ID: 632521
Sample Name: Velaro-Setup-3.0.1.exe.004
Cookbook: default.jbs
Time: 18:36:55
Date: 23/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

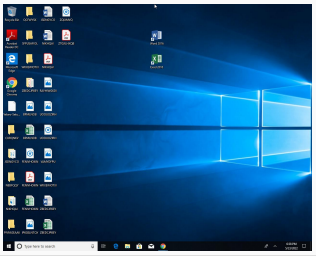
Windows Analysis Report

Velaro-Setup-3.0.1.exe.004

Overview

General Information

Sample Name:	Velaro-Setup-3.0.1.exe.004
Analysis ID:	632521
MD5:	3cb813b471cb8c..
SHA1:	154f6fcfca19795...
SHA256:	0f3cf49c4119770..



Errors

Corrupt sample or wrongly selected analyzer. Details: The RPC server is unavailable.

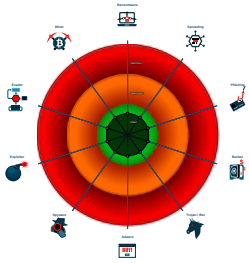
Detection

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

Signatures

Program does not show much activi...

Classification



Process Tree

- **System is w10x64**
- OpenWith.exe (PID: 6384 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

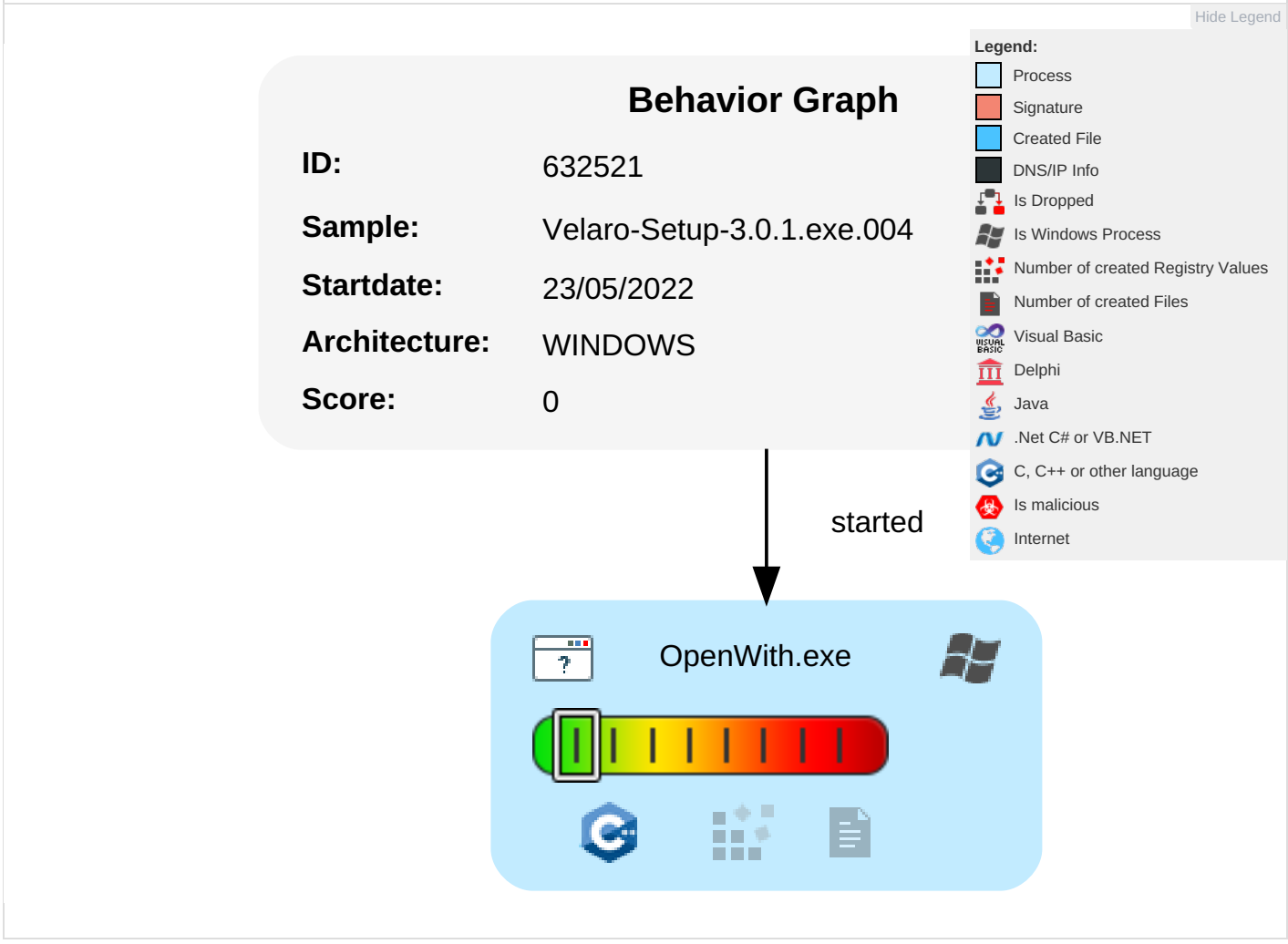
Joe Sandbox Signatures

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 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:	34.0.0 Boulder Opal
Analysis ID:	632521
Start date and time: 23/05/202218:36:55	2022-05-23 18:36:55 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Velaro-Setup-3.0.1.exe.004
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.win004@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 • Unable to launch sample, stop analysis

Errors

- Corrupt sample or wrongly selected analyzer. Details: The RPC server is unavailable.

Warnings

- Excluded IPs from analysis (whitelisted): 20.40.129.122
- Excluded domains from analysis (whitelisted): store-images.s-microsoft.com, arc.trafficmanager.net, iris-de-prod-azsc-frc.francecentral.cloudapp.azure.com, arc.msn.com

Simulations

Behavior and APIs

Time	Type	Description
18:38:09	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):	7.999982973205605
TrID:	
File name:	Velaro-Setup-3.0.1.exe.004
File size:	10485760
MD5:	3cb813b471cb8ca054dc17b2b63fafaa
SHA1:	154f6fcfca197953724da3fc512c04192fe0c1fc
SHA256:	0f3cf49c41197703e373464e4a7be354d179dc91c98441ff9172f5a916b4a586
SHA512:	1332784b574c5ae0f32bd4f7d7a8983cfecf96959995245ac42557f9beeea4732bbd998c13989883b5c65534fad36dd339741cbf7840bfe6f0d5e094a9a80aac
SSDEEP:	196608:59SpoadHdexoGzXQDFBt6h2b7jDUnyMDBi7bVseLvp2AkCucmpJH0N7pGgZ8jP6J:TSpoadHdeCGzGksXjAn54bVtLvp2AFuo
TLSH:	DDB63301FC7A6591685ECEC661E530AB99857BAB8C3149C4E03BA748317BE43DFDE84C
File Content Preview:	|(:.v.s.!.T..d{k...0..c{V?v.3-..7~..U..-...eBl2.....K...M.8..}..a..!.{U..z.s+...%.....M(...M.rT.....9)Q.y.....[..!P..[.,..R..N.....9.n#..y.....<..cE{,m....|.\'d.....; <S*...mZ.R...^....P..n.U3DW....e...0.v[~D....j....LE.4.K^...'.%3C.]..Z..1m5.....U

File Icon

Icon Hash:	74f0e4e4e4e4e0e4

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: OpenWith.exe PID: **6384**, Parent PID: **796**

General	
Target ID:	0
Start time:	18:38:08
Start date:	23/05/2022
Path:	C:\Windows\System32\OpenWith.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\OpenWith.exe -Embedding
Imagebase:	0x7ff79acd0000
File size:	111120 bytes
MD5 hash:	D179D03728E95E040A889F760C1FC402
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly