ID: 831172
Cookbook: urldownload.jbs
Time: 07:57:32
Date: 21/03/2023
Version: 37.0.0 Beryl

Table of Contents

Windows Analysis Report

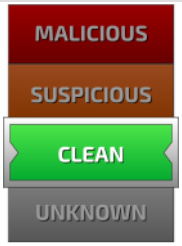
http://pdfconvertychrome.ssl.hwcdn.net/pdfconverty.exe

Overview

General Information

Sample URL:	http://pdfconvertychrome.ssl.hwcdn.net/pdfconverty.exe
Analysis ID:	831172
Infos:	

Detection

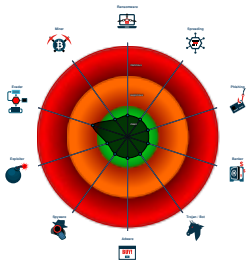


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Very long cmdline option found, this…

Classification



Process Tree

- **System is w10x64**
- cmd.exe (PID: 5736 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://pdfconvertychrome.ssl.hwcdn.net/pdfconverty.exe" > cmdline.out 2>&1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 3520 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - wget.exe (PID: 324 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://pdfconvertychrome.ssl.hwcdn.net/pdfconverty.exe" 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

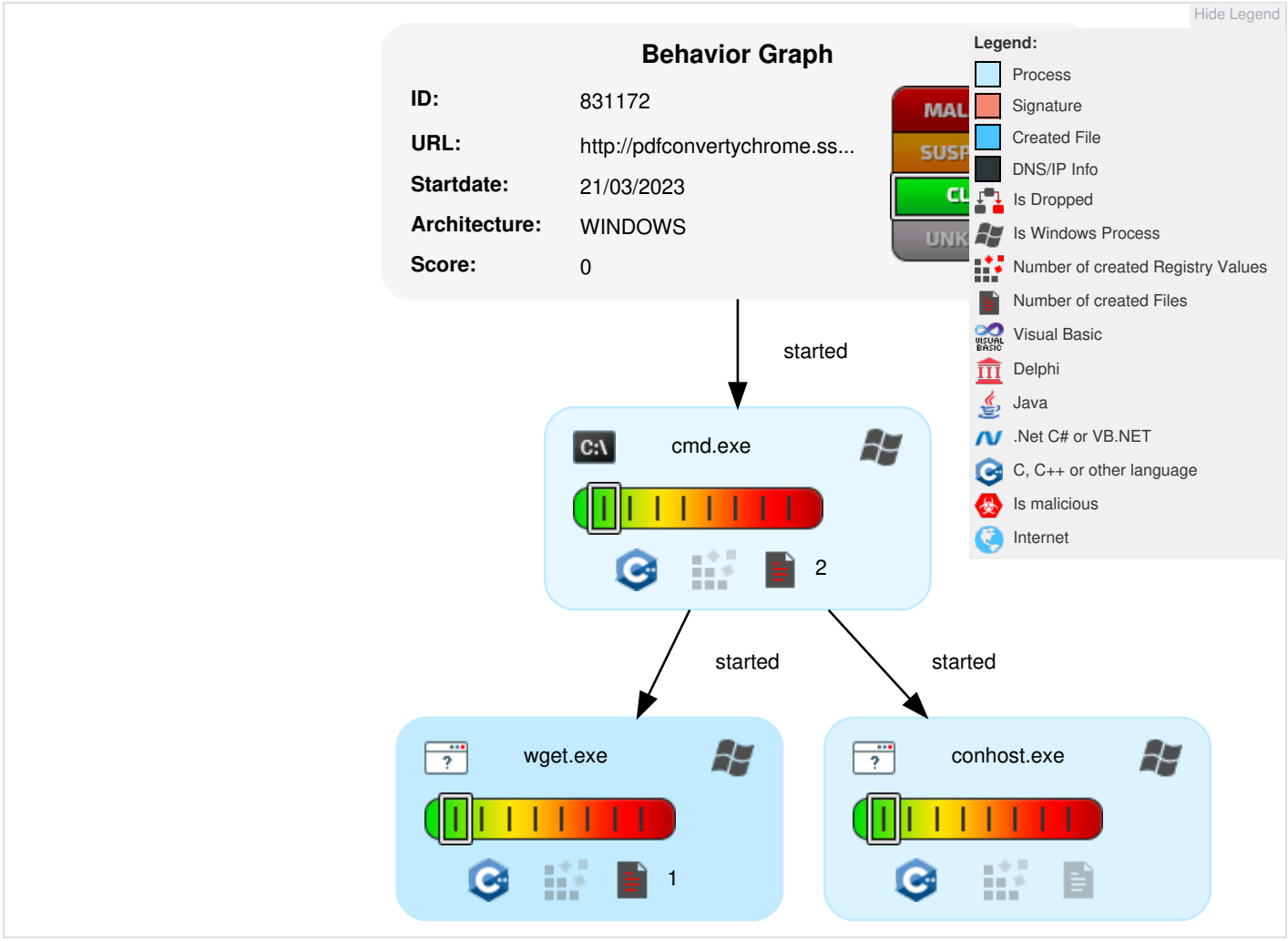
Joe Sandbox Signatures

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	1 Command and Scripting Interpreter	Path Interception	1 Process Injection	1 Masquerading	OS Credential Dumping	1 Security Software 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 System Information 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 Remote System 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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://pdfconvertychrome.ssl.hwcdn.net/pdfconverty.exe	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:	37.0.0 Beryl
Analysis ID:	831172
Start date and time:	2023-03-21 07:57:32 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	urldownload.jbs
Sample URL:	http://pdfconvertychrome.ssl.hwcdn.net/pdfconverty.exe
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, 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:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@4/1@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:	• Unable to download file

Warnings

- Excluded IPs from analysis (whitelisted): 205.185.208.154
- Excluded domains from analysis (whitelisted): pdfconvertychrome.ssl.hwcdn.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):	392
Entropy (8bit):	5.047536204042369
Encrypted:	false
SSDEEP:	12:Htpp2HdG2f2cqUI2f2tUG1De5Rhh8froB3v:NppMcgdqUIgEUGxePP8sf
MD5:	2E84C708A9A0E8A63D152466FA859A1F
SHA1:	1D79D210CBF392A99447849838B5486CDEB53A1B
SHA-256:	F681FC679BBB6601139BEBDB1AAB2B05D3FA200FFEAE2D738A26CE9877C199DA
SHA-512:	35F1BB0031EAA45912302E5C4AEA74757D39A892692291DCAFEA44A75F9452F511D5248967B4DD11E58CE5AFB6001F451296C63A92D3B924976523EE304D7055
Malicious:	false
Reputation:	low
Preview:	--2023-03-21 07:58:23-- http://pdfconvertychrome.ssl.hwcdn.net/pdfconverty.exe..Resolving pdfconvertychrome.ssl.hwcdn.net (pdfconvertychrome.ssl.hwcdn.net)... 205.185.208.154..Connecting to pdfconvertychrome.ssl.hwcdn.net (pdfconvertychrome.ssl.hwcdn.net)|205.185.208.154|:80... connected...HTTP request sent, awaiting response... 404 Not Found..2023-03-21 07:58:23 ERROR 404: Not Found.....

Static File Info

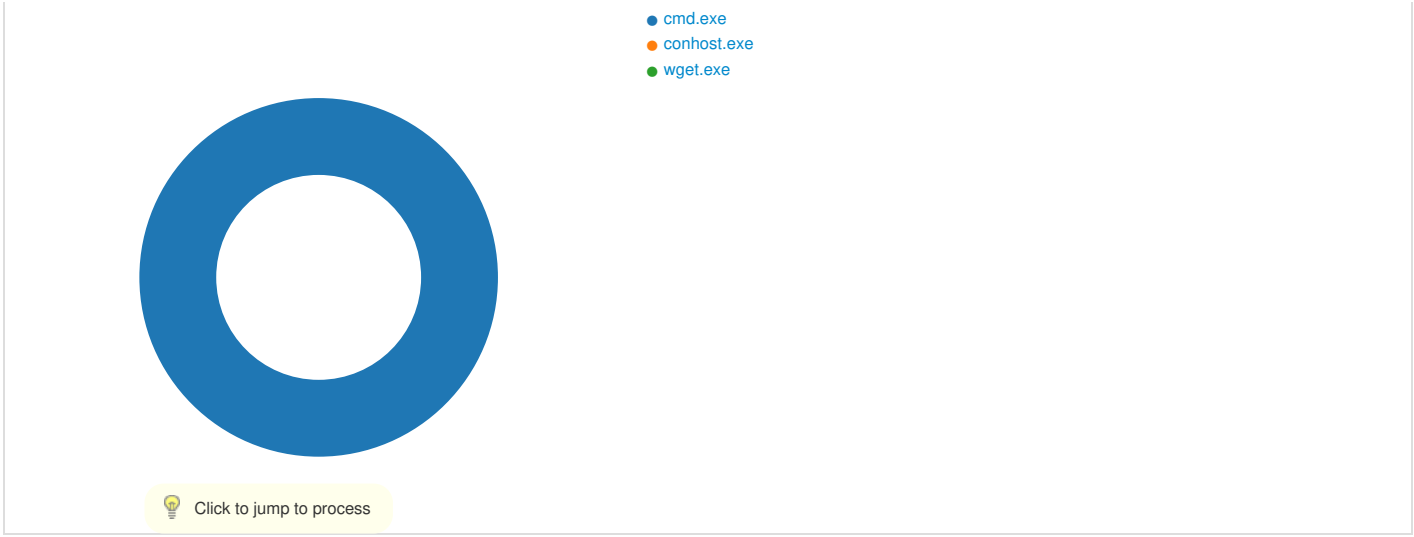
No static file info

Network Behavior

Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

Statistics

Behavior



System Behavior

Analysis Process: cmd.exe PID: **5736**, Parent PID: **1176**

General

Target ID:	0
Start time:	07:58:22
Start date:	21/03/2023
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://pdfconvertychrome.ssl.hwcdn.net/pdfconverty.exe" > cmdline.out 2>&1
Imagebase:	0xb0000
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

Analysis Process: conhost.exe PID: **3520**, Parent PID: **5736**

General

Target ID:	1
Start time:	07:58:23
Start date:	21/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: **324**, Parent PID: **5736**

General	
Target ID:	2
Start time:	07:58:23
Start date:	21/03/2023
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://pdfconvertychrome.ssl.hwcdn.net/pdfconverty.exe"
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

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	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly