ID: 632523
Cookbook: urldownload.jbs
Time: 18:38:36
Date: 23/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

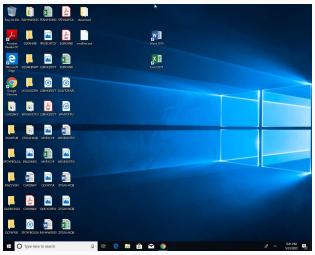
Windows Analysis Report

http://ctldl.windowsupdate.com:80/msdownload/update/v3/static/trustedr/en/CABD2A79A1076A31..

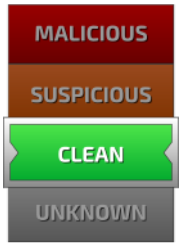
Overview

General Information

Sample URL:	http://ctldl.windowsupdate.com:80/msdownload/update/v3/static/trustedr/en/CABD2A79A1076A31F21D253635CB039D4329A5E8.crt?4d0e2557b629276c
Analysis ID:	632523
Infos:	



Detection

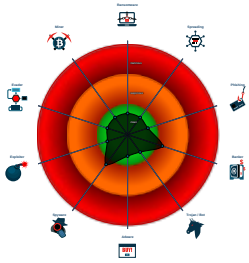


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Queries the volume information (nam…
- Drops certificate files (DER)

Classification



Process Tree

- **System is w10x64**
- cmd.exe (PID: 7164 cmdline: C:\Windows\system32\cmd.exe /c wget -t 2 -v -T 60 -P "C:\Users\user\Desktop\download" --no-check-certificate --content-disposition --user-agent="Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko" "http://ctldl.windowsupdate.com:80/msdownload/update/v3/static/trustedr/en/CABD2A79A1076A31F21D253635CB039D4329A5E8.crt?4d0e2557b629276c" > cmdline.out 2>&1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 5040 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - wget.exe (PID: 6332 cmdline: wget -t 2 -v -T 60 -P "C:\Users\user\Desktop\download" --no-check-certificate --content-disposition --user-agent="Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko" "http://ctldl.windowsupdate.com:80/msdownload/update/v3/static/trustedr/en/CABD2A79A1076A31F21D253635CB039D4329A5E8.crt?4d0e2557b629276c" MD5: 3DADB6E2ECE9C4B3E1E322E617658B60)
- **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

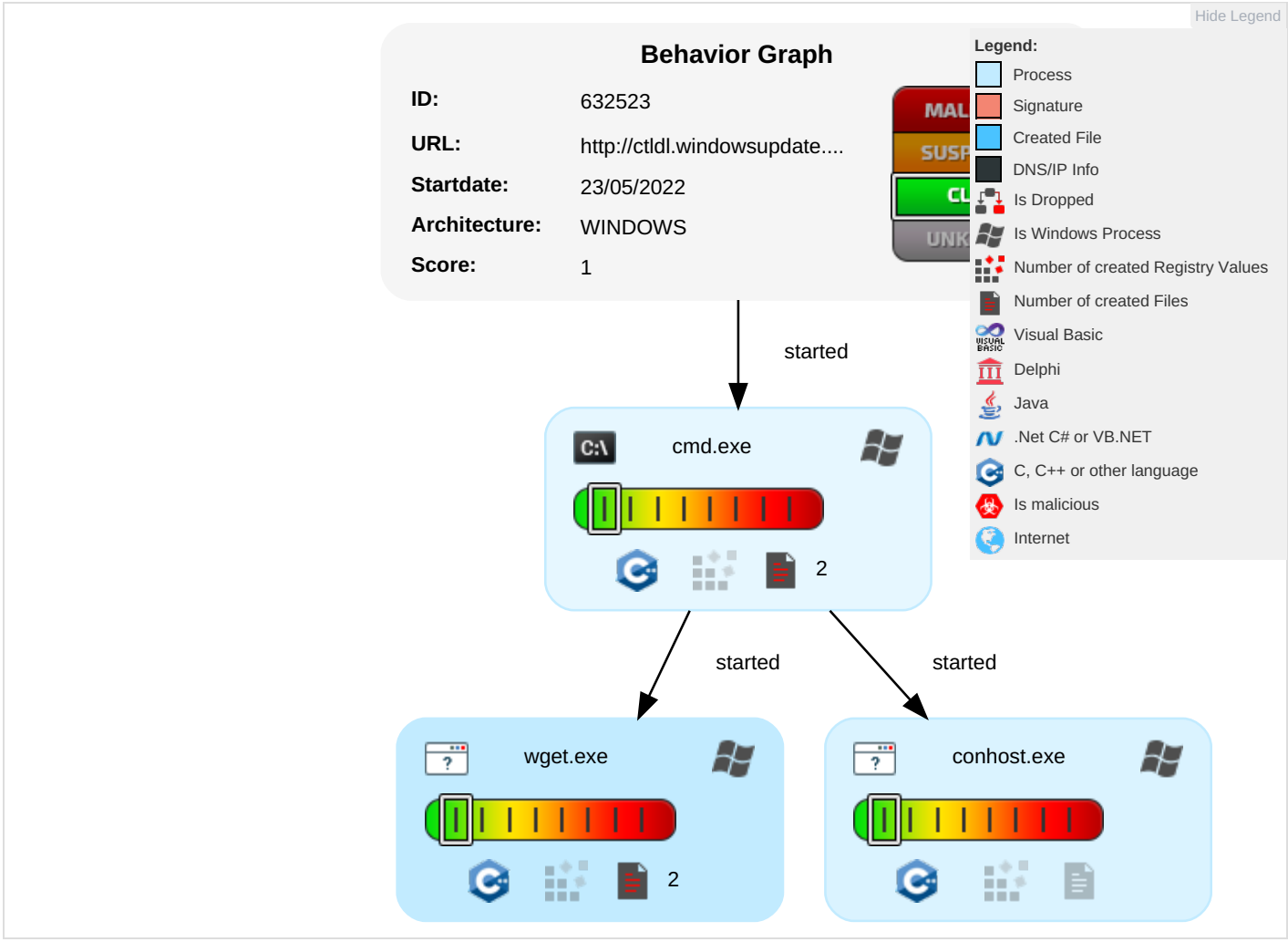
Joe Sandbox Signatures

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	1 Process Injection	1 Masquerading	OS Credential Dumping	1 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
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	1 Remote System 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

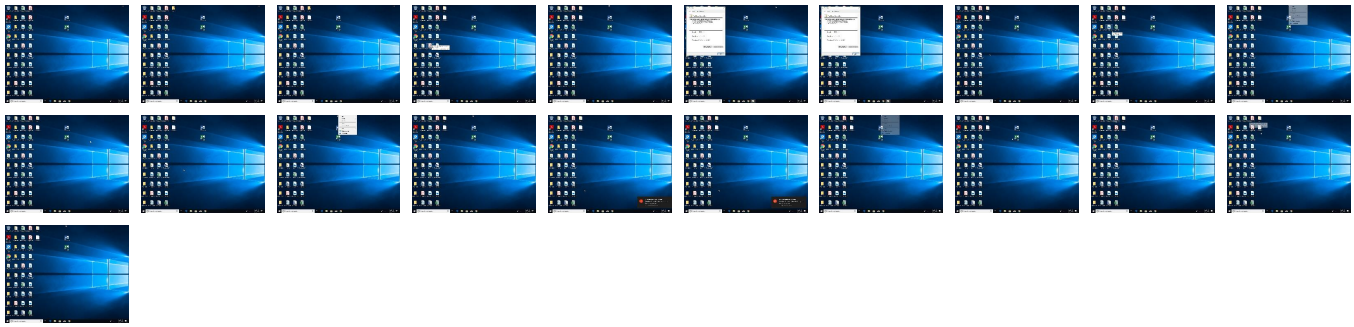
Behavior Graph



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

Source	Detection	Scanner	Label	Link
http://ctldl.windowsupdate.com:80/msdownload/update/v3/static/trustedr/en/CABD2A79A1076A31F21D253635CB039D4329A5E8.crt?4d0e2557b629276c	0%	Avira URL Cloud	safe	

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:	632523
Start date and time: 23/05/202218:38:36	2022-05-23 18:38:36 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	urldownload.jbs
Sample URL:	http://ctldl.windowsupdate.com:80/msdownload/update/v3/static/trustedr/en/CABD2A79A1076A31F21D253635CB039D4329A5E8.crt?4d0e2557b629276c
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:	23
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.win@4/2@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, rundll32.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 173.222.108.226, 173.222.108.210
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, a767.dspw65.akamai.net, arc.msn.com, wu-bg-shim.trafficmanager.net, download.windowsupdate.com.edgesuite.net, ris.api.iris.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
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\Desktop\cmdline.out

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	805
Entropy (8bit):	5.29723791471052
Encrypted:	false
SSDEEP:	12:HH5/z8a/jfaKVDT1bzp3jbG8px1De5RhKFSbNWKvjfavayiVuVWBGGAiNWKvjfaB:54SjfJd28jxePgiWajfrgluWajf1WWy
MD5:	31A03EED3CC28AB31DB9CC618EF7AE71
SHA1:	34387C0DB3D77F8D84C3AA3BF10B7148A1FC3AC9
SHA-256:	3905383C806EEAD8EE70580F8E229A1DA04774A50396ACC33F792B062D217778
SHA-512:	6267C05DB48ECFAC5A789A0BB277BB0ABAA1FD3A9CF5B6F025362ACFFBA2F0980F5DF3119FCA12A78774455F78C0E30AF28C9D88066DBD4F0BD46221B7ED2 9D
Malicious:	false
Reputation:	low
Preview:	--2022-05-23 18:39:55-- http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/CABD2A79A1076A31F21D253635CB039D4329A5E8.crt?4d0e2557b629276c..Resolving ctldl.windowsupdate.com (ctldl.windowsupdate.com)... 173.222.108.226, 173.222.108.210..Connecting to ctldl.windowsupdate.com (ctldl.windowsupdate.com)|173.222.108.226|:80... connected...HTTP request sent, awaiting response... 200 OK..Length: 1391 (1.4K) [application/x-x509-ca-cert]..Saving to: 'C:/Users/user/Desktop/download/CABD2A79A1076A31F21D253635CB039D4329A5E8.crt@4d0e2557b629276c'.... 0K . 100% 1 .96M=0.001s....2022-05-23 18:39:56 (1.96 MB/s) - 'C:/Users/user/Desktop/download/CABD2A79A1076A31F21D253635CB039D4329A5E8.crt@4d0e2557b629276c' saved [1391/1391]....

C:\Users\user\Desktop\download\CABD2A79A1076A31F21D253635CB039D4329A5E8.crt@4d0e2557b629276c

Process:	C:\Windows\SysWOW64\wget.exe
File Type:	data
Category:	dropped
Size (bytes):	1391
Entropy (8bit):	7.705940075877404
Encrypted:	false
SSDEEP:	24:ooVdTH2NMU+I3E0Ulcrgdaf3sWrATrnkC4EmCUkmGMkfQo1fSZotWzD1:ooVguI3Kcx8WIzNeCUkJMmSuMX1
MD5:	0CD2F9E0DA1773E9ED864DA5E370E74E
SHA1:	CABD2A79A1076A31F21D253635CB039D4329A5E8

SHA-256:	96BCEC06264976F37460779ACF28C5A7CFE8A3C0AAE11A8FFCEE05C0BDDF08C6
SHA-512:	3B40F27E828323F5B91F8909883A78A21C86551761F27B38029FAAEC14AF5B7AA96FB9F9CC93EE201B5EB1D0FEF17B290747E8B839D2E49A8F36C5EBF3C7C910
Malicious:	false
Reputation:	low
Preview:	0..k0..S.....@.YDc.c...0...*.H.....0O1.0...U....US1)0'..U... Internet Security Research Group1.0...U....ISRG Root X10...150604110438Z..350604110438Z0O1.0...U....US1)0'..U... Internet Security Research Group1.0...U....ISRG Root X10.."0...*.H.....0.....$s..7.+W(.....8..n<.W.x.u...jn..O(..h.lD...c...k....1.!~.3<.H..y.....!.K...qiJffl.~<p.)"......K...~....G.|.H#S.8.O.o...IW..t../.8.{.p!.u.0<.....c...O..K~.....w...{J.L.%.p..)..S$.....J.?..aQ.....cq...o[...\4ylv.;.by.../&.....6....7..6u...r.....I.....*.A..v.....5/(.l....dwnG7..Y^h..r...A)>Y>.&.$...Z.L@.F....:Qn.;.}r...xY.>Qx...../..>{J.Ks.....P.|C.t..t.....0.[q6....00\H..;..}`...).....A.....|.;F.H*..v.v..j.=...8.d..+..(.....B.".'].y...p..N..:..'Qn..d.3CO.....B0@0...U.....0...U.....0....0...U.....y.Y.{....s.....X..n0...*.H.....U.X....P.....i ')..au\.n...i/..VK..s.Y.!.~.Lq..`.9....!V..P.Y...Y.....b.E.f..|o..;.....'...}~.."....

Static File Info

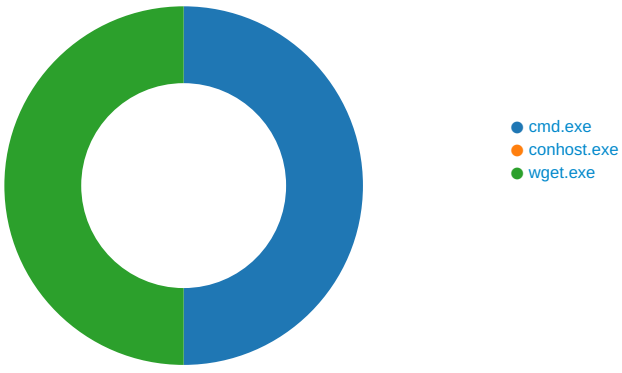
No static file info

Network Behavior

No network behavior found

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: cmd.exe PID: 7164, Parent PID: 4016

General

Target ID:	0
Start time:	18:39:52
Start date:	23/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c wget -t 2 -v -T 60 -P "C:\Users\user\Desktop\download" --no-check-certificate --content-disposition --user-agent="Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko" "http://ctldl.windowsupdate.com:80/msdownload/update/v3/static/trustedr/en/CABD2A79A1076A31F21D253635CB039D4329A5E8.crt?4d0e2557b629276c" > cmdline.out 2>&1
Imagebase:	0xdd0000

File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\cmdline.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	DDD194	CreateFileW

Analysis Process: conhost.exe PID: **5040**, Parent PID: **7164**

General

Target ID:	1
Start time:	18:39:54
Start date:	23/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7bab80000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: wget.exe PID: **6332**, Parent PID: **7164**

General

Target ID:	2
Start time:	18:39:55
Start date:	23/05/2022
Path:	C:\Windows\SysWOW64\wget.exe
Wow64 process (32bit):	true
Commandline:	wget -t 2 -v -T 60 -P "C:\Users\user\Desktop\download" --no-check-certificate --content-disposition --user-agent="Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko" "http://ctldl.windowsupdate.com:80/msdownload/update/v3/static/trustedr/en/CABD2A79A1076A31F21D253635CB039D4329A5E8.crt?4d0e2557b629276c"
Imagebase:	0x400000
File size:	3895184 bytes
MD5 hash:	3DADB6E2ECE9C4B3E1E322E617658B60
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\download\CABD2A79A1076A31F21D253635CB039D4329A5E8.crt@4d0e2557b629276c	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	46596C	fopen

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly