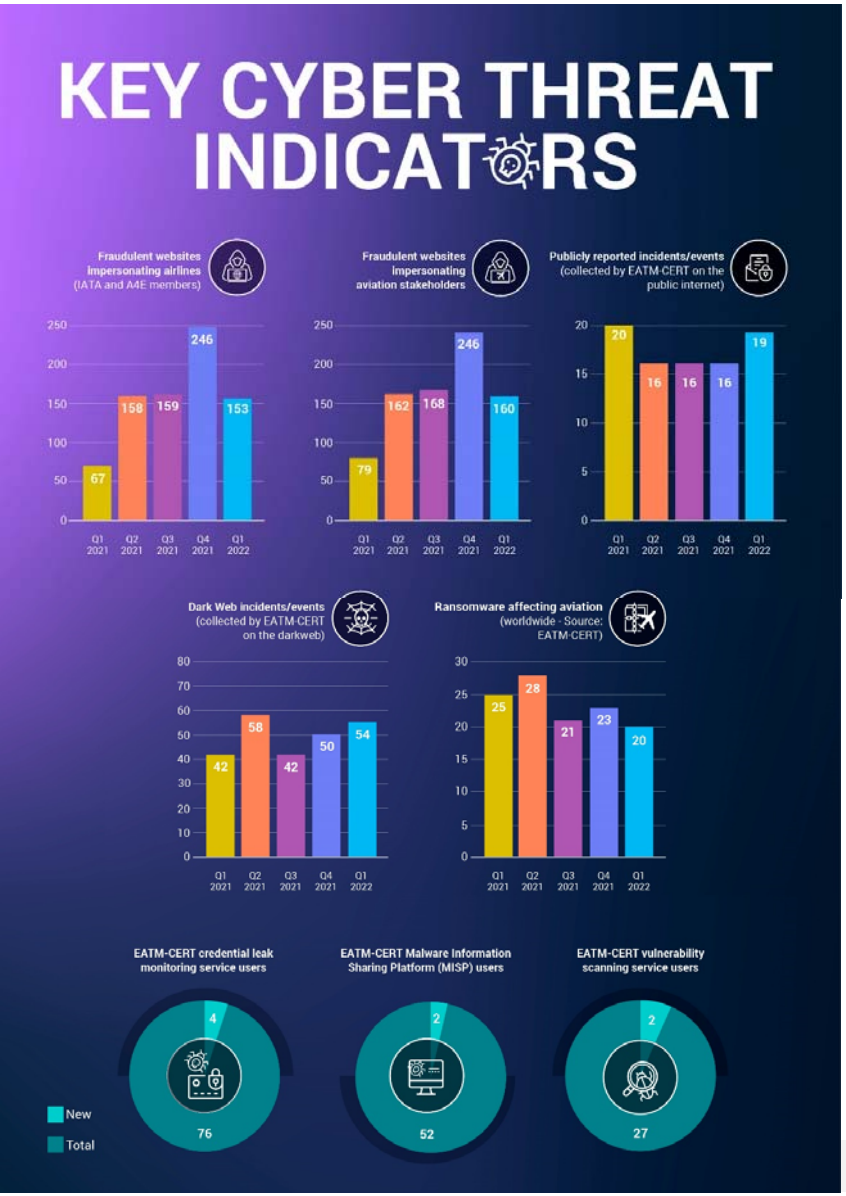


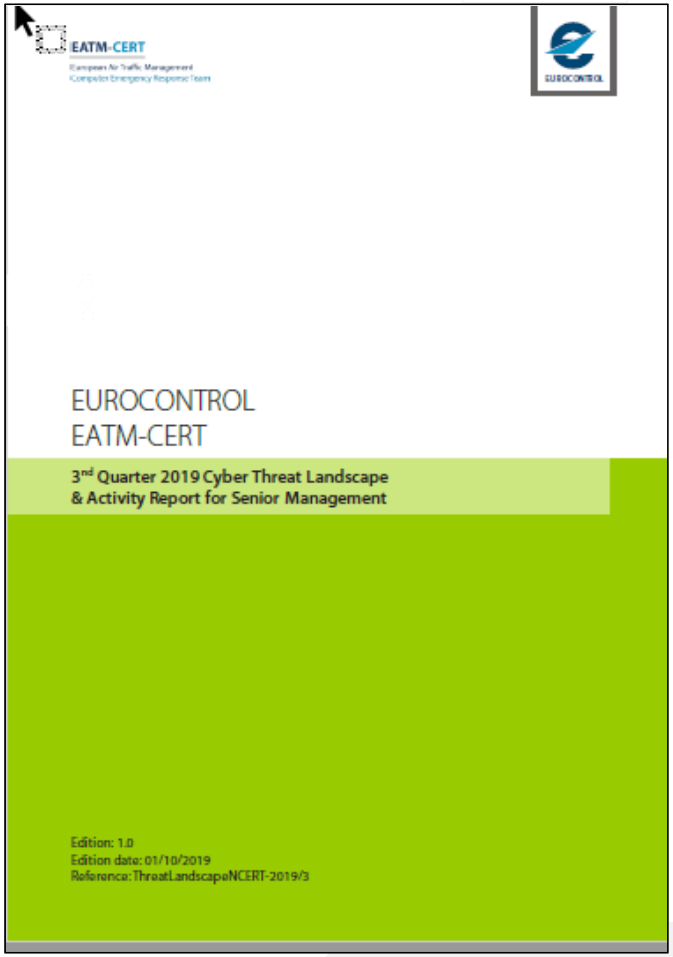



# CYBER THREAT INTELLIGENCE & INNOVATIVE CYBER-SECURITY SERVICES

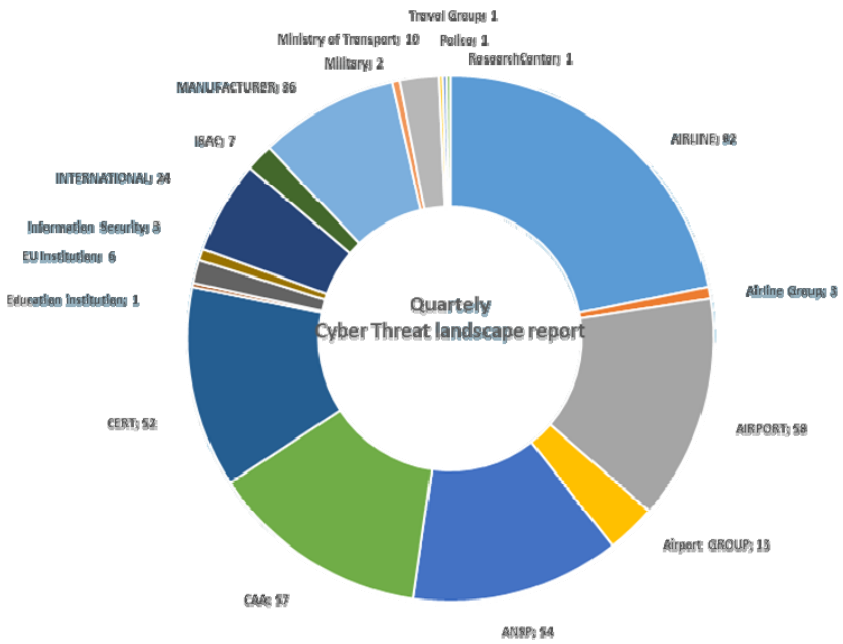
# TLP:WHITE CTI tools – raising awareness




KEY CYBER THREAT INDICATORS
Fraudulent websites impersonating airlines (IATA and A4E members)
Q1 2021: 67
Q2 2021: 158
Q3 2021: 159
Q4 2021: 246
Q1 2022: 153
Fraudulent websites impersonating aviation stakeholders
Q1 2021: 79
Q2 2021: 162
Q3 2021: 168
Q4 2021: 246
Q1 2022: 160
Publicly reported incidents/events (collected by EATM-CERT on the public internet)
Q1 2021: 20
Q2 2021: 16
Q3 2021: 16
Q4 2021: 16
Q1 2022: 19
Dark Web incidents/events (collected by EATM-CERT on the darkweb)
Q1 2021: 42
Q2 2021: 58
Q3 2021: 42
Q4 2021: 50
Q1 2022: 54
Ransomware affecting aviation (worldwide - Source: EATM-CERT)
Q1 2021: 25
Q2 2021: 28
Q3 2021: 21
Q4 2021: 23
Q1 2022: 20
EATM-CERT credential leak monitoring service users
4
76
EATM-CERT Malware Information Sharing Platform (MISP) users
2
52
EATM-CERT vulnerability scanning service users
2
27
New
Total

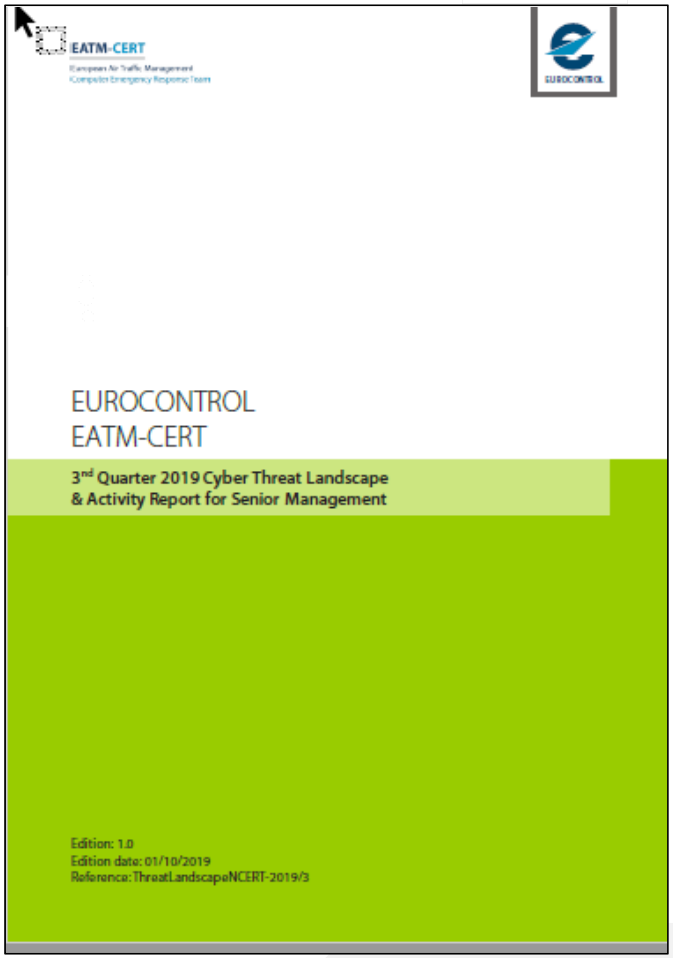

EATM-CERT
EUROCONTROL
EATM-CERT
3rd Quarter 2019 Cyber Threat Landscape
& Activity Report for Senior Management
Edition: 1.0
Edition date: 01/10/2019
Reference: ThreatLandscapeNCERT-2019/3

# Quarterly cyber threat landscape report

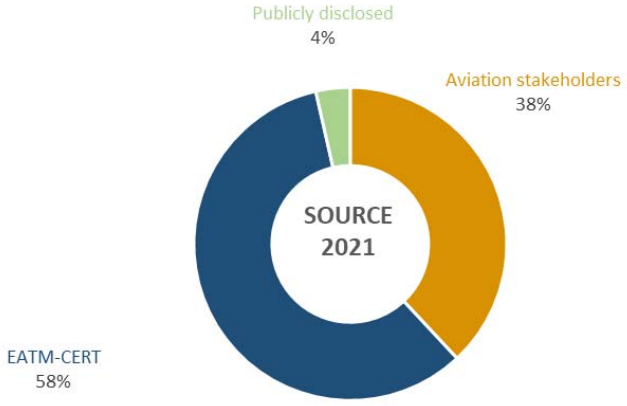


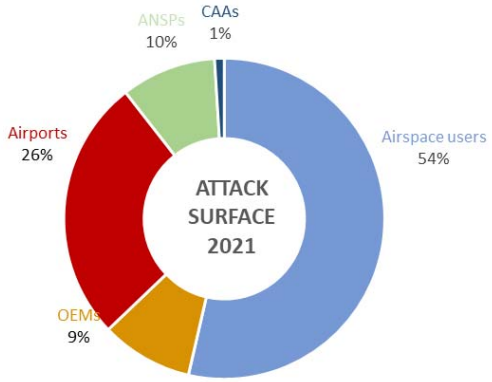

421 organisations

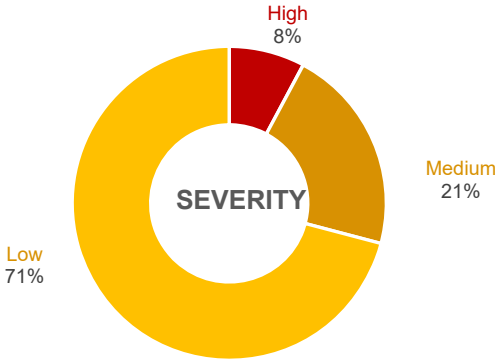
1,223 individuals

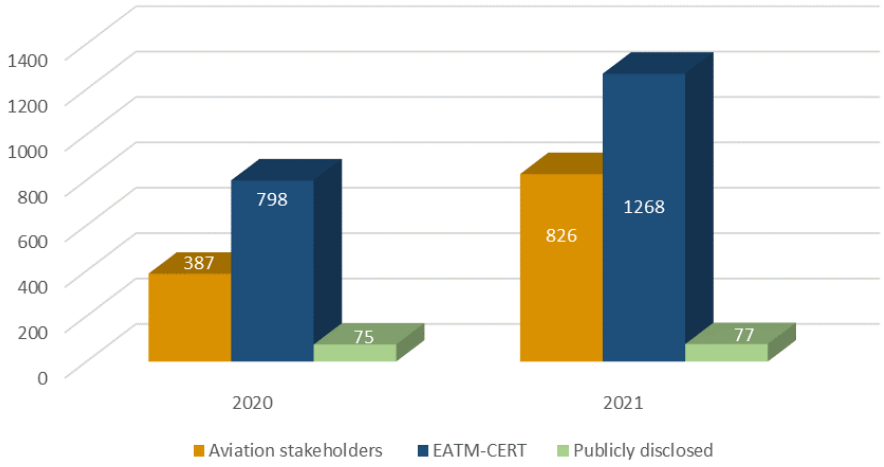


# EATM-CERT 2022 report on cyber in aviation




TLP:GREEN

**Swissport**
@swissportNews

⚠ A part of #Swissport's IT infrastructure was subject to a ransomware attack. The attack has been largely contained, and we are working actively to fully resolve the issue as quickly as possible. Swissport regrets any impact the incidence has had on our service delivery.

# Lockbit ransomware colpisce la compagnia Aerea Hi Fly

Pubblicato il 15 Febbraio 2022
By **Redazione**

## Israeli Defense Company E.M.I.T. Aviation Consulting Targeted by LockBit 2.0 Ransomware

October 4, 2021 CIM Team

E.M.I.T. Aviation Consulting Ltd, an Israeli aerospace and defense company, was targeted by the LockBit 2.0 ransomware gang. Cyber attackers claim to have stolen information from the firm and threaten to release it on the gang's dark web leak site if the firm does not pay a ransom.

E.M.I.T. Aviation Consulting Ltd came into existence in 1986. The firm has designed and assembled complete aircraft, tactical and sub-tactical UAV systems, and portable integrated reconnaissance systems.

According to the threat intelligence firm Cyble, the ransomware gang has stolen databases containing over 6TB of data and is asking a $50M ransom:

## Bangkok Airways hit by LockBit ransomware attack, loses lotsa data after refusing to pay

Partial credit card numbers appear and, worse still, passengers' meal preferences

Tue 31 Aug

Laura Dobberstein

16

Bangkok Airways has revealed it was the victim of a cyberattack from ransomware group LockBit on August 23rd, resulting in the publishing of stolen data.

Bangkok Airways' announcement about the matter came last Thursday, a day after LockBit posted a message on its dark web portal threatening the airline to pay a ransom or suffer a data leak.

The airline was given five days to sort payment, but instead of coughing up it disclosed the breach. LockBit responded by publishing the lot. Competing claims about the resulting data dump rate it at 103GB and over 200GB.

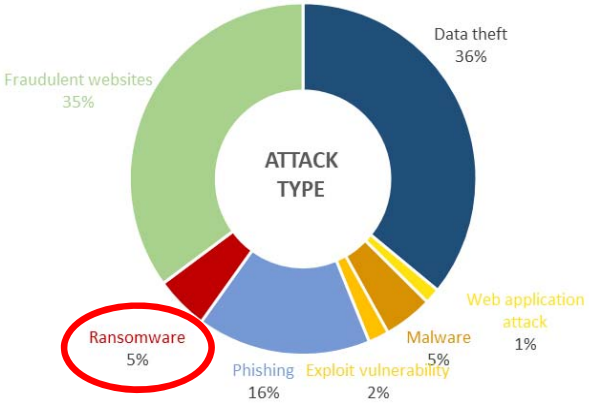
## L'École Nationale de l'Aviation Civile frappée avec le ransomware Hive

**L'ENAC a été frappée, durant le week-end du 12 mars, par une cyberattaque impliquant le ransomware Hive. Ses activités sont fortement perturbées. Une rançon de 1,2 million de dollars est demandée.**

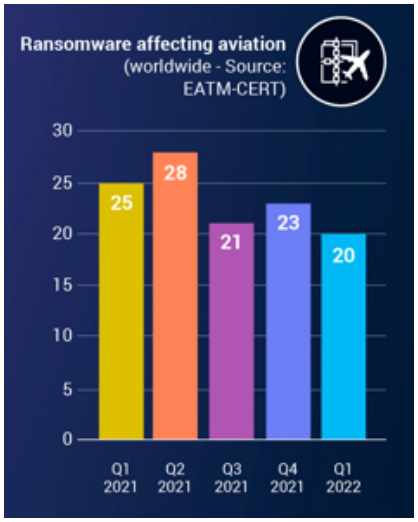
# Ransomware in aviation (global)

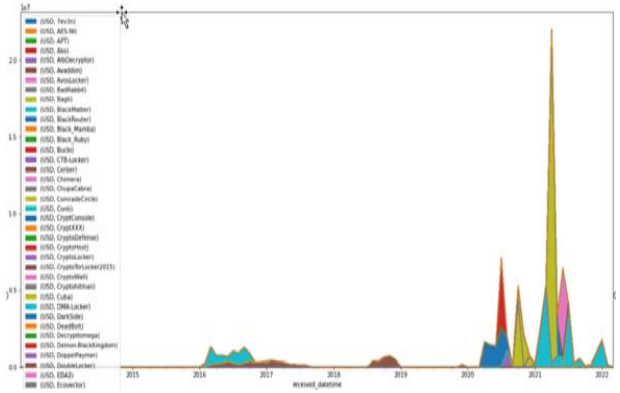
2020
One/week

2021
Two/week




Out of 1.260 events

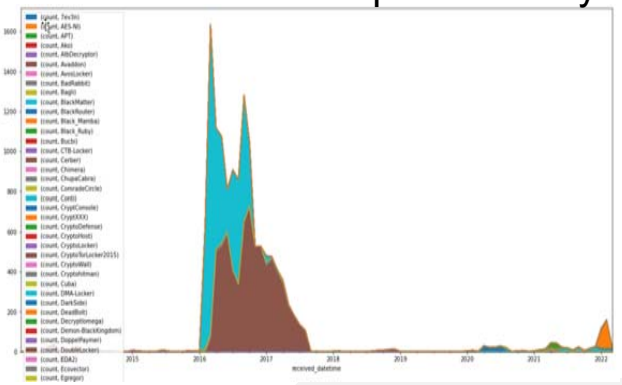


Amount of money earned monthly

All sectors

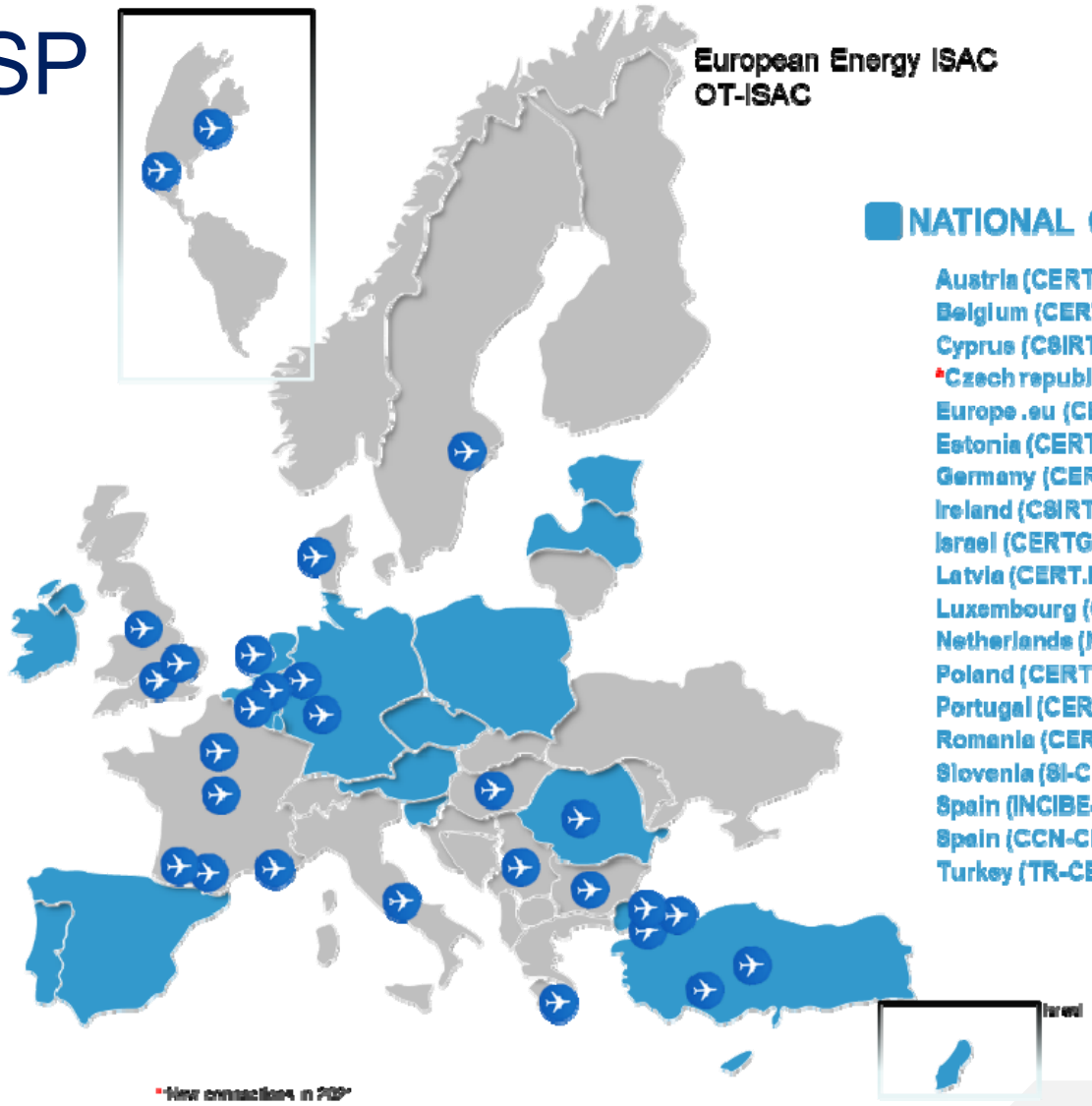
Number of ransoms paid monthly



# MISP

## Aviation Stakeholders

- *Austria – AUSTROCONTROL(ANSP)
- Bulgaria - BULATSA (ANSP)
- Denmark - NAVIAIR (ANSP)
- Europe - ECCSA (test)
- France - CERT-AIRBUS A/C
- France - Groupe ADP
- *France - DGAC
- France - Cert-IST (Thales)
- Germany - DLH-OE –Lufthansa Group
- Germany - Frankfurt Airport
- Greece - HANSP
- Hungary - HungaroControl (ANSP)
- International – EUROCONTROL
- International – EUROCONTROL-NM
- International – EUROCONTROL-MUAC
- *International – OT-ISAC
- International – IATA
- International – AMADEUS
- *Italy - Aeroporto Di Roma
- Mexico - Aero Mexico Airlines
- Netherlands - Schiphol Airport
- Romania - CAA-RO
- *Serbia - SMATSA (ANSP)
- *Sweden - Swedavia (airports)
- Turkey - CERT-THY (Turkish Airlines)
- Turkey - DHMI (ANSP)
- *Turkey - IGA Istanbul Airport
- *Turkey - Celebi Ground ops
- Turkey – SGIA Airport
- UK - British Airways
- UK - Heathrow Airport
- *UK – Manchester Airport Group




*New connections in 202*

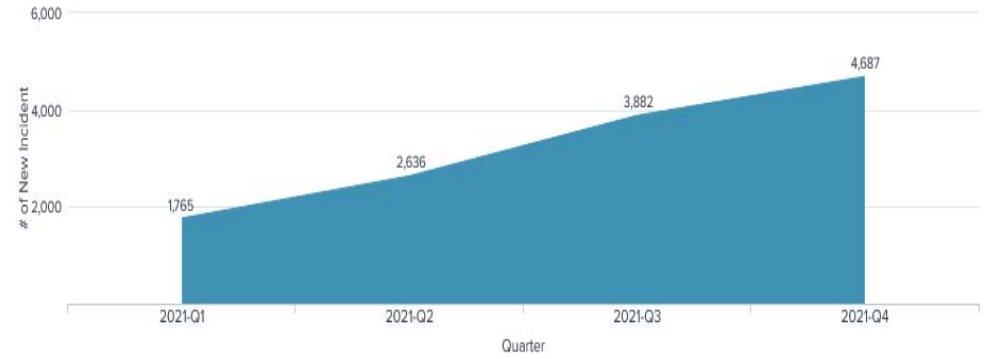
European Energy ISAC
OT-ISAC

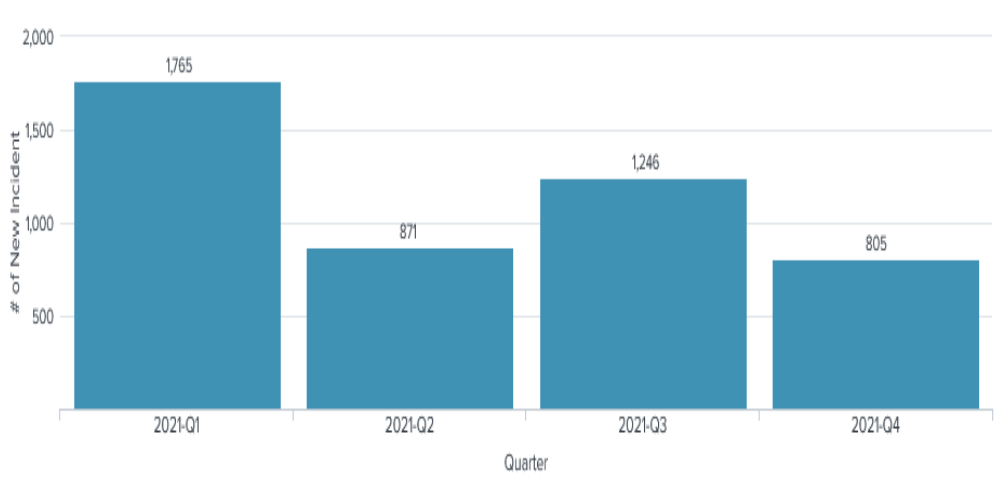
EUROCONTROL

## NATIONAL CERT/NCSC

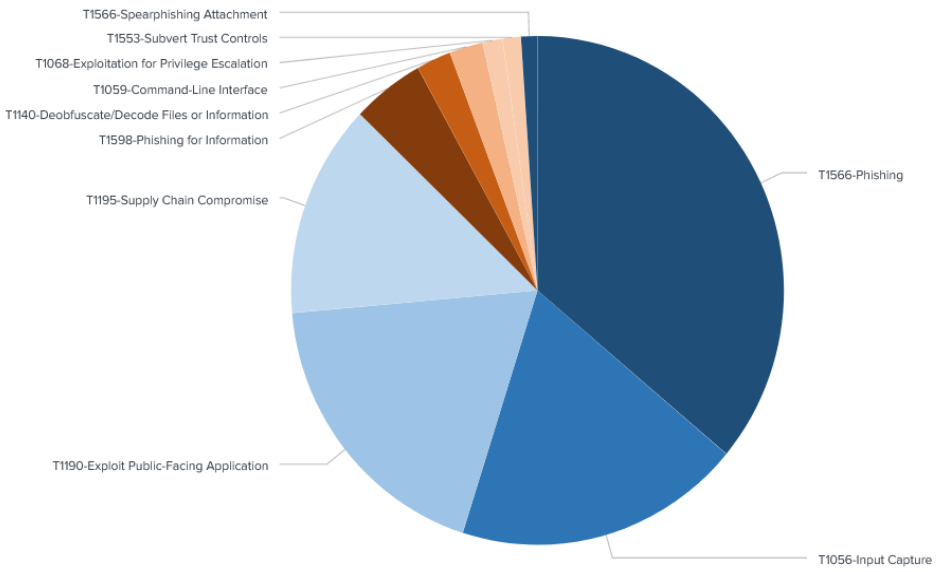
- Austria (CERT.at)
- Belgium (CERT.be)
- Cyprus (CSIRT-CY)
- *Czech republic (CSIRT.cz)
- Europe .eu (CERT-EU)
- Estonia (CERT-EE)
- Germany (CERT-Bund)
- Ireland (CSIRT-IE)
- Israel (CERTGOVIL)
- Latvia (CERT.LV)
- Luxembourg (CIRCL)*
- Netherlands (NCSC-NL)
- Poland (CERT.GOV.PL)
- Portugal (CERT-PT)
- Romania (CERT-RO)
- Slovenia (SI-CERT)
- Spain (INCIBE-CERT)
- Spain (CCN-CERT)
- Turkey (TR-CERT)

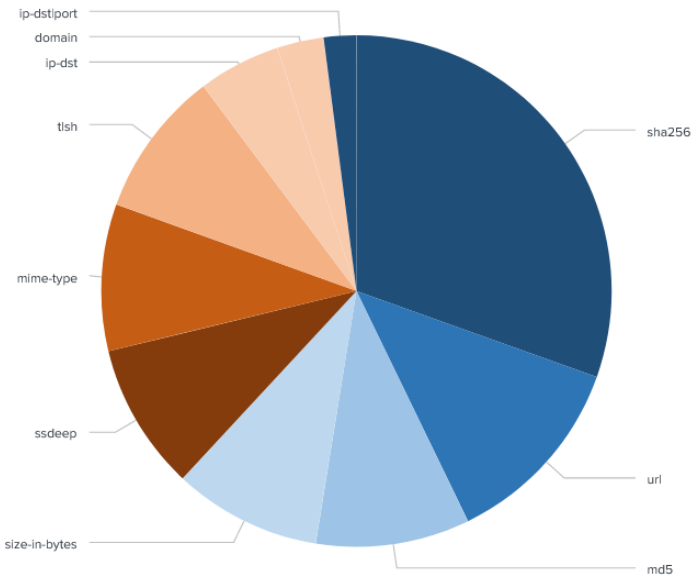
# Data on MISP (all sectors)



# Data on MISP (all sectors)




Top10 MITRE ATT&CK techniques on MISP

# MISP - Integration


SIEM

splunk>

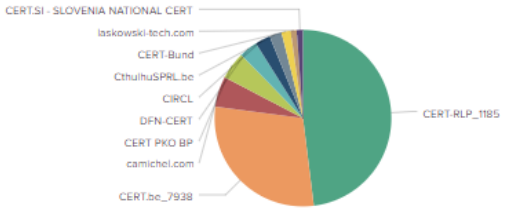
MISP
Threat Sharing

FIREWALL

MISP High Level Alerts

| event_info | count | percent |
|---|---|---|
| Daily Emotet IoCs and Notes for 01/13/20 | 4104 | 45.978042 |
| Daily Emotet IoCs and Notes for 12/30/19 | 1634 | 18.306072 |
| Daily Emotet IoCs and Notes for 01/06/20 | 1620 | 18.149227 |
| What the continued escalation of tensions in the Middle East means for security | 630 | 7.058033 |
| [PT ESC] TA505 | 297 | 3.327358 |
| THALLIUM/Kimsuky_Infrastructure | 116 | 1.299574 |
| IPs from APT34 Leaked Tools and Expanded Infrastructure monitoring page from RiskIQ | 108 | 1.209948 |
| OSINT 20191231B: Microsoft Thallium Sinkhole Domain Siblings by ThreatConnect | 104 | 1.165136 |
| OSINT - More than a Dozen Obfuscated APT33 Botnets Used for Extreme Narrow Targeting | 54 | 0.604974 |
| Dustman samples | 48 | 0.537755 |

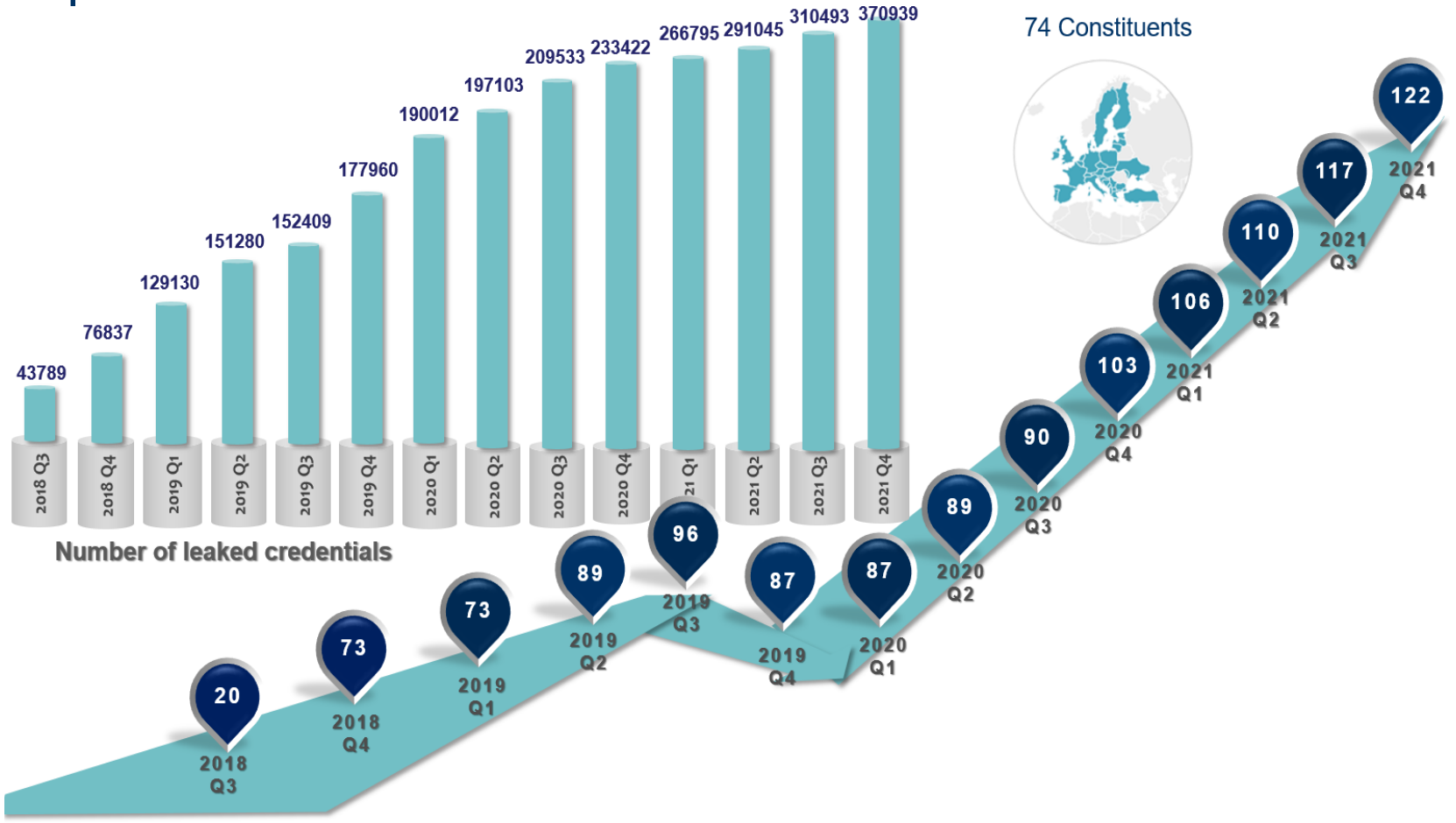
Last 30 days MISP CERT Activity




MISP Events Trend - YESTERDAY

658 -53

# Compromised accounts



# Scams impersonating EUROCONTROL Staff

From: Veronique Martou] mailto:vmartou.eurocontrolcrco.int@gmail.com [
Sent: Tuesday, January 30, 2018 9:08 AM
To: XXXX
Subject: RE: Payment Query/Eurocontrol Charges

Dear Sirs,
we have sent a couple of emails to your accounts payable team without receiving any responses. please kindly avail us with the status of the invoices sent to you for the months of September to December 2017, to enable us reconcile our accounts and update your records in preparation of the upcoming audit of accounts. we regret all inconveniences and plead that you bear with us.note also that EUROCONTROL will not hesitate to take a strict enforcement measures and possible detention of your aircraft will be the inevitable consequence if you delay further to comply with this demands.

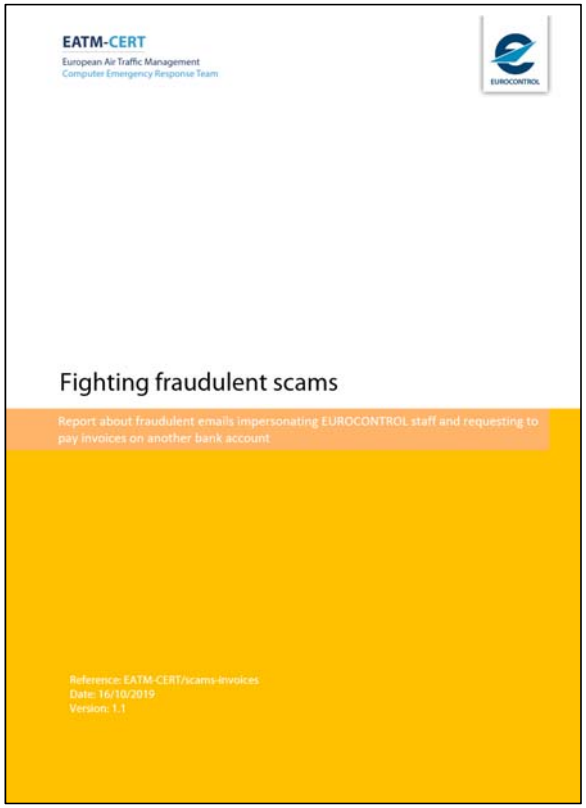
NB;PLEASE KINDLY FORWARD A COPY OF YOUR RESPONSES TO TO OUR ACCOUNTS TEAM AT r3.crco@euro-control.net FOR PROMPT ACTIONS.

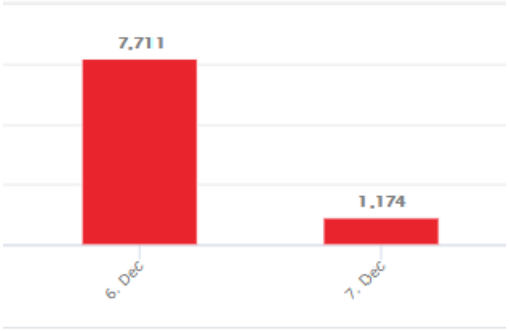
thanks for your cooperation and understanding.

we await your prompt response.

my best regards

Veronique Martou
Finance and Revenue Manager
Collection of Charges
CRCO/R4 EUROCONTROL
96Rue de la Fusee 1130
Brussels.
Email:r3.crco@euro-control.net






```
Subject: Unpaid Invoices
To: me <r3.crco@eurocontrol.int>
From: r3.crco <r3.crco@eurocontrol.int>
Date: Sun, 06 Dec 2020 20:49:05 -0800
Reply-To: r3.crco <r3.crcoeurocontrol.ints@gmail.com>

You will not see this in a MIME-aware mail reader.
--===============0666264462==
Content-Type: text/plain; charset="iso-8859-1"
MIME-Version: 1.0
Content-Transfer-Encoding: quoted-printable
Content-Description: Mail message body

Dear Accounts Team,     Would you please let us know the status of your Oct=
ober November and December invoices. On review of your files,  We discovere=
d that these invoices are still in arrears.    Kindly please confirm the st=
atus of these invoices below.    501018200123 501028991020 501900189028    =
 Please let us know if payment has been paid or not. Provide the copy of th=
e proof of payment with Invoice number and amount.   So as to enable us rec=
oncile and update your account accordingly.   In order to make sure that th=
e bills you receive are authentic, please consult and download them from th=
e CRCO Extranet For Airspace users (CEFA): https://www.eurocontrol.int/tool=
/cefa Kindly send us a copy stamped by return mail from now on.   We have s=
ent out new invoices for your reference kindly notify us by return mail whe=
n you receive it.     Thanks once again for your understanding and cooperat=
ion.   Kind Regards, Nancy Coveliers Collection of Charges CECO/R4 EUROCONT=
ROL  96 Rue de la Fusee 1130 Brussels Email: r3.crco@eurocontrol.int Teleph=
one: +32 460 222 485
--===============0666264462==
```

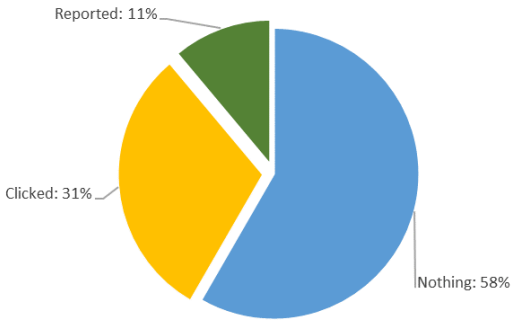
| | Server Name | | From: domain count | Message count | IP count |
|---|---|---|---|---|---|
| ▾ | *.ozbirtr.com | Identify as Legitimate | 1 | 9,021 | 1 |

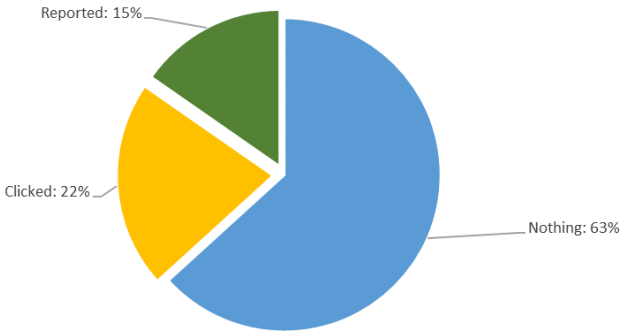
| From: Domain | IP | PTR | Country | Messages | Policy Applied | Override Reason | DKIM DMARC | DKIM Raw | DKIM d= | DKIM Selectors | SPF DMARC | SPF Raw | SPF Domain |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| eurocontrol.int | 185.104.112.181 | server.ozbirtr.com | | 8711 | Reject | none | fail | none | none | | fail | fail | eurocontrol.int |

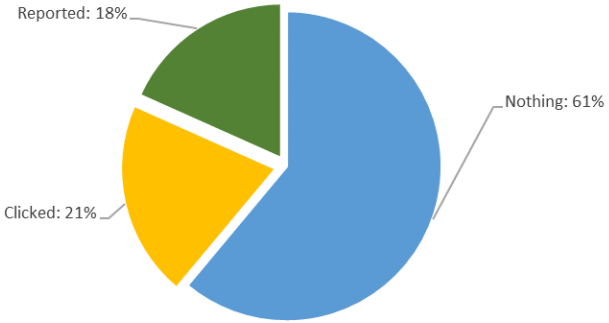
Reported scams using this email @ r3.crcoeurocontrol.ints@gmail.com : 5

# Phishing awareness campaigns

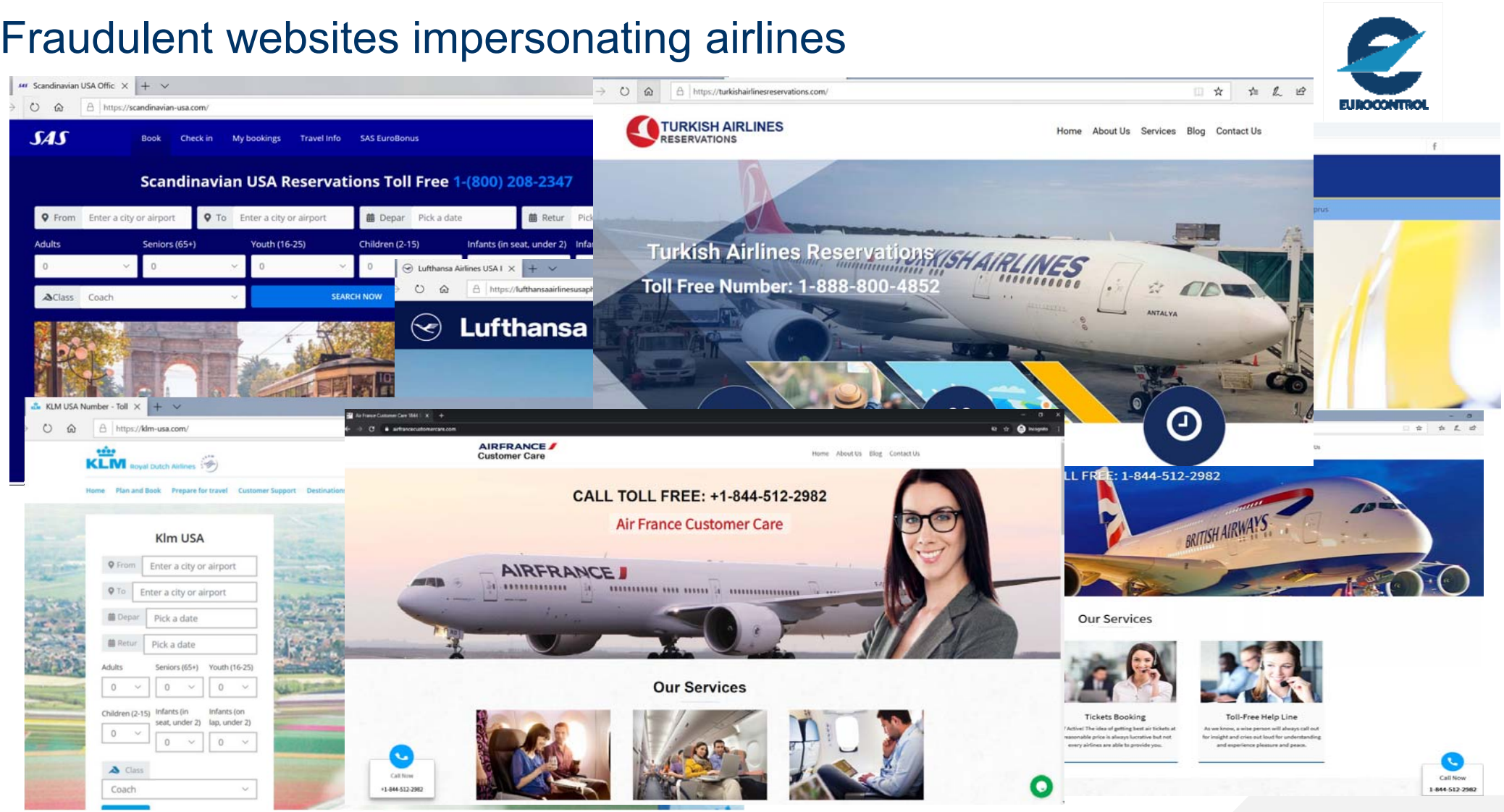
- Tested within EUROCONTROL (2 campaigns)
- Available for your own use by Q2/2021



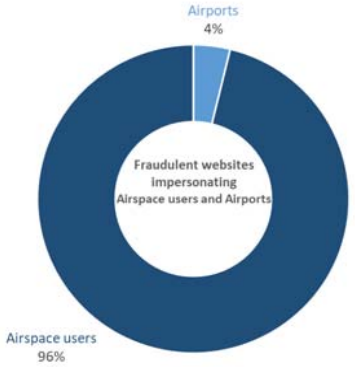



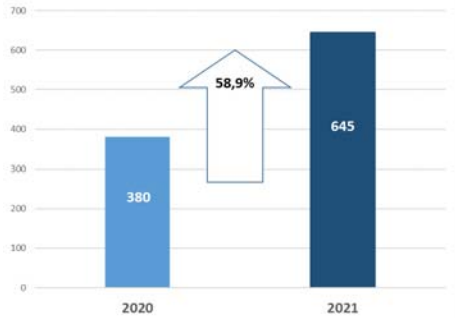



# Fraudulent websites impersonating airlines



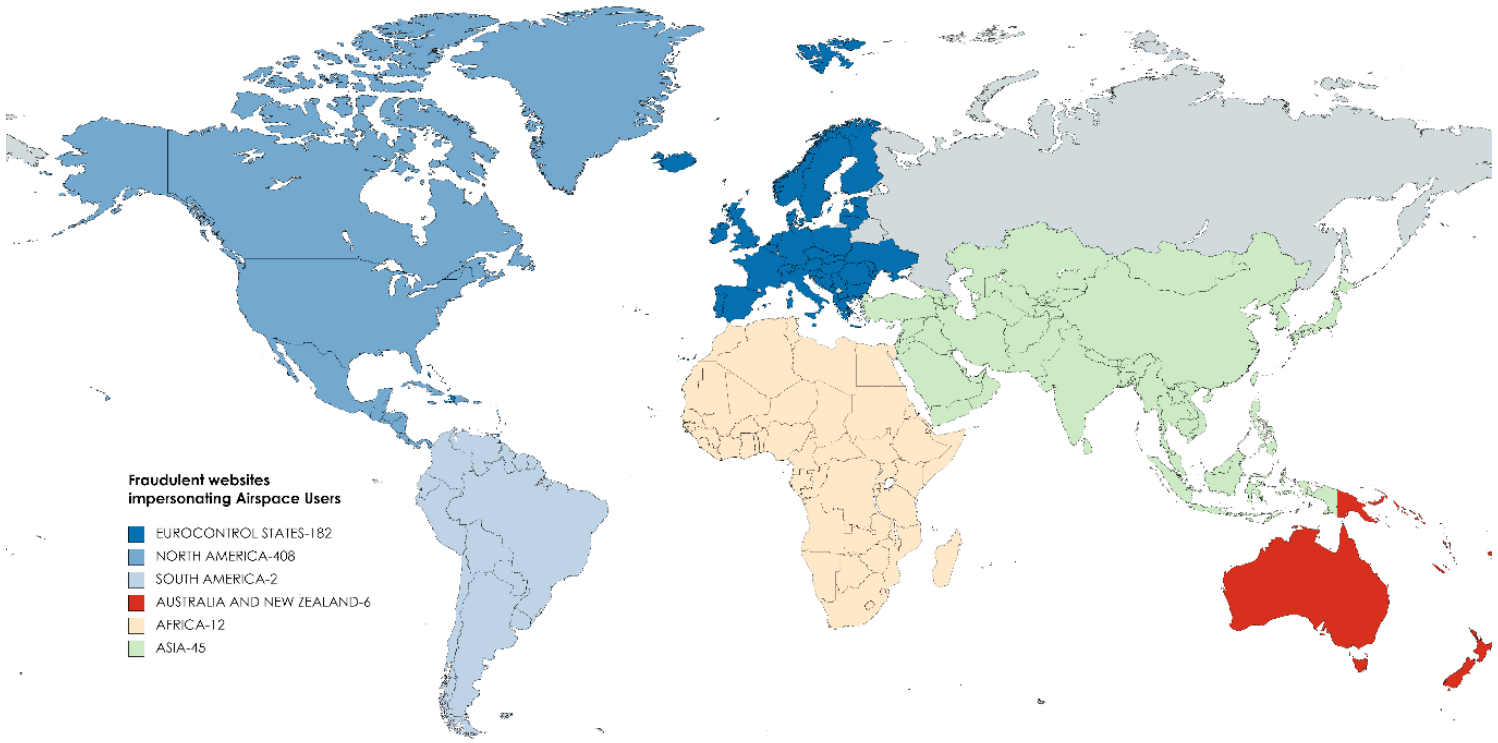
# Fraudulent websites impersonating airlines



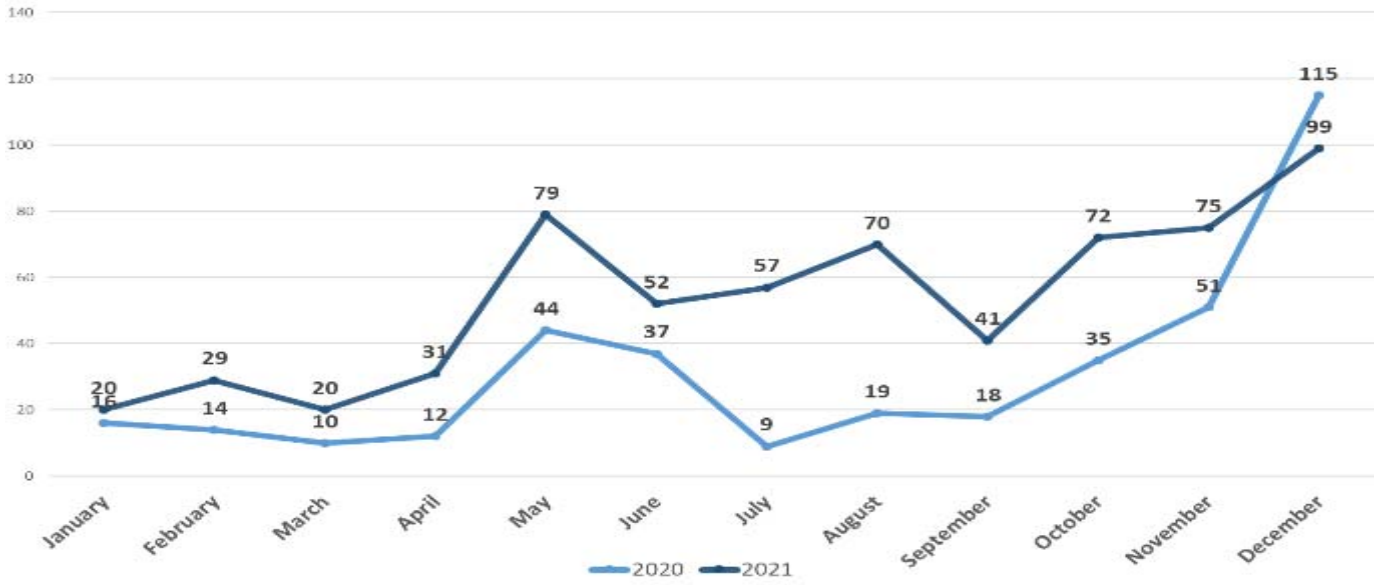

Annual number of fraudulent websites impersonating Airspace Users and Airports as detected by EATM-CERT

# Fraudulent websites impersonating airlines

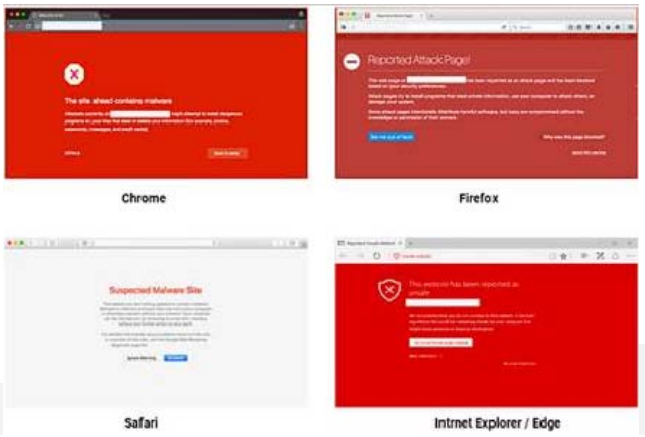



Monthly number of fraudulent websites impersonating Airspace Users, members of IATA or A4E, as detected by EATM-CERT

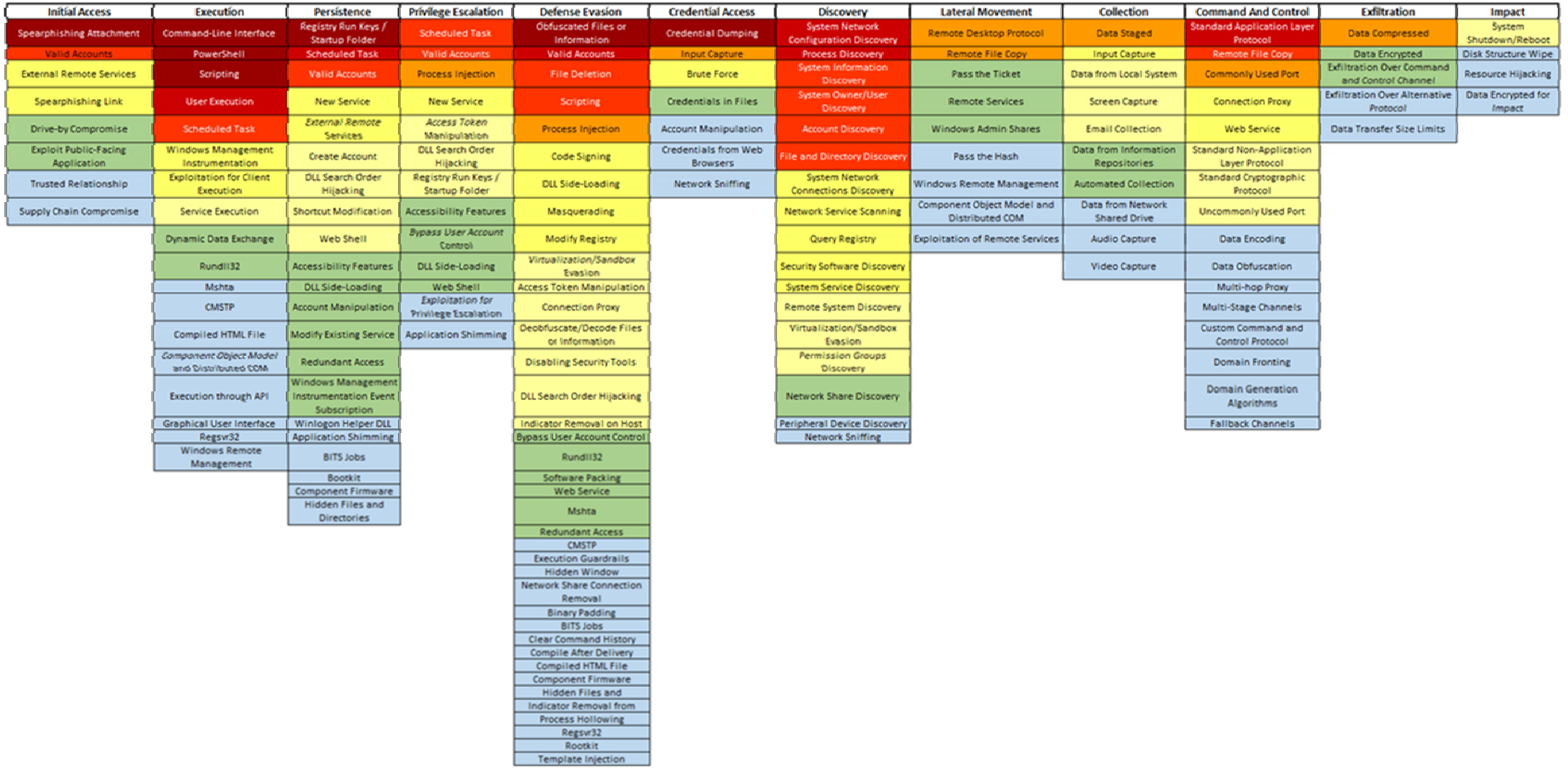
# Fraudulent websites impersonating airlines



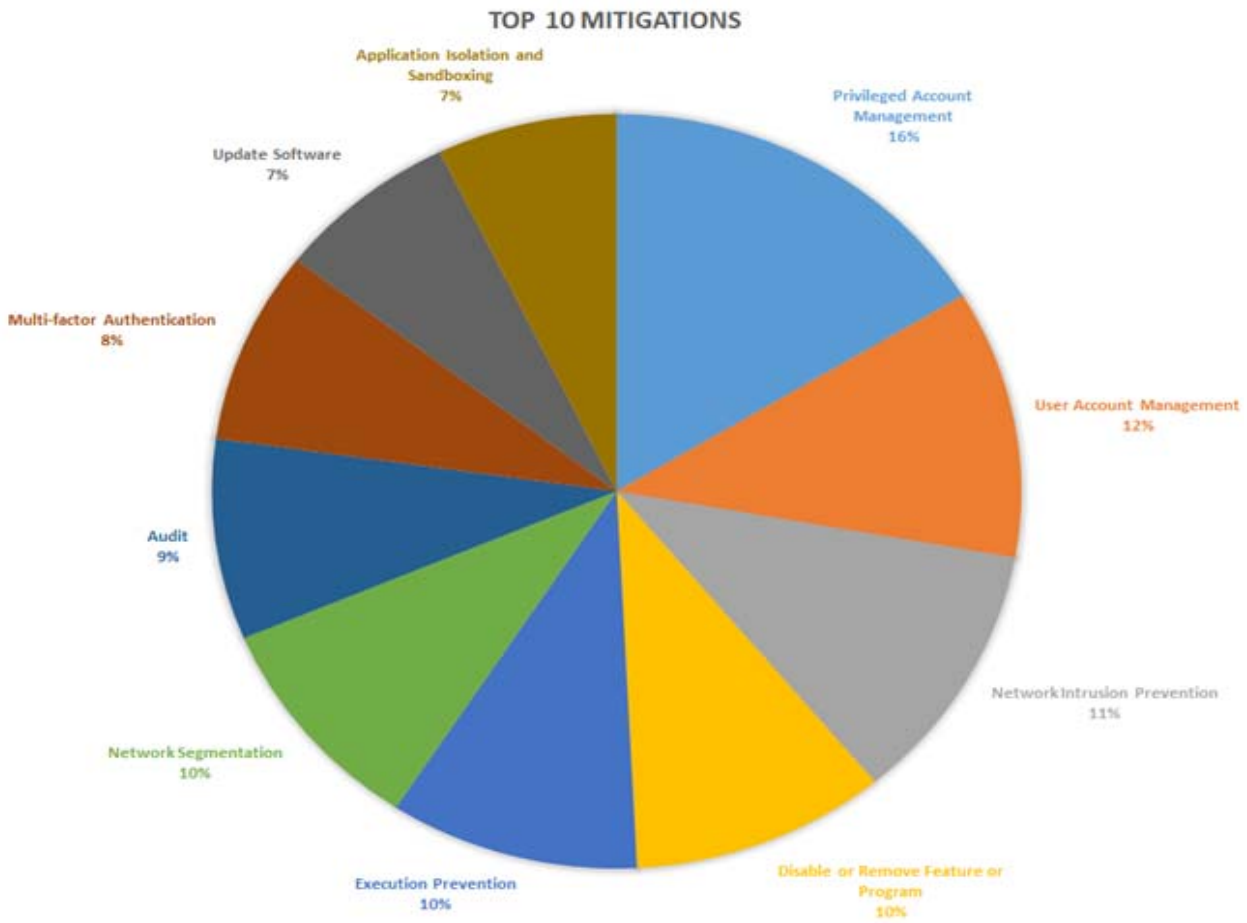

Yearly financial impact : ~1Bn$ (IATA)



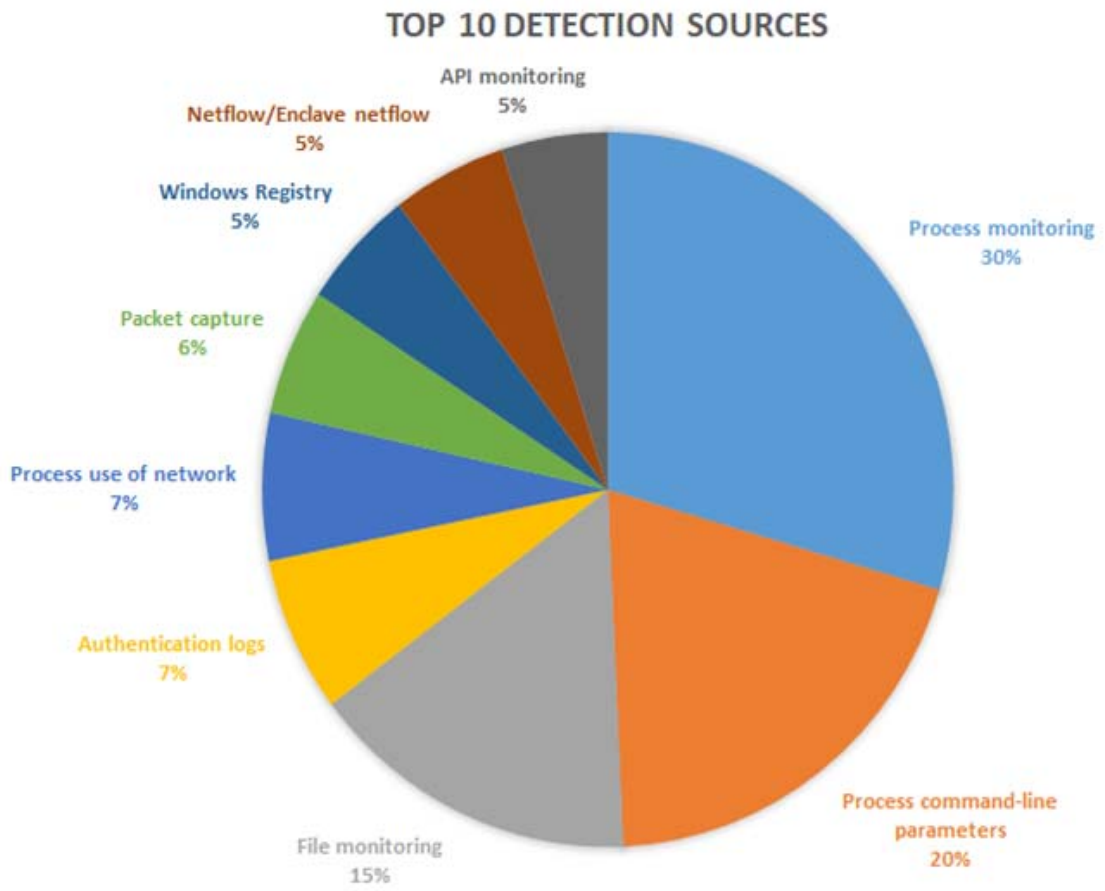
# MITRE ATT&CK : Techniques most commonly used to attack aviation



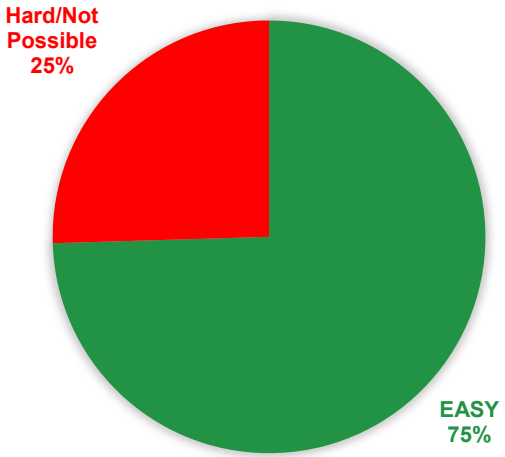
# Top 10 Mitigation Means



# Top Detection Means



## MITIGATION POSSIBILITY




| Tactic | Technique |
|---|---|
| Persistence | Registry Run Keys / Startup Folder |
| Discovery | System Network Configuration Discovery |
| Discovery | Process Discovery |
| Defense Evasion | File Deletion |
| Discovery | System Information Discovery |
| Discovery | System Owner/User Discovery |
| Discovery | File and Directory Discovery |
| Collection | Data Staged |
| Credential Access | Input Capture |
| Defense Evasion | Code Signing |
| Discovery | System Network Connections Discovery |
| Collection | Input Capture |
| Discovery | Query Registry |
| Discovery | Security Software Discovery |
| Discovery | System Service Discovery |
| Collection | Data from Local System |
| Discovery | Remote System Discovery |
| Collection | Screen Capture |
| Defense Evasion | Virtualization/Sandbox Evasion |
| Defense Evasion | Deobfuscate/Decode Files or Information |
| Discovery | Permission Groups Discovery |
| Discovery | Network Share Discovery |
| Exfiltration | Data Encrypted |
| Collection | Data from Network Shared Drive |
| Defense Evasion | Network Share Connection Removal |
| Discovery | Peripheral Device Discovery |
| Impact | System Shutdown/Reboot |
| Collection | Audio Capture |
| Defense Evasion | Binary Padding |
| Defense Evasion | Compile After Delivery |
| Persistence | Component Firmware |
| Execution | Graphical User Interface |
| Persistence | Hidden Files and Directories |
| Defense Evasion | Indicator Removal from Tools |
| Defense Evasion | Process Hollowing |
| Impact | Resource Hijacking |
| Defense Evasion | Rootkit |
| Collection | Video Capture |

- For APTs targeting aviation, only 75% of techniques have Mitigations Means
- 25% of the techniques are very hard/impossible to mitigate
- Detection is vital