ID: 318075
Cookbook: urldownload.jbs
Time: 16:00:43
Date: 16/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

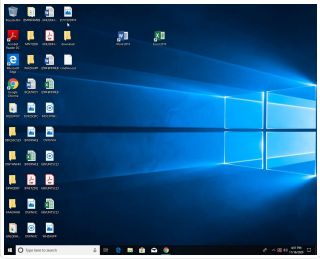
Analysis Report http://195.3.146.118

Overview

General Information

Sample URL:	http://195.3.146.118
Analysis ID:	318075

Most interesting Screenshot:



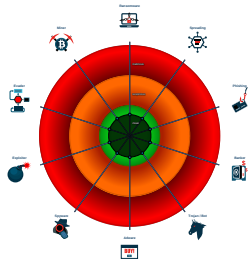
Detection

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

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- cmd.exe (PID: 6196 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://195.3.146.118' > cmdline.out 2>&1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 4460 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - wget.exe (PID: 6280 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://195.3.146.118' MD5: 3DADB6E2ECE9C4B3E1E322E617658B60)
- **cleanup**

Malware Configuration

No configs have been found

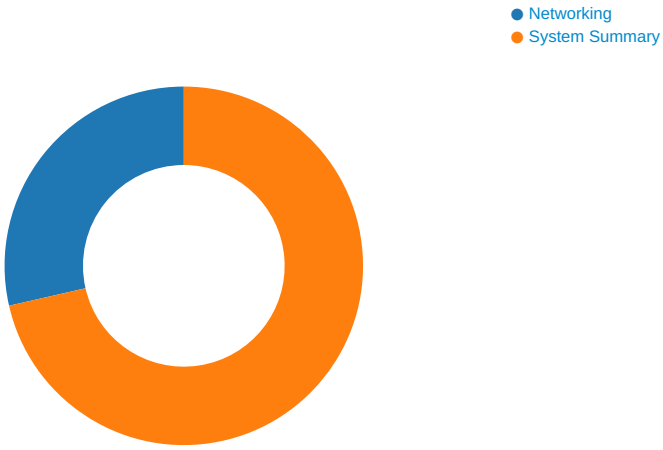
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

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	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://195.3.146.118	4%	Virustotal		Browse
http://195.3.146.118	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://195.3.146.118/&	0%	Avira URL Cloud	safe	
http://195.3.146.118Y	0%	Avira URL Cloud	safe	
http://195.3.146.118/o	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://195.3.146.118U	0%	Avira URL Cloud	safe	
http://195.3.146.118/	0%	Avira URL Cloud	safe	
http://195.3.146.118/:	0%	Avira URL Cloud	safe	

Domains and IPs

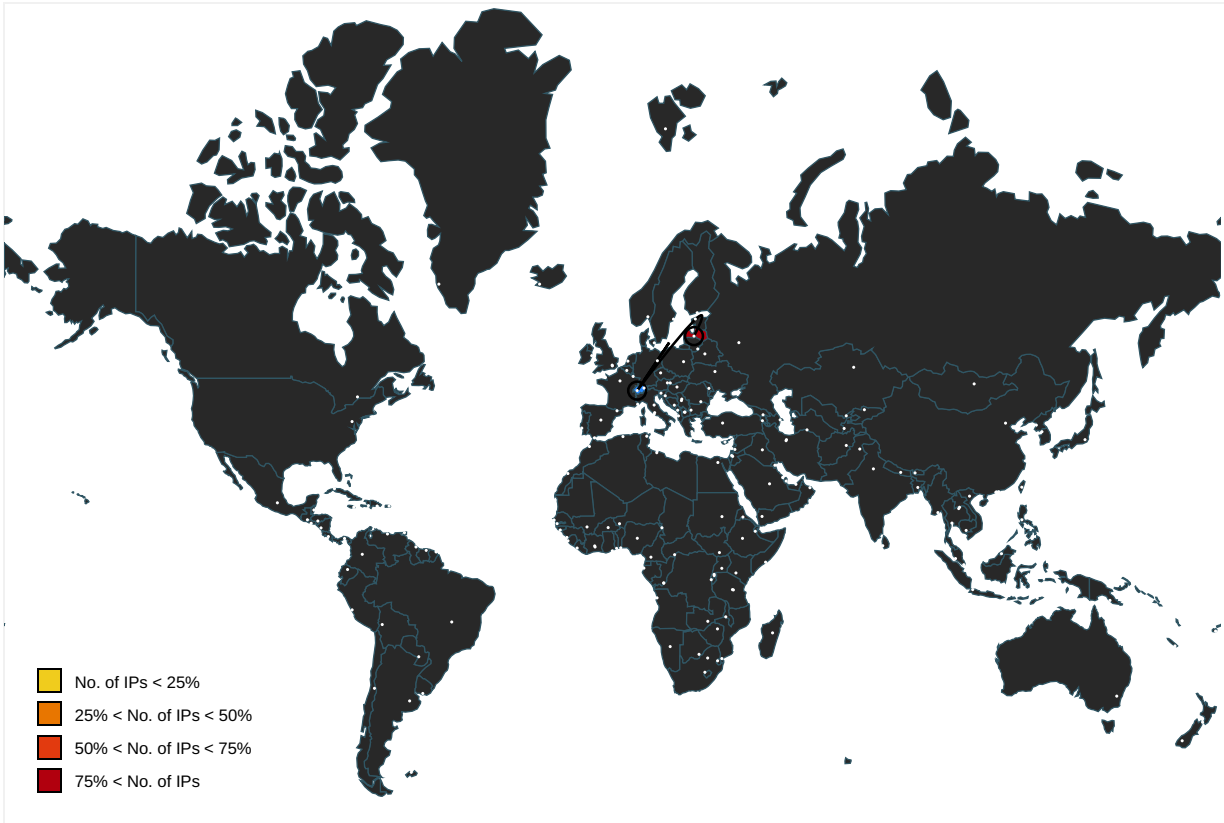
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://195.3.146.118/&	wget.exe, 00000003.00000002.666109282.0000000001065000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://195.3.146.118	wget.exe, 00000003.00000002.666091115.0000000000B90000.00000004.00000020.sdmp	false		unknown
http://195.3.146.118Y	wget.exe, 00000003.00000002.666104570.0000000001060000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	low
http://195.3.146.118/o	wget.exe, 00000003.00000002.666109282.0000000001065000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://195.3.146.118U	wget.exe, 00000003.00000002.666104570.0000000001060000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	low
http://195.3.146.118/	cmdline.out.3.dr	false	• Avira URL Cloud: safe	unknown
http://195.3.146.118/:	wget.exe, 00000003.00000002.666109282.0000000001065000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
195.3.146.118	unknown	Latvia		41390	RN-DATA-LV	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	318075
Start date:	16.11.2020
Start time:	16:00:43
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	urldownload.jbs
Sample URL:	http://195.3.146.118
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:	CLEAN
Classification:	clean0.win@4/1@0/1
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 • Exclude process from analysis (whitelisted): svchost.exe

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):	261
Entropy (8bit):	4.857334191994133
Encrypted:	false
SSDEEP:	6:HVoTaB5Qo6puT8fmcAk2u4TaBccWFdQo6puT8fmcAk29zN:HVoTaBOLmcgZTaBcNFSLmcg9h
MD5:	DF4F7D4717A240992BBA473422B8840F
SHA1:	F057F267B568FB30CB25A194A2BFDC3661BD7EB9
SHA-256:	438CFE74AFDF410423D5C18EC132F1B67A5F24693B99B130619FC95C971323BC
SHA-512:	459BC4868AA668EEAD2ADFC7CFD42351993DC565C6A973C705F9857FD4308C05ECCEBF656E4208948868A33BC6900632F0248C84A777F3DB2F2E445F19F93B5
Malicious:	false
Reputation:	low
Preview:	--2020-11-16 16:01:36-- http://195.3.146.118/..Connecting to 195.3.146.118:80... failed: Bad file descriptor...Retrying.....--2020-11-16 16:01:39-- (try: 2) http://195 .3.146.118/..Connecting to 195.3.146.118:80... failed: Bad file descriptor...Giving up.....

Static File Info

No static file info

Network Behavior

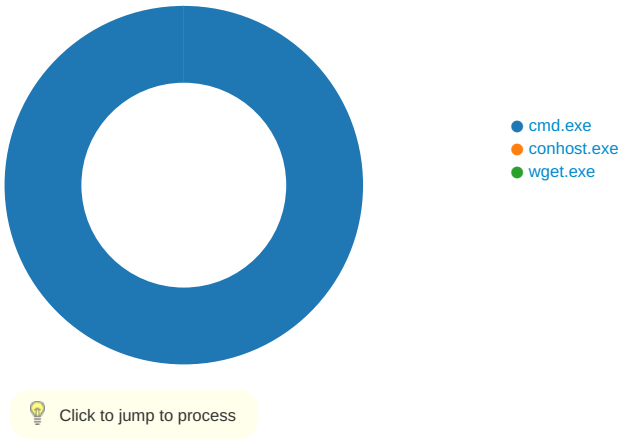
TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 16, 2020 16:01:37.469351053 CET	49735	80	192.168.2.4	195.3.146.118
Nov 16, 2020 16:01:37.513782978 CET	80	49735	195.3.146.118	192.168.2.4
Nov 16, 2020 16:01:38.024802923 CET	49735	80	192.168.2.4	195.3.146.118
Nov 16, 2020 16:01:38.069238901 CET	80	49735	195.3.146.118	192.168.2.4
Nov 16, 2020 16:01:38.571538925 CET	49735	80	192.168.2.4	195.3.146.118
Nov 16, 2020 16:01:38.615900993 CET	80	49735	195.3.146.118	192.168.2.4
Nov 16, 2020 16:01:39.638573885 CET	49737	80	192.168.2.4	195.3.146.118
Nov 16, 2020 16:01:39.682914019 CET	80	49737	195.3.146.118	192.168.2.4
Nov 16, 2020 16:01:40.196751118 CET	49737	80	192.168.2.4	195.3.146.118
Nov 16, 2020 16:01:40.241127014 CET	80	49737	195.3.146.118	192.168.2.4
Nov 16, 2020 16:01:40.743801117 CET	49737	80	192.168.2.4	195.3.146.118
Nov 16, 2020 16:01:40.788055897 CET	80	49737	195.3.146.118	192.168.2.4

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: cmd.exe PID: 6196 Parent PID: 2440

General

Start time:	16:01:35
Start date:	16/11/2020
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://195.3.146.118' > cmdline.out 2>&1
Imagebase:	0x11d0000
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	11DD194	CreateFileW

Analysis Process: conhost.exe PID: 4460 Parent PID: 6196

General

Start time:	16:01:35
Start date:	16/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 6280 Parent PID: 6196

General

Start time:	16:01:36
Start date:	16/11/2020
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://195.3.146.118'
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 Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis