

JOESandbox Cloud BASIC



**ID:** 753411

**Sample Name:** Payment Advice  
for Imax November 23, 2022,  
1%3A46%3A16 PM.txt

**Cookbook:** default.jbs

**Time:** 19:18:55

**Date:** 24/11/2022

**Version:** 36.0.0 Rainbow Opal

# Table of Contents

Table of Contents	2
Windows Analysis Report Payment Advice for Imax November 23, 2022, 1%3A46%3A16 PM.txt	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Yara Signatures	3
Sigma Signatures	3
Snort Signatures	3
Joe Sandbox Signatures	4
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	5
Initial Sample	5
Dropped Files	5
Unpacked PE Files	6
Domains	6
URLs	6
Domains and IPs	6
Contacted Domains	6
World Map of Contacted IPs	6
General Information	6
Warnings	6
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	7
IPs	7
Domains	7
ASNs	7
JA3 Fingerprints	7
Dropped Files	7
Created / dropped Files	7
Static File Info	7
General	7
File Icon	8
Network Behavior	8
Statistics	8
System Behavior	8
Analysis Process: notepad.exePID: 2156, Parent PID: 3452	8
General	8
File Activities	8
Disassembly	8

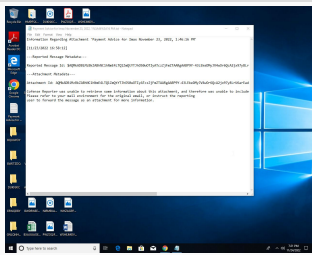
# Windows Analysis Report

Payment Advice for Imax November 23, 2022, 1%3A46%3A16 PM.txt

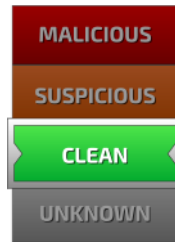
## Overview

### General Information

Sample Name:	Payment Advice for Imax November 23, 2022, 1%3A46%3A16 PM.txt
Analysis ID:	753411
MD5:	32c514a2cccc4d..
SHA1:	2a626cb812d5ad..
SHA256:	4641d4821a3be2..



### Detection

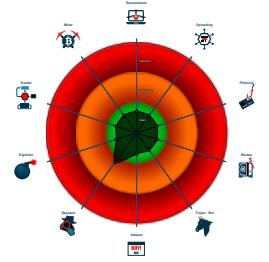


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

### Signatures

Queries the volume information (nam...

### Classification



## Process Tree

- System is w10x64
- notepad.exe (PID: 2156 cmdline: "C:\Windows\system32\notepad.exe" C:\Users\user\Desktop\Payment Advice for Imax November 23, 2022, 1%3A46%3A16 PM.txt MD5: BB9A06B8F2DD9D24C77F389D7B2B58D2)
- cleanup

## Malware Configuration

No configs have been found

## Yara Signatures

No yara matches

## Sigma Signatures

No Sigma rule has matched

## Snort Signatures

No Snort rule has matched

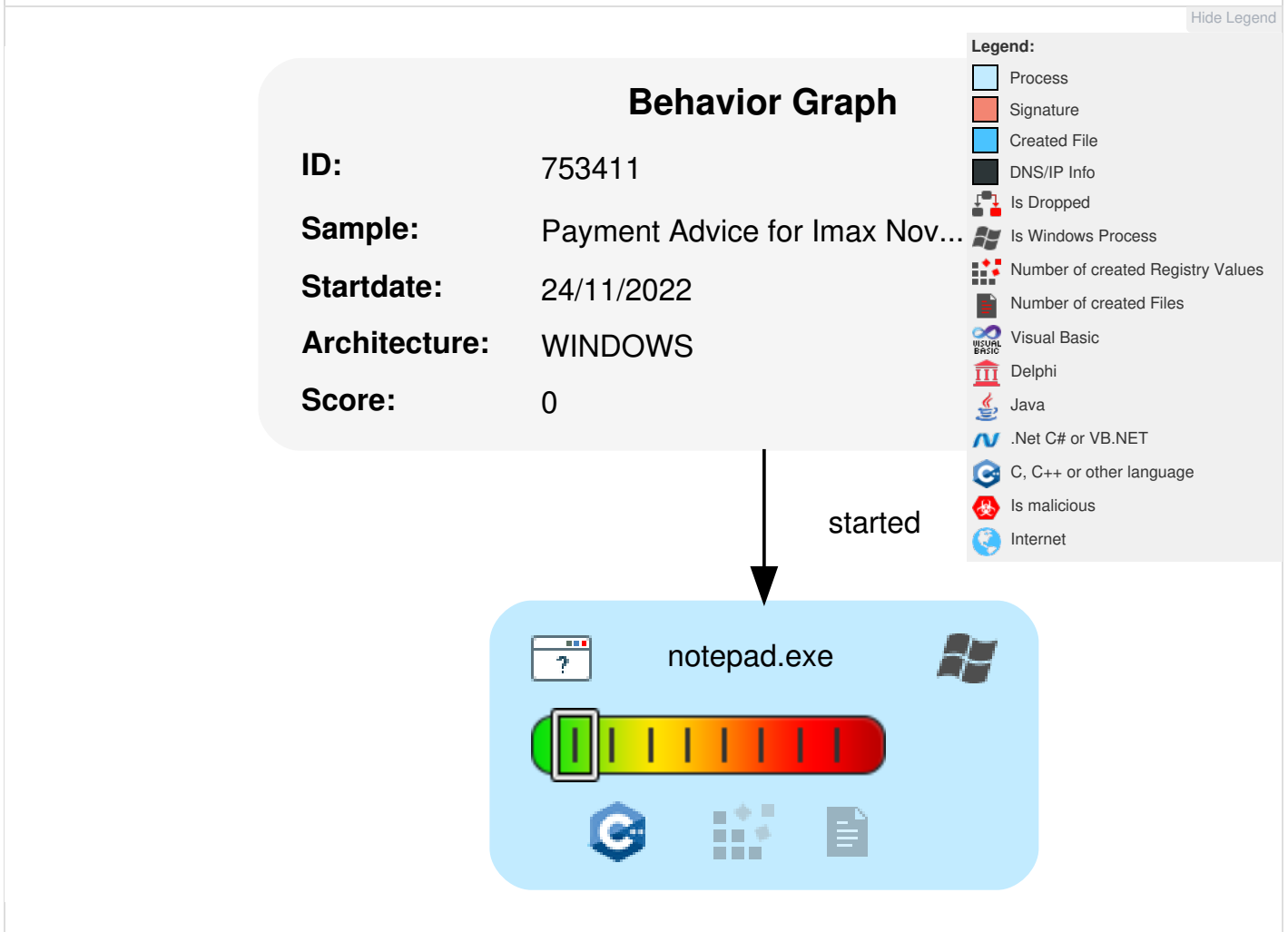
## Joe Sandbox Signatures

There are no malicious signatures, [click here to show all signatures](#).

## Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Direct Volume Access	OS Credential Dumping	System Information Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

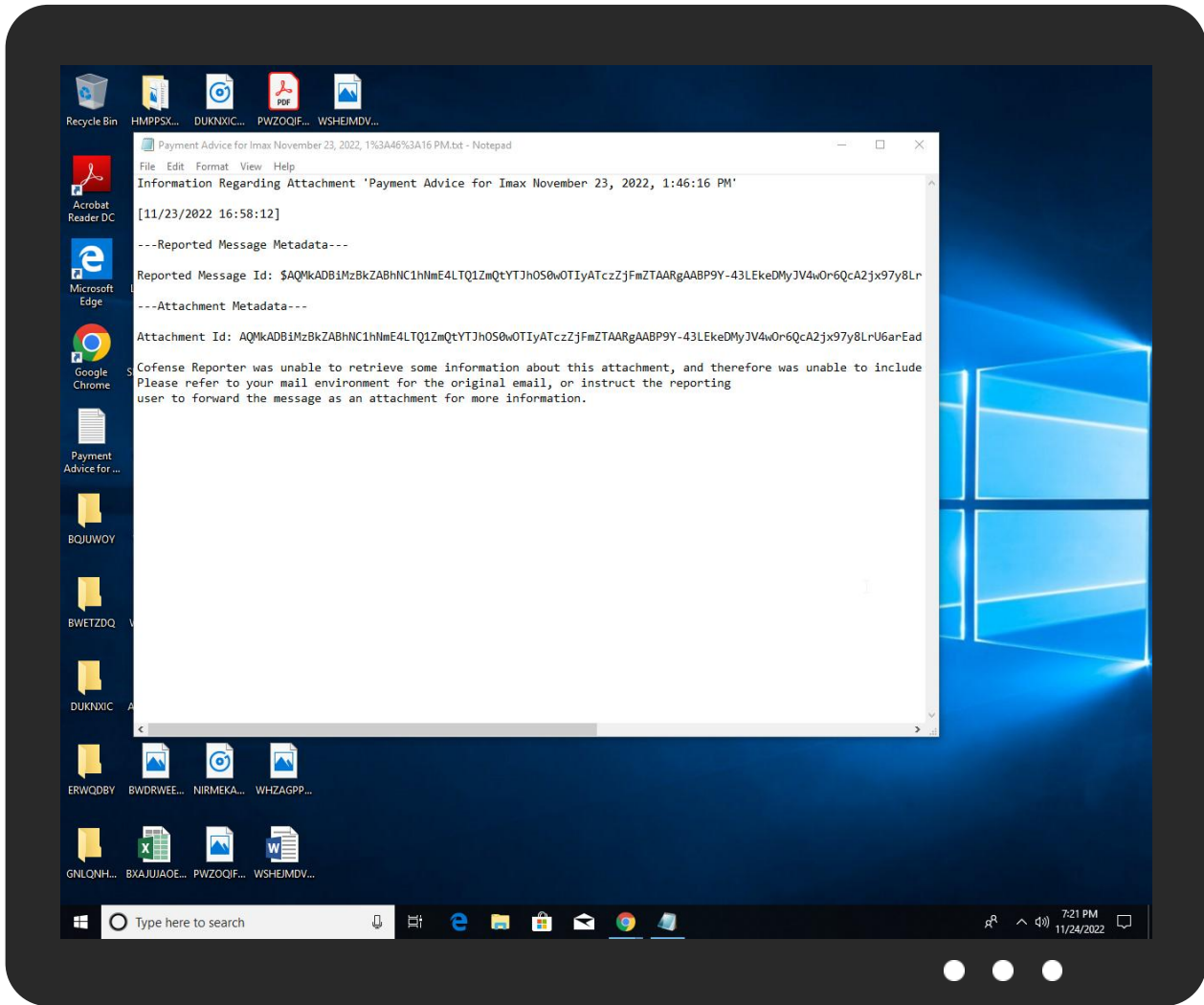
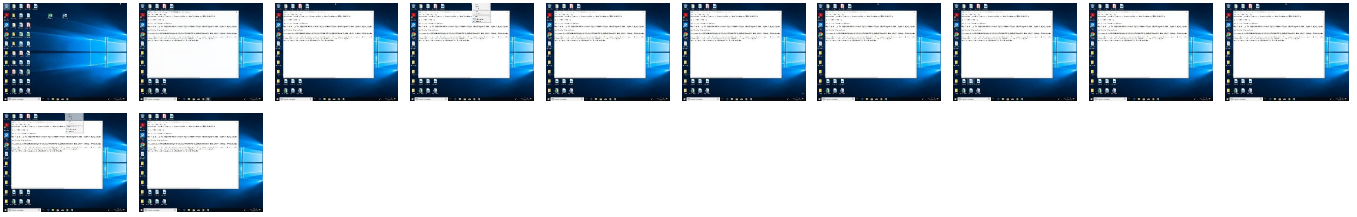
## Behavior Graph



## Screenshots

### Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

No Antivirus matches

### 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

### World Map of Contacted IPs

⊘ No contacted IP infos

## General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	753411
Start date and time:	2022-11-24 19:18:55 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Payment Advice for Imax November 23, 2022, 1%3A46%3A16 PM.txt
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	12
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:	<ul style="list-style-type: none"><li>• HCA enabled</li><li>• EGA enabled</li><li>• HDC enabled</li><li>• AMSI enabled</li></ul>
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.winTXT@1/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	<ul style="list-style-type: none"><li>• Successful, ratio: 100%</li><li>• Number of executed functions: 0</li><li>• Number of non-executed functions: 0</li></ul>
Cookbook Comments:	<ul style="list-style-type: none"><li>• Found application associated with file extension: .txt</li></ul>


## Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Not all processes were analyzed, report is missing behavior information

- Report size getting too big, too many NtProtectVirtualMemory calls found.


## Simulations

### Behavior and APIs


 No simulations

## Joe Sandbox View / Context


### IPs

 No context


### Domains

 No context


### ASNs

 No context


### JA3 Fingerprints

 No context

### Dropped Files

 No context

## Created / dropped Files

 No created / dropped files found

## Static File Info

### General

File type:	ASCII text, with CRLF line terminators
Entropy (8bit):	5.503841975330305
TrID:	
File name:	Payment Advice for Imax November 23, 2022, 1%3A46%3A16 PM.txt
File size:	857
MD5:	32c514a2cccc4dc45ead40c3f876d7e7
SHA1:	2a626cb812d5add14991989397242070c6584f05
SHA256:	4641d4821a3be256f99bfb07cbfc9b2f77670b91af83fac011a55f2c910a9ecc
SHA512:	747477d18a9c5399b03d5a56fd8e9a8efcd6b9e3c7b63db47846775f9471f2fe5f667d67553df29ea7920ad22820dfd884cc788a3bec581bf1599eb37dfa0f2
SSDEEP:	12:DxPy+ifsMfsoWl6/SuWmyo1zI6/SuWQCiahiE5poT+Ay5yPq5q;l+iEWJW3SuWm7V3SuWN3oiAeyiQ
TLSH:	F3111230635E3477A03FE7E137470F60BD51E91000593DCCAED4118A6252DE663AF0B8
File Content Preview:	Information Regarding Attachment 'Payment Advice for Imax November 23, 2022, 1:46:16 PM'....[11/23/2022 16:58:12].....Reported Message Metadata---.....Reported Message Id: \$AQMkADBiMzBkZABhNC1hNmE4LTQ1ZmQlYtJhOS0wOTlyATczZjFmZTAARgAABP9Y-43LEkeDMYJV4wOr6

## File Icon



Icon Hash: 74f4e4e4e4e4e4e4

## Network Behavior

⊘ No network behavior found

## Statistics

⊘ No statistics

## System Behavior

**Analysis Process: notepad.exe** PID: 2156, Parent PID: 3452

### General

Target ID:	0
Start time:	19:19:48
Start date:	24/11/2022
Path:	C:\Windows\System32\notepad.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\notepad.exe" C:\Users\user\Desktop\Payment Advice for Imax November 23, 2022, 1%3A46%3A16 PM.txt
Imagebase:	0x7ff7296f0000
File size:	245760 bytes
MD5 hash:	BB9A06B8F2DD9D24C77F389D7B2B58D2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

## Disassembly

⊘ No disassembly