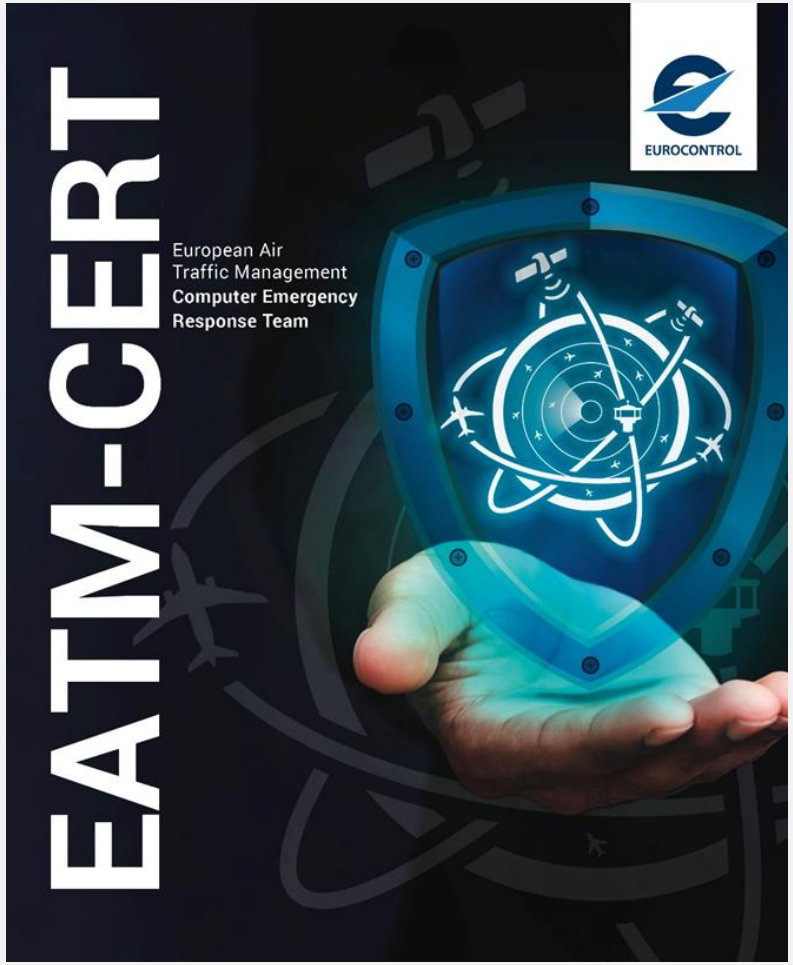
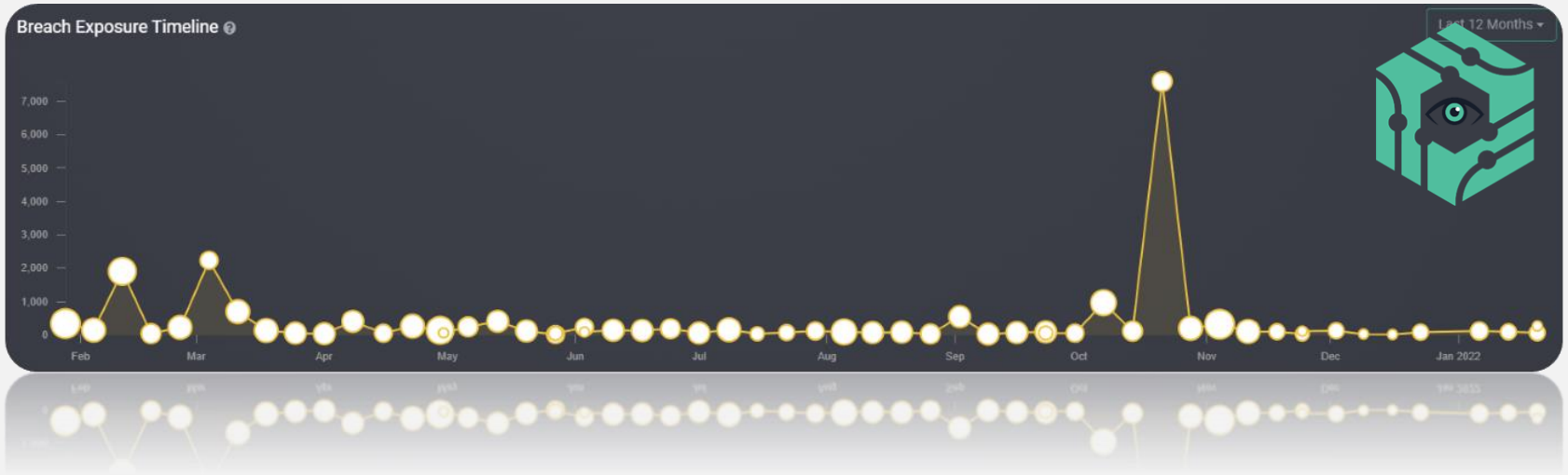
EATM-CERT services

- Credential leaks
- Fraudulent web sites
- Frequent flyer account access
- Exchange of cyber info/intel
- Pentest
- CYBERG

- Common PKI



Credential Leaks



SpyCloud

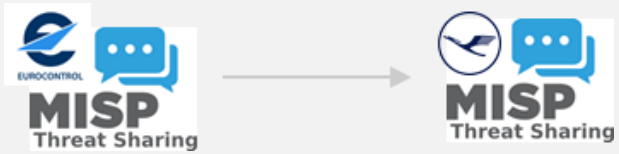
Sharing and exchanging cyber threat intelligence

MISP (Malware Information Sharing Platform)

Lufthansa Group regularly receives MISP events by EATM CERT-

These events include:

- Relevant and high quality indicators of compromise
- Information about current Tactics, Techniques, and Procedures (TTPs)



Benefits:

- Improve detection and blocking
- Avoid duplicate work
- Quick way to search, pivot, contextualize, and validate indicators (during incidents)

Direct team/team exchange

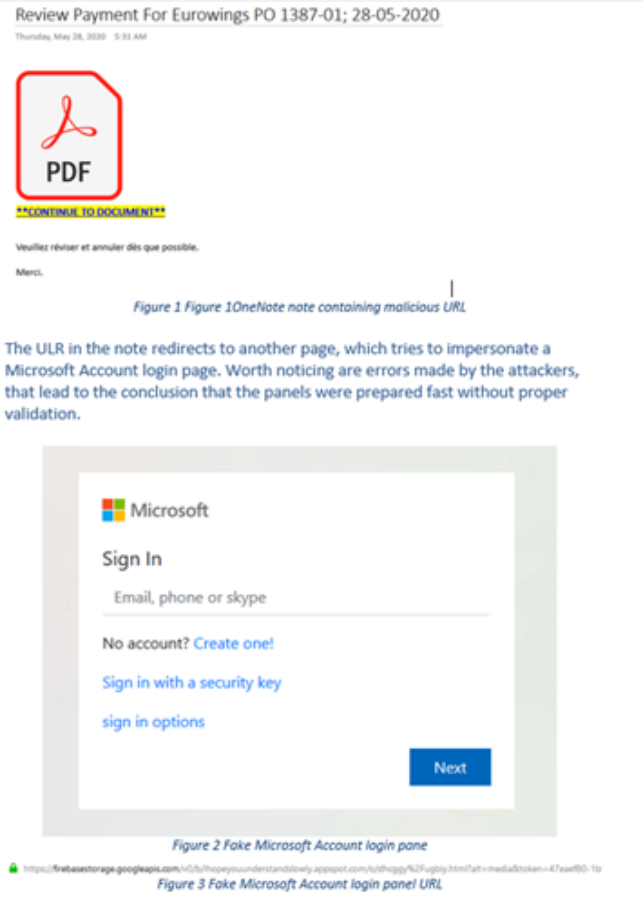


Figure 1 Figure 1OneNote note containing malicious URL

The ULR in the note redirects to another page, which tries to impersonate a Microsoft Account login page. Worth noticing are errors made by the attackers, that lead to the conclusion that the panels were prepared fast without proper validation.

Figure 2 Fake Microsoft Account login pane

Figure 3 Fake Microsoft Account login panel URL

Austrian Lufthansa SWISS LUFTHANSA GROUP

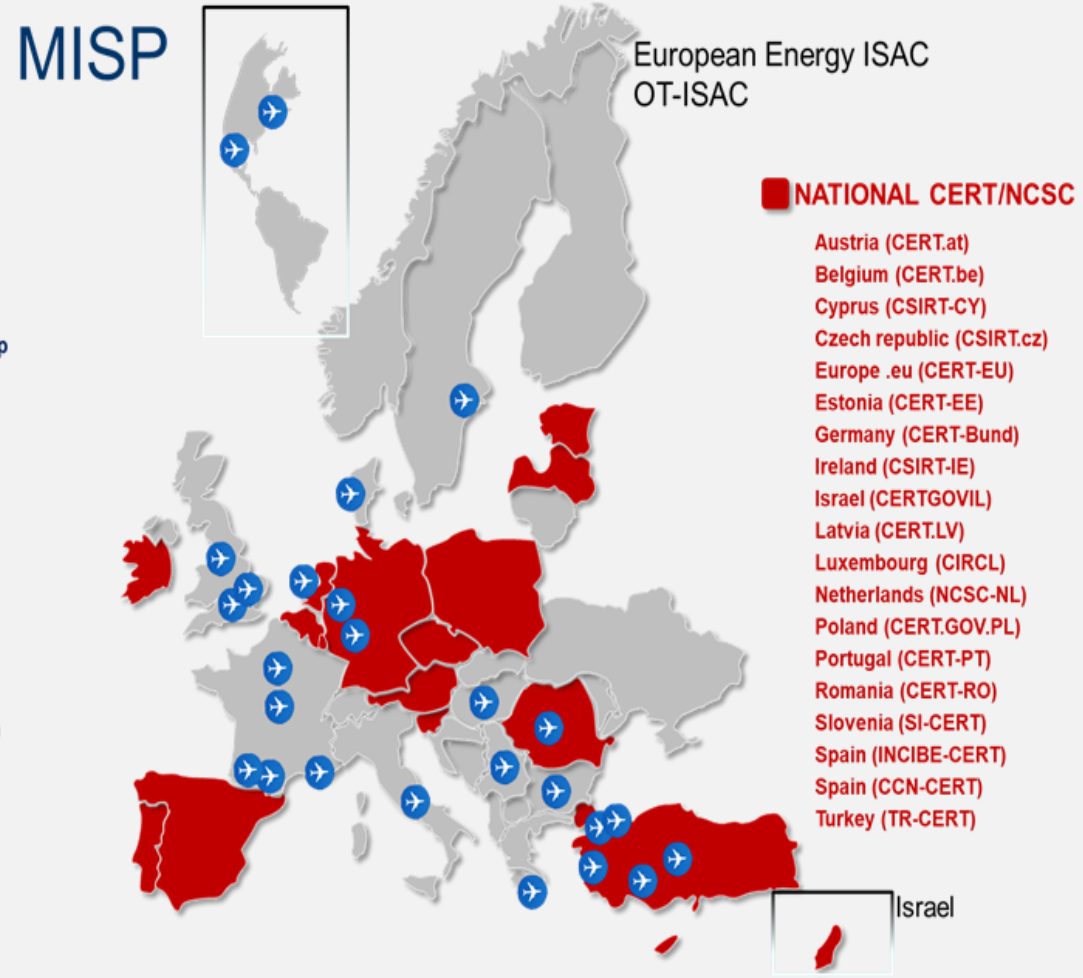
Automated exchange of cyber intel (IOCs, TTPs, …)

- MISP (Malware Information Sharing Platform)

MISP Threat Sharing

Aviation stakeholders

- Bulgaria - BULATSA (ANSP)
- Denmark - NAVIAIR (ANSP)
- Europe - ECCSA (test)
- France - CERT-AIRBUS A/C
- France - Groupe ADP
- France - DSNA
- France - Cert-IST (Thales)
- Germany - DLH-DE –Lufthansa Group
- Germany - Frankfurt Airport
- Greece - HANSP
- Hungary - HungaroControl (ANSP)
- 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



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)

Other topics LHG airlines are contributing and taking advantage of

- Participation to NDTECH/IMT/CYBERg
- Participation to the Common PKI CEF co-funded project

➢ Pentest by EATM-CERT

- Scope scenarios:
  - distribute malware code via computing packages and take over internal application incl. server.
  - Use simple computing to read out and transmit the original data from 3rd client or in a version where the original data can be determined
  - Manipulate the result so that the calculation can be manipulated (faking the result).

➢ EATM CERT has gained an enourmeous know-how