CYBER SECURITY AND RESILIENCE SYMPOSIUM

TOWARDS A RESILIENT AVIATION CYBERSPACE

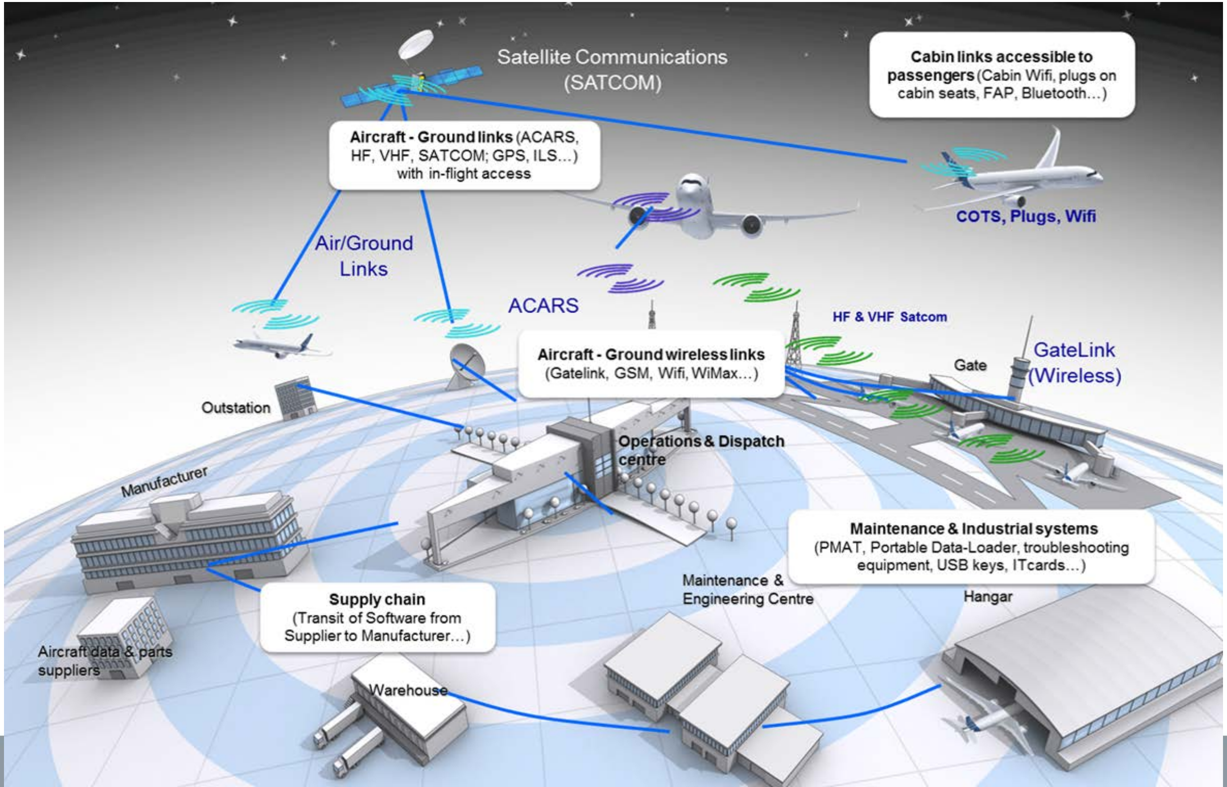
AMMAN, JORDAN | 15-17 OCTOBER 2019

EUROCONTROL’s view on cyber risk, threats and challenges in ATM

Patrick MANA

EATM-CERT Manager

Complexity of Securing the Aviation Ecosystem



Satellite Communications (SATCOM)

Cabin links accessible to passengers (Cabin Wifi, plugs on cabin seats, FAP, Bluetooth…)

Aircraft - Ground links (ACARS, HF, VHF, SATCOM; GPS, ILS…) with in-flight access

COTS, Plugs, Wifi

Air/Ground Links

ACARS

HF & VHF Satcom

Aircraft - Ground wireless links (Gatelink, GSM, Wifi, WiMax…)

Gate

GateLink (Wireless)

Outstation

Operations & Dispatch centre

Manufacturer

Maintenance & Industrial systems (PMAT, Portable Data-Loader, troubleshooting equipment, USB keys, ITcards…)

Maintenance & Engineering Centre

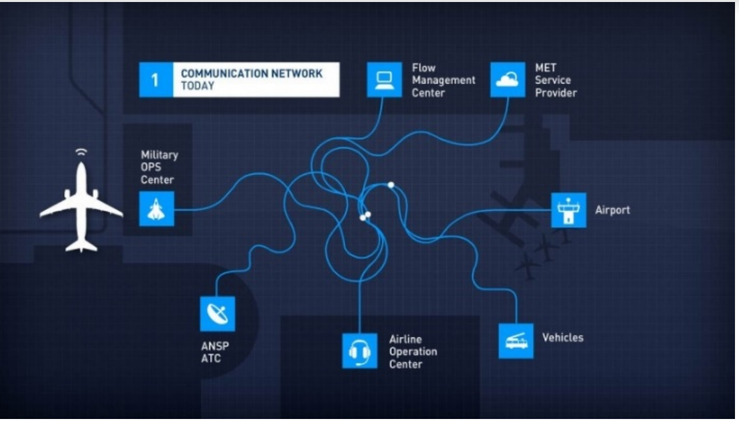
Hangar

Supply chain (Transit of Software from Supplier to Manufacturer…)

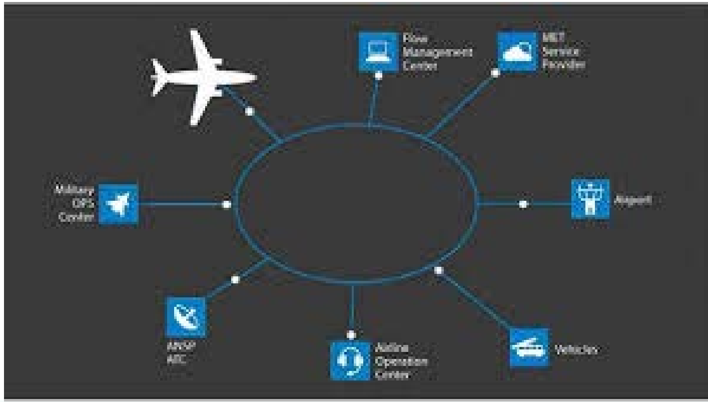
Aircraft data & parts suppliers

Warehouse

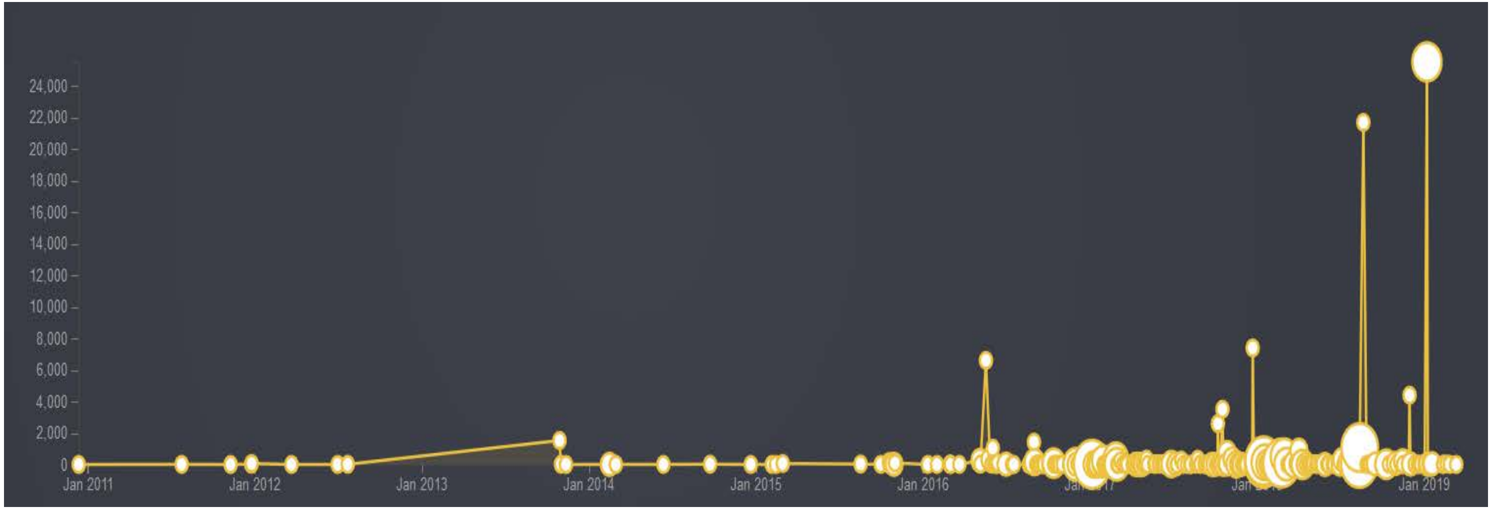
Evolution of ATM – towards digitalization



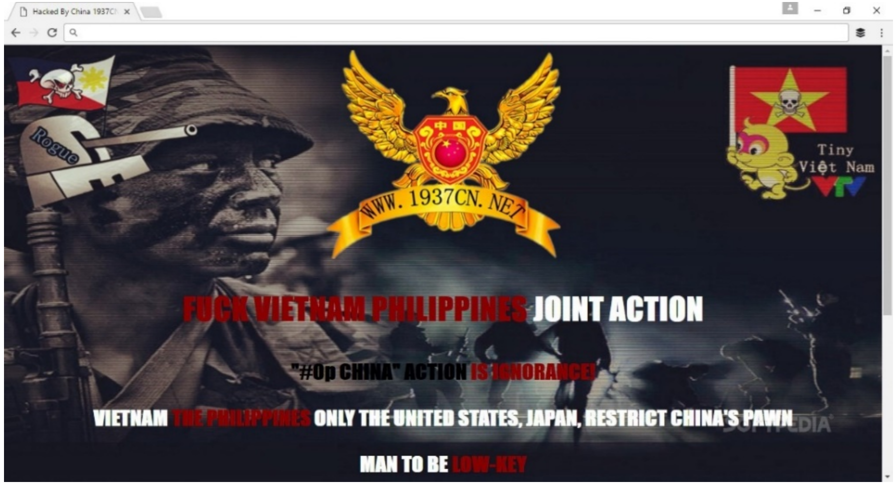
=>



Cyber threat/risk dynamic



State-sponsored / Geo-political



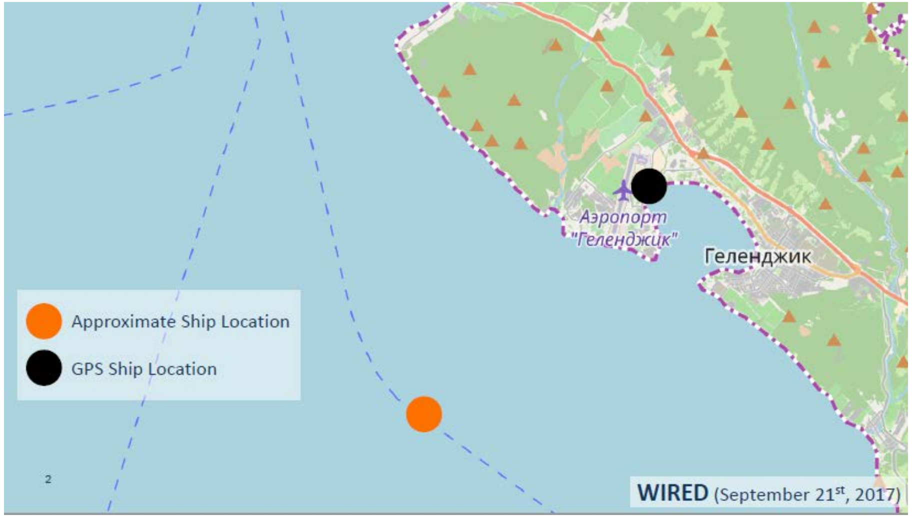
FUCK VIETNAM PHILIPPINES JOINT ACTION

"#Op CHINA" ACTION IS IGNORANCE!

VIETNAM THE PHILIPPINES ONLY THE UNITED STATES, JAPAN, RESTRICT CHINA'S PAWN

MAN TO BE LOW-KEY

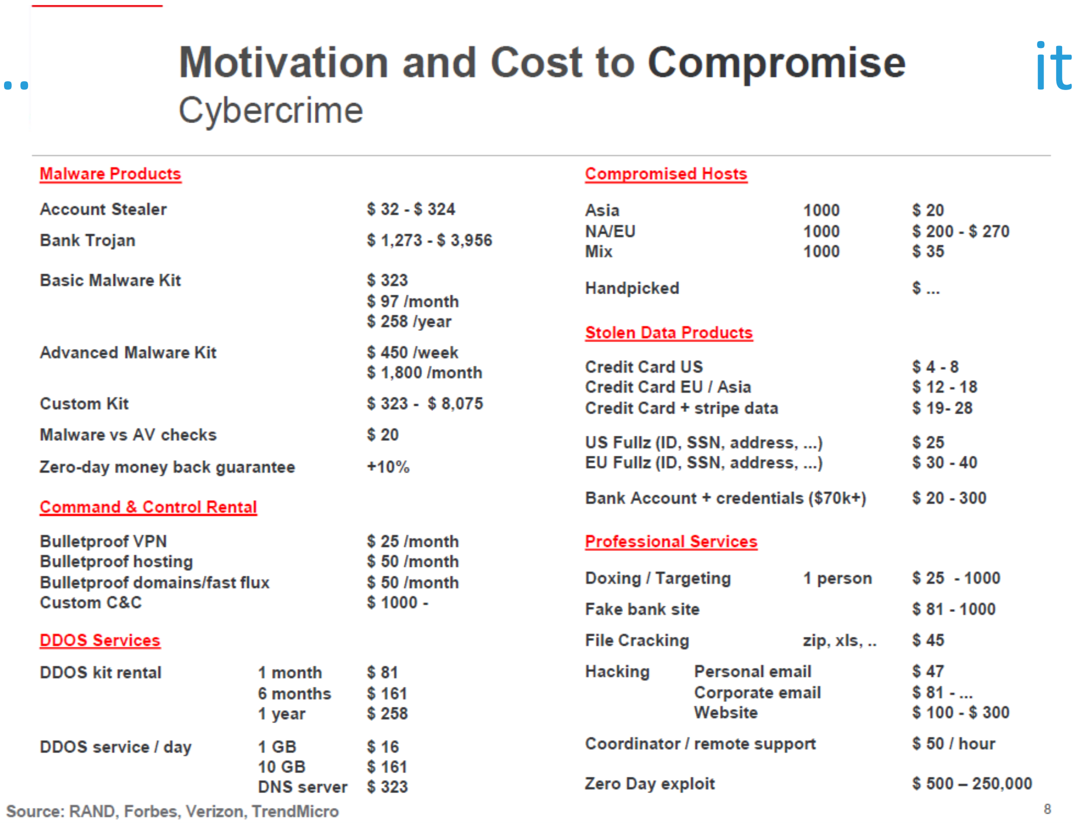
Non aviation specific



WIRED (September 21st, 2017)

VEHICLE MINI GPS JAMMER
PLUGS INTO LIGHTER SOCKET AND BEGINS WORKING INSTANTLY
THE GPS SIGNAL BLOCKER FROM

Cyber-crime … it’s an industry



Motivation and Cost to Compromise
Cybercrime

Malware Products

Account Stealer	$ 32 - $ 324
Bank Trojan	$ 1,273 - $ 3,956
Basic Malware Kit	$ 323 $ 97 /month $ 258 /year
Advanced Malware Kit	$ 450 /week $ 1,800 /month
Custom Kit	$ 323 - $ 8,075
Malware vs AV checks	$ 20
Zero-day money back guarantee	+10%

Command & Control Rental

Bulletproof VPN	$ 25 /month
Bulletproof hosting	$ 50 /month
Bulletproof domains/fast flux	$ 50 /month
Custom C&C	$ 1000 -

DDOS Services

DDOS kit rental	1 month	$ 81
	6 months	$ 161
	1 year	$ 258
DDOS service / day	1 GB	$ 16
	10 GB	$ 161
	DNS server	$ 323

Compromised Hosts

Asia	1000	$ 20
NA/EU	1000	$ 200 - $ 270
Mix	1000	$ 35
Handpicked		$ ...

Stolen Data Products

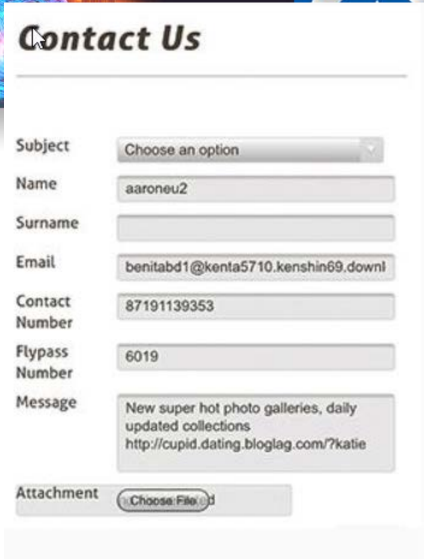
Credit Card US	$ 4 - 8
Credit Card EU / Asia	$ 12 - 18
Credit Card + stripe data	$ 19- 28
US Fullz (ID, SSN, address, ...)	$ 25
EU Fullz (ID, SSN, address, ...)	$ 30 - 40
Bank Account + credentials ($70k+)	$ 20 - 300

Professional Services

Doxing / Targeting	1 person	$ 25 - 1000
Fake bank site		$ 81 - 1000
File Cracking	zip, xls, ..	$ 45
Hacking	Personal email	$ 47
	Corporate email	$ 81 - ...
	Website	$ 100 - $ 300
Coordinator / remote support		$ 50 / hour
Zero Day exploit		$ 500 – 250,000

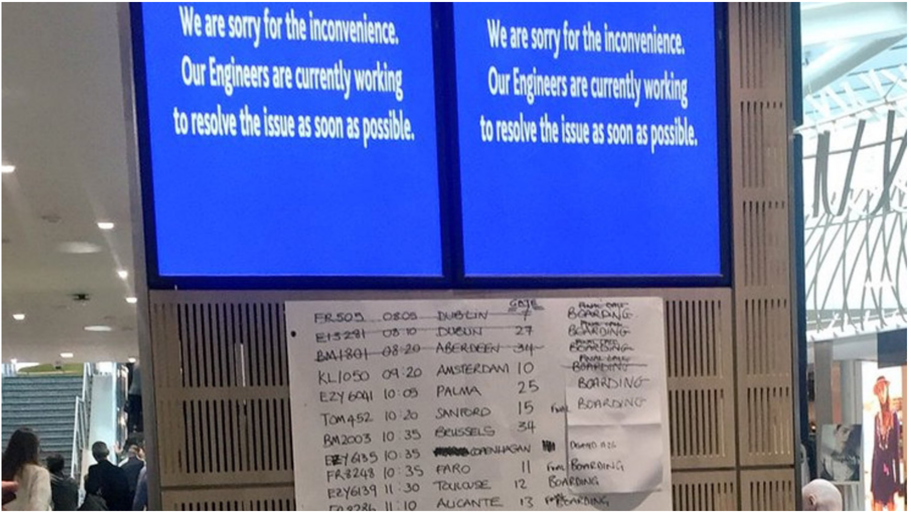
Source: RAND, Forbes, Verizon, TrendMicro

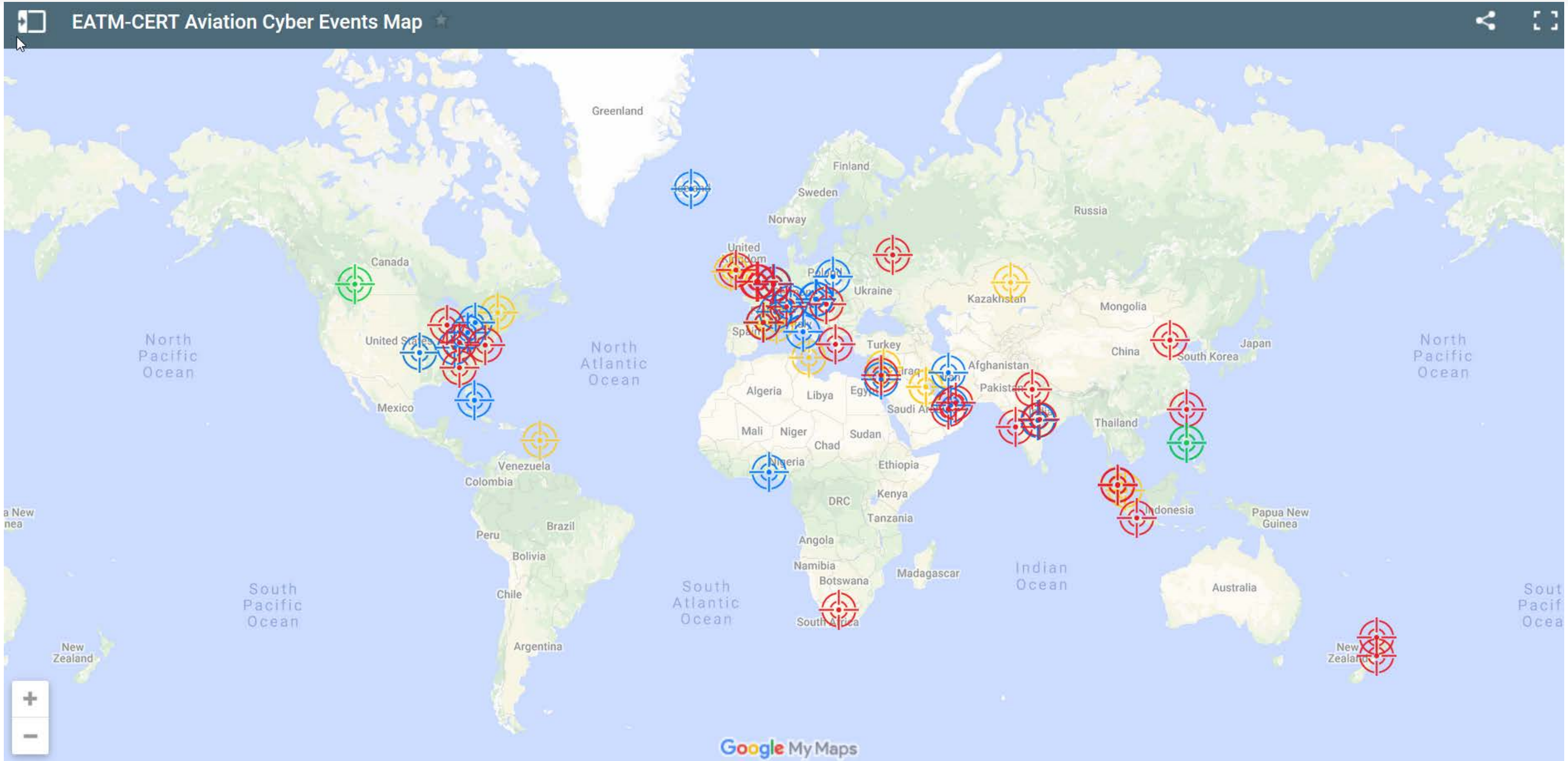
Cyber-crime e.g. ransomware



Contact Us

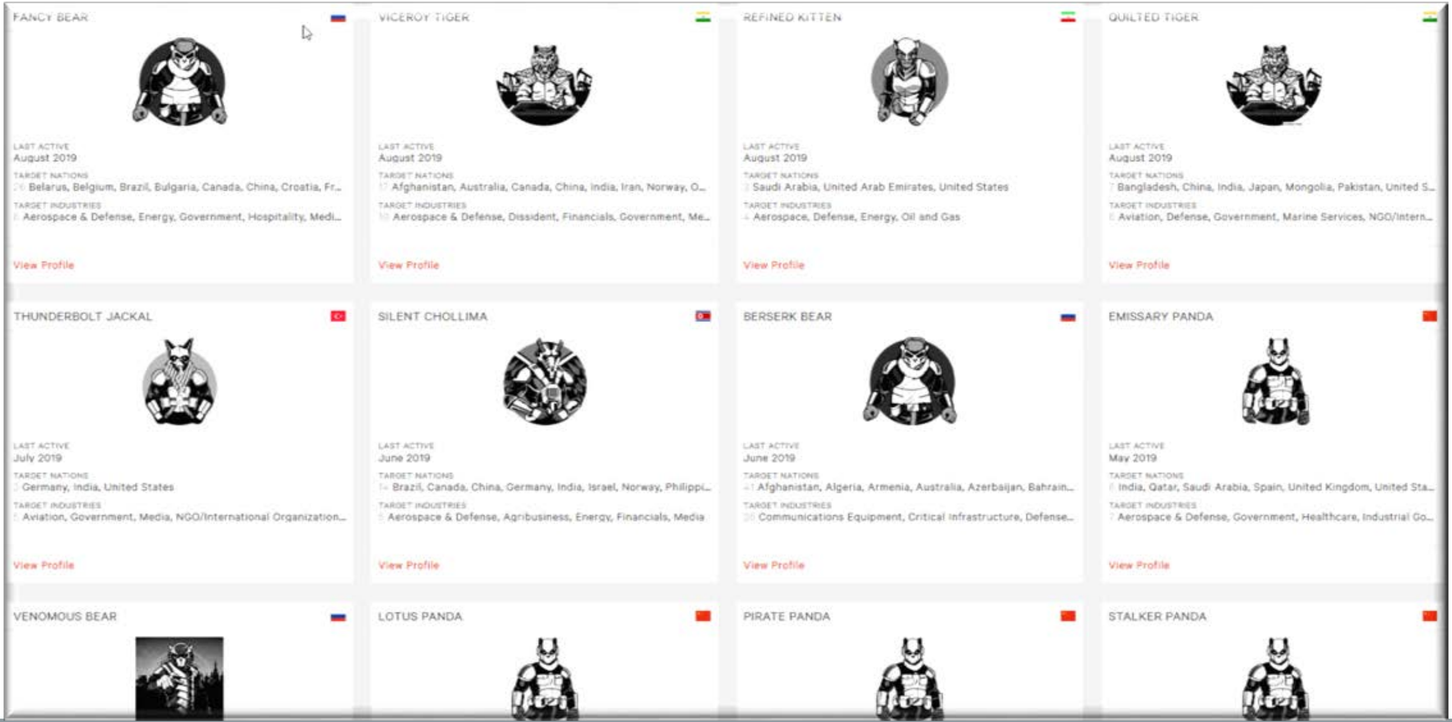
Subject	Choose an option
Name	aaroneu2
Surname	
Email	benitabd1@kenta5710.kenshin69.downl
Contact Number	87191139353
Flypass Number	6019
Message	New super hot photo galleries, daily updated collections http://cupid.dating.bloglag.com/?katie
Attachment	Choose File


We are sorry for the inconvenience.
Our Engineers are currently working
to resolve the issue as soon as possible.
We are sorry for the inconvenience.
Our Engineers are currently working
to resolve the issue as soon as possible.
GATE
~~FR505 0805 DUBLIN 7~~ FINAL CALL BOARDING
~~EI3281 08 10 DUBLIN~~ 27 FINAL CALL BOARDING
~~BM1801 08 20 ABERDEEN 34~~ FINAL CALL BOARDING
KL1050 09 20 AMSTERDAM 10 FINAL CALL ~~BOARDING~~ BOARDING
EZY6041 10:05 PALMA 25 BOARDING
TOM452 10 20 SANFORD 15 FINAL BOARDING
BM2003 10 35 BRUSSELS 34
EZY6135 10:35 COPENHAGAN DELAYED 11:26
FR8248 10:35 FARO 11 FINAL BOARDING
EZY6139 11:30 TOULOUSE 12 BOARDING
FR8286 11:10 ALICANTE 13 FINAL BOARDING



EATM-CERT Aviation Cyber Events Map

Hackers groups (APTs) … some !



FANCY BEAR

LAST ACTIVE
August 2019
TARGET NATIONS
26 Belarus, Belgium, Brazil, Bulgaria, Canada, China, Croatia, Fr…
TARGET INDUSTRIES
8 Aerospace & Defense, Energy, Government, Hospitality, Medi…

View Profile

VICEROY TIGER

LAST ACTIVE
August 2019
TARGET NATIONS
17 Afghanistan, Australia, Canada, China, India, Iran, Norway, O…
TARGET INDUSTRIES
10 Aerospace & Defense, Dissident, Financials, Government, Me…

View Profile

REFINED KITTEN

LAST ACTIVE
August 2019
TARGET NATIONS
3 Saudi Arabia, United Arab Emirates, United States
TARGET INDUSTRIES
4 Aerospace, Defense, Energy, Oil and Gas

View Profile

QUILTED TIGER

LAST ACTIVE
August 2019
TARGET NATIONS
7 Bangladesh, China, India, Japan, Mongolia, Pakistan, United S…
TARGET INDUSTRIES
6 Aviation, Defense, Government, Marine Services, NGO/Intern…

View Profile

THUNDERBOLT JACKAL

LAST ACTIVE
July 2019
TARGET NATIONS
3 Germany, India, United States
TARGET INDUSTRIES
5 Aviation, Government, Media, NGO/International Organization…

View Profile

SILENT CHOLLIMA

LAST ACTIVE
June 2019
TARGET NATIONS
14 Brazil, Canada, China, Germany, India, Israel, Norway, Philippi…
TARGET INDUSTRIES
5 Aerospace & Defense, Agribusiness, Energy, Financials, Media

View Profile

BERSERK BEAR

LAST ACTIVE
June 2019
TARGET NATIONS
41 Afghanistan, Algeria, Armenia, Australia, Azerbaijan, Bahrain…
TARGET INDUSTRIES
20 Communications Equipment, Critical Infrastructure, Defense…

View Profile

EMISSARY PANDA

LAST ACTIVE
May 2019
TARGET NATIONS
6 India, Qatar, Saudi Arabia, Spain, United Kingdom, United Sta…
TARGET INDUSTRIES
7 Aerospace & Defense, Government, Healthcare, Industrial Go…

View Profile

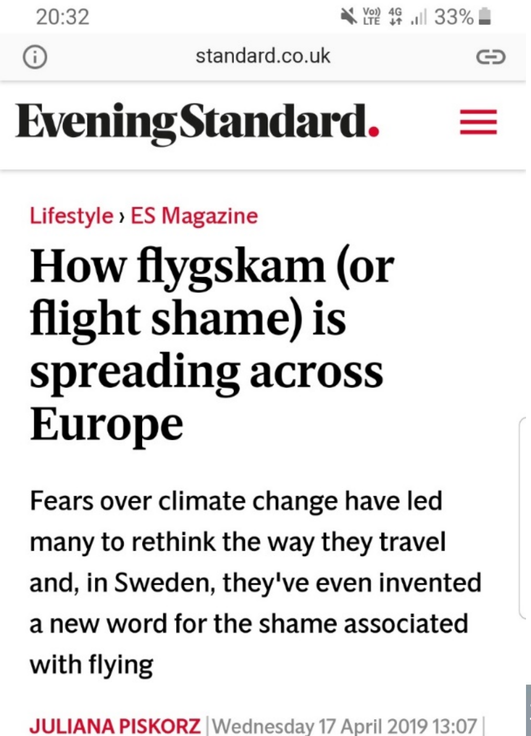
VENOMOUS BEAR

LOTUS PANDA

PIRATE PANDA

STALKER PANDA

Hacktivism more and more e.g. environmentalists



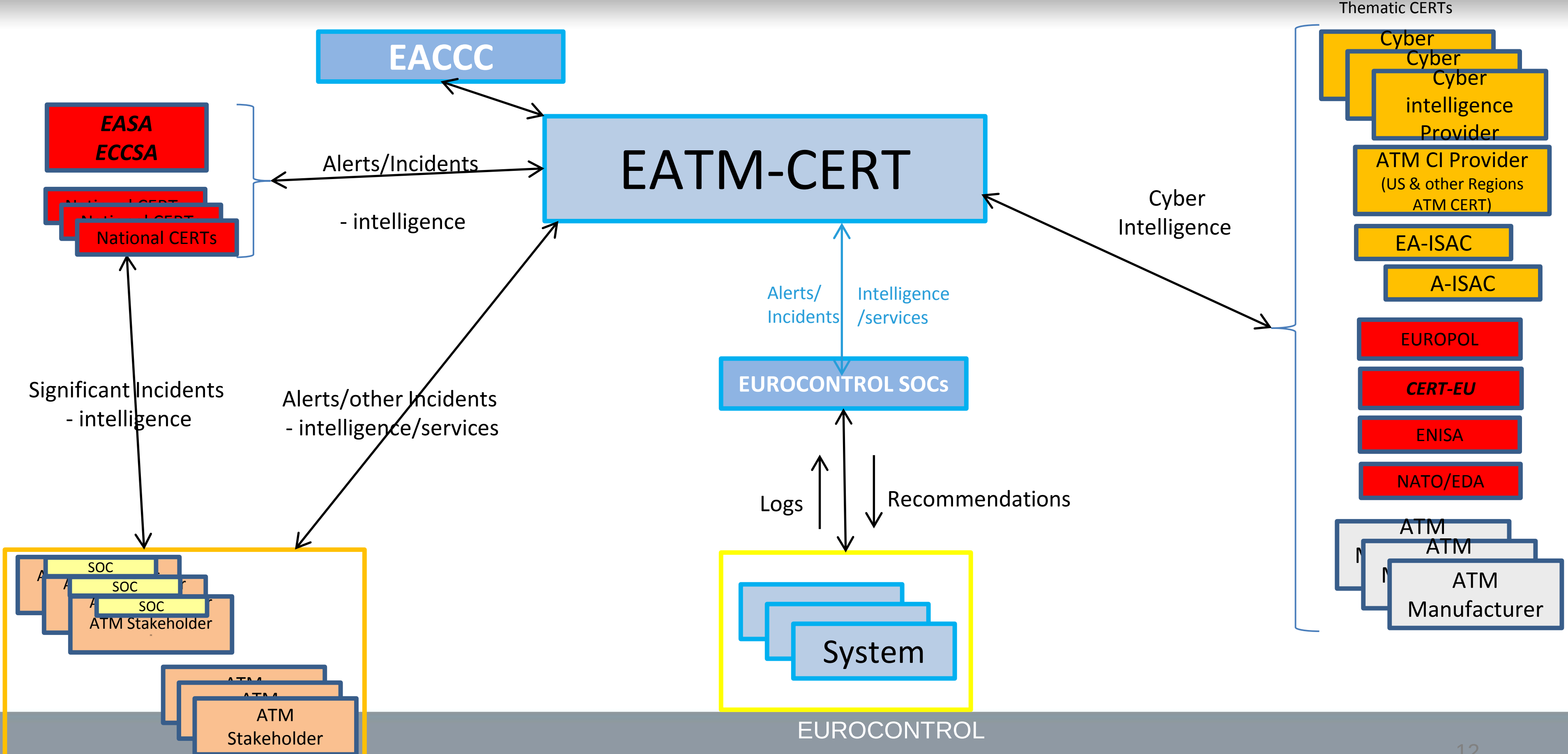
Evening Standard.

Lifestyle › ES Magazine

How flygskam (or flight shame) is spreading across Europe

Fears over climate change have led many to rethink the way they travel and, in Sweden, they've even invented a new word for the shame associated with flying

JULIANA PISKORZ | Wednesday 17 April 2019 13:07 |



EACCC

EATM-CERT

EASA ECCSA

National CERTs

Alerts/Incidents

- intelligence

Cyber Intelligence

Thematic CERTs

Cyber intelligence Provider

ATM CI Provider (US & other Regions ATM CERT)

EA-ISAC

A-ISAC

EUROPOL

CERT-EU

ENISA

NATO/EDA

ATM Manufacturer

Alerts/ Incidents

Intelligence /services

EUROCONTROL SOCs

Logs

Recommendations

System

Significant Incidents - intelligence

Alerts/other Incidents - intelligence/services

SOC

ATM Stakeholder

ATM Stakeholder

EATM-CERT services

Initial set of 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. Support to incident response / Artefacts analysis
8. Training - workshop for aviation Stakeholders
9. TLP:WHITE CTI tools – raising awareness

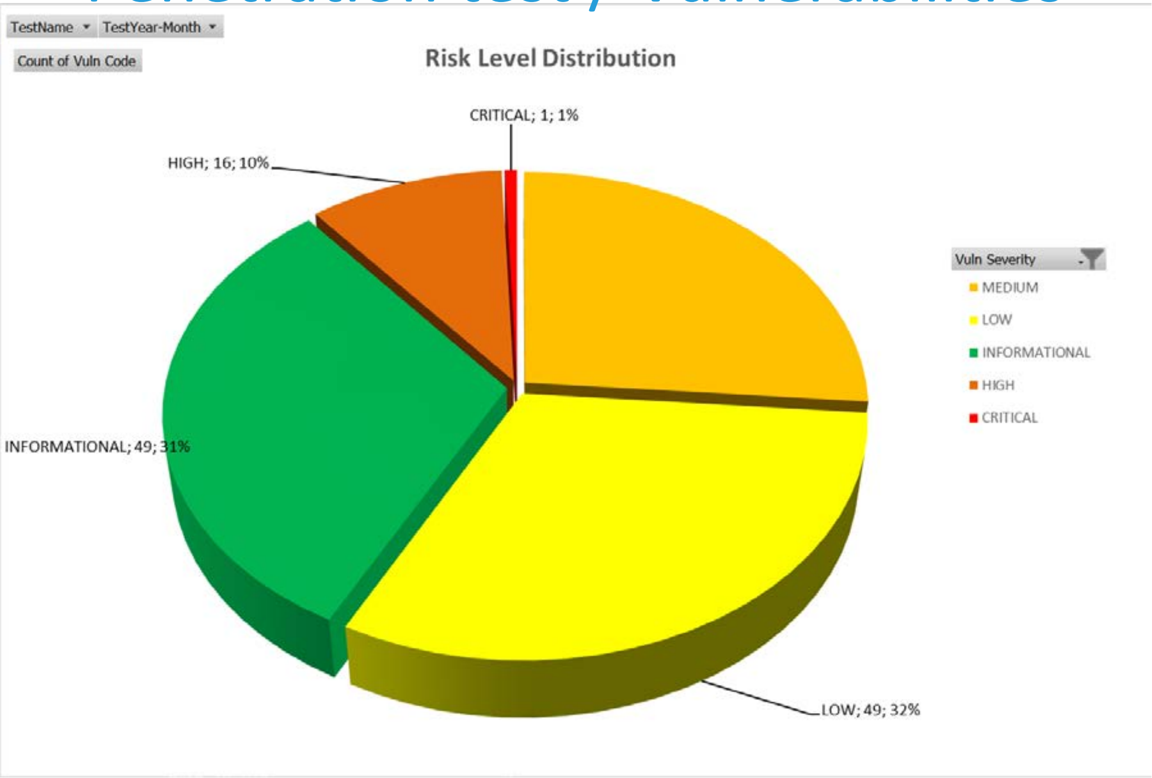
Future services:

1. Vulnerability scanning of Aviation Stakeholders
2. Vulnerability watch
3. Training exercises (table-top & technical)

EATM-CERT
European Air Traffic Management
Computer Emergency Response Team

EUROCONTROL

Penetration test / Vulnerabilities



2 - Bank transfer scams via email

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

2 - Bank transfer scams via email

Domain name	Domain closure: status	Attempts count
eurcontrolint.net	Suspended	51
eurocontroladmin.net	Suspended	29
euro-controlint.net	Suspended	16
euro-control-int.org	Suspended	14
eurocontrotint.net	Suspended	13
euro-control.net	Suspended	9
eurocontolint.net	Suspended	7
eurocontrolaudits.net	Suspended	4
euro-control.org	Suspended	3
eurocontrolaudit.net	Suspended	3
euro-controlinc.com	Suspended	2
eurocontroint.net	Suspended	1
eurocontrolints.net	Suspended	1

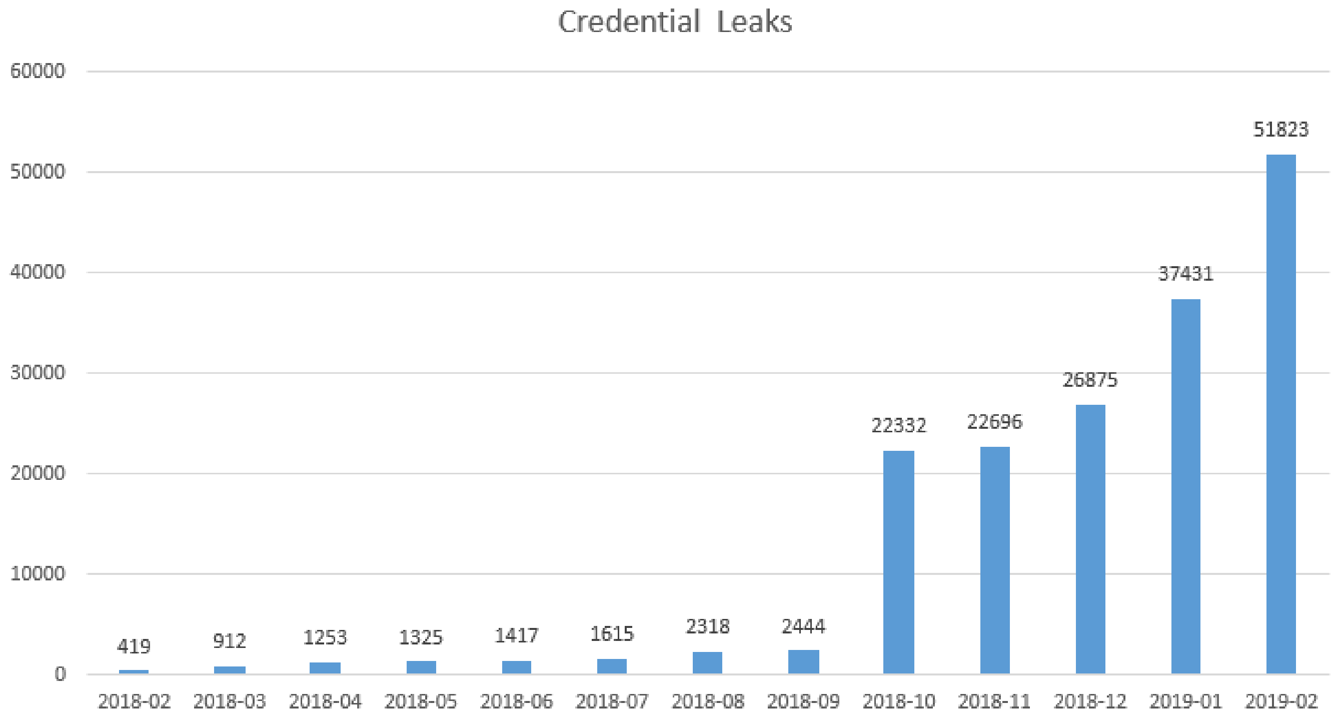
3 - Credentials leaks service

- EUROCONTROL: since 01/2018 (provided by SpyCloud)
- Test phase till end 2018

- Many Stakeholders subscribed (approx. 90: ANSPs, AUs, AOs)
- Very positive feedback

- As conclusive, then the service is proposed to be provided for the next 3 years + 2 optional one-year to all those willing to benefit from it:
  - Procurement (open CFT) by EUROCONTROL
  - Service paid using EUROCONTROL budget

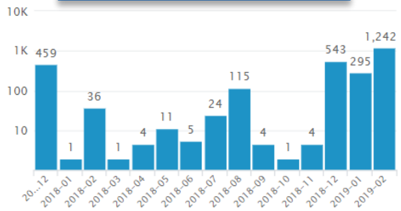
3 - Credentials leaks service



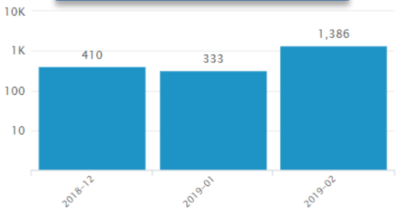
password leaks: 97%

3 - Credentials leaks service

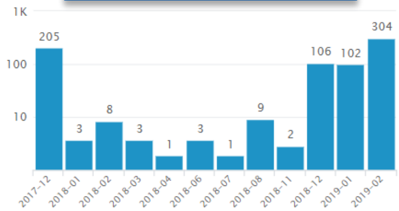
[redacted]



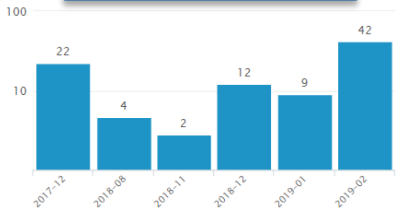
[redacted]



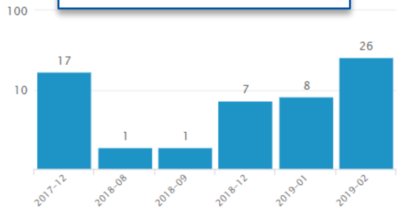
[redacted]



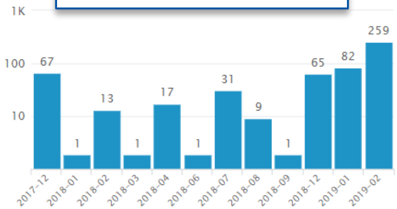
[redacted]



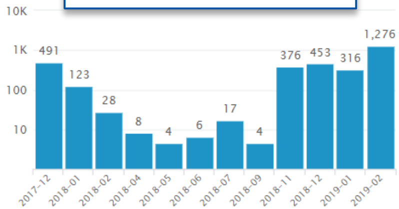
[redacted]



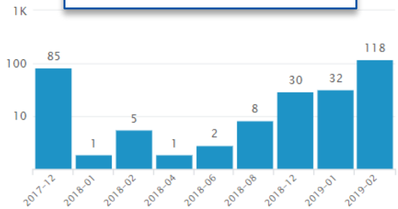
[redacted]



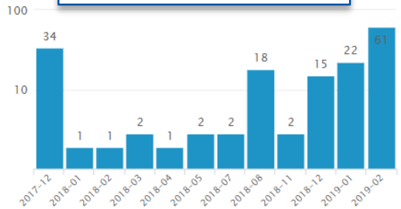
[redacted]



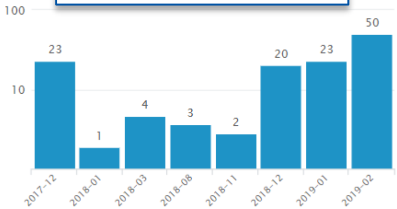
[redacted]



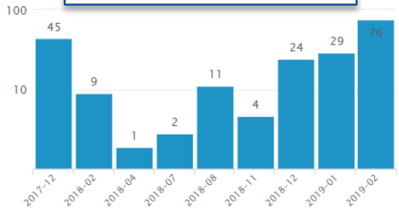
[redacted]



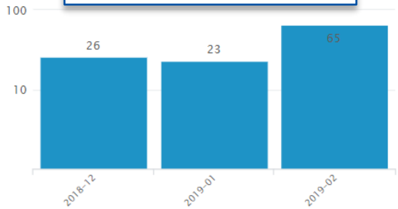
[redacted]



[redacted]



[redacted]



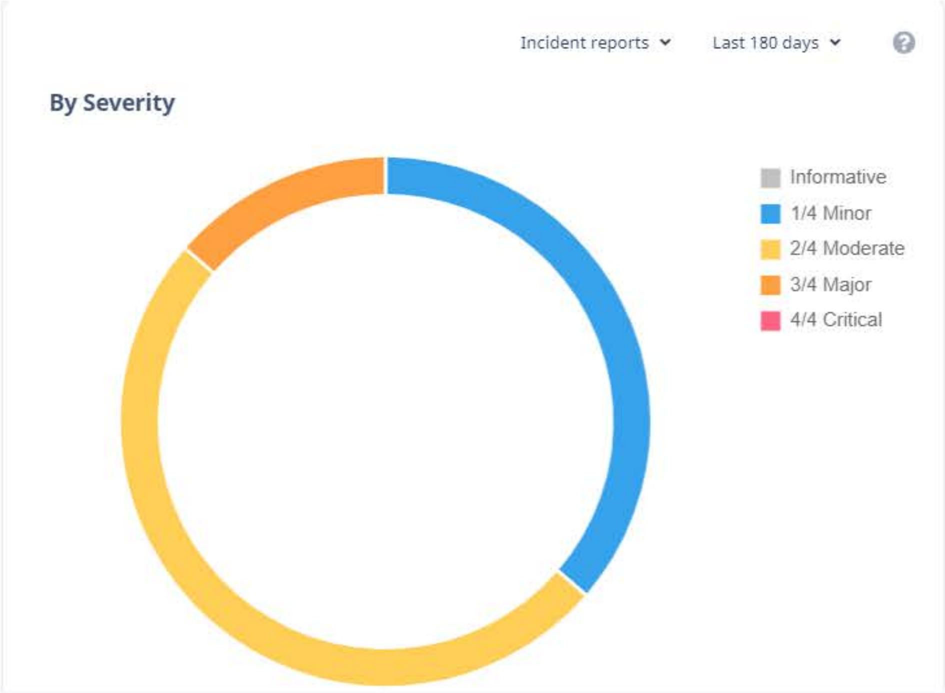
4 - Document/information leak service

- 1st 6-month Service test phase – completed (June 2019)
- S2-2019 contract signed

- Some ANSPs - candidate testers - joined

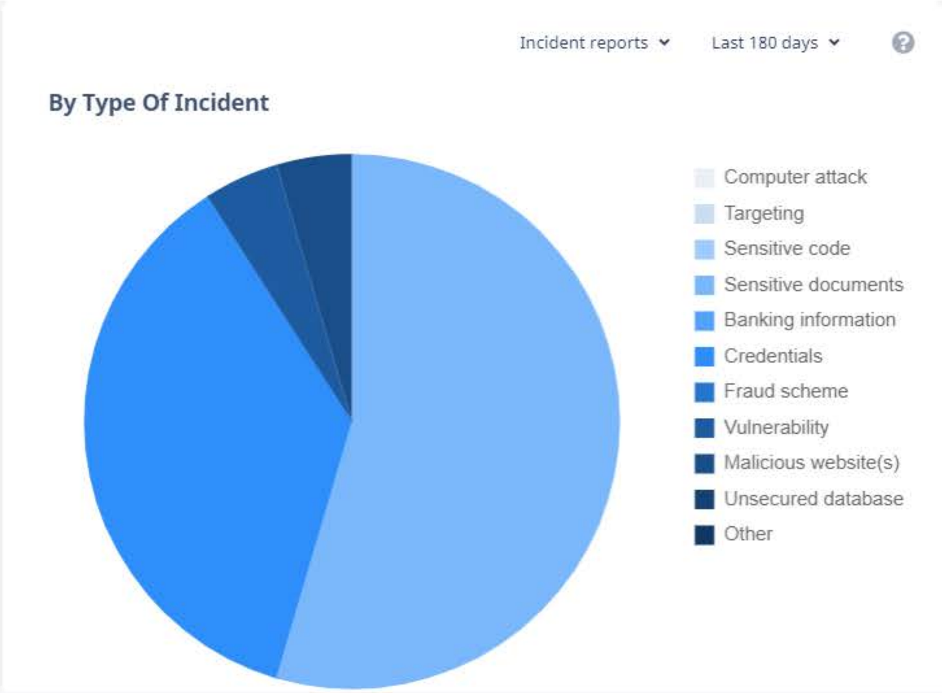
- Main lessons learned:
  - 80-90% of leaks are coming from contractors
  - Service that requires to be further investigated
  - Need to be a first level of centralisation as it requires a pre-analysis (reduce false/positive)

4 - Cyber-security service: doc/info leaks



Incident reports ▾ Last 180 days ▾

By Severity



Incident reports ▾ Last 180 days ▾

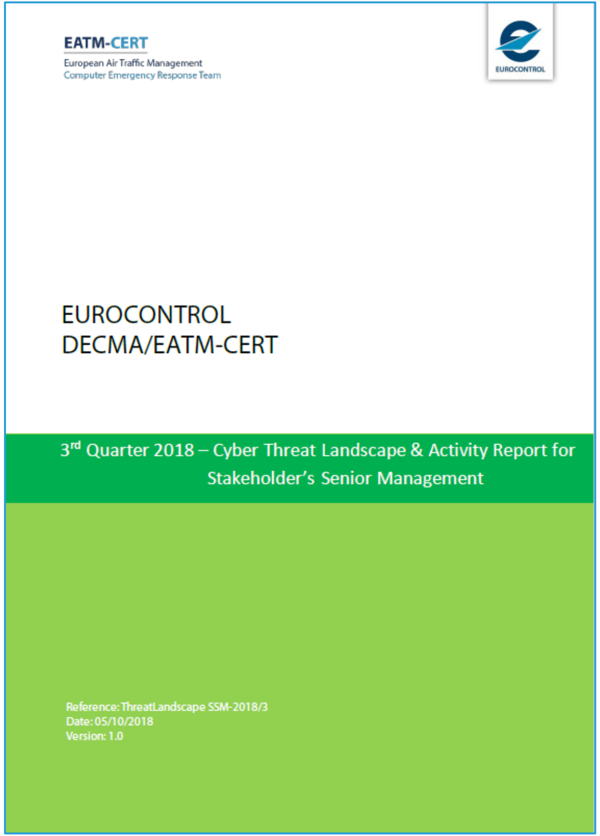
By Type Of Incident

5 – Cyber Threat Intelligence (CTI) and feeds for aviation

- 1st 6-month Service test phase – completed (June 2019)
- S2-2019 contract signed

- Main lessons learned:
  - Lot of information - need to sort out what is relevant – big data/AI tool needed
  - Resource consuming
  - Are CTI vendors the best source of information for aviation vs aviation stakeholders ?
  - Valuable for feeds not originating from aviation but relevant to aviation

6 - Raising Senior Management awareness



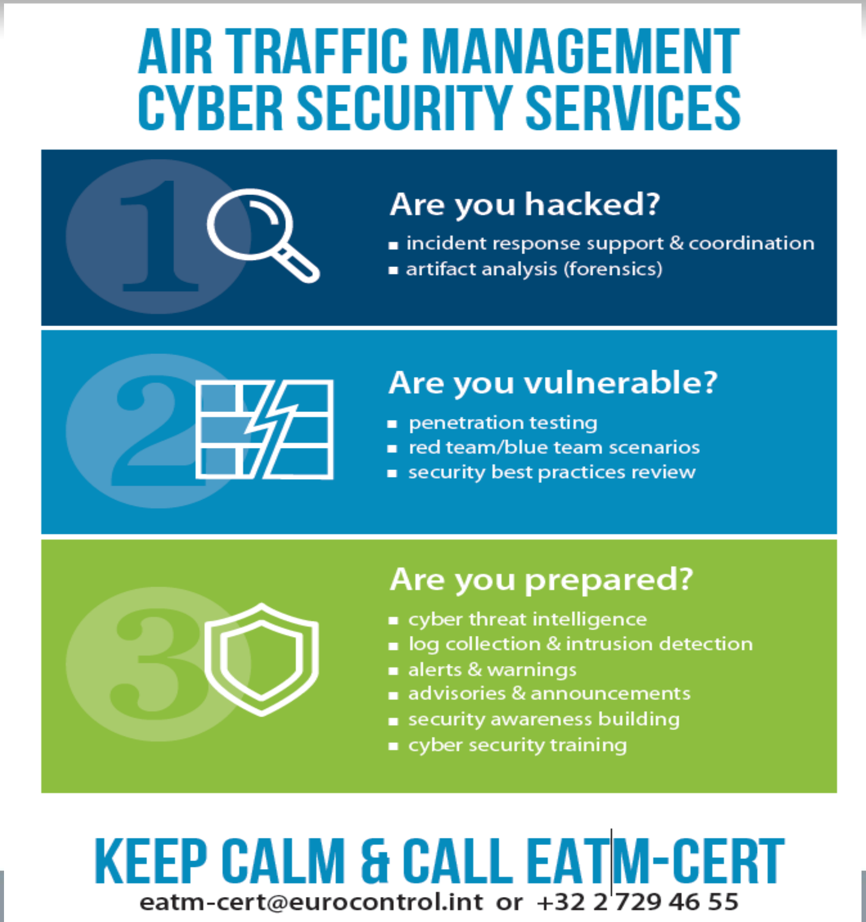
EATM-CERT
European Air Traffic Management
Computer Emergency Response Team

EUROCONTROL

EUROCONTROL
DECMA/EATM-CERT

3rd Quarter 2018 – Cyber Threat Landscape & Activity Report for Stakeholder's Senior Management

Reference: ThreatLandscape SSM-2018/3
Date: 05/10/2018
Version: 1.0



AIR TRAFFIC MANAGEMENT CYBER SECURITY SERVICES

Are you hacked?

- incident response support & coordination
- artifact analysis (forensics)

Are you vulnerable?

- penetration testing
- red team/blue team scenarios
- security best practices review

Are you prepared?

- cyber threat intelligence
- log collection & intrusion detection
- alerts & warnings
- advisories & announcements
- security awareness building
- cyber security training

KEEP CALM & CALL EATM-CERT

eatm-cert@eurocontrol.int or +32 2 729 46 55

CYBER SECURITY AND RESILIENCE SYMPOSIUM

TOWARDS A RESILIENT AVIATION CYBERSPACE

AMMAN, JORDAN | 15-17 OCTOBER 2019

Thank You