ID: 632518
Sample Name: Swift Confirmation for kmasson.msg
Cookbook: default.jbs
Time: 18:34:53
Date: 23/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

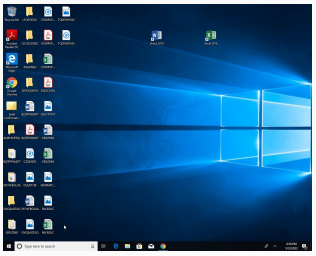
Windows Analysis Report

Swift Confirmation for kmasson.msg

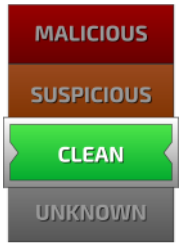
Overview

General Information

Sample Name:	Swift Confirmation for kmasson.msg
Analysis ID:	632518
MD5:	0996450ba30552.
SHA1:	cc49a93bf6f8946..
SHA256:	0e0a1c85a43597..



Detection

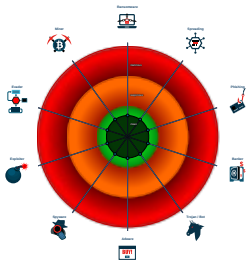


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Program does not show much activi…

Classification



Process Tree

- **System is w10x64**
- OUTLOOK.EXE (PID: 4068 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\OUTLOOK.EXE" /f "C:\Users\user\Desktop\Swift Confirmation for kmasson.msg MD5: 7DD935BA9B57D9D7EFF63C67653E70B5)
- **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

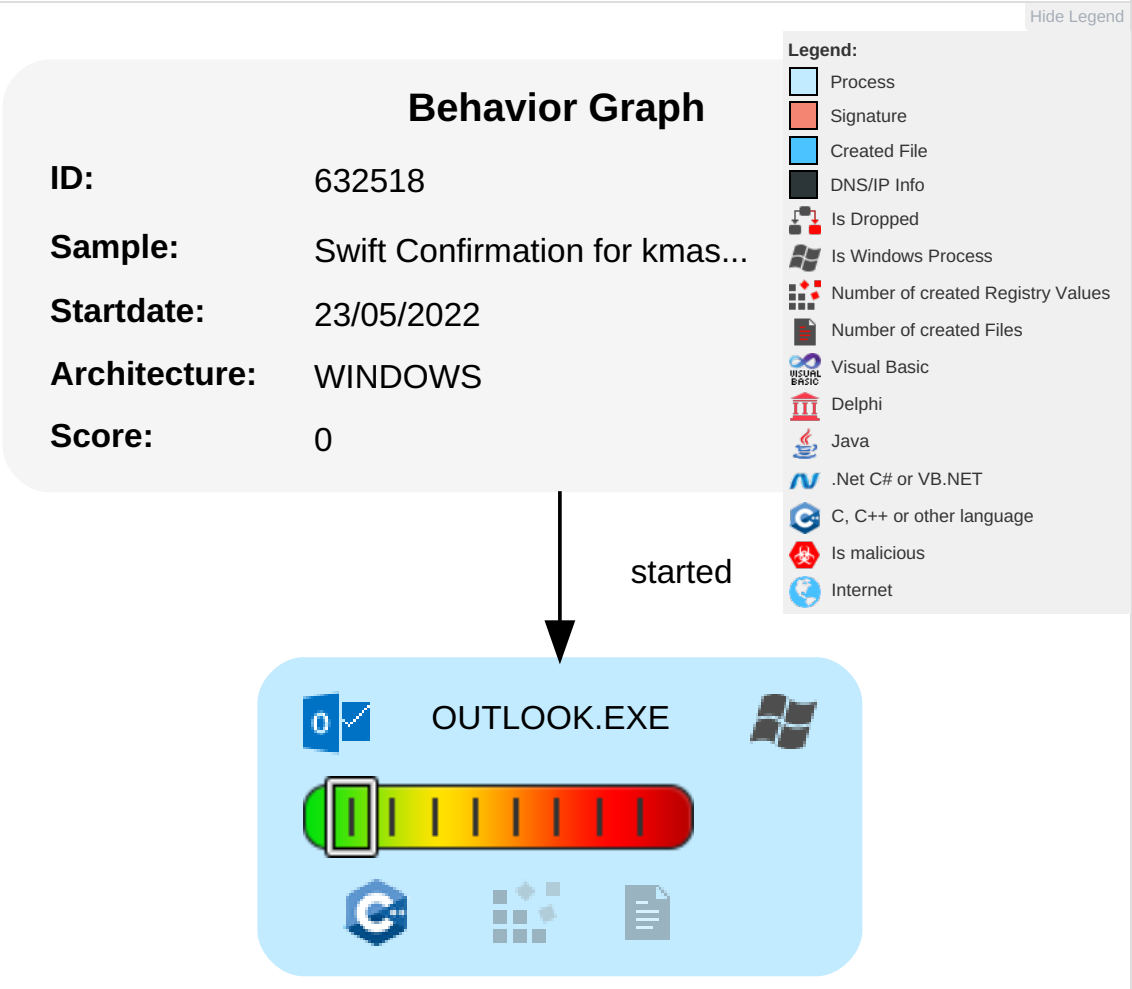
Joe Sandbox Signatures

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

Mitre Att&ck Matrix

No Mitre Att&ck techniques found

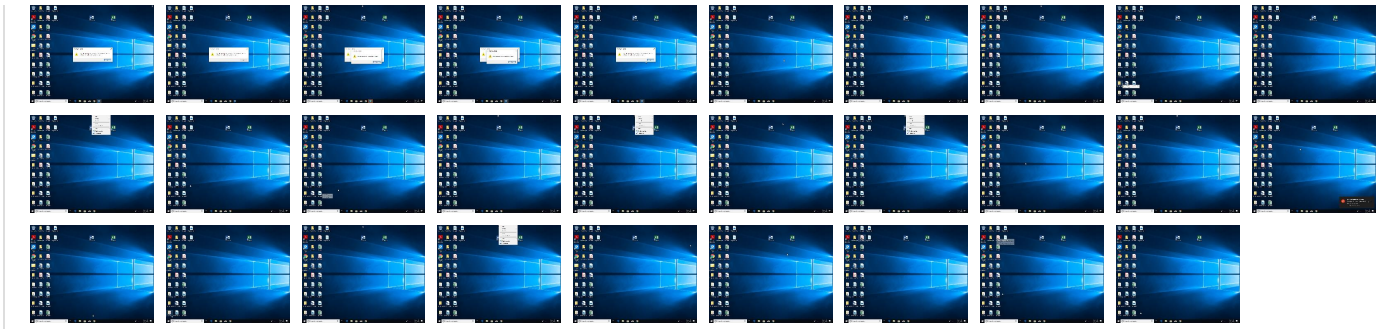
Behavior Graph



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:	34.0.0 Boulder Opal
Analysis ID:	632518
Start date and time: 23/05/202218:34:53	2022-05-23 18:34:53 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Swift Confirmation for kmasson.msg
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:	16
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:	CLEAN
Classification:	clean0.winMSG@1/0@0/0
Cookbook Comments:	• Found application associated with file extension: .msg • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 20.223.24.244
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, arc.msn.com, ris.api.iris.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- Not all processes where analyzed, report is missing behavior information

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:	CDFV2 Microsoft Outlook Message
Entropy (8bit):	6.2333125377401135
TrID:	• Outlook Message (71009/1) 58.92% • Outlook Form Template (41509/1) 34.44% • Generic OLE2 / Multistream Compound File (8008/1) 6.64%
File name:	Swift Confirmation for kmasson.msg
File size:	216576
MD5:	0996450ba305529923ebe63dc9d40329
SHA1:	cc49a93bf6f8946319eab667ac6e0ad5bbe4d9a5
SHA256:	0e0a1c85a4359759eb751607d07b4904029a8a0178bd1d95d57922eec46e87a1
SHA512:	c2672cf6704116a6cfbd5bb89edfa43605a3e73e90835bd5c8b5124ed346cde18f13a1982dd2922b082cee1adbd69baa921aa7e29206c3e2f0a98809901b04aa
SSDEEP:	3072:SjFXdRMaiFIKVvr0NOZ7hFV+yw2B1IyiCFJyrISwVAx8ZoyFF8feTIh1DYFmsxyv:SJrMaiuwZVFVmCPmx8ZZ8feg1DYtyv
TLSH:	4F245C7563EA1572EFB56F703CF6245B2226FCCA3430040F960E77888278ED67991A6D
File Content Preview:	.....>.....y...z...{.....

File Icon

Icon Hash:	bac0f992edfcdf00

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: OUTLOOK.EXE PID: 4068, Parent PID: 1460

General	
Target ID:	0
Start time:	18:36:22
Start date:	23/05/2022
Path:	C:\Program Files (x86)\Microsoft Office\Office16\OUTLOOK.EXE
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Microsoft Office\Office16\OUTLOOK.EXE" /f "C:\Users\user\Desktop\Swift Confirmation for kmasson.msg
Imagebase:	0xcf0000
File size:	23291112 bytes
MD5 hash:	7DD935BA9B57D9D7EFF63C67653E70B5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

No disassembly