ID: 458978
Sample Name: winmail.dat
Cookbook: default.jbs
Time: 23:49:56
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

Windows Analysis Report winmail.dat

Overview

General Information

Sample Name:	winmail.dat
Analysis ID:	458978
MD5:	f400ce74448bae6.
SHA1:	0b3af38a819dd56.
SHA256:	da55960ccd1db7..

Errors

- Nothing to analyse, Joe Sandbox has not found any analysis process or sample
- Corrupt sample or wrongly selected analyzer. Details: 80040153

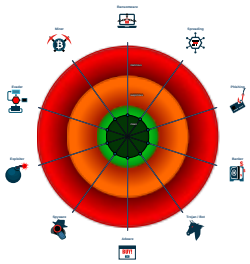
Detection

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

Signatures

No high impact signatures.

Classification



Malware Configuration

No configs have been found

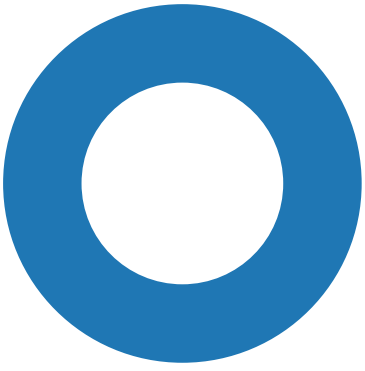
Yara Overview

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
winmail.dat	0%	Virustotal		Browse

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:	458978
Start date:	03.08.2021
Start time:	23:49:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 1m 37s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	winmail.dat
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:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	UNKNOWN
Classification:	unknown0.winDAT@0/0@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Unable to launch sample, stop analysis
Warnings:	Show All • Exclude process from analysis (whitelisted): svchost.exe
Errors:	• Nothing to analyse, Joe Sandbox has not found any analysis process or sample • 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

No created / dropped files found

Static File Info

General

File type:	Transport Neutral Encapsulation Format
Entropy (8bit):	7.115606498151222
TrID:	• Transport Neutral Encapsulation Format (4004/1) 80.00% • XMill compressed XML (1001/1) 20.00%
File name:	winmail.dat
File size:	6006
MD5:	f400ce74448bae6b6326d4cae797ebce
SHA1:	0b3af38a819dd5671e7f29153f126664be268e1a
SHA256:	da55960ccd1db7bc1a39b1d9a47fe174d30619c99935cdb878d4d059e6bbf519
SHA512:	fce0eac95b7e07a3e28827f9d50ff27860158b81a16f622f68d28c227d689dae76d3a0e2d00ddd551955abea93470626275ece1d83ccea978ce698682ba562c0
SSDEEP:	96:olJsjPcPqcPBbGlG/HMc/0LInF8W6yqhenbhdLR759jSWXbAcyT33W6Ey2Nyt+H5:oc2cPqcPBbGwEc/0LIaWMUhdLR99jSWl
File Content Preview:	x.>".....IPM.Microsoft Mail.Note.1.....&.....).....+.....1.....d...PCDFEB09.....Q...k.D.{g.....u.....$.....H

File Icon

Icon Hash:	74f0e4e4e4e4e0e4

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Disassembly