ID: 392889
Cookbook: browseurl.jbs
Time: 23:53:08
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?_=1618365050047 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
General Information 8
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 13
No static file info 13
Network Behavior 13
Network Port Distribution 13
TCP Packets 13
UDP Packets 14
DNS Queries 16
DNS Answers 16
HTTPS Packets 16
Code Manipulations 16
Statistics 16
Behavior 17
System Behavior 17
Analysis Process: iexplore.exe PID: 6892 Parent PID: 800 17
General 17
File Activities 17
Registry Activities 17
Analysis Process: iexplore.exe PID: 6956 Parent PID: 6892 17

General 18
File Activities 18
Analysis Process: wscript.exe PID: 4592 Parent PID: 6892 18
General 18
File Activities 18
Disassembly 18
Code Analysis 18

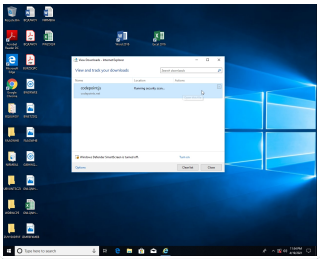
Analysis Report http://codepoints.net/static/js/codepoin…

Overview

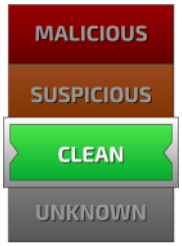
General Information

Sample URL:	http://codepoints.net/static/js/codepoint.js!3c67217e710120291b75e8c13546e320?_=1618365050047
Analysis ID:	392889
Infos:	

Most interesting Screenshot:



Detection

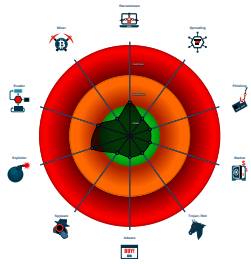


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Found WSH timer for Javascript or V…
- Potential browser exploit detected (p…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6892 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6956 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6892 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - wscript.exe (PID: 4592 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\codepoint.js' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- **cleanup**

Malware Configuration

No configs have been found

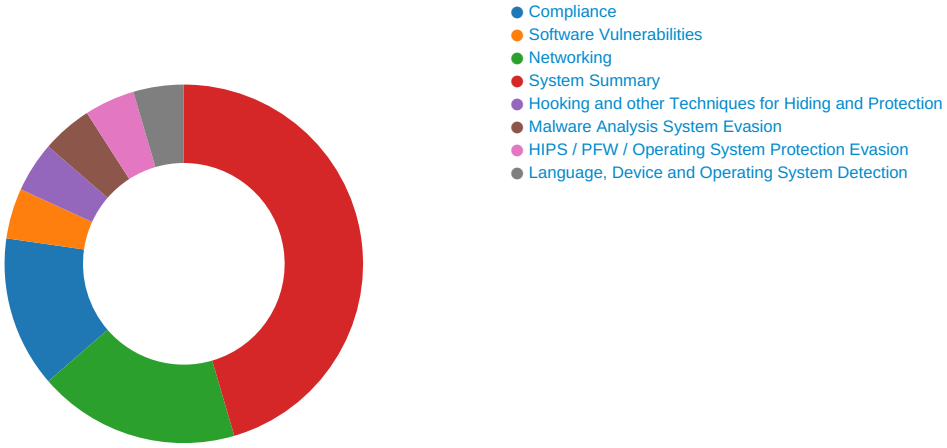
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



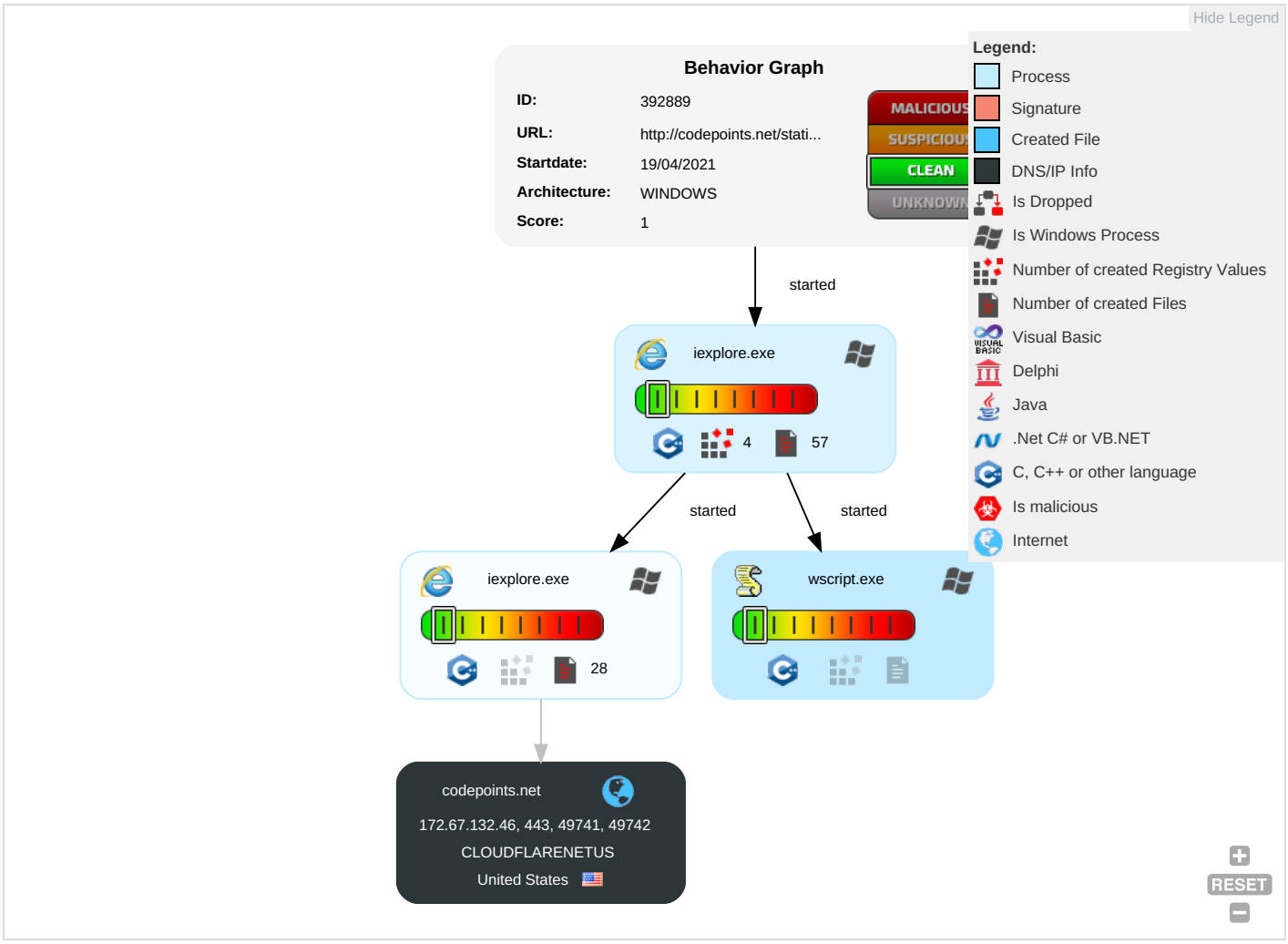
Click to jump to signature section

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 2	Masquerading 1	OS Credential Dumping	Process Discovery 1	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	Exploitation for Client Execution 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 2	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	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	System Information Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

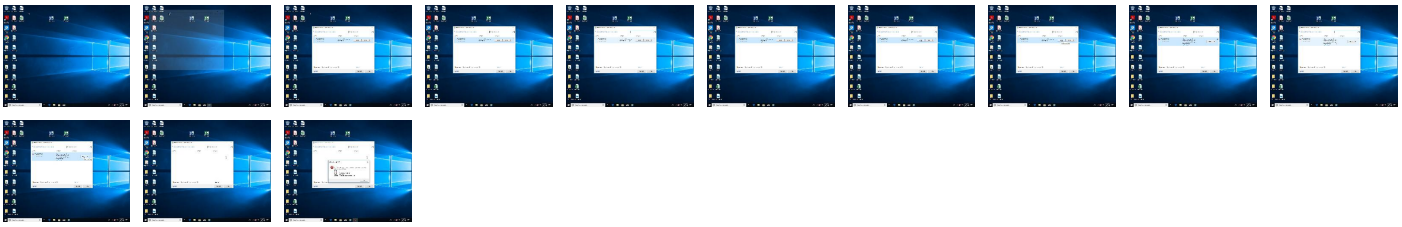
Behavior Graph

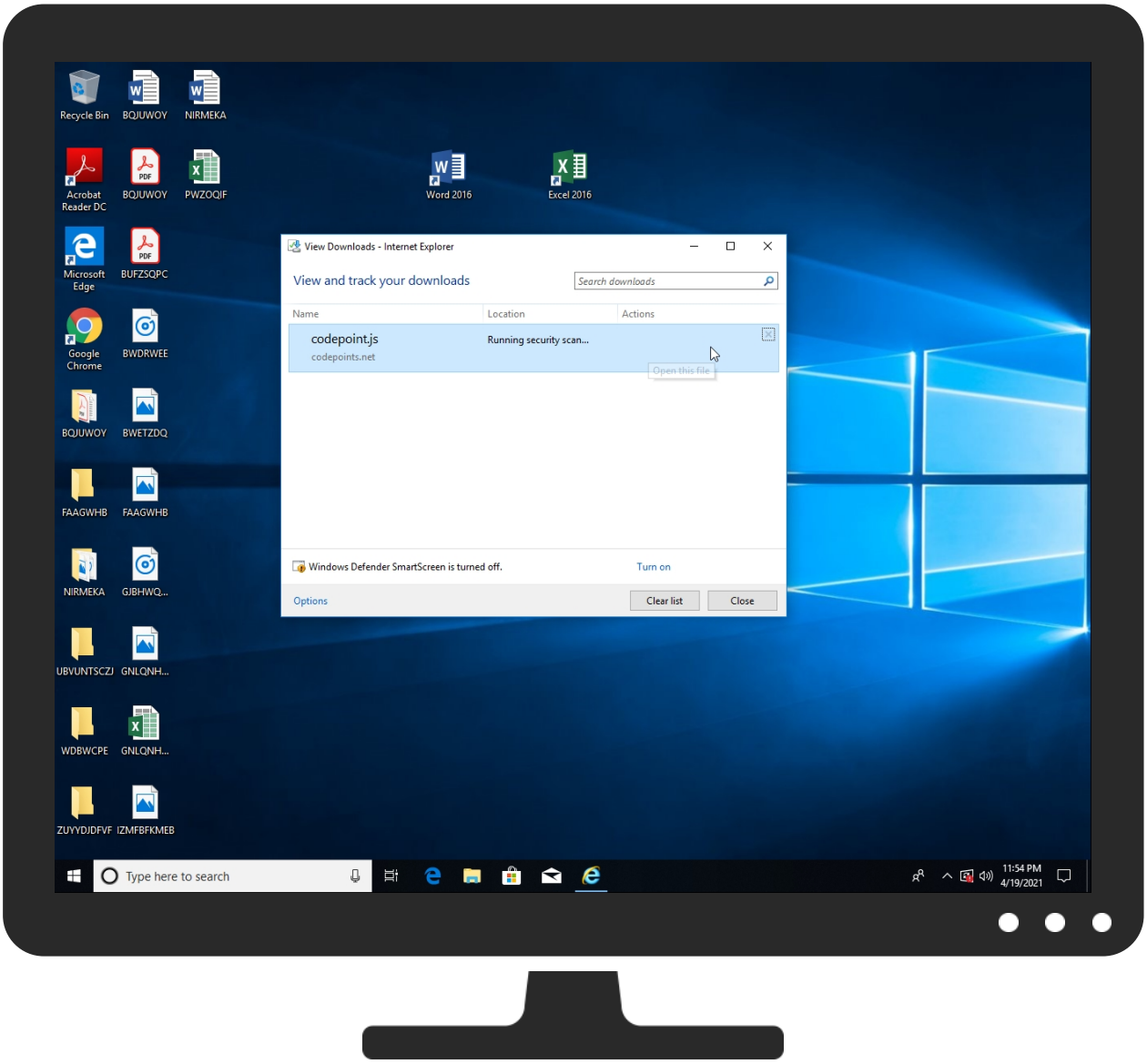


Screenshots

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	
0	1%	Virustotal		Browse

Domains and IPs

Contacted Domains

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

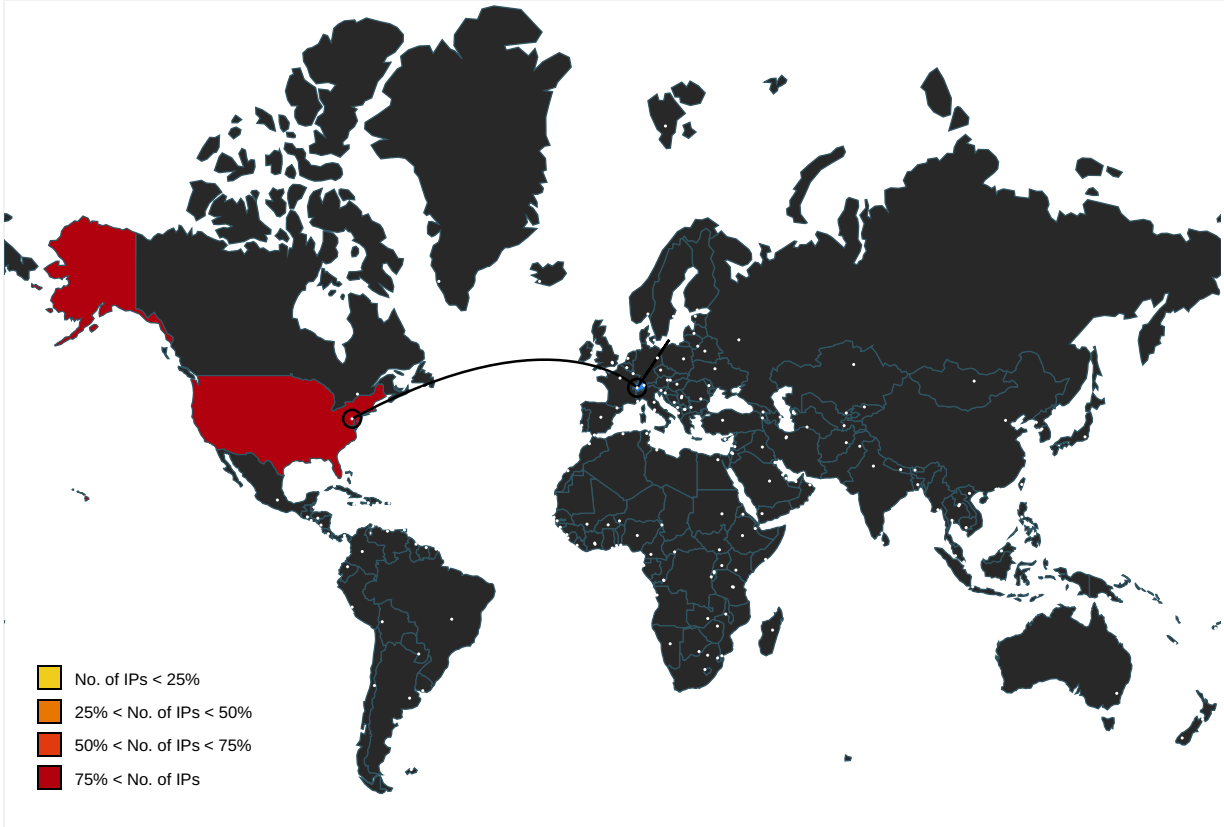
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
0	false	• 1%, Virustotal, Browse	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://use.typekit.net	wscript.exe, 0000000D.00000003.729131342.00000209392D1000.00000004.00000001.sdmp	false		high
http://https://use.typekit.net:G	wscript.exe, 0000000D.00000003.729206190.000002093930D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	392889
Start date:	19.04.2021

Start time:	23:53:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.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:	19
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.win@5/9@1/1
EGA 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
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.255.188.83, 168.61.161.212, 40.88.32.150, 88.221.62.148, 20.82.209.104, 92.122.213.194, 92.122.213.247, 152.199.19.161, 52.155.217.156, 20.54.26.129, 2.20.142.210, 2.20.142.209, 20.49.157.6 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, go.microsoft.com, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, ie9comview.vo.msecnd.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtProtectVirtualMemory 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\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{BACD341B-A159-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	32344
Entropy (8bit):	1.7941498862400327
Encrypted:	false
SSDEEP:	192:r+ZFZl2SpWSptSgHifSg0UAazMSL0MSBSZ0eMCkUZASt00Q2p2:rKr8zUNgN0VO0jk03k00m
MD5:	63C210596BA8430CE15F8FB3B6D249D1
SHA1:	5D50CCB96AF48C9F6293B3992B00F81A1017B046
SHA-256:	11BD99350A5AF2948531B54D8A6EB5731614F6E32CD2DE35FA33588CCA1F0675
SHA-512:	4E93A90B23F5DC6CD4B33662B886C6ACC381FC3F658A31C59468B25FE7F2B3E0EC03427F36CAADF9F96ADEFF648DC148AB6D05390E7404AB51C0BF9052073BC
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r.y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{BACD341D-A159-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.5981621410564495
Encrypted:	false
SSDEEP:	48:IwKGcprXGwpawG4pQgGrapbSR9GQpB2GHHpceTGUpQBWGcpm:ruZBQw6+BSpj12u6Eg
MD5:	1C2972613848EC9E93E2E068F4FAC735
SHA1:	A03BD40A142E7E7D95FF7D3B5715E22597DDFECD
SHA-256:	7394474F9BB1DEC697CF0303BDAAB1E9A01208DCC63B01D210671F687E52303E
SHA-512:	A1324B49C150527682587BE193E2BB939BFC71E4D2919E807F2685535CF05D9D88BBE16995C7649F4F978042C0EB827A2E9623C18A22B2C3735715B29EF2D986
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{BACD341D-A159-11EB-90EB-ECF4BBEA1588}.dat	
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\codepoint.js.m2r13t2.partial	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.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+WU3ex7lVB3vCg+nMo9mNaOHf8cKXJXac:hAw3ClGoVKXJXD
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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\codepoint.js.m2r13t2.partial:Zone.Identifier	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:gAWY3n:qY3n
MD5:	FBCCF14D504B7B2DBCB5A5BDA75BD93B
SHA1:	D59FC84CDD5217C6CF74785703655F78DA6B582B
SHA-256:	EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913
SHA-512:	AA1D2B1EA3C9DE3CCADB319D4E3E3276A2F27DD1A5244FE72DE2B6F94083DDDC762480482C5C2E53F803CD9E3973DDEFC68966F974E124307B5043E654443E 8
Malicious:	false
Reputation:	low
Preview:	[ZoneTransfer]..ZoneId=3..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\codepoint.js:Zone.Identifier	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	very short file (no magic)
Category:	modified
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:W:W
MD5:	ECCBC87E4B5CE2FE28308FD9F2A7BAF3
SHA1:	77DE68DAECD823BABBB58EDB1C8E14D7106E83BB
SHA-256:	4E07408562BEDB8B60CE05C1DECFE3AD16B72230967DE01F640B7E4729B49FCE
SHA-512:	3BAFBF08882A2D10133093A1B8433F50563B93C14ACD05B79028EB1D1279902724145098065199450142 3A66C276AE26C43B739BC65C4E16B10C3AF6C202AEBB
Malicious:	false
Reputation:	low
Preview:	3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\codepoint[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\codepoint[1].js	
Size (bytes):	31433
Entropy (8bit):	5.334704231959762
Encrypted:	false
SSDEEP:	768:hkhSZhy+WU3ex7lVB3vCg+nMo9mNaOHf8cKXJXac:hAw3ClGoVKXJXD
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,dep
s: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.g
roupIndex].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
```

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	89
Entropy (8bit):	4.502442319249751
Encrypted:	false
SSDEEP:	3:oVXU1fzW8JOGXnE1fVCn:o9Up6qEpVC
MD5:	EAB023F74C7A0D3B35935F1D7C242560
SHA1:	2034F413A40B4A08AAB3DD2232C9E75CB082EC72
SHA-256:	DA7B11CFA7DCC7523DA89A6020DB5EA07912CE8FB8A16ADE8E61CC150D6E1CA5
SHA-512:	C33D88140A2476D9349099BF6EF7FFB40130AB956B70913F1456CFF8BBC34E3582DF9130238703AB0180B18E744DDCC439C03829EF59DF04AC8544E41C5580BA
Malicious:	false
Reputation:	low
Preview:	[2021/04/19 23:53:54.263] Latest deploy version: ..[2021/04/19 23:53:54.263] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DFF10E4E5C2FE6A606.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	29989
Entropy (8bit):	0.3305105966046147
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lw39lw39l2h/9l2Z9law:kBqoxKAuvScS+gmh+QBy
MD5:	87D717A7239FBFCFA6CE0CA547C583F0
SHA1:	D1F8622B5CBA4F9D8CE762090A64825CB05EDBB3
SHA-256:	958EDB88873835EDEA1CDD82D0128ADA5BEC43242C062E4DB2967499455E639D
SHA-512:	1B17FD22E5ECCCEC39926AD279C3E7F279E3A0B37DFF5AD2F531D9577C0FC15A2F97B4B28C01FA193AA34CD1E86B08C2D9FAECEA1CF23ACFA86D1CB5DC0E 3D68
Malicious:	false
Reputation:	low

Preview:

```
............................*%..H..M..{y..+.0...(.................. ..............................................*%..H..M..{y..+.0...(.................. ..........................................................................................
..................................................................................................................................................................................................................................................
..................................................................................................................................................................................................................................................
..........................................................................................................................................................................
```

C:\Users\user\AppData\Local\Temp\~DFF181345E7CC054BD.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12981
Entropy (8bit):	0.44336979889492417
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fRIF9l8fRw9lTqSYfUn9QES:c9lLh9lLh9lIn9lIn9log9low9lWSsU6
MD5:	42CBB93022266593F3358865644E168C
SHA1:	995496AF94565B4FE101551FBE96E86159406F7F
SHA-256:	1C4C5610D495EAB04D485C792486E339F6A8A83FF9CC7738D35AC3F9C2698F52

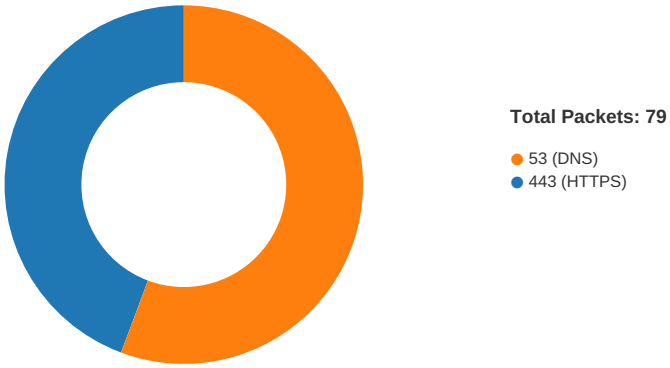
C:\Users\user\AppData\Local\Temp\~DFF181345E7CC054BD.TMP	
SHA-512:	E50FD016C2C724AAF32AE28A6C74375F48A41C4D8A3BD3769939CC97A559F196C97C49DD753DAA263FCF71D30F8EC3EA3B2AFD27FF5D768C04D965157D98FD8
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

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 23:53:54.975366116 CEST	49741	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:53:54.975625038 CEST	49742	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:53:55.028001070 CEST	443	49742	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.028196096 CEST	49742	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:53:55.028794050 CEST	443	49741	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.028918982 CEST	49741	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:53:55.039735079 CEST	49741	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:53:55.039845943 CEST	49742	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:53:55.092560053 CEST	443	49742	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.092945099 CEST	443	49741	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.096431971 CEST	443	49741	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.096483946 CEST	443	49741	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.096546888 CEST	49741	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:53:55.096590996 CEST	49741	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:53:55.099276066 CEST	443	49742	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.099323988 CEST	443	49742	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.099378109 CEST	49742	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:53:55.099450111 CEST	49742	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:53:55.141254902 CEST	49742	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:53:55.141336918 CEST	49741	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:53:55.148056030 CEST	49742	443	192.168.2.4	172.67.132.46

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 19, 2021 23:53:55.148190975 CEST	49741	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:53:55.148210049 CEST	49742	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:53:55.193818092 CEST	443	49742	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.194015980 CEST	443	49742	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.194118023 CEST	49742	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:53:55.194148064 CEST	443	49742	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.194226027 CEST	49742	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:53:55.194334984 CEST	443	49741	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.194813967 CEST	443	49741	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.194849014 CEST	443	49741	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.194906950 CEST	49741	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:53:55.194957018 CEST	49741	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:53:55.195952892 CEST	49742	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:53:55.196392059 CEST	49741	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:53:55.200213909 CEST	443	49742	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.200261116 CEST	443	49742	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.200916052 CEST	443	49742	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.200943947 CEST	443	49741	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.200968981 CEST	443	49741	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.201105118 CEST	49742	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:53:55.201205969 CEST	49741	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:53:55.288170099 CEST	443	49742	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.288214922 CEST	443	49741	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.315992117 CEST	443	49742	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.316023111 CEST	443	49742	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.316046000 CEST	443	49742	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.316061020 CEST	443	49742	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.316086054 CEST	443	49742	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.316102028 CEST	443	49742	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.316142082 CEST	49742	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:53:55.316327095 CEST	49742	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:53:55.316525936 CEST	443	49742	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.316553116 CEST	443	49742	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.316581964 CEST	49742	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:53:55.316625118 CEST	49742	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:53:55.317790031 CEST	443	49742	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.317821980 CEST	443	49742	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.317877054 CEST	49742	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:53:55.317898035 CEST	49742	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:53:55.318979025 CEST	443	49742	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.319009066 CEST	443	49742	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.319062948 CEST	49742	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:53:55.319086075 CEST	49742	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:53:55.320161104 CEST	443	49742	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.320187092 CEST	443	49742	172.67.132.46	192.168.2.4
Apr 19, 2021 23:53:55.320357084 CEST	49742	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:53:55.320379019 CEST	49742	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:54:10.300618887 CEST	49742	443	192.168.2.4	172.67.132.46
Apr 19, 2021 23:54:10.300745010 CEST	49741	443	192.168.2.4	172.67.132.46

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 19, 2021 23:53:46.515996933 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:53:46.567748070 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 19, 2021 23:53:47.310153961 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:53:47.367610931 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 19, 2021 23:53:48.240883112 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:53:48.300683975 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 19, 2021 23:53:49.060908079 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:53:49.121968031 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 19, 2021 23:53:49.955579042 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:53:50.004164934 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 19, 2021 23:53:51.012029886 CEST	51726	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 19, 2021 23:53:51.063780069 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 19, 2021 23:53:51.937895060 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:53:51.986617088 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 19, 2021 23:53:53.318337917 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:53:53.375696898 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 19, 2021 23:53:53.667521954 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:53:53.731132984 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 19, 2021 23:53:54.497611046 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:53:54.546381950 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 19, 2021 23:53:54.884290934 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:53:54.961283922 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 19, 2021 23:53:55.336338043 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:53:55.385243893 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 19, 2021 23:53:56.268110037 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:53:56.325206041 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 19, 2021 23:53:57.103991032 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:53:57.162662029 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 19, 2021 23:53:57.993885994 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:53:58.049508095 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 19, 2021 23:53:58.806931973 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:53:58.858587980 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 19, 2021 23:53:59.930802107 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:53:59.979367018 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 19, 2021 23:54:00.723134041 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:54:00.771675110 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 19, 2021 23:54:01.595043898 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:54:01.645509958 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 19, 2021 23:54:02.619385958 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:54:02.679955959 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 19, 2021 23:54:15.911190987 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:54:15.984669924 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 19, 2021 23:54:20.449359894 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:54:20.511166096 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 19, 2021 23:54:23.664849043 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:54:23.713591099 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 19, 2021 23:54:24.674622059 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:54:24.732996941 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 19, 2021 23:54:25.688848972 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:54:25.746259928 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 19, 2021 23:54:27.704555035 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:54:27.753149033 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 19, 2021 23:54:31.720577002 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:54:31.777987957 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 19, 2021 23:54:32.448478937 CEST	59172	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:54:32.563456059 CEST	53	59172	8.8.8.8	192.168.2.4
Apr 19, 2021 23:54:33.100658894 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:54:33.233350992 CEST	53	62420	8.8.8.8	192.168.2.4
Apr 19, 2021 23:54:33.261826038 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:54:33.320349932 CEST	53	60579	8.8.8.8	192.168.2.4
Apr 19, 2021 23:54:33.804673910 CEST	50183	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:54:33.883384943 CEST	53	50183	8.8.8.8	192.168.2.4
Apr 19, 2021 23:54:34.307898998 CEST	61531	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:54:34.386250019 CEST	53	61531	8.8.8.8	192.168.2.4
Apr 19, 2021 23:54:34.932460070 CEST	49228	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:54:34.989706993 CEST	53	49228	8.8.8.8	192.168.2.4
Apr 19, 2021 23:54:35.714381933 CEST	59794	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:54:35.771601915 CEST	53	59794	8.8.8.8	192.168.2.4
Apr 19, 2021 23:54:36.296214104 CEST	55916	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:54:36.355124950 CEST	53	55916	8.8.8.8	192.168.2.4
Apr 19, 2021 23:54:37.148894072 CEST	52752	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:54:37.197535038 CEST	53	52752	8.8.8.8	192.168.2.4
Apr 19, 2021 23:54:37.968961954 CEST	60542	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:54:38.029148102 CEST	53	60542	8.8.8.8	192.168.2.4
Apr 19, 2021 23:54:38.484452009 CEST	60689	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 19, 2021 23:54:38.544632912 CEST	53	60689	8.8.8.8	192.168.2.4
Apr 19, 2021 23:54:40.879432917 CEST	64206	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:54:40.944780111 CEST	53	64206	8.8.8.8	192.168.2.4
Apr 19, 2021 23:54:52.588983059 CEST	50904	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:54:52.648052931 CEST	53	50904	8.8.8.8	192.168.2.4
Apr 19, 2021 23:54:52.668716908 CEST	57525	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:54:52.728681087 CEST	53	57525	8.8.8.8	192.168.2.4
Apr 19, 2021 23:54:55.850220919 CEST	53814	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:54:55.919131041 CEST	53	53814	8.8.8.8	192.168.2.4
Apr 19, 2021 23:55:27.933608055 CEST	53418	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:55:27.991823912 CEST	53	53418	8.8.8.8	192.168.2.4
Apr 19, 2021 23:55:29.759084940 CEST	62833	53	192.168.2.4	8.8.8.8
Apr 19, 2021 23:55:29.831799984 CEST	53	62833	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 23:53:54.884290934 CEST	192.168.2.4	8.8.8.8	0xe404	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 23:53:54.961283922 CEST	8.8.8.8	192.168.2.4	0xe404	No error (0)	codepoints.net		172.67.132.46	A (IP address)	IN (0x0001)
Apr 19, 2021 23:53:54.961283922 CEST	8.8.8.8	192.168.2.4	0xe404	No error (0)	codepoints.net		104.21.12.155	A (IP address)	IN (0x0001)

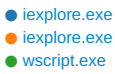
HTTPS Packets

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 23:53:55.096483946 CEST	172.67.132.46	443	192.168.2.4	49741	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=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Jul 24 02:00:00 CEST 2020	Sat Jul 24 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					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		
Apr 19, 2021 23:53:55.099323988 CEST	172.67.132.46	443	192.168.2.4	49742	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=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Jul 24 02:00:00 CEST 2020	Sat Jul 24 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					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



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6892 Parent PID: 800

General

Start time:	23:53:52
Start date:	19/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff684880000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6956 Parent PID: 6892

General

Start time:	23:53:53
Start date:	19/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6892 CREDAT:17410 /prefetch:2
Imagebase:	0x1120000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wscript.exe PID: 4592 Parent PID: 6892

General

Start time:	23:54:34
Start date:	19/04/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\codepoint.js'
Imagebase:	0x7ff7a5d90000
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