ID: 580248
Sample Name: download
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 00:38:46
Date: 01/03/2022
Version: 34.0.0 Boulder Opal

Table of Contents

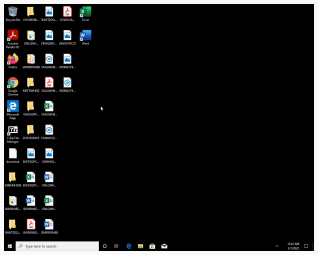
Windows Analysis Report

download

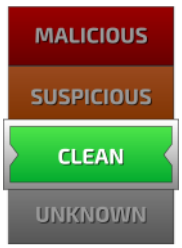
Overview

General Information

Sample Name:	download
Analysis ID:	580248
MD5:	4842e206e4cfff2..
SHA1:	80c9820ff2efe8a..
SHA256:	2acab1228e8935..



Detection

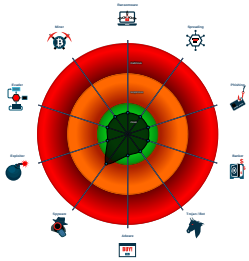


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Program does not show much activi…
- Queries the volume information (nam…
- Found detection on Joe Sandbox Cl…

Classification



Process Tree

- **System is start**
- WaaSMedicAgent.exe (PID: 7852 cmdline: C:\Windows\System32\WaaSMedicAgent.exe 355dc96661d9005cd453302c33619d95 IggQ2QzsV0Si9oeB.0.0.0 MD5: F9414EA5636ABD325993E280C181955F)
  - conhost.exe (PID: 7828 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: C5E9B1D1103EDCEA2E408E9497A5A88F)
- **cleanup**

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Joe Sandbox Signatures

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

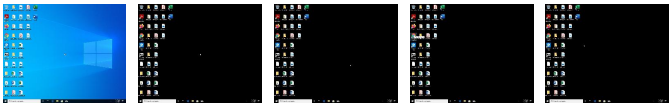
Mitre Att&ck Matrix

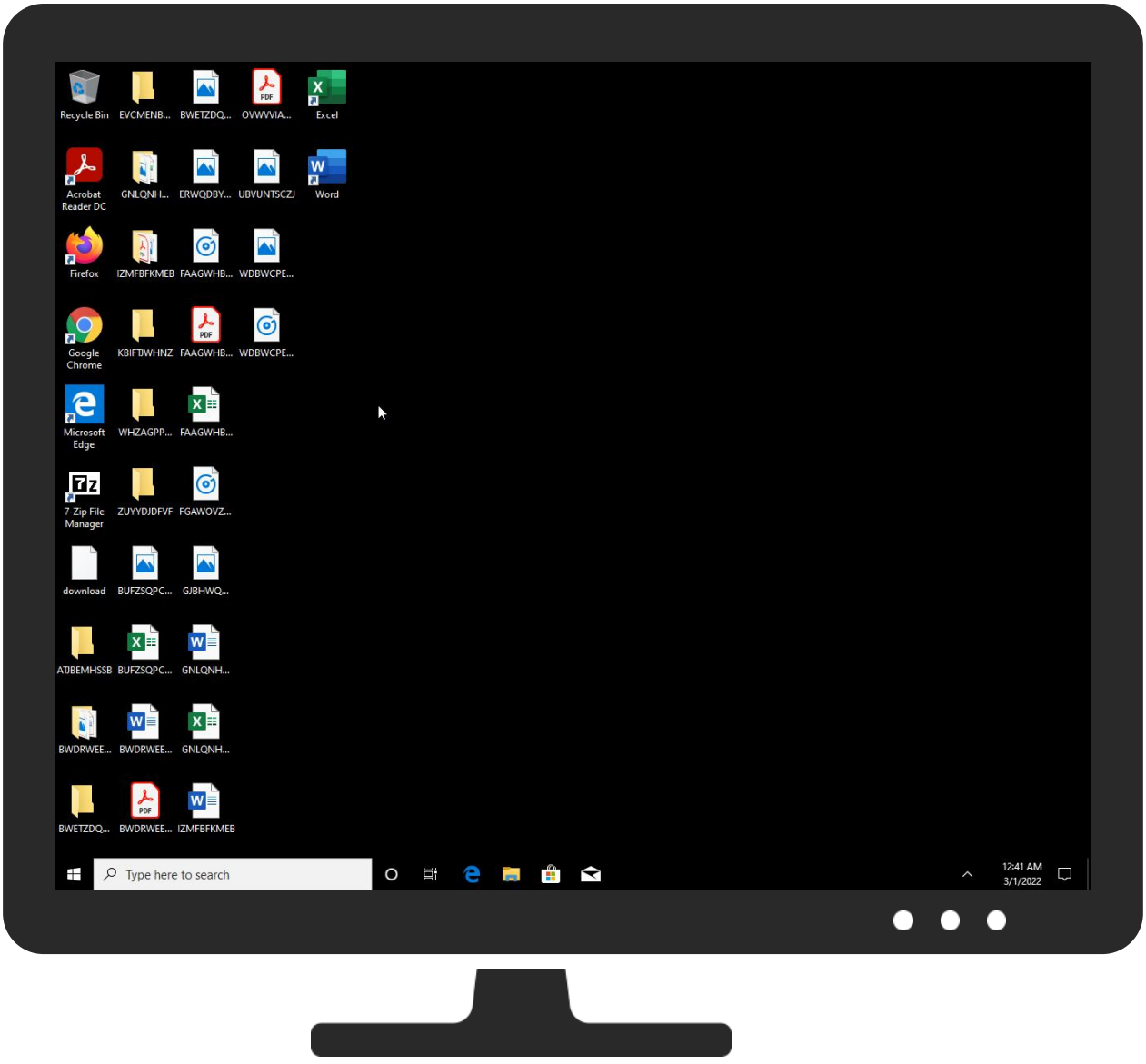
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	1 Process Injection	OS Credential Dumping	1 2 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

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:	580248
Start date:	01.03.2022
Start time:	00:38:46
Joe Sandbox Product:	CloudBasic
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	download
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Number of analysed new started processes analysed:	18
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:	• EGA enabled
Analysis Mode:	stream
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.win@2/0@0/0

Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): SIHClient.exe, svchost.exe
- Excluded domains from analysis (whitelisted): login.live.com, slscr.update.microsoft.com, nexusrules.officeapps.live.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.

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:	4842e206e4cfff2954901467ad54169e
SHA1:	80c9820ff2efe8aa3d361df7011ae6eee35ec4f0
SHA256:	2acab1228e8935d5dfdd1756b8a19698b6c8b786c90f87993ce9799a67a96e4e
SHA512:	ff537b1808fcb03cfb52f768fbd7e7bd66baf6a8558ee5b8f2a02f629e021aa88a1df7a8750bae1f04f3b9d86da56f0bdcba2fdbc81d366da6c97eb76ecb6cba
SSDEEP:	3:w:w
File Content Preview:	0....

File Icon

Icon Hash:	74f0e4e4e4e4e0e4