

JoeSandbox Cloud BASIC



ID: 392890

Cookbook: urldownload.jbs

Time: 23:56:19

Date: 19/04/2021

Version: 31.0.0 Emerald

Table of Contents

Table of Contents	2
Analysis Report	
http://codepoints.net/static/js/codepoint.js!3c67217e710120291b75e8c13546e320?_	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Yara Overview	4
Sigma Overview	4
Signature Overview	4
Mitre Att&ck Matrix	5
Behavior Graph	5
Screenshots	6
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	7
Domains	7
URLs	7
Domains and IPs	8
Contacted Domains	8
Contacted URLs	8
URLs from Memory and Binaries	8
Contacted IPs	8
Public	8
Private	8
General Information	9
Simulations	9
Behavior and APIs	9
Joe Sandbox View / Context	10
IPs	10
Domains	10
ASN	10
JA3 Fingerprints	10
Dropped Files	10
Created / dropped Files	10
Static File Info	11
No static file info	11
Network Behavior	11
Network Port Distribution	11
TCP Packets	11
UDP Packets	12
DNS Queries	13
DNS Answers	13
HTTP Request Dependency Graph	13
HTTP Packets	13
HTTPS Packets	14
Code Manipulations	14
Statistics	14
Behavior	14
System Behavior	15
Analysis Process: cmd.exe PID: 7108 Parent PID: 1284	15
General	15

File Activities	15
File Created	15
Analysis Process: conhost.exe PID: 7128 Parent PID: 7108	15
General	15
Analysis Process: wget.exe PID: 6188 Parent PID: 7108	16
General	16
File Activities	16
File Created	16
Analysis Process: wscript.exe PID: 6728 Parent PID: 6032	16
General	16
File Activities	17
Disassembly	17
Code Analysis	17

Analysis Report http://codepoints.net/static/js/codepoin...

Overview

General Information

Sample URL:

http://codepoints.net/static/js/codepoint.js!3c67217e710120291b75e8c13546e320?_=1618365050047

Analysis ID:

392890

Infos:

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Score:

1

Range:

0 - 100

Whitelisted:

false

Confidence:

80%

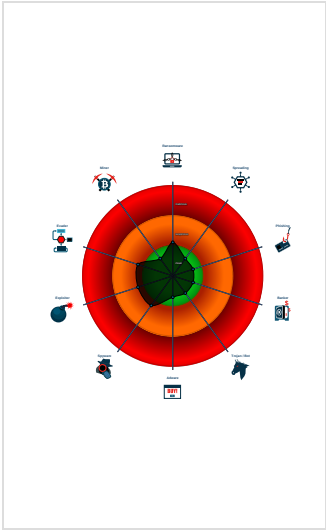
Signatures

Found WSH timer for Javascript or V...

Queries the volume information (nam...

Uses code obfuscation techniques (...)

Classification



Startup

- System is w10x64
- cmd.exe** (PID: 7108 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://codepoints.net/static/js/codepoint.js!3c67217e710120291b75e8c13546e320?_=1618365050047' >cmdline.out 2>&1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
 - conhost.exe** (PID: 7128 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
 - wget.exe** (PID: 6188 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://codepoints.net/static/js/codepoint.js!3c67217e710120291b75e8c13546e320?_=1618365050047' MD5: 3DADB6E2ECE9C4B3E1E322E617658B60)
 - wscript.exe** (PID: 6728 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\Desktop\download\codepoint.js!3c67217e710120291b75e8c13546e320@_=1618365050047.js' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- cleanup

Malware Configuration

No configs have been found

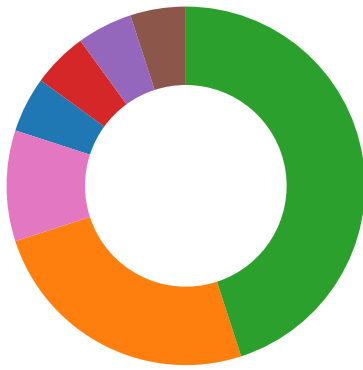
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



- Compliance
- Networking
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Language, Device and Operating System Detection

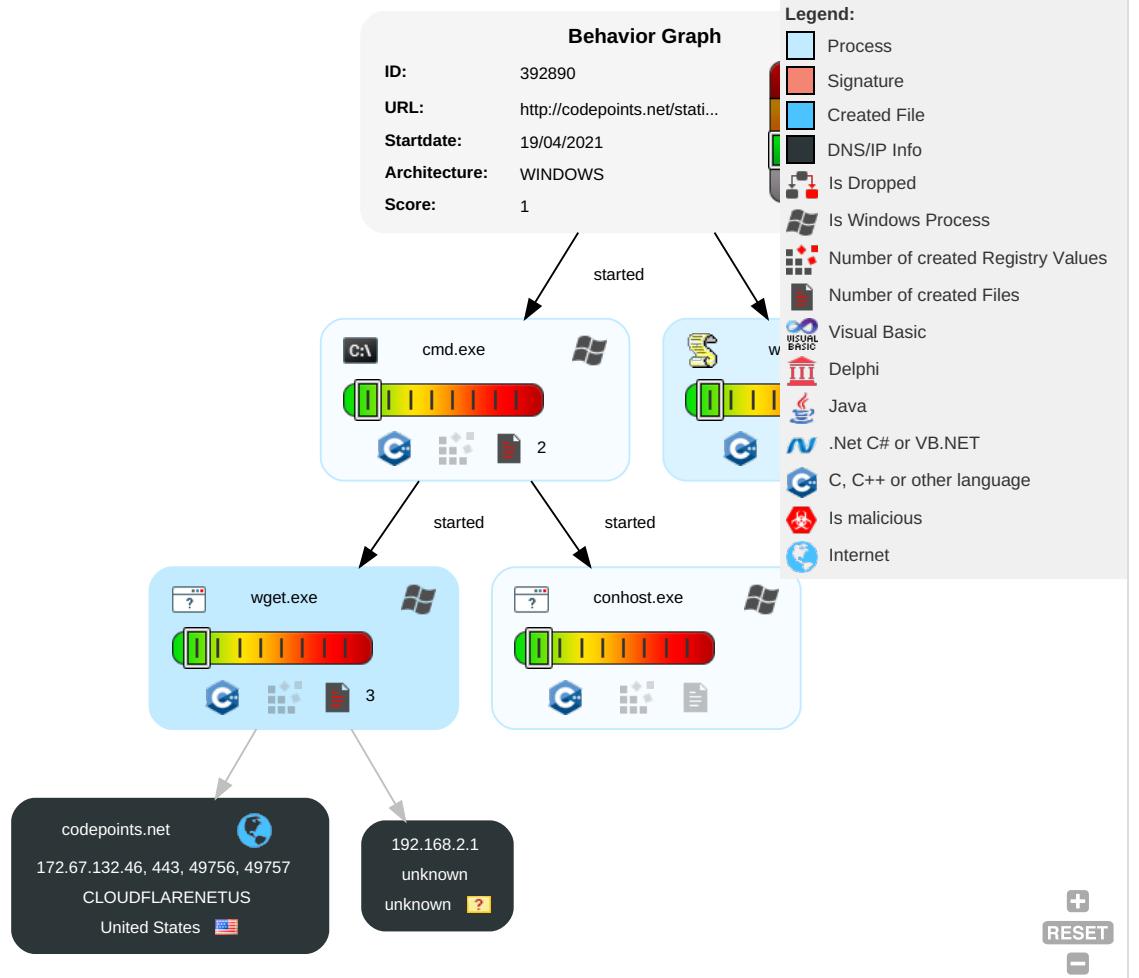
💡 Click to jump to signature section

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	Scripting 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	System Information Discovery 1 2	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	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	Remote System Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap		Carrier Billing Fraud

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://codepoints.net/static/js/codepoint.js!3c67217e710120291b75e8c13546e320?_=1618365050047	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://https://use.typekit.net:G	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
codepoints.net	172.67.132.46	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://codepoints.net/static/js/codepoint.js!3c67217e710120291b75e8c13546e320?_=1618365050047	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://use.typekit.net	wscript.exe, 00000004.00000003 .644926297.000001E10A792000.00 000004.00000001.sdmp	false		high
http://https://use.typekit.net:G	wscript.exe, 00000004.00000003 .645147006.000001E10A7DB000.00 000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://codepoints.net/static/js/codepoint.js	cmdline.out.2.dr	false		high
http://codepoints.net/static/js/codepoint.js	wget.exe, 00000002.00000002.64 0905312.0000000000B40000.00000 004.00000020.sdmp, cmdline.out.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.132.46	codepoints.net	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	392890
Start date:	19.04.2021
Start time:	23:56:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	urldownload.jbs
Sample URL:	http://codepoints.net/static/js/codepoint.js!3c67217e710120291b75e8c13546e320?_=1618365050047
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:	5
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@5/3@1/2
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 • Stop behavior analysis, all processes terminated
Warnings:	Show All • Exclude process from analysis (whitelisted): svchost.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 104.43.193.48, 40.88.32.150, 52.255.188.83 • Excluded domains from analysis (whitelisted): skypedataprddcoleus15.cloudapp.net, skypedataprddcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, skypedataprddcolcus16.cloudapp.net, watson.telemetry.microsoft.com, skypedataprddcolcus15.cloudapp.net • Execution Graph export aborted for target wget.exe, PID 6188 because there are no executed function • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

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\luser\Desktop\cmdline.out

Process:	C:\Windows\SysWOW64\wget.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1084
Entropy (8bit):	5.158605751644497
Encrypted:	false
SSDEEP:	24:PoGM1ZWw+2ZWXxeP6xMZovPoxMM2ZWSxePgSb7FnN6Kb71:AGAWwXZWxbexCZWSYb+KbJ
MD5:	499EEFC60ADFE5425E5B2662B63E459C
SHA1:	22F0C635D5D645E832C084A3039BEF90D0CD0F9E
SHA-256:	4C3983BA84EFC540F73F75A54375171A15FBF216469DD5D06D67AD47F7F14465
SHA-512:	B74D6D28B6EAA6D19B612DAA86AC6E965CB23E5D58C5447BB47BE187F5460940EF9329A589029C5FE73F6BF41DA0A498F79EE20F3560D5B82879477AEDDA625D
Malicious:	false
Reputation:	low
Preview:	--2021-04-19 23:57:03-- http://codepoints.net/static/js/codepoint.js!3c67217e710120291b75e8c13546e320?_=1618365050047..Resolving codepoints.net (codepoints.net)... 172.67.132.46, 104.21.12.155..Connecting to codepoints.net (codepoints.net)[172.67.132.46]:80... connected...HTTP request sent, awaiting response... 301 Moved Permanently..Location: https://codepoints.net/static/js/codepoint.js!3c67217e710120291b75e8c13546e320?_=1618365050047 [following]..--2021-04-19 23:57:03-- https://codepoints.net/static/js/codepoint.js!3c67217e710120291b75e8c13546e320?_=1618365050047..Connecting to codepoints.net (codepoints.net)[172.67.132.46]:443... connected...HTTP request sent, awaiting response... 200 OK..Length: unspecified [application/javascript]..Saving to: 'C:/Users/user/Desktop/download/codepoint.js!3c67217e710120291b75e8c13546e320@_1618365050047'.... OK 352K=0.09s....2021-04-19 23:57:04 (352 KB/s) - 'C:/Users/user/Desktop/downl

C:\Users\luser\Desktop\download\wget-hsts

Process:	C:\Windows\SysWOW64\wget.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	173
Entropy (8bit):	5.135446645530035
Encrypted:	false
SSDEEP:	3:SY2FyFARLibwFAM9CxnOLVFzDwlVhyJxWQ5RdkA8dyDFs0XRcRBsWaov:SYeRLibA0noH9VhyJQQ5oA8UDi5xSWT
MD5:	12EEDA5DB822588D995F9481D35EFBED
SHA1:	CAA0F4033F580F969D906396D9B4F8384F2FBAF3
SHA-256:	F5C45299A53223ABB1B3222A47614D9BF2BA89B778278B440371515BF25EF80D
SHA-512:	B971ADFF69992DAE09974A9683C4A46C86E50A36F3007C544E449E391856C8099821E0178D996C58FA4DB06E2BA195340DA4D7005417629948FD8A7910A6B1C6
Malicious:	false
Reputation:	low
Preview:	# HSTS 1.0 Known Hosts database for GNU Wget...# Edit at your own risk...# <hostname>.<port>.<incl. subdomains>.<created>.<max-age>..codepoints.net.0.0.1618869424.31536000..

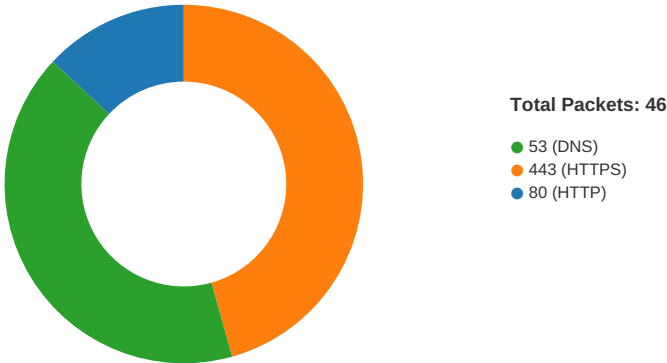
C:\Users\user1\Desktop\download\codepoint.js!3c67217e710120291b75e8c13546e320@_ =1618365050047	
Process:	C:\Windows\SysWOW64\wget.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	31433
Entropy (8bit):	5.334704231959762
Encrypted:	false
SSDEEP:	768:hkhSZhy+WU3ex7IVB3vCg+nMo9mNaOHf8cKXJXac:hAw3CIGoVKXJXD
MD5:	3C67217E710120291B75E8C13546E320
SHA1:	AA9D4DC6BCB030B4B3669D98D1F2474D60544A5C
SHA-256:	BC3DAD26E9361E22809C5DA883066BFC4C724FDFBD552BB6E048F7DF5353FA38
SHA-512:	8F2EA8352350BBEE3E7E43F258D0607778BB27695F9E664F06E3689B1B6C1696FEC7C34122F882F8EBC726F0D4D47035C1E10A2EF52CDC6E5B497F9096AD0459
Malicious:	false
Reputation:	low
Preview:	!function(a){function b(a,b,e){return 4===arguments.length?c.apply(this,arguments):void d(a,{declarative:!0,deps:b,declare:e})}function c(a,b,c,e){d(a,{declarative:!1,deps:b,executingRequire:c,execute:e})}function d(a,b){b.name=a,a in n (n[a]=b),b.normalizedDeps=b.deps}function e(a,b){if(b[a.groupIndex]=b[a.groupIndex] [],-1===o.call(b[a.groupIndex],a)){b[a.groupIndex].push(a);for(var c=0,d=a.normalizedDeps.length;d>c;c++){var f=a.normalizedDeps[c],g=n[f];if(g&&!g.evaluated){var h=a.groupIndex+(g.declarative?a.declarative):if(void 0===g.groupIndex g.groupIndex<h){if(void 0!==g.groupIndex&&(b[g.groupIndex].splice(o.call(b[g.groupIndex],g),1),0===b[g.groupIndex].length))throw new TypeError("Mixed dependency cycle detected");g.groupIndex=h}e(g,b)}}}function f(a){var b=n[a];b.groupIndex=0;var c=[];e(b,c);for(var d=!b.declarative==c.length%2,f=c.length-1,f>=0,f--){for(var g=c[f],i=0;i<g.length;i++){var k=g[i];d?h(k):j(k)}d=!d}}function g(a){return s[a]}(s[a]={name:a,dependencies:[],exp

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 19, 2021 23:57:03.519366980 CEST	49756	80	192.168.2.4	172.67.132.46
Apr 19, 2021 23:57:03.571017981 CEST	80	49756	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:03.571142912 CEST	49756	80	192.168.2.4	172.67.132.46
Apr 19, 2021 23:57:03.572415113 CEST	49756	80	192.168.2.4	172.67.132.46
Apr 19, 2021 23:57:03.623956919 CEST	80	49756	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:03.673808098 CEST	80	49756	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:03.673851967 CEST	80	49756	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:03.673914909 CEST	49756	80	192.168.2.4	172.67.132.46
Apr 19, 2021 23:57:03.766424894 CEST	49757	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:57:03.818058968 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:03.818173885 CEST	49757	443	192.168.2.4	172.67.132.46

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 19, 2021 23:57:03.822818041 CEST	49757	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:57:03.875365019 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:03.879390955 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:03.879448891 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:03.879513979 CEST	49757	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:57:03.882630110 CEST	49757	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:57:03.935578108 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:03.935746908 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:03.938401937 CEST	49757	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:57:03.989964008 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:04.108247995 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:04.108270884 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:04.108290911 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:04.108304024 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:04.108319044 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:04.108335972 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:04.108350992 CEST	49757	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:57:04.108352900 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:04.108372927 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:04.108380079 CEST	49757	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:57:04.108396053 CEST	49757	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:57:04.108416080 CEST	49757	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:57:04.109473944 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:04.109492064 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:04.109659910 CEST	49757	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:57:04.110627890 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:04.110646963 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:04.110697985 CEST	49757	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:57:04.111912966 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:04.111929893 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:04.111999035 CEST	49757	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:57:04.113037109 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:04.113058090 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:04.113158941 CEST	49757	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:57:04.114347935 CEST	49756	80	192.168.2.4	172.67.132.46
Apr 19, 2021 23:57:04.114356995 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:04.114382982 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:04.114444017 CEST	49757	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:57:04.115513086 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:04.115535975 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:04.115586042 CEST	49757	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:57:04.116678953 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:04.116703033 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:04.116754055 CEST	49757	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:57:04.118690014 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:04.118721962 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:04.118782043 CEST	49757	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:57:04.119077921 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:04.119107008 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:04.119172096 CEST	49757	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:57:04.120260954 CEST	443	49757	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:04.168994904 CEST	80	49756	172.67.132.46	192.168.2.4
Apr 19, 2021 23:57:04.169087887 CEST	49756	80	192.168.2.4	172.67.132.46
Apr 19, 2021 23:57:04.170644999 CEST	49757	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:57:04.579210043 CEST	49757	443	192.168.2.4	172.67.132.46

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 19, 2021 23:56:55.975506067 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:56:56.024126053 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 19, 2021 23:56:56.861954927 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:56:56.923043966 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 19, 2021 23:56:57.825664997 CEST	56794	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 19, 2021 23:56:57.874341011 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 19, 2021 23:57:00.310434103 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:57:00.359138966 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 19, 2021 23:57:01.310204029 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:57:01.361684084 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 19, 2021 23:57:02.209863901 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:57:02.258493900 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 19, 2021 23:57:03.230737925 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:57:03.281030893 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 19, 2021 23:57:03.451055050 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:57:03.509973049 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 19, 2021 23:57:04.222884893 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:57:04.272931099 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 19, 2021 23:57:05.138631105 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:57:05.188189983 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 19, 2021 23:57:06.364178896 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:57:06.424177885 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 19, 2021 23:57:07.255764008 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:57:07.307087898 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 19, 2021 23:57:08.427530050 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:57:08.476598978 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 19, 2021 23:57:09.322879076 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:57:09.373547077 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 19, 2021 23:57:11.222143888 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:57:11.280639887 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 19, 2021 23:57:12.014138937 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:57:12.075429916 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 19, 2021 23:57:12.836302996 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:57:12.887886047 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 19, 2021 23:57:13.731420994 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:57:13.784745932 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 19, 2021 23:57:14.555850983 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:57:14.615953922 CEST	53	56448	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 19, 2021 23:57:03.451055050 CEST	192.168.2.4	8.8.8.8	0x983f	Standard query (0)	codepoints.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 19, 2021 23:57:03.509973049 CEST	8.8.8.8	192.168.2.4	0x983f	No error (0)	codepoints.net		172.67.132.46	A (IP address)	IN (0x0001)
Apr 19, 2021 23:57:03.509973049 CEST	8.8.8.8	192.168.2.4	0x983f	No error (0)	codepoints.net		104.21.12.155	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

codepoints.net
--

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49756	172.67.132.46	80	C:\Windows\SysWOW64\lwget.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
Apr 19, 2021 23:57:03.572415113 CEST	961	OUT	GET /static/js/codepoint.js!3c67217e710120291b75e8c13546e320?_=1618365050047 HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko Accept: */* Accept-Encoding: identity Host: codepoints.net Connection: Keep-Alive
Apr 19, 2021 23:57:03.673808098 CEST	967	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 19 Apr 2021 21:57:03 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d3be4f12ed524a7cd3868342ba1761cd71618869423; expires=Wed, 19-May-21 21:57:03 GMT; path=/; domain=.codepoints.net; HttpOnly; SameSite=Lax Location: https://codepoints.net/static/js/codepoint.js!3c67217e710120291b75e8c13546e320?_=1618365050047 CF-Cache-Status: DYNAMIC cf-request-id: 098dbc25f80000002aab92e000000001 Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a.nel.cloudflare.com/vreport?s=NNQcSV3PT8t8qOGllCLeYqxt0Ndnw7ZU4GCDzEAq4iGppRU5ExR7aW7prz0%2FYemWCQ6Z9kdCaVNDNRsOQQeuvDvtZn0uB1xRhM6mGSOHig%3D%3D"}]}\nNEL: {"max_age":604800,"report_to":"cf-nel"}\nServer: cloudflare\nCF-RAY: 642962e98c9c002a-LHR\nalt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400\nData Raw: 61 32 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 0d 0a\nData Ascii: a2<html><head><title>301 Moved Permanently</title></head><body><center> 301 Moved Permanently </center><hr><center>nginx</center></body></html>

HTTPS Packets

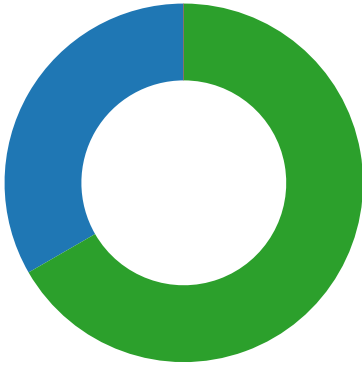
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 19, 2021 23:57:03.879448891 CEST	172.67.132.46	443	192.168.2.4	49757	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Jul 24 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Sat Jul 24 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49200-159-52393-52392-52394-49195-49199-158-49188-49192-107-49187-49191-103-49162-49172-57-49161-49171-51-157-156-61-60-53-47-255,0-11-10-35-22-23-13,29-23-25-24,0-1-2	807fca46d9d0cf63adf4e5e80e414bbe
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior

- cmd.exe
- conhost.exe
- wget.exe
- wscript.exe



Click to jump to process

System Behavior

Analysis Process: cmd.exe PID: 7108 Parent PID: 1284

General

Start time:	23:57:01
Start date:	19/04/2021
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://codepoints.net/static/js/codepoint.js!3c67217e710120291b75e8c13546e320?_1618365050047' > 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: 7128 Parent PID: 7108

General

Start time:	23:57:02
Start date:	19/04/2021
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: 6188 Parent PID: 7108

General

Start time:	23:57:03
Start date:	19/04/2021
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://codepoints.net/static/js/codepoint.js!3c67217e710120291b75e8c13546e320?_=1618365050047'
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\codepoint.js!3c67217e710120291b75e8c13546e320@_1618365050047	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	46596C	fopen
C:\Users\user\Desktop\download\wget-hsts	read attributes synchronize generic read 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
-----------	--------	--------	------------	-------	----------------	--------

Analysis Process: wscript.exe PID: 6728 Parent PID: 6032

General

Start time:	23:57:05
Start date:	19/04/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\Desktop\download\codepoint.js!3c67217e710120291b75e8c13546e320@_1618365050047.js'
Imagebase:	0x7ff6c83b0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Disassembly

Code Analysis