



الهيئة العامة للطيران المدني
GENERAL CIVIL AVIATION AUTHORITY



Third Meeting of the Air Navigation System Implementation Group (ANSIG/3) ATM Data and Cyber Security Portal

Cairo, Egypt, 2-4 July 2018

United Arab Emirates



الهيئة العامة للطيران المدني
GENERAL CIVIL AVIATION AUTHORITY



Outline

- Introduction
- ATM Data & Cyber Security Portal
- ADCS Portal
- ADCS Portal Enhancements
- Conclusion



الهيئة العامة للطيران المدني
GENERAL CIVIL AVIATION AUTHORITY



Introduction

With the continuous evolution of ATM systems and the interconnectivity enhancements throughout the region it is essential to ensure that adequate cyber security measures are in place.

As per the MIDANPIRG 16/26 decision the ATM Data and Security Action Group(ADSAG) was established with the UAE taking the lead for the Mid region to develop, in co-ordination with the other states, a security baseline for the various systems in use.

As part of this security initiative 7 Minimum Security Baseline (MSB) documents were created which cover the various technologies and systems in use within our industry.



الهيئة العامة للطيران المدني
GENERAL CIVIL AVIATION AUTHORITY



Introduction

These documents were presented in WP 12 at this year's CNS SG/8 and an ADSAG group meeting was scheduled at the MID office from 24-26 June 2018, where after the documents will be finalised.

The MSB's will then be presented at the MIDANPIRG 17 for endorsement by the ICAO Mid Office.

As a further enhancement to the MSB's an online portal, known as the ATM Data and Cyber Security Portal, has been developed by the UAE to allow ANSP's to report cyber events as well as share knowledge and information on cyber security incidents.



الهيئة العامة للطيران المدني
GENERAL CIVIL AVIATION AUTHORITY



ATM Data & Cyber Security Portal

- This prototype portal is not intended to be a comprehensive solution for cyber security but rather a platform where cyber events can be logged, information related to cyber attacks shared and discussions held on various cyber topics on the forum.
- To ensure this is not abused by outside users, access will be restricted to approved ANSP/industry users only.
- Access will be requested via a template provided on the website and once approved, we will provide the user credentials to the respective applicant.
- Usage of the portal will be monitored to ensure user compliance and prevent misuse of the portal.
- This prototype portal will be undergoing testing and enhancements, based on feedback from users until Q1 2019.



الهيئة العامة للطيران المدني
GENERAL CIVIL AVIATION AUTHORITY



ATM Data & Cyber Security Portal

- This portal has been developed from scratch and is fully customizable.
- We will be hosting the site on a dedicated, secured server at SZC and access and site issues can be reported to the adcs@szc.gcaa.ae.
- The address for this portal is <https://www.adcsportal.com>
- The planned implementation date for the portal will be will be in conjunction with MIDANPIRG 17.



ADCS Portal – Home Page

No user logged in –
Read only mode

Home Page - ATM DATA x

Secure | https://www.adcsportal.com/Default

ATM DATA AND CYBER SECURITY PORTAL

Register Log in

الهيئة العامة للطيران المدني
GENERAL CIVIL AVIATION AUTHORITY

Search...

- Dashboard
- Categories
- Useful links

Top 6 REPORTED INCIDENT TYPES

| | | | | | |
|------------------------------|------------------------------|------------------------------|------------------------------|------------------------------|------------------------------|
| 3 | 1 | 1 | 1 | 1 | 1 |
| Botnet Attacks | Backdoor Attacks | Adware Attacks | Email Spoofing | Fatigue Issues | SQL Injections |
| View Details | View Details | View Details | View Details | View Details | View Details |

Category wise reported incidents report

| Attack type | Number |
|------------------|--------|
| Adware Attacks | 1 |
| Backdoor Attacks | 1 |
| Botnet Attacks | 3 |
| Email Spoofing | 1 |
| Fatigue Issues | 1 |
| Injections | 1 |

Last 8 reported incidents

| ID | Attack type | Detail |
|----|------------------|------------------------|
| 8 | Email Spoofing | Detail |
| 7 | Backdoor Attacks | Detail |
| 6 | Fatigue Issues | Detail |
| 5 | Botnet Attacks | Detail |
| 4 | Botnet Attacks | Detail |
| 3 | Adware Attacks | Detail |
| 2 | SQL Injections | Detail |
| 1 | Botnet Attacks | Detail |

Dashboard view of the various reported attacks/events

Quick access for last 8 reported events



ADCS Portal – Registration Page

ATM DATA AND CYBER SECURITY PORTAL

Register Log in

Search...

Dashboard

Categories

- View all Rported incidents
- Network & Systems Attacks
- View all Network & Systems Attacks
- Botnets
- Malwares
- Ransomware
- Worms & Trojans
- DDoS
- Registry Attacks

Sign up form

Your Name
Enter Full Name

Your Email
Enter Email

Password
Enter Password

Company Name
Enter Company

Designation
Enter Designation

Country
Select Country

Register

All fields are mandatory and subject to verification.



ADCS Portal – Registration Process

Secure | <https://www.adcsportal.com/firmconfirmation>

- Application submitted.
- A verification email is then sent to the user for approval.
- Once the user approves the link an email is sent to the ADCS Admin for final approval.
- Once approved by ADCS Admin the user receives an email notification and the account is active.



Thank You!

Thank you for your ATM Data and Cyber Security Portal registration application. Your application has been received and is under review. You shall receive an email upon completion of this request. If you cannot find the email in your inbox, kindly check your spam or junk email folder.



ADCS Portal – Home Page & User Login

User logged in –
Read/Write
mode

The screenshot shows the ADCS Portal home page. At the top, there is a navigation bar with the text "ATM DATA AND CYBER SECURITY PORTAL" and a user greeting "Welcome! CNS Duty Engineer" with a "Log Out" link. On the left, there is a sidebar menu with options: "Dashboard", "Categories", "Useful links", "Submit your incident", and "Forum Area". A search bar is also present. The main content area is titled "Top 6 REPORTED INCIDENT TYPES" and displays six cards with the following counts: Botnet Attacks (3), Backdoor Attacks (1), Adware Attacks (1), Email Spoofing (1), Fatigue Issues (1), and SQL Injections (1). Below this is a "Category wise reported incidents report" bar chart showing the same data. To the right, there is a table titled "Last 8 reported incidents" with columns for ID, Attack type, and Detail.

| Incident Type | Count |
|------------------|-------|
| Botnet Attacks | 3 |
| Backdoor Attacks | 1 |
| Adware Attacks | 1 |
| Email Spoofing | 1 |
| Fatigue Issues | 1 |
| SQL Injections | 1 |

| Attack type | Number |
|------------------|--------|
| Adware Attacks | 1 |
| Backdoor Attacks | 1 |
| Botnet Attacks | 3 |
| Email Spoofing | 1 |
| Fatigue Issues | 1 |
| SQL Injections | 1 |

| ID | Attack type | Detail |
|----|------------------|------------------------|
| 8 | Email Spoofing | Detail |
| 7 | Backdoor Attacks | Detail |
| 6 | Fatigue Issues | Detail |
| 5 | Botnet Attacks | Detail |
| 4 | Botnet Attacks | Detail |
| 3 | Adware Attacks | Detail |
| 2 | SQL Injections | Detail |
| 1 | Botnet Attacks | Detail |

Submission of incidents and the forum are available when user is logged in.



ADCS Portal – Submission of an Incident

INCIDENT REPORTING FORM

GENERAL INFORMATION

Authority Name:

Submitted by: Type of attack: Select Attack Type

Date of incident: Time of incident:

INCIDENT DETAILS

Source IP: Source country: Select Country

Target hostname: Target OS: Select OS

Target application: Attack status: Select Status

Attack Details:

IMPACT DETAILS & REMEDY

Attack Impact: Select Impact Attack Cause: Select Cause

Attack Remedy: Select Remedy

Remedy Details:

PREVENTION DETAILS

If you were able to prevent the attack, kindly elaborate how and what made it possible for you to prevent it?

LESSONS LEARNIT

Incident reporting form.
The more information that is added the more robust and comprehensive the database will be.



الهيئة العامة للطيران المدني
GENERAL CIVIL AVIATION AUTHORITY



ADCS Portal – Forum Page

ATM DATA AND CYBER SECURITY PORTAL

Welcome! CNS Duty Engineer Log Out

الهيئة العامة للطيران المدني
GENERAL CIVIL AVIATION AUTHORITY

Search... Q

- Dashboard
- Categories <
- Useful links <
- Submit your incident
- Forum Area <

Sub your post

Post form

Title

Message

Post

© 2018 - SZC GCAA



ADCS Portal – Forum Post example

ATM DATA AND CYBER SECURITY PORTAL Welcome! CNS Duty Engineer [Log Out](#)

الهيئة العامة للطيران المدني
GENERAL CIVIL AVIATION AUTHORITY

Search...

- [Dashboard](#)
- [Categories](#) <
- [Useful links](#) <
- [Submit your incident](#)
- [Forum Area](#) <

Forum discussion board

→

Post created by user

→

Comments posted by various users

→

Post Comments

Post form

Title

Message
Hi all. Just a notification for all, we have received a suspicious email and web link from an a company called ANSPstarsolutions that supposedly provides ANSP software for ATFM solutions.
Has anyone on the forum heard of this company and are they a legitimate company as I cannot get a lot of information online about them?

Comments

CNS User
6/21/2018 9:23:43 AM
Yes we have received the same email and web link from this company. We went and did an MX record lookup on their domain and it is found to be a fake website. We suggest that you avoid opening any links and files received from them

Shahzad
6/21/2018 10:17:04 AM
Hello, It is never advisable to open any link or attachment which you are not aware of even if it comes from apparently a legitimate company/website because phishing scams usually contain spoofed email addresses of legitimate companies as well which may lead to malicious websites. We would suggest to always redirect such emails to your IT/Security department for analyses and investigation purposes and never try opening them yourself. Speaking about this specific email you mentioned, we did a little bit of investigation and can confirm it a phishing scam email as the sender email address has failed the reverse DNS lookup, thereby making it fake/spoofed domain

© 2018 - SZC GCAA



الهيئة العامة للطيران المدني
GENERAL CIVIL AVIATION AUTHORITY



ADCS Portal Enhancements

- An updated and more comprehensive forum
- More robust backend configuration
- Updating of submitted tickets by the respective user.



الهيئة العامة للطيران المدني
GENERAL CIVIL AVIATION AUTHORITY



Conclusion

- The ADCS Portal is available online and states are urged to register and provide feedback on additional enhancements.
- The use of this portal is to share knowledge in conjunction with the MSB's and will ensure a far more robust and secure data connectivity within the region.
- There is no 100% secure cyber solution available however having the best possible processes and diligence in place will greatly improve our resilience to attacks and ensure safe air navigation services within the MID region.



الهيئة العامة للطيران المدني
GENERAL CIVIL AVIATION AUTHORITY

