Phishing Analysis Report - 003

Case Number: 003
Report By: Rishab H Shorey
Documented on: 12/15/2002
File Name: Attachment-01
File Link: https://bazaar.abuse.ch/download/c5a8e91cbe9b76da5bf8/

Headers

==========

Language:
Spanish

Date of Email:
October 11, 2025

To: N/A (Phishing POT)
From: Jacqueline Salazar (PDF Content)

Subject Line:
N/A

Return-Path:
N/A

Sender IP:
172.67.157.25

ASN Information
AS13335 CLOUDFLARENET

Resolve Host:

Message-ID:
N/A (This is a attachment analysis File)

E-Mail Authentication Details
N/A

URLs

==========

Fanged URL:
hxxps[://]ct[.]almacencancuns[.]pro/0SEN711

Attachments

==========

Attachment Name:
3afef6872b721b25349bd9083f46b61461c022eab3f46354ac92dff4a2a6b881.pdf

Attachment Link:
3afef6872b721b25349bd9083f46b61461c022eab3f46354ac92dff4a2a6b881 - rishab shorey.pdf

MD5:
e5007368ce88eea1cd7890e5f142c797

SHA1:
d454f56be3f3eee2912db68c67dcbde0b3ca1373

SHA256:
3afef6872b721b25349bd9083f46b61461c022eab3f46354ac92dff4a2a6b881

Description

==========

An email attachment ticket was raised, due to which the analysis of the attachment begins by extracting raw information of the cover letter which is smartly given with a link of a portfolio that is a potential Network based IOC's.

The attempt was to send a portfolio to a modelling agency. It could be sent to an advertising agent or a known modeling Spanish agency , by setting up a tempting malicious "Honey Trap".

Tools Used For Analysis

==========

- URL Void
- Virus Total
- Threat Cop
- URL2PNG
- PDF2GO
- Cisco Threat Intelligence
- Google Translate
- Hybrid Analysis

Artifact Analysis

==========

Sender Analysis:
The sender's profile doesn't seem legitimate as the senders TLD doesn't seem known or heard before but considering the IP belong to a known and accountable service. Hence, it could be the only reason as to why that email has been sent over, by passing all authentication checks.

Fanged URL:
hxxps[://]ct[.]almacencancuns[.]pro/0SEN711

URL Analysis:
After extracting important Network IOC (IP address) and conducting a through look up the URL has undergone multiple redirect and ends up landing on a fake Error Page, which is created using icons, images. The status code is 403. We have used tools to identify and confirm that the there is positive signs of Malicious Activity. It mostly is a spyware attempted to be uploaded onto the system. There is JS scripts hidden among the file probably upon clicking which has been identified that could cause a potential harm to the system

Attachment Analysis:
The attachment is a PDF file and it has trojan, and spyware embedded into the file. Users who intent to download it from the mail could potentially be exploited to this malicious attack.

Verdict

==========

This could be a serious threat towards any of big known modelling agencies in Spain. There contains spyware and trojan in the PDF and suspicious JS scripts running in the link which could potentially make the system crash or access some files of the user. There was also a file path after extracting the raw contents of the file which could most likely be linked to the portfolio button. These red flags, identified is a serious threat and potential to harm the victim machine it was sent on.

E-Mail Classification (Based on Attachment, Links or Redirect)

==========

High (Should try containing and sent further to L2 for overview)

Defense Actions

==========

Considering it was a Spyware and Trojan malicious file sent to the victim machine we aren't sure to which pool of people the email or the file has been sent. The mode of transportation seems a mail and hence we take the following measures:

- We make sure that we block irrelevant TLD which isn't verified which has never been sent or seen in the official database. We implement firewall rules to practice good security, and we ensure that all the systems firewalls are up and running

- We send a immediate full system scan, and removing files specially with the string name mentioned.

- We also ensure to enable rules for only accepting files from models who follow certain format as mentioned in the rules book.

- We take the necessary steps to ensure every endpoint is up to date with their security patches.

- We ensure that there is no kind of process which are running behind the scenes.

- We give prompt immediate actions to change passwords, and ask every user to enable MFA.

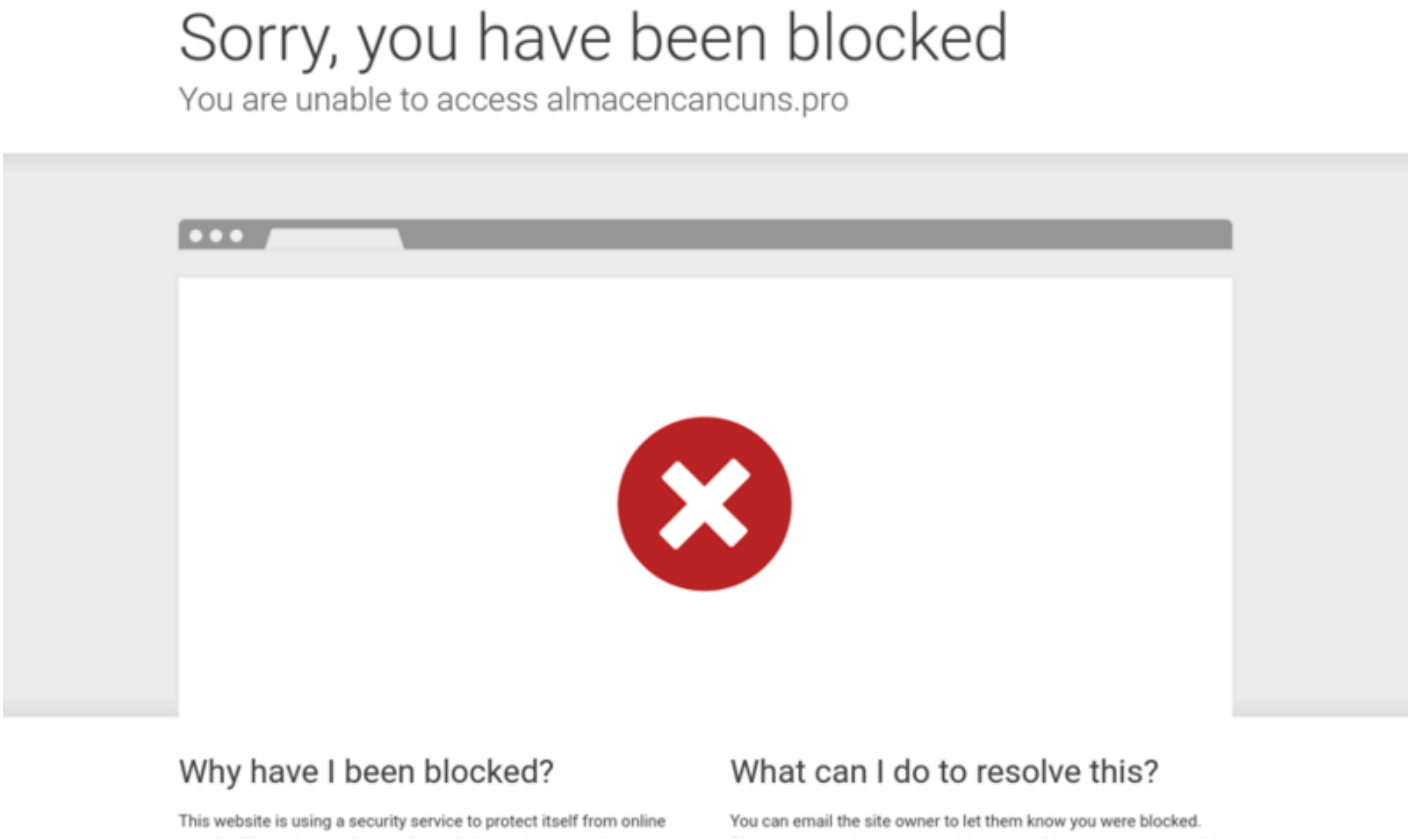
Rishab H Shorey

_____

Image For Reference

==========

Attachment for Site Pictures:



Attachment for File Preview:

Presentacion - Jacqueline Salazar

Estimado(a) senor(a):

Mi nombre es **Jacqueline Salazar** y soy modelo de lenceria. He seleccionado algunas imagenes que reflejan mi estilo, mi elegancia y la forma en que transmito confianza frente a la camara.

Cada sesion captura una energia unica y una historia detras de cada mirada. Prefiero que las imagenes hablen por si solas... pero estoy segura de que despertaran su curiosidad.

Le invito a descubrir una parte de mi trabajo que combina profesionalismo, sensualidad y actitud.

VER MI PORTAFOLIO