Supporting
European
Aviation

EUROCONTROL

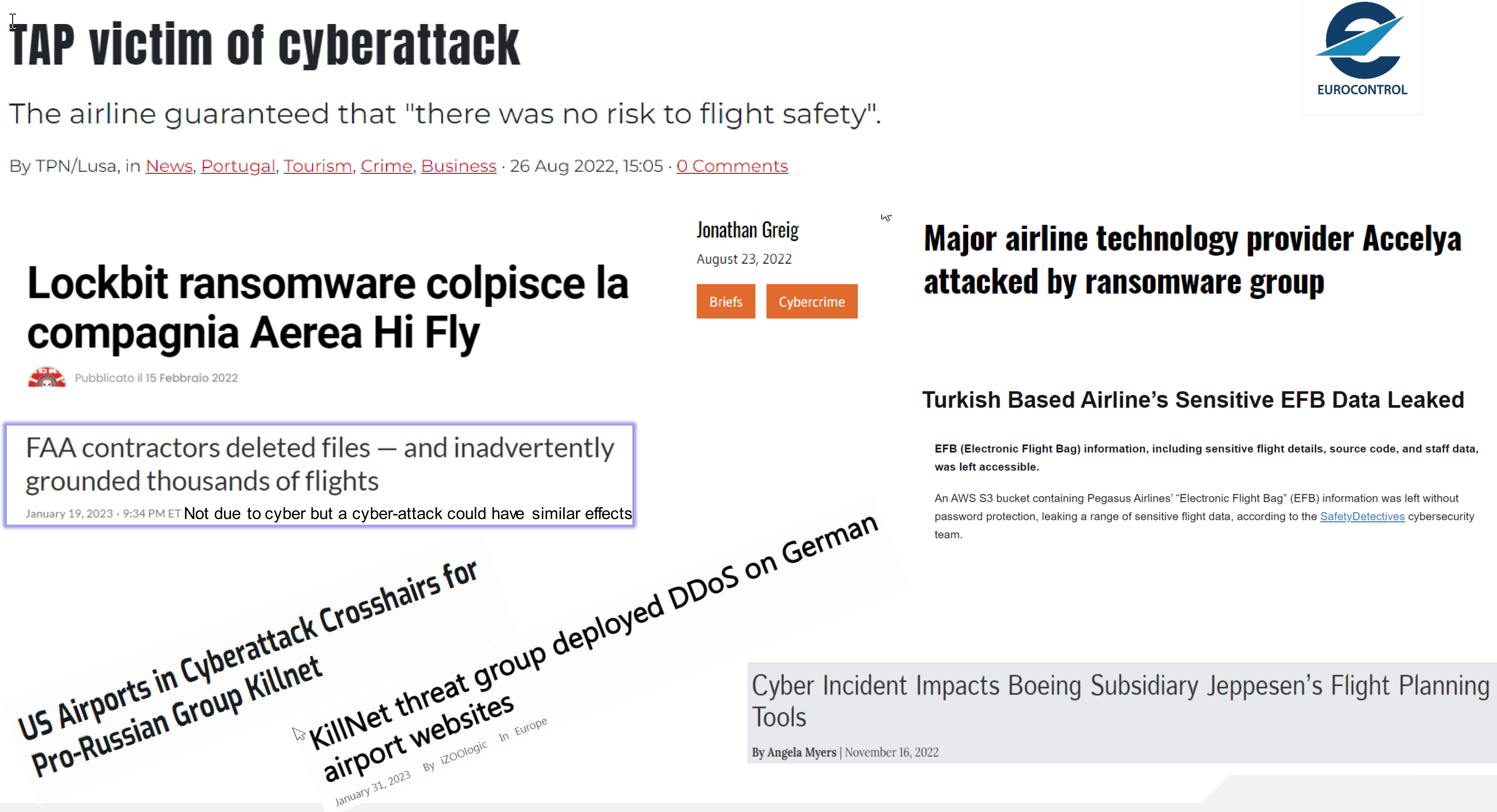
AI/ML for cyber

FLY AI Forum 2023

Patrick Mana
EATM-CERT

20 April 2023

CONSORTIUM COORDINATOR sesar DEPLOYMENT MANAGER
FOUNDING MEMBER sesar JOINT UNDERTAKING
NETWORK MANAGER



TAP victim of cyberattack

The airline guaranteed that "there was no risk to flight safety".

By TPN/Lusa, in News, Portugal, Tourism, Crime, Business · 26 Aug 2022, 15:05 · 0 Comments

Lockbit ransomware colpisce la compagnia Aerea Hi Fly

Pubblicato il 15 Febbraio 2022

Jonathan Greig

August 23, 2022

Briefs Cybercrime

Major airline technology provider Accelya attacked by ransomware group

Turkish Based Airline's Sensitive EFB Data Leaked

EFB (Electronic Flight Bag) information, including sensitive flight details, source code, and staff data, was left accessible.

An AWS S3 bucket containing Pegasus Airlines' "Electronic Flight Bag" (EFB) information was left without password protection, leaking a range of sensitive flight data, according to the SafetyDetectives cybersecurity team.

FAA contractors deleted files — and inadvertently grounded thousands of flights

January 19, 2023 · 9:34 PM ET Not due to cyber but a cyber-attack could have similar effects

US Airports in Cyberattack Crosshairs for Pro-Russian Group Killnet

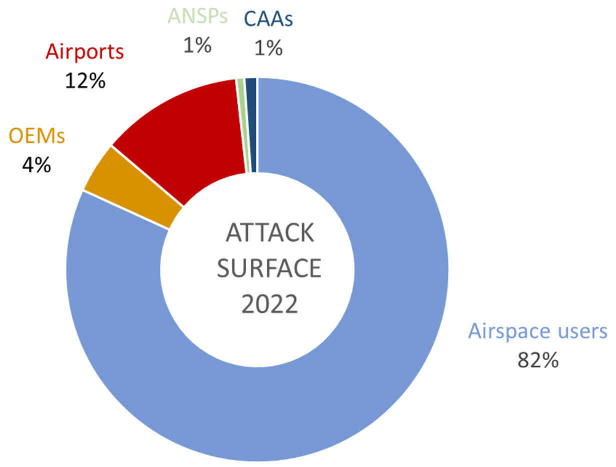
KillNet threat group deployed DDoS on German airport websites

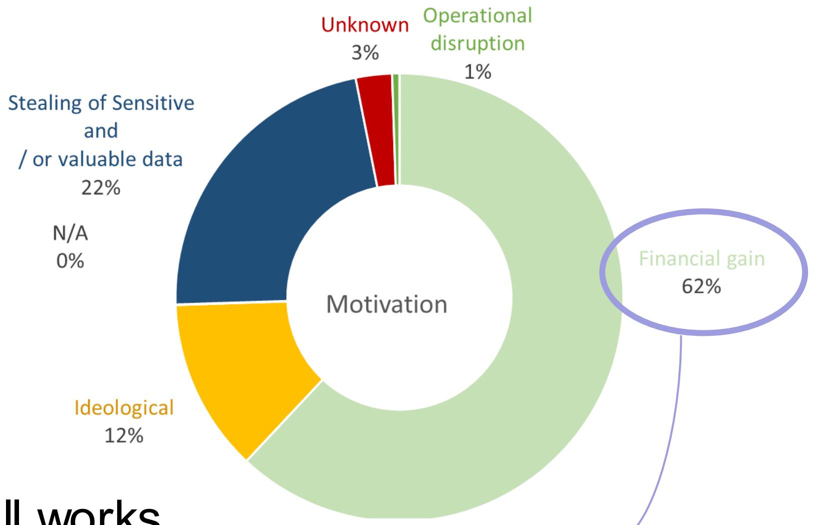
January 31, 2023 By iZOOlogic In Europe

Cyber Incident Impacts Boeing Subsidiary Jeppesen's Flight Planning Tools

By Angela Myers | November 16, 2022

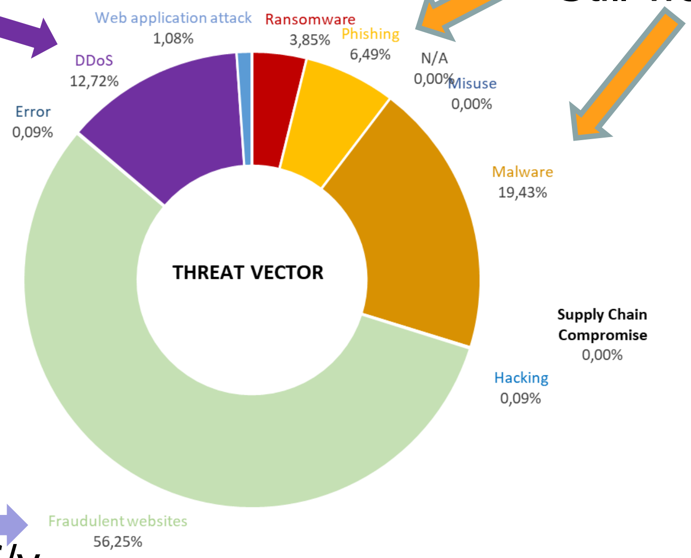
Aviation cyber threat landscape (2022) - limited data so far as event collection campaign still on-going



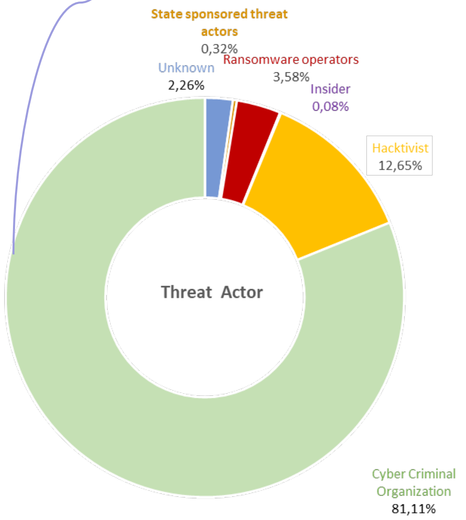


War in Ukraine

Still works



1Bn€/y

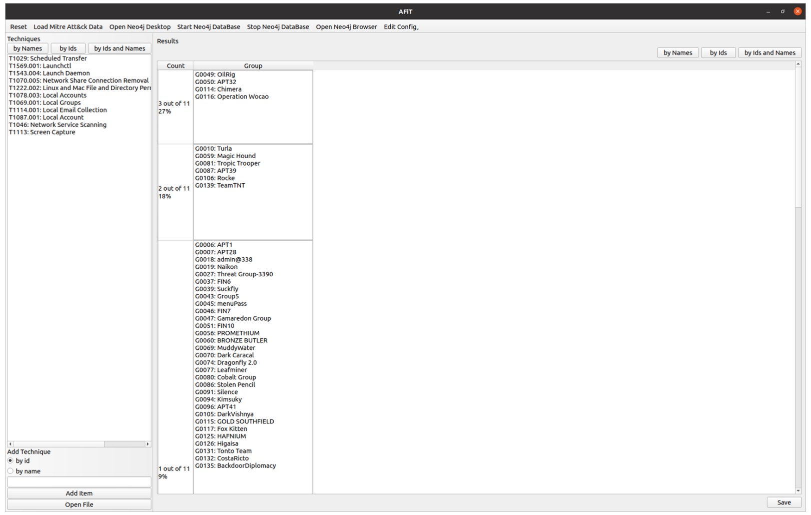


AI/ML app for cyber

- Three app either under development or about to:
  - Aviation documents - COMPLETED

  - Password cracker – First part based on RNN

  - MITRE ATT&CK tool – Start 12/2022

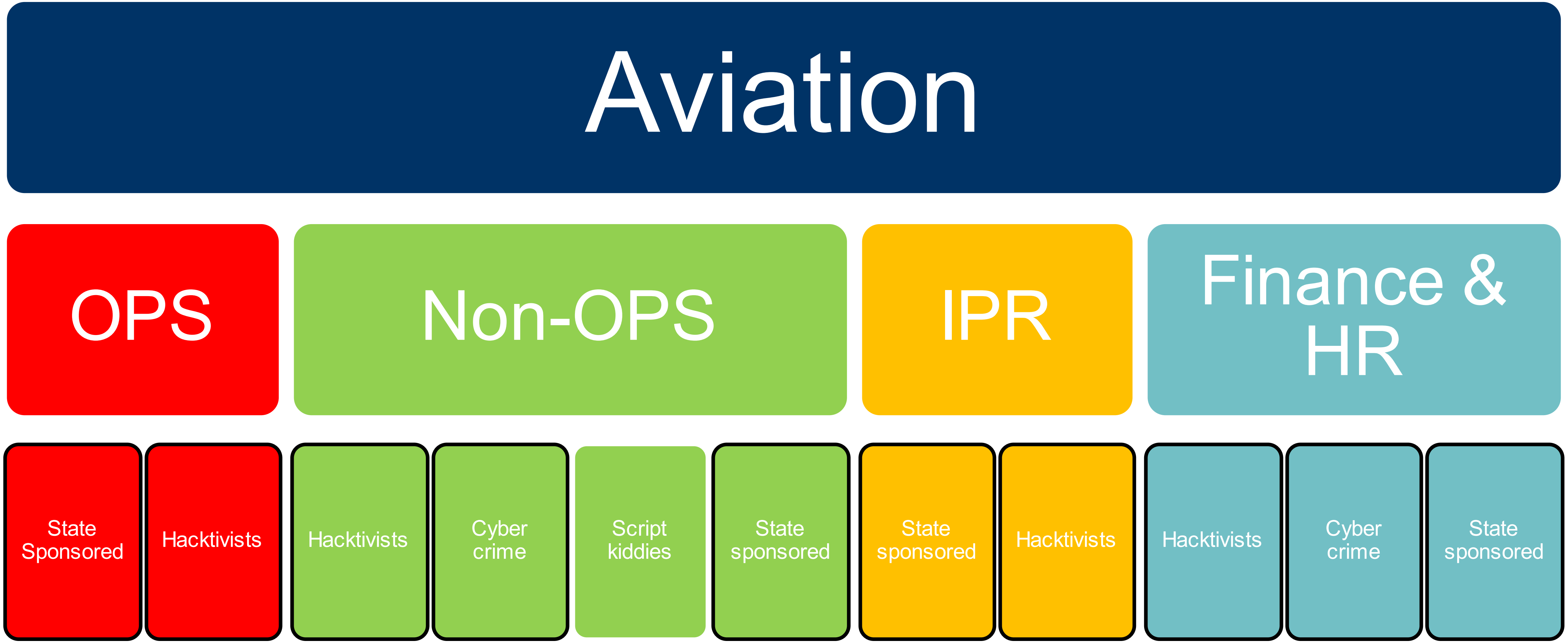


T1029: Scheduled Transfer
T1569.001: Launchctl
T1543.004: Launch Daemon
T1070.005: Network Share Connection Removal
T1222.002: Linux and Mac File and Directory Perı
T1078.003: Local Accounts
T1069.001: Local Groups
T1114.001: Local Email Collection
T1087.001: Local Account
T1046: Network Service Scanning
T1113: Screen Capture

Count	Group
3 out of 11 27%	G0049: OilRig G0050: APT32 G0114: Chimera G0116: Operation Wocao
2 out of 11 18%	G0010: Turla G0059: Magic Hound G0081: Tropic Trooper G0087: APT39 G0106: Rocke G0139: TeamTNT
1 out of 11 9%	G0006: APT1 G0007: APT28 G0018: admin@338 G0019: Naikon G0027: Threat Group-3390 G0037: FIN6 G0039: Suckfly G0043: Group5 G0045: menuPass G0046: FIN7 G0047: Gamaredon Group G0051: FIN10 G0056: PROMETHIUM G0060: BRONZE BUTLER G0069: MuddyWater G0070: Dark Caracal G0074: Dragonfly 2.0 G0077: Leafminer G0080: Cobalt Group G0086: Stolen Pencil G0091: Silence G0094: Kimsuky G0096: APT41 G0105: DarkVishnya G0115: GOLD SOUTHFIELD G0117: Fox Kitten G0125: HAFNIUM G0126: Higaisa G0131: Tonto Team G0132: CostaRicto G0135: BackdoorDiplomacy

Add Technique
● by id
○ by name

Simplified Threat Model



Aviation

OPS

- State Sponsored
- Hacktivists

Non-OPS

- Hacktivists
- Cyber crime
- Script kiddies
- State sponsored

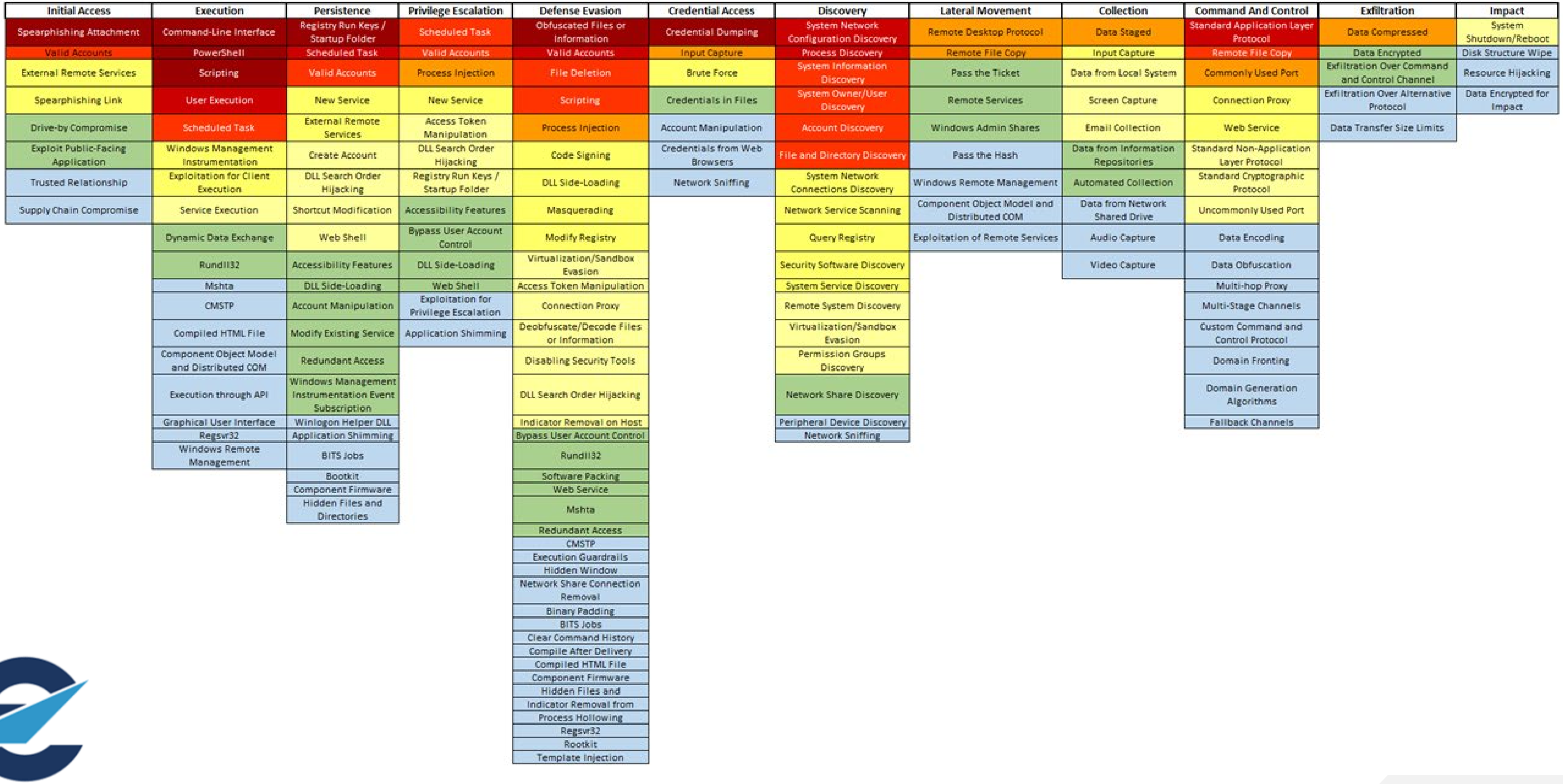
IPR

- State sponsored
- Hacktivists

Finance & HR

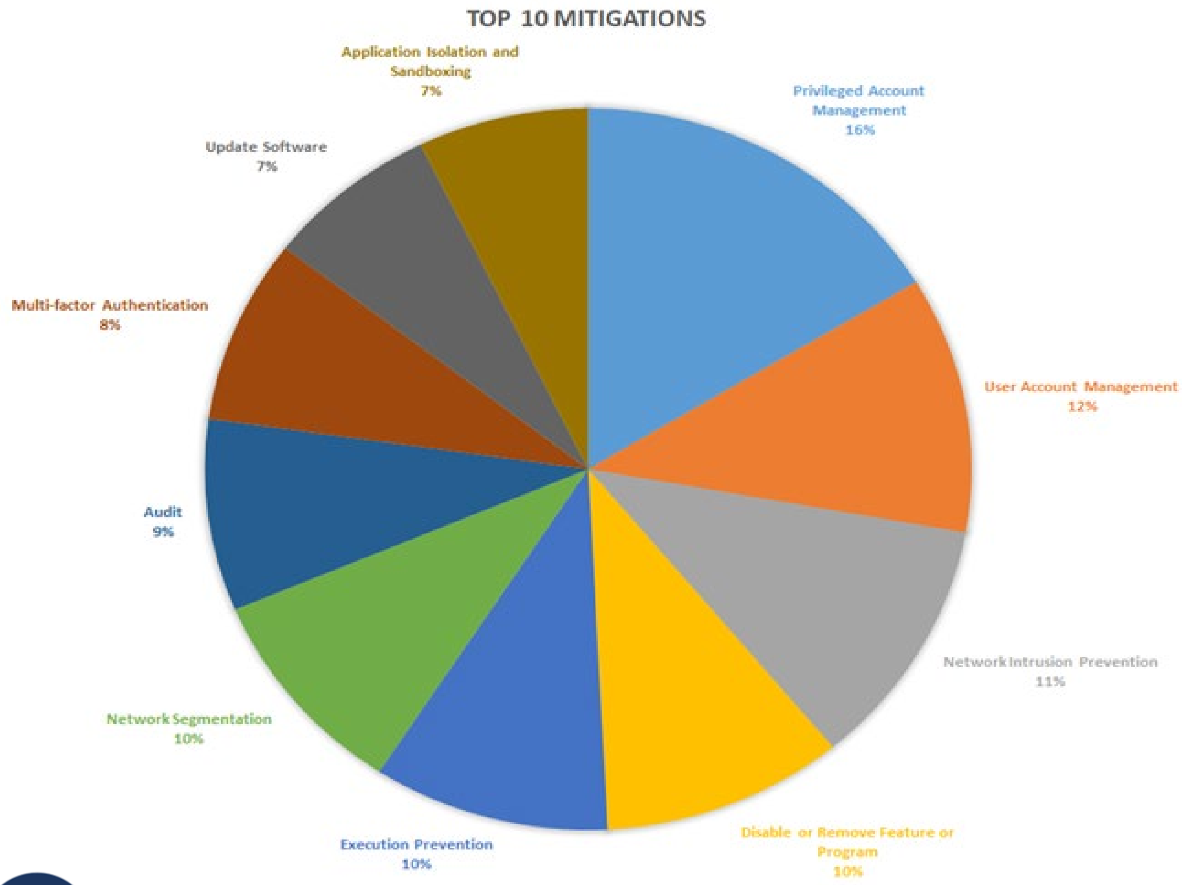
- Hacktivists
- Cyber crime
- State sponsored

MITRE ATT&CK: Techniques mostly used to attack aviation

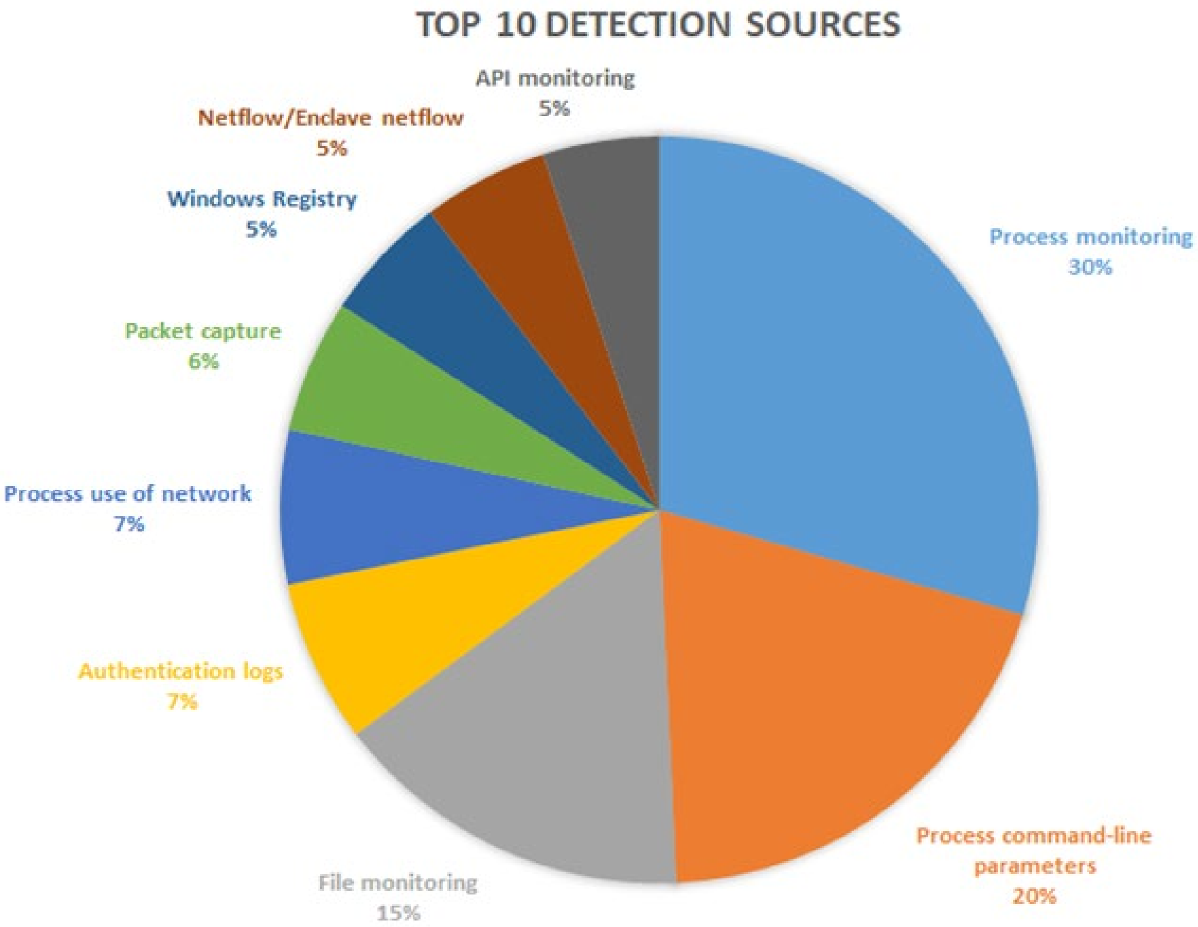


Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
Spearphishing Attachment	Command-Line Interface	Registry Run Keys / Startup Folder	Scheduled Task	Obfuscated Files or Information	Credential Dumping	System Network Configuration Discovery	Remote Desktop Protocol	Data Staged	Standard Application Layer Protocol	Data Compressed	System Shutdown/Reboot
Valid Accounts	PowerShell	Scheduled Task	Valid Accounts	Valid Accounts	Input Capture	Process Discovery	Remote File Copy	Input Capture	Remote File Copy	Data Encrypted	Disk Structure Wipe
External Remote Services	Scripting	Valid Accounts	Process Injection	File Deletion	Brute Force	System Information Discovery	Pass the Ticket	Data from Local System	Commonly Used Port	Exfiltration Over Command and Control Channel	Resource Hijacking
Spearphishing Link	User Execution	New Service	New Service	Scripting	Credentials in Files	System Owner/User Discovery	Remote Services	Screen Capture	Connection Proxy	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Drive-by Compromise	Scheduled Task	External Remote Services	Access Token Manipulation	Process Injection	Account Manipulation	Account Discovery	Windows Admin Shares	Email Collection	Web Service	Data Transfer Size Limits	
Exploit Public-Facing Application	Windows Management Instrumentation	Create Account	DLL Search Order Hijacking	Code Signing	Credentials from Web Browsers	File and Directory Discovery	Pass the Hash	Data from Information Repositories	Standard Non-Application Layer Protocol		
Trusted Relationship	Exploitation for Client Execution	DLL Search Order Hijacking	Registry Run Keys / Startup Folder	DLL Side-Loading	Network Sniffing	System Network Connections Discovery	Windows Remote Management	Automated Collection	Standard Cryptographic Protocol		
Supply Chain Compromise	Service Execution	Shortcut Modification	Accessibility Features	Masquerading		Network Service Scanning	Component Object Model and Distributed COM	Data from Network Shared Drive	Uncommonly Used Port		
	Dynamic Data Exchange	Web Shell	Bypass User Account Control	Modify Registry		Query Registry	Exploitation of Remote Services	Audio Capture	Data Encoding		
	Rundll32	Accessibility Features	DLL Side-Loading	Virtualization/Sandbox Evasion		Security Software Discovery		Video Capture	Data Obfuscation		
	Mshta	DLL Side-Loading	Web Shell	Access Token Manipulation		System Service Discovery			Multi-hop Proxy		
	CMSTP	Account Manipulation	Exploitation for Privilege Escalation	Connection Proxy		Remote System Discovery			Multi-Stage Channels		
	Compiled HTML File	Modify Existing Service	Application Shimming	Deobfuscate/Decode Files or Information		Virtualization/Sandbox Evasion			Custom Command and Control Protocol		
	Component Object Model and Distributed COM	Redundant Access		Disabling Security Tools		Permission Groups Discovery			Domain Fronting		
	Execution through API	Windows Management Instrumentation Event Subscription		DLL Search Order Hijacking		Network Share Discovery			Domain Generation Algorithms		
	Graphical User Interface	Winlogon Helper DLL		Indicator Removal on Host		Peripheral Device Discovery			Fallback Channels		
	Regsvr32	Application Shimming		Bypass User Account Control		Network Sniffing					
	Windows Remote Management	BITS Jobs		Rundll32							
		Bootkit		Software Packing							
		Component Firmware		Web Service							
		Hidden Files and Directories		Mshta							
				Redundant Access							
				CMSTP							
				Execution Guardrails							
				Hidden Window							
				Network Share Connection Removal							
				Binary Padding							
				BITS Jobs							
				Clear Command History							
				Compile After Delivery							
				Compiled HTML File							
				Component Firmware							
				Hidden Files and							
				Indicator Removal from							
				Process Hollowing							
				Regsvr32							
				Rootkit							
				Template Injection							

Top 10 Mitigation Means



Top Detection Means



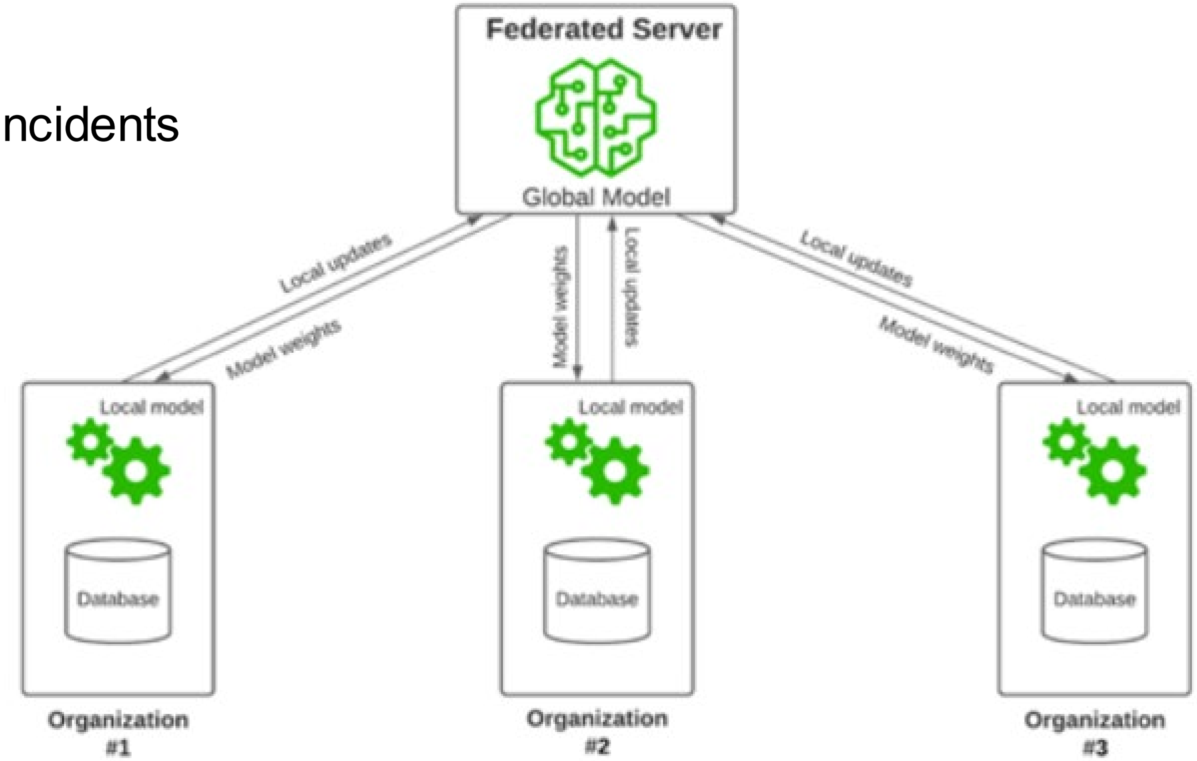
Improving the attribution of cyber-attacks?

- Why
  - To anticipate attacks using similar techniques by similar threat actors
  - To prioritise protection, detection and mitigation means

- How
  - AI/ML app trained on aviation related cyber-incidents

- Challenges
  - Data cannot be shared (sensitive)
  - No one wants to host such sensitive info

- Solution => Federated learning



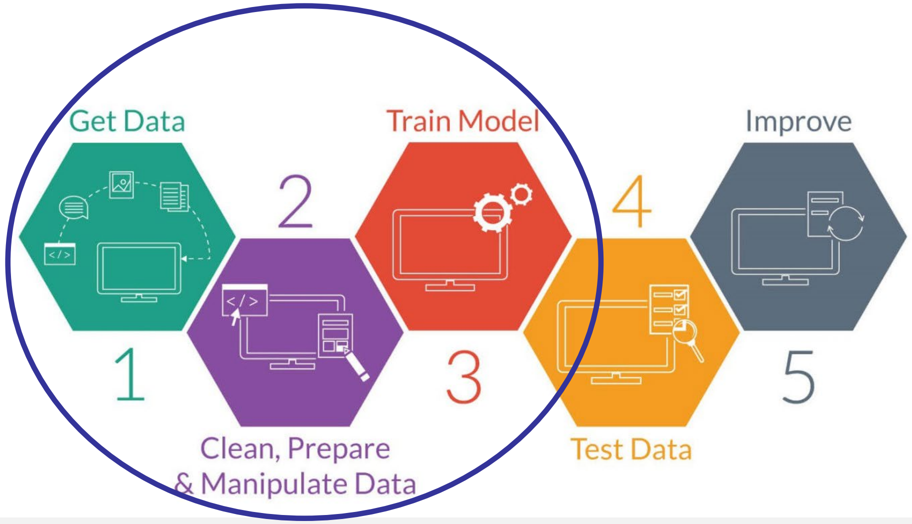
- Federated learning applies to other fields than cyber

Can AI/ML help to attribute cyber-attacks?

[redacted]

EASTERN WORLD
WESTERN WORLD

=> FEDERATED LEARNING



SUPPORTING EUROPEAN AVIATION