

JOESandbox Cloud BASIC



ID: 650814
Sample Name: download
Cookbook: default.jbs
Time: 02:34:36
Date: 23/06/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents	2
Windows Analysis Report download	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
Antivirus, Machine Learning and Genetic Malware Detection	4
Initial Sample	5
Dropped Files	5
Unpacked PE Files	5
Domains	5
URLs	5
Domains and IPs	5
Contacted Domains	5
World Map of Contacted IPs	5
General Information	5
Errors	6
Warnings	6
Simulations	6
Behavior and APIs	6
Joe Sandbox View / Context	6
IPs	6
Domains	6
ASNs	6
JA3 Fingerprints	6
Dropped Files	6
Created / dropped Files	6
Static File Info	7
General	7
File Icon	7
Network Behavior	7
Statistics	7
System Behavior	7
Analysis Process: OpenWith.exePID: 4400, Parent PID: 804	7
General	7
Disassembly	8

Windows Analysis Report


download

Overview

General Information

Sample Name:	download
Analysis ID:	650814
MD5:	4842e206e4cfff2..
SHA1:	80c9820ff2efe8a..
SHA256:	2acab1228e8935..
Errors	
⚠ Corrupt sample or wrongly selected analyzer. Details: The interface is unknown.	

Detection

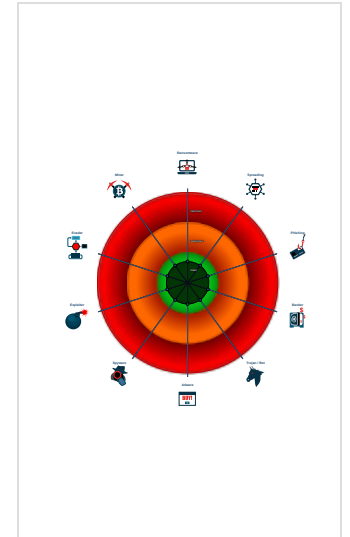


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%


Signatures

Program does not show much activi...

Classification



Process Tree

- System is w10x64
-  OpenWith.exe (PID: 4400 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

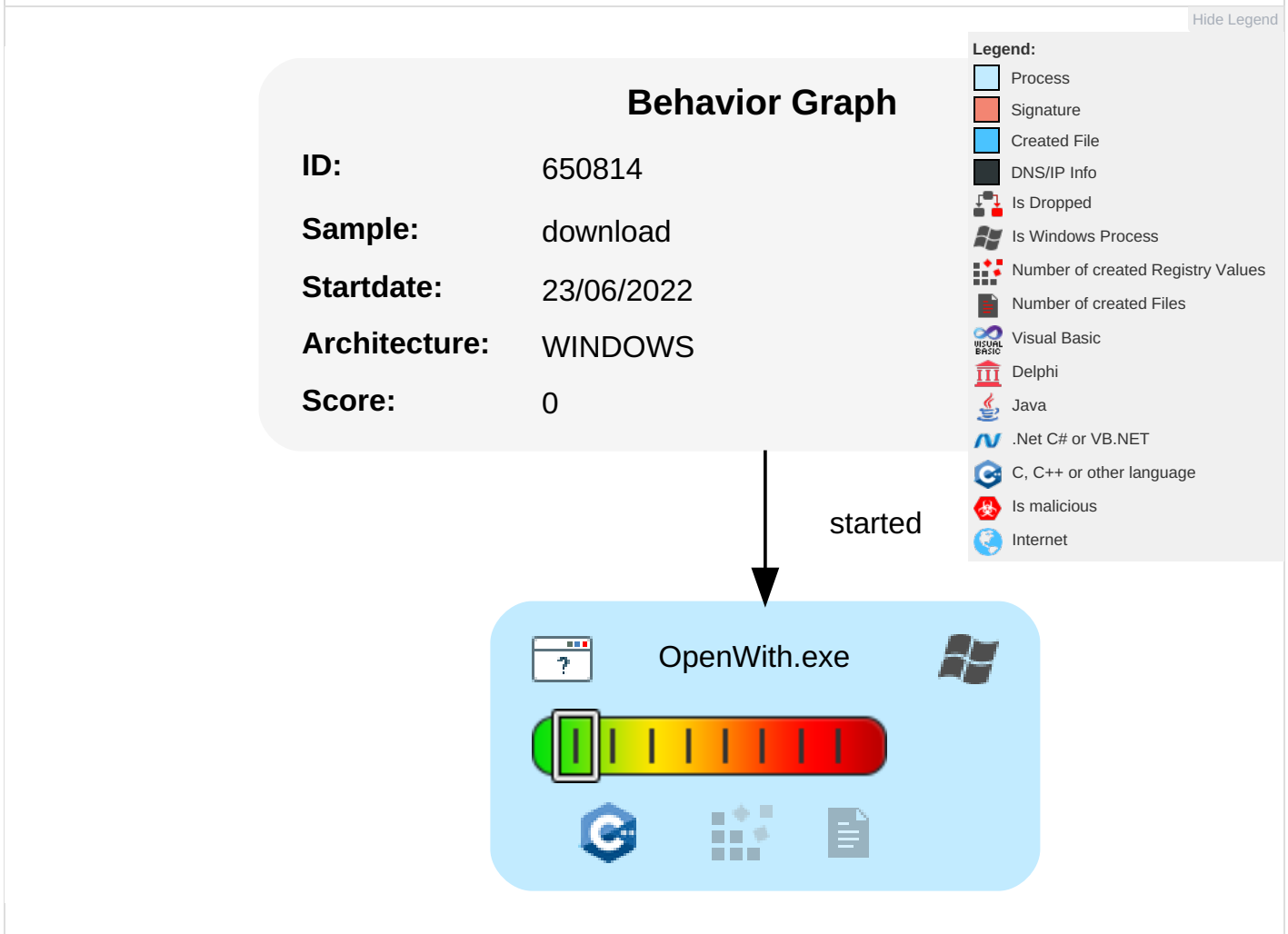
Joe Sandbox Signatures

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





Antivirus, Machine Learning and Genetic Malware Detection


Initial Sample				
Source	Detection	Scanner	Label	Link
download	0%	Virustotal		Browse
download	0%	Metadefender		Browse
download	0%	ReversingLabs		


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:	35.0.0 Citrine
Analysis ID:	650814
Start date and time: 23/06/202202:34:36	2022-06-23 02:34:36 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	download
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:	3
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"> • HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	UNKNOWN

Classification:	unknown0.win@1/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	<ul style="list-style-type: none"> • Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	<ul style="list-style-type: none"> • Adjust boot time • Enable AMSI • Unable to launch sample, stop analysis

Errors

- Corrupt sample or wrongly selected analyzer. Details: The interface is unknown.

Warnings

- Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe
- Excluded IPs from analysis (whitelisted): 20.82.210.154
- Excluded domains from analysis (whitelisted): store-images.s-microsoft.com, arc.trafficmanager.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, arc.msn.com


Simulations

Behavior and APIs


Time	Type	Description
02:35:39	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):	1.9219280948873623
TrID:	
File name:	download
File size:	5
MD5:	4842e206e4cff2954901467ad54169e
SHA1:	80c9820ff2efe8aa3d361df7011ae6eee35ec4f0
SHA256:	2acab1228e8935d5dfdd1756b8a19698b6c8b786c90f87993ce9799a67a96e4e
SHA512:	ff537b1808fcb03cfb52f768fbd7e7bd66baf6a8558ee5b8f2a02f629e021aa88a1df7a8750bae1f04f3b9d86da56f0bdcba2fdb81d366da6c97eb76ecb6cba
SSDEEP:	3:w:w
TLSH:	
File Content Preview:	0....

File Icon



Icon Hash:	74f0e4e4e4e4e0e4
------------	------------------

Network Behavior

No network behavior found

Statistics

No statistics


System Behavior

Analysis Process: OpenWith.exe PID: 4400, Parent PID: 804

General

Target ID:	0
Start time:	02:35:38
Start date:	23/06/2022
Path:	C:\Windows\System32\OpenWith.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\OpenWith.exe -Embedding
Imagebase:	0x7ff663070000
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