

JOESandbox Cloud BASIC



ID: 613355

Sample Name: download

Cookbook: default.jbs

Time: 18:55:25

Date: 21/04/2022

Version: 34.0.0 Boulder Opal

Table of Contents

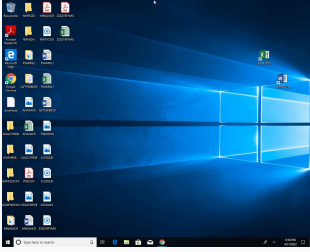
Table of Contents	2
Windows Analysis Report download	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Yara Signatures	3
Sigma Signatures	3
Snort Signatures	3
Joe Sandbox Signatures	4
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	6
Initial Sample	6
Dropped Files	6
Unpacked PE Files	6
Domains	6
URLs	6
Domains and IPs	7
Contacted Domains	7
World Map of Contacted IPs	7
General Information	7
Warnings	7
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	8
IPs	8
Domains	8
ASNs	8
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	8
Static File Info	8
General	8
File Icon	8
Network Behavior	9
Statistics	9
System Behavior	9
Analysis Process: OpenWith.exePID: 6948, Parent PID: 812	9
General	9
File Activities	9
Registry Activities	9
Disassembly	9

Windows Analysis Report

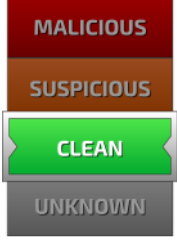
download

Overview

General Information

Sample Name:	download
Analysis ID:	613355
MD5:	4842e206e4cff2..
SHA1:	80c9820ff2efe8a..
SHA256:	2acab1228e8935..
	

Detection

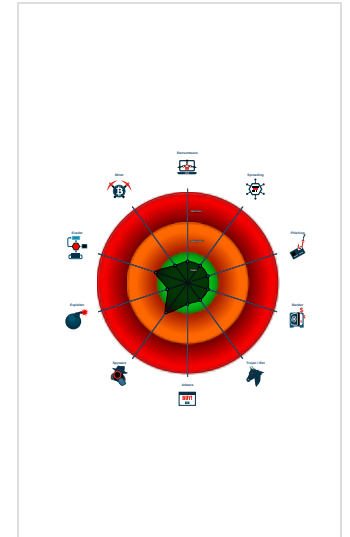


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	100%


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: 6948 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

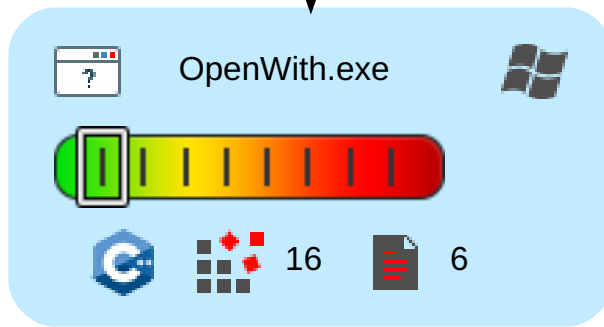
Behavior Graph

Behavior Graph

ID: 613355
Sample: download
Startdate: 21/04/2022
Architecture: WINDOWS
Score: 1

- Process
- Signature
- Created File
- DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

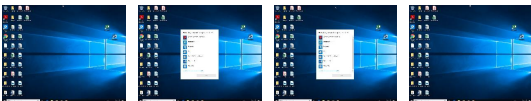
started



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
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:	34.0.0 Boulder Opal
Analysis ID:	613355
Start date and time: 21/04/202218:55:25	2022-04-21 18:55:25 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 58s
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:	2
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:	CLEAN
Classification:	clean1.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• Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): backgroundTaskHost.exe
- Excluded IPs from analysis (whitelisted): 20.40.136.238
- Excluded domains from analysis (whitelisted): iris-de-prod-azsc-frc-b.francecentral.cloudapp.azure.com, store-images.s-microsoft.com, arc.trafficmanager.net, arc.msn.com
- 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
18:56:36	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:	ff537b1808fcb03cfb52f768fbd7e7bd66baf6a8558ee5b8f2a02f629e021aa88a1df7a8750bae1f04f3b9d86da56f0bdcba2fdbc81d366da6c97eb76ecb6cba
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: 6948, Parent PID: 812

General

Target ID:	0
Start time:	18:56:36
Start date:	21/04/2022
Path:	C:\Windows\System32\OpenWith.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\OpenWith.exe -Embedding
Imagebase:	0x7ff72d4d0000
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