

JoeSandbox Cloud BASIC



ID: 458983

Cookbook: urldownload.jbs

Time: 00:19:42

Date: 04/08/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report http://45.227.255.235:39486/dwm6.exe	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Yara Overview	3
Sigma Overview	3
Jbx Signature Overview	3
Networking:	4
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	4
Thumbnails	4
Antivirus, Machine Learning and Genetic Malware Detection	5
Initial Sample	5
Dropped Files	5
Unpacked PE Files	5
Domains	5
URLs	5
Domains and IPs	6
Contacted Domains	6
URLs from Memory and Binaries	6
Contacted IPs	6
Public	6
General Information	6
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	7
IPs	7
Domains	7
ASN	7
JA3 Fingerprints	7
Dropped Files	7
Created / dropped Files	7
Static File Info	7
No static file info	7
Network Behavior	8
Network Port Distribution	8
TCP Packets	8
Code Manipulations	8
Statistics	8
Behavior	8
System Behavior	8
Analysis Process: cmd.exe PID: 2140 Parent PID: 4864	8
General	8
File Activities	8
File Created	8
Analysis Process: conhost.exe PID: 5816 Parent PID: 2140	8
General	8
Analysis Process: wget.exe PID: 5320 Parent PID: 2140	9
General	9
File Activities	9
Disassembly	9
Code Analysis	9

Windows Analysis Report http://45.227.255.235:39486/d...

Overview

General Information

Sample URL:

http://45.227.255.235:39486/dwm6.exe

Analysis ID:

458983

Infos:

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Score:

20

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Connects to many ports of the same...

Classification

Process Tree

System is w10x64

cmd.exe (PID: 2140 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://45.227.255.235:39486/dwm6.exe' > cmdline.out 2>&1 MD5: F3BDBE3BB6F734E357235F4D5898582D)

conhost.exe (PID: 5816 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

wget.exe (PID: 5320 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://45.227.255.235:39486/dwm6.exe' MD5: 3DADB6E2ECE9C4B3E1E322E617658B60)

cleanup

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

Copyright Joe Security LLC 2021

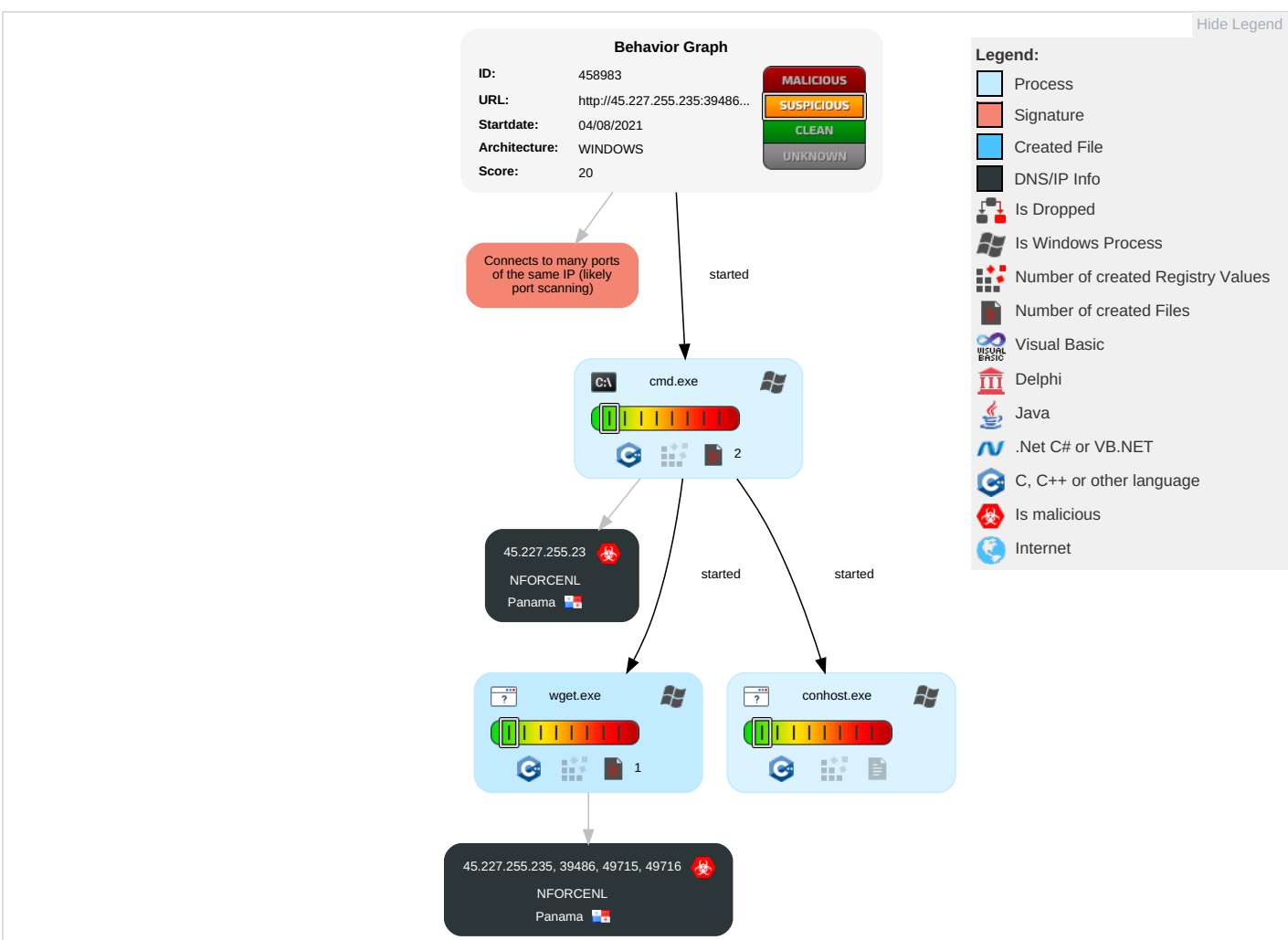
Page 3 of 9

Connects to many ports of the same IP (likely port scanning)

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	Process Injection 1	Masquerading 1	OS Credential Dumping	System Information Discovery 1	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	Process Injection 1	LSASS Memory	Application Window 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://45.227.255.235:39486/dwm6.exe	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://45.227.255.235:39486/dwm6.exe4	0%	Avira URL Cloud	safe	
http://45.227.255.235:39486/dwm6.exe#	0%	Avira URL Cloud	safe	
http://45.227.255.235:39486/dwm6.exe3	0%	Avira URL Cloud	safe	
http://45.227.255.235:39486/dwm6.exe-	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.227.255.23	unknown	Panama		43350	NFORCENL	true
45.227.255.235	unknown	Panama		43350	NFORCENL	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458983
Start date:	04.08.2021
Start time:	00:19:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 1m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	urldownload.jbs
Sample URL:	http://45.227.255.235:39486/dwm6.exe
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:	4
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:	SUS
Classification:	sus20.troj.win@4/1@0/2
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 • Unable to download file
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\Desktoplcmdline.out	
Process:	C:\Windows\SysWOW64\lwget.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	299
Entropy (8bit):	4.960976512383863
Encrypted:	false
SSDEEP:	6:HxEA4hV7uiXCtAk2uPEEcWF37uiXCtAk29zN:HxE3hVjCtgqEENF3jCtg9h
MD5:	049248EA43A59DBEFB87DE30D360A4BB
SHA1:	E005B5760BEC48B55E39C88AB773BE4D3271C03E
SHA-256:	9DFDDBC1A76052CF9B83D18852ECFD008200D8234041242EA465BEDC17202B84
SHA-512:	ACFB1EE866CA136049EE354CF47690591D365E878CB253D99E828C248865F06AFA1F0581B96D45E4D6077FD8B67867E3D4D286B171876DF21995DBF7E9699A9C
Malicious:	false
Reputation:	low
Preview:	--2021-08-04 00:20:28-- http://45.227.255.235:39486/dwm6.exe..Connecting to 45.227.255.235:39486... failed: Bad file descriptor...Retrying.....--2021-08-04 00:20:30-- (try: 2) http://45.227.255.235:39486/dwm6.exe..Connecting to 45.227.255.235:39486... failed: Bad file descriptor...Giving up.....

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

Code Manipulations

Statistics

Behavior

 Click to jump to process

System Behavior

Analysis Process: cmd.exe PID: 2140 Parent PID: 4864

General

Start time:	00:20:26
Start date:	04/08/2021
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://45.227.255.235:39486/dwm6.exe' > cmdline.out 2>&1
Imagebase:	0xbd0000
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

Show Windows behavior

File Created

Analysis Process: conhost.exe PID: 5816 Parent PID: 2140

General

Start time:	00:20:27
Start date:	04/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: 5320 Parent PID: 2140

General

Start time:	00:20:28
Start date:	04/08/2021
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://45.227.255.235:39486/dwm6.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

Show Windows behavior

Disassembly

Code Analysis