ID: 632621
Sample Name:
message_v2.rpmsg
Cookbook: default.jbs
Time: 20:36:37
Date: 23/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

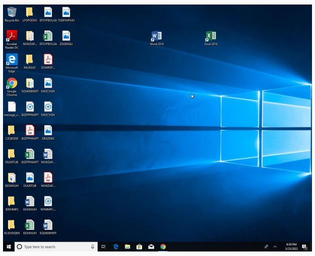
Windows Analysis Report

message_v2.rpmsg

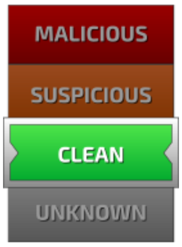
Overview

General Information

Sample Name:	message_v2.rpmsg
Analysis ID:	632621
MD5:	13ddafc6d76f4c4..
SHA1:	5ad15f36a878b6..
SHA256:	b8c268070d1e5e..



Detection

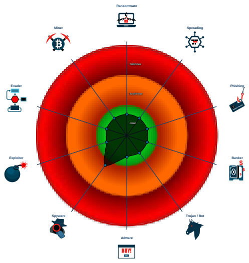


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Program does not show much activi…
- Queries the volume information (nam…
- Monitors certain registry keys / valu…

Classification



Process Tree

- **System is w10x64**
- OpenWith.exe (PID: 7036 cmdline: C:\Windows\system32\OpenWith.exe -Embedding MD5: D179D03728E95E040A889F760C1FC402)
- **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**

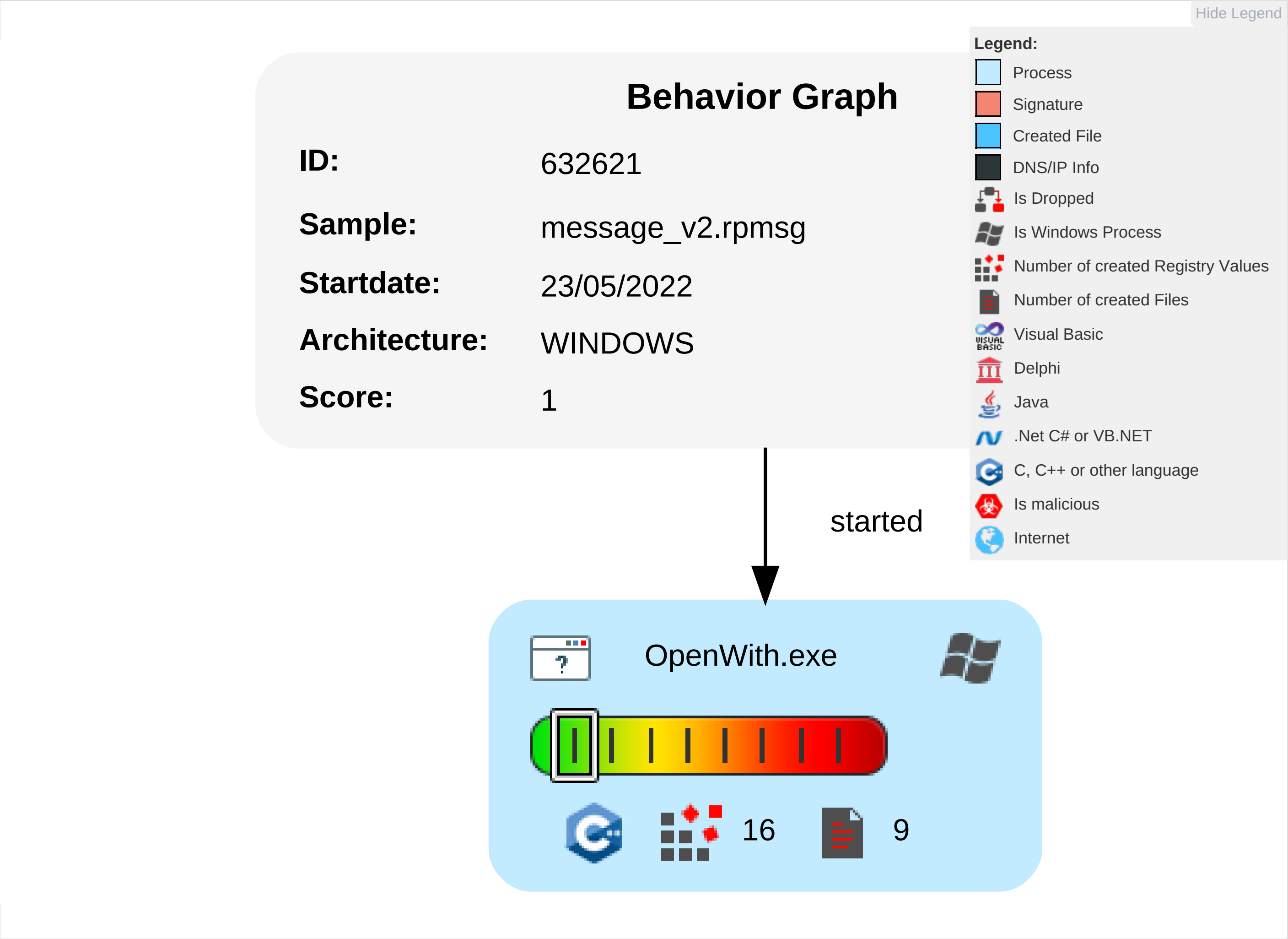
Joe Sandbox Signatures

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	1 Query Registry	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
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	1 File and Directory Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	1 1 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Behavior Graph



Behavior Graph

ID: 632621

Sample: message_v2.rpmsg

Startdate: 23/05/2022

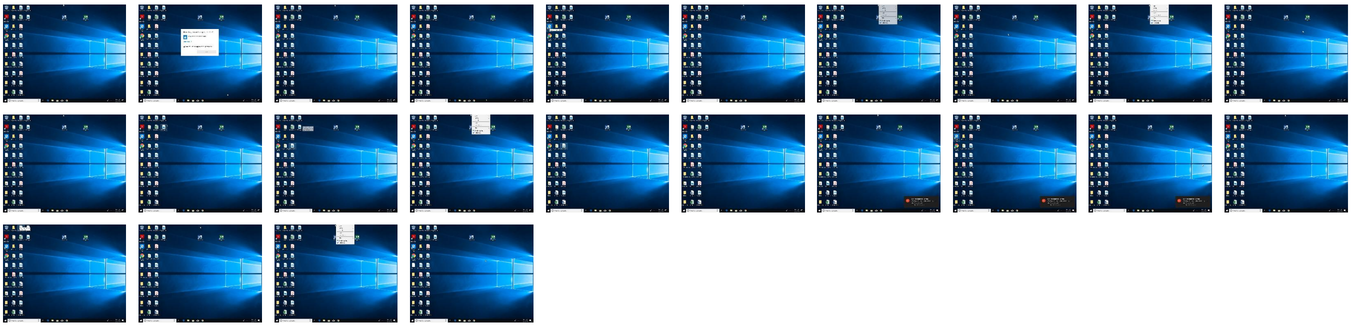
Architecture: WINDOWS

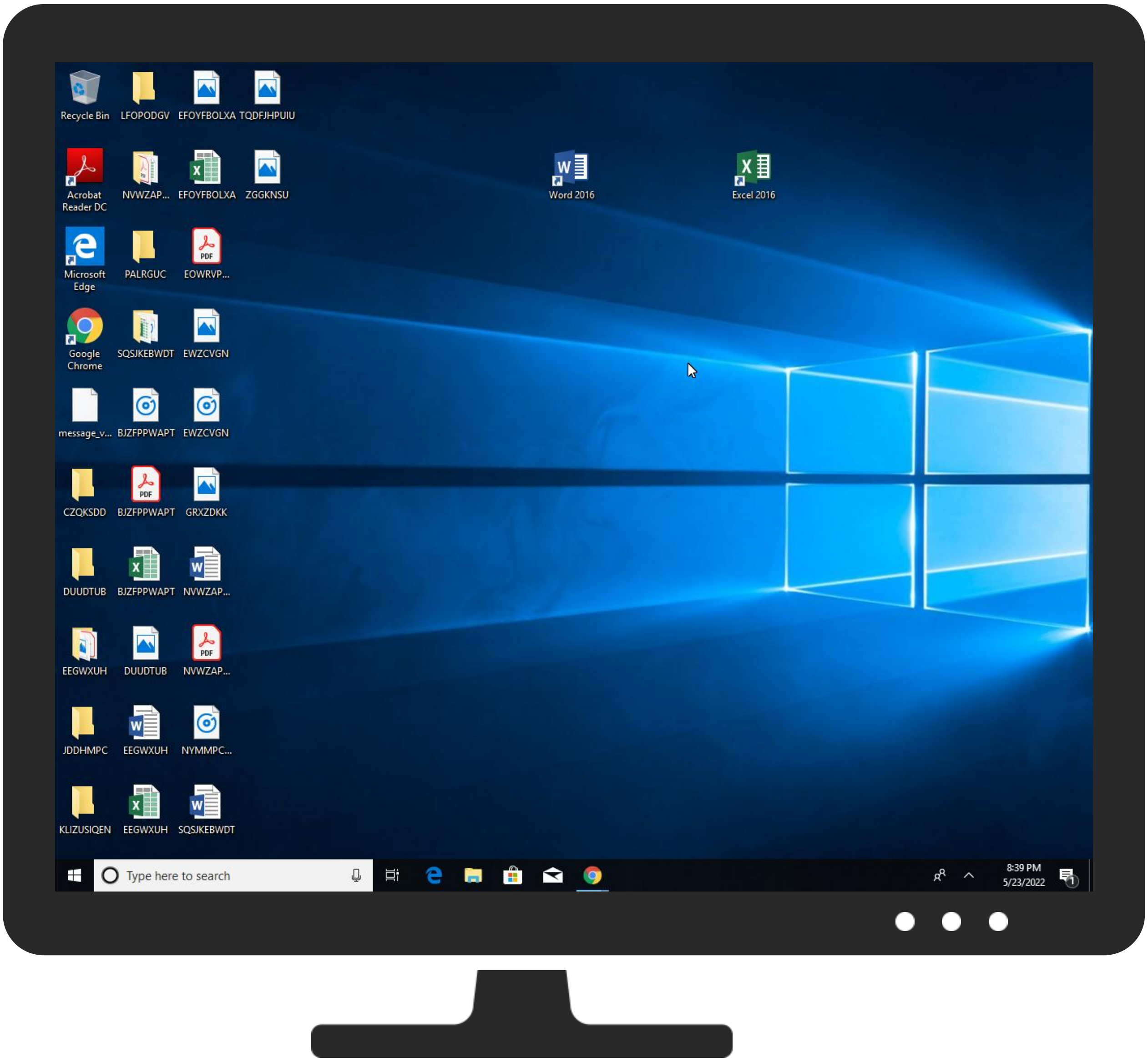
Score: 1

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

Source	Detection	Scanner	Label	Link
message_v2.rpmsg	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**

World Map of Contacted IPs

⊘ **No contacted IP infos**

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	632621
Start date and time: 23/05/202220:36:37	2022-05-23 20:36:37 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	message_v2.rpmsg
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:	21
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:	clean1.winRPMSG@1/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• 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 domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:37:43	API Interceptor	1x Sleep call for process: OpenWith.exe modified

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:	data
Entropy (8bit):	7.983834277312526
TrID:	
File name:	message_v2.rpmsg
File size:	386559
MD5:	13ddafc6d76f4c4e65b2220dc085da69
SHA1:	5ad15f36a878b66665b6546c9bf473c0aabfc4f5
SHA256:	b8c268070d1e5e16162680051dd6a15266a1e21bf0100e3f7310d10c8192b2a3
SHA512:	bd88e8f792625bd8119e2d77b2fcb577e000e0d1c493692ac4681d76bd205e32e17349d57055db28c3774dd183ce1799ce5bfd04b3976fa6da2a3fdd4a947066
SSDEEP:	6144:GAmEfWiFUUzA2frlgdxYkHD3pxDITGaupQtoOmy+nL4HioBpVfY8jdIwsa3L4:r/CM6d+e/IdiQ6Omy+nLSioZac3E
TLSH:	7C8412A9BA800EB3C03282FB9B53F2FB9D9544648581DE95F5C197C92940B5D9CBBF30
File Content Preview:	v..`................x...wX.G...Y.bT<.Q......41A=...`...H1@..b.....]Q..{.QPc..b...K,$jl...e................|3.N.s!6........xj....>s.dz...N}..h4.>....gd.........N?].A^...........c.........{(sP_.lT@.'.. .....@a.AQ.Cq.@I.Bi.AY.CyT@ETBex........>....Z..:..O..

File Icon

Icon Hash:	74f0e4e4e4e4e0e4

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: OpenWith.exe

PID: **7036**, Parent PID: **812**

General

Target ID:	0
Start time:	20:37:43
Start date:	23/05/2022
Path:	C:\Windows\System32\OpenWith.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\OpenWith.exe -Embedding
Imagebase:	0x7ff703930000
File size:	111120 bytes
MD5 hash:	D179D03728E95E040A889F760C1FC402
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	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly