


**ID:** 502674
**Sample Name:** Official notification.jpg
**Cookbook:** default.jbs
**Time:** 08:52:37
**Date:** 14/10/2021
**Version:** 33.0.0 White Diamond

# Table of Contents


Table of Contents 2
Windows Analysis Report Official notification.jpg 3
- Overview 3
  - General Information 3
  - Detection 3
  - Signatures 3
  - Classification 3
- Malware Configuration 3
- Yara Overview 3
- Sigma Overview 3
- Jbx Signature Overview 3
- Mitre Att&ck Matrix 4
- Antivirus, Machine Learning and Genetic Malware Detection 4
  - Initial Sample 4
  - Dropped Files 4
  - Unpacked PE Files 4
  - Domains 4
  - URLs 4
- Domains and IPs 4
  - Contacted Domains 4
  - Contacted IPs 4
- General Information 4
- Simulations 5
  - Behavior and APIs 5
- Joe Sandbox View / Context 5
  - IPs 5
  - Domains 5
  - ASN 5
  - JA3 Fingerprints 5
  - Dropped Files 5
- Created / dropped Files 5
- Static File Info 6
  - General 6
  - File Icon 6
- Network Behavior 6
- Code Manipulations 6
- Statistics 6
- System Behavior 6
- Disassembly 6


Copyright Joe Security LLC 2021

# Windows Analysis Report Official notification.jpg

## Overview

### General Information

| | |
|---|---|
| Sample Name: | Official notification.jpg |
| Analysis ID: | 502674 |
| MD5: | 5977a9dd06aad2.. |
| SHA1: | dabb0d916acd3b.. |
| SHA256: | aa3c3bf3e7ae7e4. |

**Errors**

⚠ Nothing to analyse, Joe Sandbox has not found any analysis process or sample

⚠ Corrupt sample or wrongly selected analyzer. Details: 80040153

### Detection

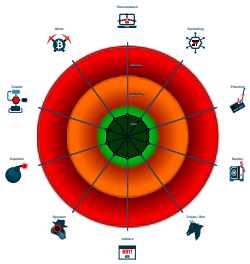



| | |
|---|---|
| Score: | 0 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 80% |

### Signatures

**No high impact signatures.**

### Classification



## Malware Configuration

**No configs have been found**

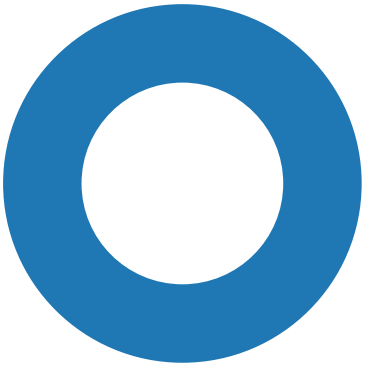
## Yara Overview

**No yara matches**

## Sigma Overview

**No Sigma rule has matched**

## Jbx Signature Overview



● System Summary

Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

## Mitre Att&ck Matrix

**No Mitre Att&ck techniques found**

## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| Official notification.jpg | 0% | Virustotal | | Browse |
| Official notification.jpg | 0% | ReversingLabs | | |

### Dropped Files

**No Antivirus matches**

### Unpacked PE Files

**No Antivirus matches**

### Domains

**No Antivirus matches**

### URLs

**No Antivirus matches**

## Domains and IPs

### Contacted Domains

**No contacted domains info**

### Contacted IPs

**No contacted IP infos**

## General Information

| | |
|---|---|
| Joe Sandbox Version: | 33.0.0 White Diamond |
| Analysis ID: | 502674 |
| Start date: | 14.10.2021 |
| Start time: | 08:52:37 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 1m 49s |

Copyright Joe Security LLC 2021

| | |
|---|---|
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | Official notification.jpg |
| Cookbook file name: | default.jbs |
| Analysis system description: | Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211 |
| Number of analysed new started processes analysed: | 1 |
| Number of new started drivers analysed: | 0 |
| Number of existing processes analysed: | 0 |
| Number of existing drivers analysed: | 0 |
| Number of injected processes analysed: | 0 |
| Technologies: | • EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | UNKNOWN |
| Classification: | unknown0.winJPG@0/0@0/0 |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Unable to launch sample, stop analysis |
| Warnings: | Show All<br>• Exclude process from analysis (whitelisted): dllhost.exe<br>• Excluded IPs from analysis (whitelisted): 23.203.141.148<br>• Excluded domains from analysis (whitelisted): e12564.dspb.akamaiedge.net, store-images.s-microsoft.com, store-images.s-microsoft.com-c.edgekey.net |
| Errors: | • Nothing to analyse, Joe Sandbox has not found any analysis process or sample<br>• Corrupt sample or wrongly selected analyzer. Details: 80040153 |

# Simulations

## Behavior and APIs

**No simulations**

# Joe Sandbox View / Context

## IPs

**No context**

## Domains

**No context**

## ASN

**No context**

## JA3 Fingerprints

**No context**

## Dropped Files

**No context**

# Created / dropped Files

Copyright Joe Security LLC 2021

**No created / dropped files found**

# Static File Info

## General

| | |
|---|---|
| File type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 2481x3508, frames 3 |
| Entropy (8bit): | 7.883924601268516 |
| TrID: | • JFIF JPEG Bitmap (4007/3) 50.02%<br>• JPEG Bitmap (3003/1) 37.49%<br>• MP3 audio (1001/1) 12.50% |
| File name: | Official notification.jpg |
| File size: | 1237275 |
| MD5: | 5977a9dd06aad2ec899c66f477034c3c |
| SHA1: | dabb0d916acd3b7a41d5ed7169ec5bcb3f676dc8 |
| SHA256: | aa3c3bf3e7ae7e4c4a8bf46b5672507c1079e21c2f384f64f2941777d0ac2c40 |
| SHA512: | e2829b7265ea8a2b1542ba23cd6e26d78d2c364421eb946f3a93b3d886bfe8b73e7b474d9cacc5888167708a4e9529f40392fea2c6083a459d715a6c76b4418a |
| SSDEEP: | 24576:pTm5Ad8u6lcK4W9hNK4BxSfQCtsyQJi2CDrbntb:M3u6lB9hceO/ntb |
| File Content Preview: | .....JFIF.....,..... ICC_PROFILE.....mntrRGB XYZ .....acspAPPL.....-..... .....desc.....\|cprt...x...(wtpt.....bkpt.....rXYZ.....gXYZ.....bXYZ.....r |

## File Icon



| | |
|---|---|
| Icon Hash: | 74f0f0e4c6d6e0e4 |

# Network Behavior

**No network behavior found**

# Code Manipulations

# Statistics

# System Behavior

# Disassembly