ID: 458986
Cookbook: urldownload.jbs
Time: 00:27:39
Date: 04/08/2021
Version: 33.0.0 White Diamond

Table of Contents

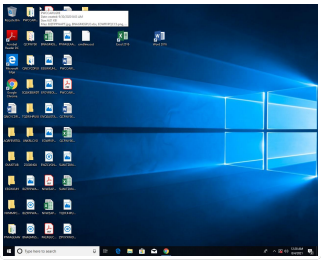
Windows Analysis Report http://45.227.255.235:39486/d…

Overview

General Information

Sample URL:	http://45.227.255.235:39486/dwm7.exe
Analysis ID:	458986
Infos:	

Most interesting Screenshot:



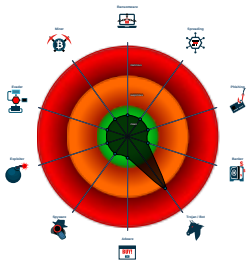
Detection

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: 4692 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/dwm7.exe' > cmdline.out 2>&1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 2492 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - wget.exe (PID: 2996 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/dwm7.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

Networking:

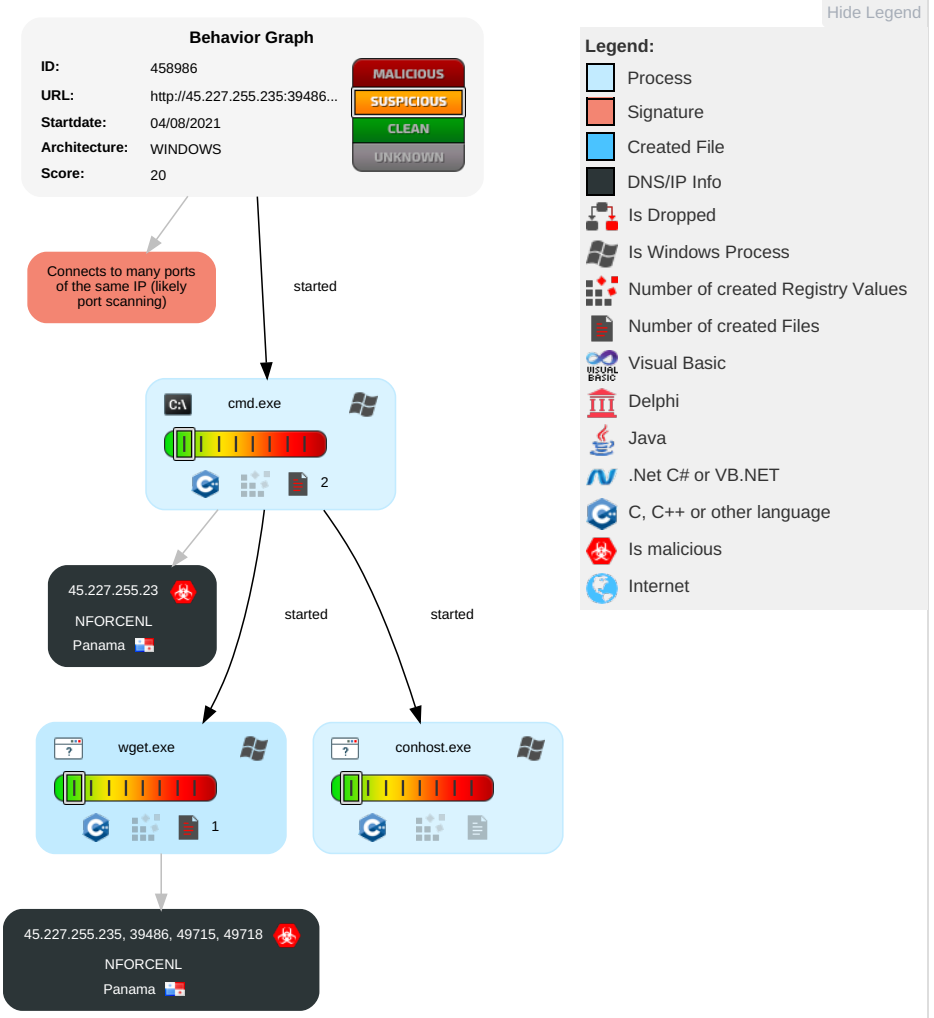
Connects to many ports of the same IP (likely port scanning)

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

Hide Legend



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/dwm7.exe	1%	Virustotal		Browse
http://45.227.255.235:39486/dwm7.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/dwm7.exe%	0%	Avira URL Cloud	safe	
http://45.227.255.235:39486/dwm7.exe5	0%	Avira URL Cloud	safe	
http://45.227.255.235:39486/dwm7.exe2	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:	458986
Start date:	04.08.2021
Start time:	00:27:39
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 1m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	urldownload.jbs
Sample URL:	http://45.227.255.235:39486/dwm7.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\Desktop\cmdline.out	
Process:	C:\Windows\SysWOW64\wget.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	299
Entropy (8bit):	4.963889471045623
Encrypted:	false
SSDEEP:	6:HxEHNL4j7uiXCtAk2uPEZXcWFb4j7uiXCtAk29zN:HxEtkjjCtgqEZXNFUjjCtg9h
MD5:	A34E01E3C5E075659AFB90E7378DB2CC
SHA1:	906E6FDE94A30BFA588D5912699A8ABF77DC580B
SHA-256:	F4A4A6E5787F0E60550A9D3015BAF6941E11C0444EA9E07C577EE553B5ED06A5
SHA-512:	21A0BBA33F3948192C26EE723841DDE98ABE8857704CB85CE26BD69580C1F8D677F1BCC0B17B5B67EEDCCAC3C7812E2A2266D813CF79E405BF42A798720409 5
Malicious:	false
Reputation:	low
Preview:	--2021-08-04 00:28:26-- http://45.227.255.235:39486/dwm7.exe..Connecting to 45.227.255.235:39486... failed: Bad file descriptor...Retrying.....--2021-08-04 00:28:28-- (try: 2) http://45.227.255.235:39486/dwm7.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: 4692 Parent PID: 1788

General

Start time:	00:28:24
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/dwm7.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: 2492 Parent PID: 4692

General

Start time:	00:28:25
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: 2996 Parent PID: 4692

General

Start time:	00:28:26
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/dwm7.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