ID: 830987
Cookbook: browseurl.jbs
Time: 22:33:37
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

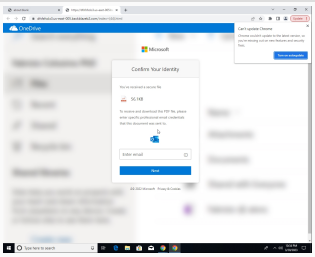
Windows Analysis Report

https://dfsfsfsd.s3.us-east-005.backblazeb2.com/index+(44).html

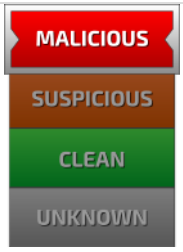
Overview

General Information

Sample URL:	http://https://dfsfsfsd.s3.us-east-005.backblazeb2.com/index+(44).html
Analysis ID:	830987
Infos:	



Detection



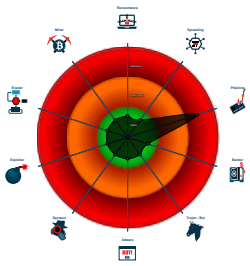
HTMLPhisher

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected HtmlPhish10
- Phishing site detected (based on log…
- Phishing site detected (based on im…
- HTML body contains low number of …
- Invalid T&C link found
- No HTML title found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 3176 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 848 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1928 --field-trial-handle=1644,i,2101607640442121641,12480239808714859300,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 4900 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://dfsfsfsd.s3.us-east-005.backblazeb2.com/index+(44).html MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
dropped/chromecache_121	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

HTML

Source	Rule	Description	Author	Strings
61093.0.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Phishing

Yara detected HtmlPhish10

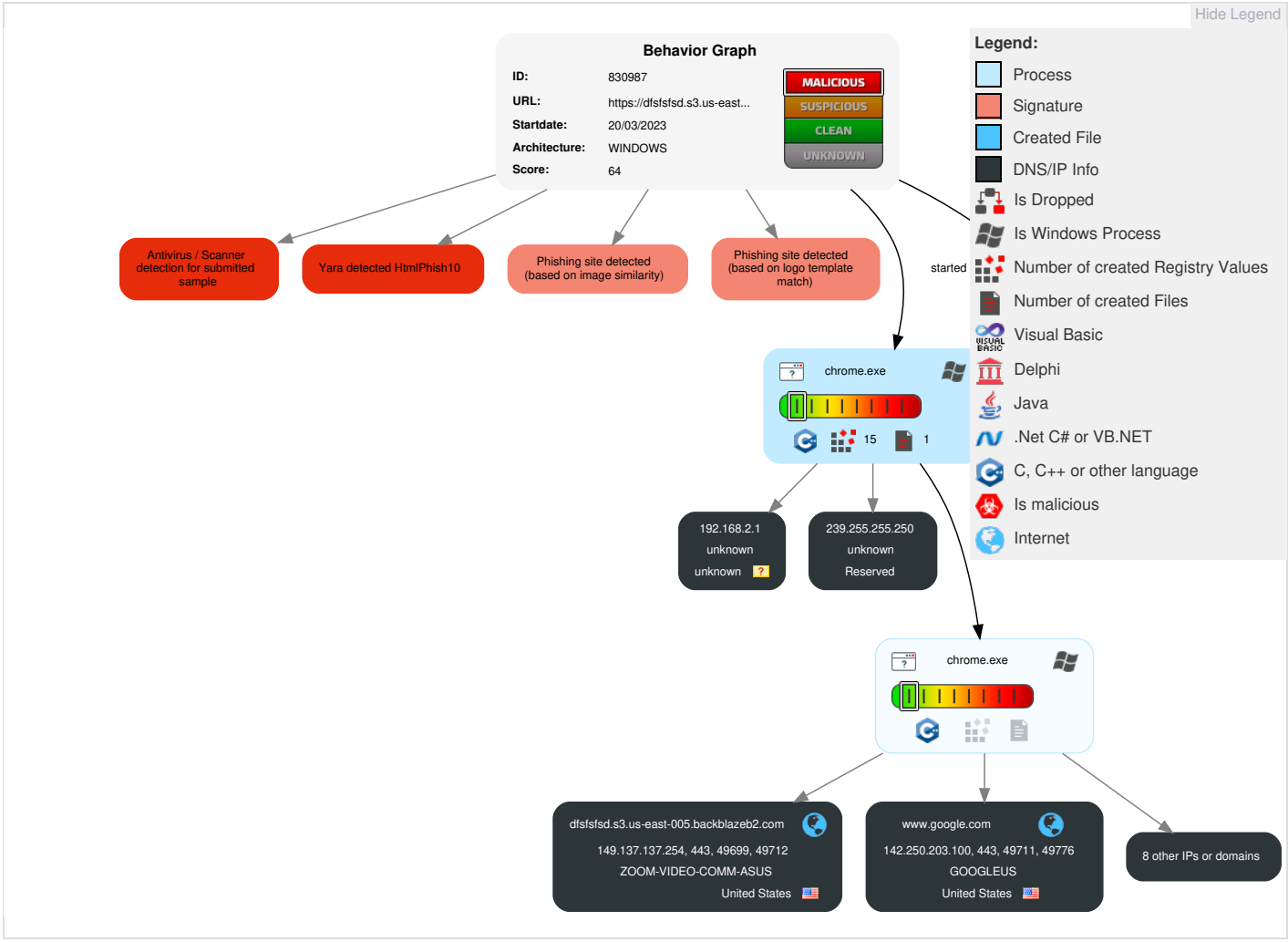
Phishing site detected (based on logo template match)

Phishing site detected (based on image similarity)

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	1 Process Injection	2 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	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	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	4 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

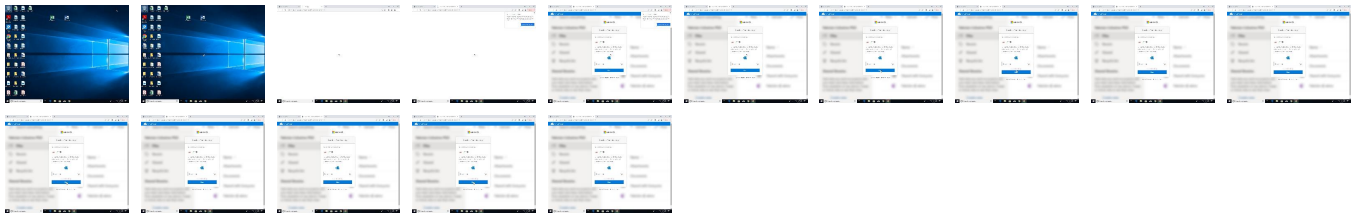
Behavior Graph

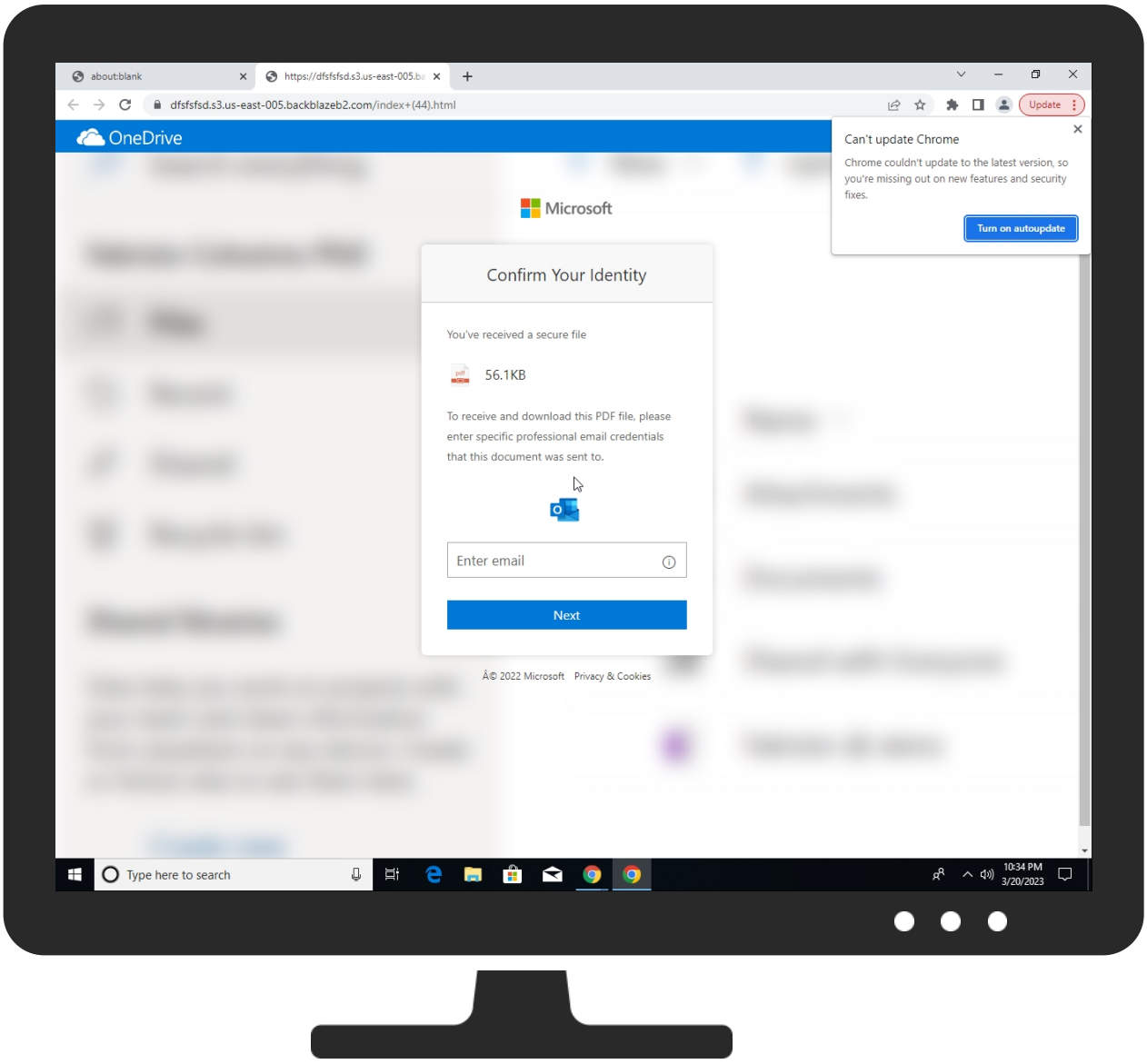


Screenshots

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://https://dfsfsfsd.s3.us-east-005.backblazeb2.com/index+(44).html	1%	Virustotal		Browse
http://https://dfsfsfsd.s3.us-east-005.backblazeb2.com/index+(44).html	0%	Avira URL Cloud	safe	
http://https://dfsfsfsd.s3.us-east-005.backblazeb2.com/index+(44).html	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://https://nwschool.ac.th/qazxcc/index.php	0%	Avira URL Cloud	safe	
http://https://dfsfsfsd.s3.us-east-005.backblazeb2.com/favicon.ico	0%	Avira URL Cloud	safe	
http://https://dfsfsfsd.s3.us-east-005.backblazeb2.com/index+(44).html	1%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
stackpath.bootstrapcdn.com	104.18.10.207	true	false		high
accounts.google.com	142.250.203.109	true	false		high
cdnjs.cloudflare.com	104.17.25.14	true	false		high
dfsfsfsd.s3.us-east-005.backblazeb2.com	149.137.137.254	true	false		unknown
maxcdn.bootstrapcdn.com	104.18.11.207	true	false		high
c-0001.c-msedge.net	13.107.4.50	true	false		unknown
www.google.com	142.250.203.100	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
clients2.google.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high

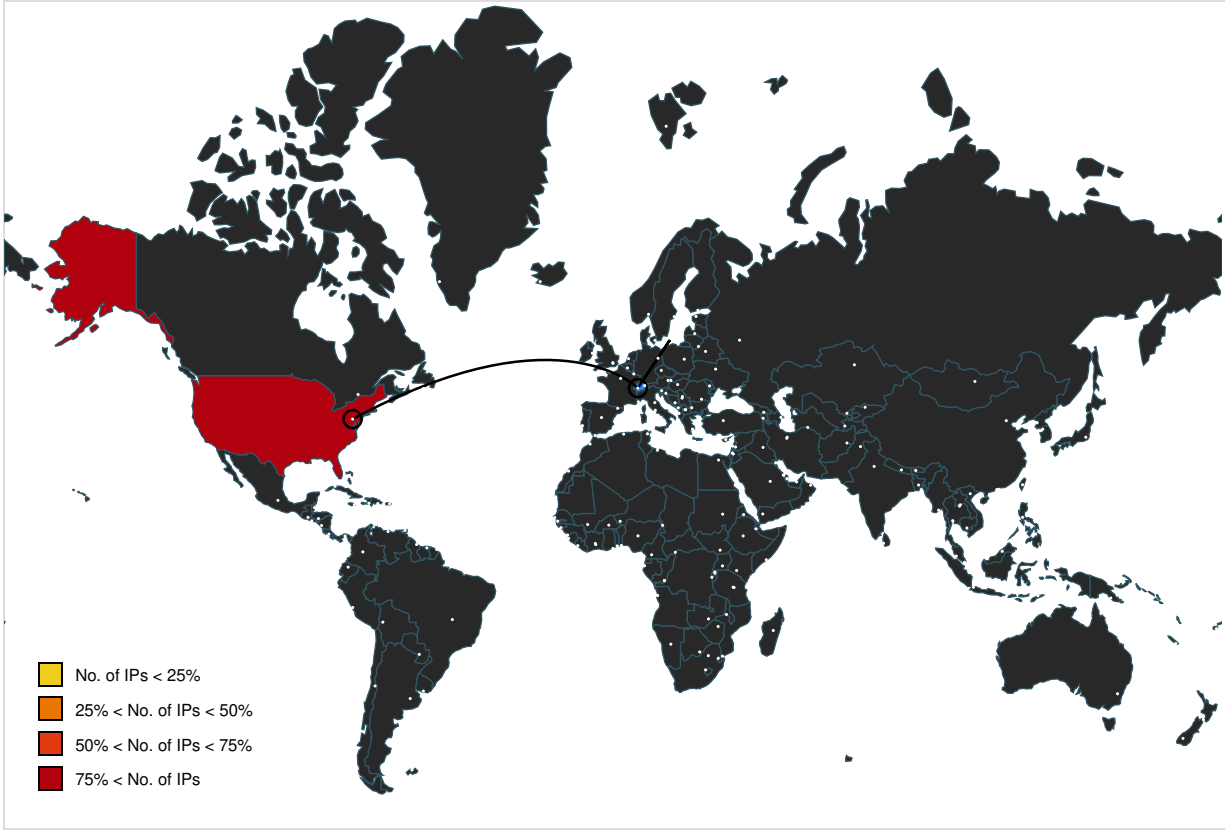
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://dfsfsfsd.s3.us-east-005.backblazeb2.com/index+(44).html	true	• 1%, Virustotal, Browse	unknown
http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://dfsfsfsd.s3.us-east-005.backblazeb2.com/index+(44).html	true	• 1%, Virustotal, Browse	unknown
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=104.0.5112.81&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/js/bootstrap.min.js	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js	false		high
http://https://dfsfsfsd.s3.us-east-005.backblazeb2.com/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/twbs/bootstrap/graphs/contributors)	chromecache_123.1.dr, chromecache_125.1.dr	false		high
http://https://getbootstrap.com)	chromecache_127.1.dr, chromecache_125.1.dr	false	• Avira URL Cloud: safe	low
http://https://code.jquery.com/jquery-3.2.1.slim.min.js	chromecache_121.1.dr	false		high
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	chromecache_123.1.dr, chromecache_127.1.dr, chromecache_125.1.dr	false		high
http://https://nwschool.ac.th/qazxcc/index.php	chromecache_121.1.dr	false	• Avira URL Cloud: safe	unknown
http://opensource.org/licenses/MIT).	chromecache_120.1.dr	false		high
http://https://getbootstrap.com/)	chromecache_123.1.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.18.10.207	stackpath.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
142.250.203.100	www.google.com	United States		15169	GOOGLEUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
149.137.137.254	dfsfsfsd.s3.us-east-005.backblazeb2.com	United States		30103	ZOOM-VIDEO-COMM-ASUS	false
104.18.11.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
104.17.25.14	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
142.250.203.109	accounts.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830987
Start date and time:	2023-03-20 22:33:37 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://dfsfsfsd.s3.us-east-005.backblazeb2.com/index+(44).html
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	14
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:	MAL
Classification:	mal64.phis.win@26/9@9/10
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 8.238.85.254, 8.248.143.254, 8.248.149.254, 8.238.191.126, 8.241.126.121, 93.184.221.240, 142.250.203.99, 3
  4.104.35.123, 172.217.168.10, 69.16.175.10, 69.16.175.42, 142.250.203.106, 216.58.215.234, 172.217.168.42
- Excluded domains from analysis (whitelisted): www.bing.com, fg.download.windowsupdate.com.c.footprint.net, fonts.googleapis.com, cds.s5x3j6q5.hwcdn.net, fs.microsoft.com, content-a
  utofill.googleapis.com, dual-a-0001.a-msedge.net, fonts.gstatic.com, ajax.googleapis.com, wu.ec.azureedge.net, ctldl.windowsupdate.com, clientservices.googleapis.com, www-www.bing.
  com.trafficmanager.net, wu-bg-shim.trafficmanager.net, wu.azureedge.net, edgedl.me.gvt1.com, www-bing-com.dual-a-0001.a-msedge.net, bg.apr-52dd2-0503.edgecastdns.net,
  cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, update.googleapis.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

Chrome Cache Entry: 120

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (19015)
Category:	downloaded
Size (bytes):	19188
Entropy (8bit):	5.212814407014048
Encrypted:	false
SSDEEP:	384:+CbuG4xGNoDic2UjKPafxwC5b/4xQviOJU7QzxzivDdE3pcGdjkd/9jt3B+Kb964:zb4xGmiJfaf7gxQvVU7eziv+cSjknZ3f
MD5:	70D3FDA195602FE8B75E0097EED74DDE
SHA1:	C3B977AA4B8DFB69D651E07015031D385DED964B
SHA-256:	A52F7AA54D7BCAAFA056EE0A050262DFC5694AE28DEE8B4CAC3429AF37FF0D66
SHA-512:	51AFFB5A8CFD2F93B473007F6987B19A0A1A0FB970DDD59EF45BD77A355D82ABBBD60468837A09823496411E797F05B1F962AE93C725ED4C00D514BA40269D1
Malicious:	false
Reputation:	low
URL:	http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js
Preview:	/*. Copyright (C) Federico Zivolo 2017. Distributed under the MIT License (license terms are at http://opensource.org/licenses/MIT).. */(function(e,t){'object'==typeof exports&&'undefined'!=typeof module?module.exports=t():'function'==typeof define&&define.amd?define(t):e.Popper=t()})(this,function(){'use strict';function e(e){return e&&'[object Function]'==={}.toString.call(e)}function t(e,t){if(1!==e.nodeType)return[];var o=getComputedStyle(e,null);return t?o[t]:o}function o(e){return'HTML'===e.nodeName?e:e.parentNode||e.host}function n(e){if(!e)return document.body;switch(e.nodeName){case'HTML':case'BODY':return e.ownerDocument.body;case'#document':return e.body;}var i=t(e),r=i.overflow,p=i.overflowX,s=i.overflowY;return /(auto|scroll)/.test(r+s+p)?e:n(o(e))}function r(e){var o=e&&e.offsetParent,i=o&&o.nodeName;return i&&'BODY'!==i&&'HTML'!==i?-1!==['TD','TABLE'].indexOf(o.nodeName)&&'static'===t(o,'position')?r(o):o:e?e.ownerDocument.documentElement:document.documentElement}functio

Chrome Cache Entry: 121

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text, with very long lines (49885), with CRLF line terminators
Category:	downloaded
Size (bytes):	882335
Entropy (8bit):	6.029784958544243
Encrypted:	false
SSDEEP:	24576:UkeW2Gb7AXLwwKoaxOkZW7FFRl8j6W9Lwv:FnWNEGVtVv
MD5:	779AC7EB624E45DDDA8A95DFE830263C
SHA1:	6AF9804E308475C08B45D9B276E345C88ED3E689
SHA-256:	5E9120662DF96B611855A9D0E9918269205EFD64358DE0491695882986148910
SHA-512:	207D9E3D210F29D7DBD54FF626F43698633841506509A69D0831028A4233AC3CE153EC788B9D53B570EC332045F8DF00C8FB30248D759BB75F971930AF467301
Malicious:	false
Reputation:	low
URL:	http://https://dfsfsfsd.s3.us-east-005.backblazeb2.com/index+(44).html
Preview:	<html>..<link rel='stylesheet prefetch' href='https://fonts.googleapis.com/css?family=Open+Sans:600'>..<style>....html {...line-height: 1.15;...-ms-text-size-adjust: 100%;...-webkit-text-size-adjust: 100%..}..body {...height: 100%;...margin: 0..}..article, aside, footer, header, nav, section {...display: block..}..h1 {...font-size: 2em;...margin: .67em 0..}..figcaption, figure, main {...display: block..}..figure {...margin: 1em 40px..}..hr {...box-sizing: content-box;...height: 0;...overflow: visible..}..pre {...font-family: monospace, monospace;...font-size: 1em..}..a {...background-color: transparent;...-webkit-text-decoration-skip: objects..}..abbr[title] {...border-bottom: none;...text-decoration: underline;...text-decoration: underline dotted..}..b, strong {...font-weight: inherit..}..b, strong {...font-weight: bolder..}..code, kbd, samp {...font-family: monospace, monospace;...font-size: 1em..}..dfn {...font-style: italic..}..mark {...background-color: #ff0;...color: #000..}..sma

Chrome Cache Entry: 122

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (32012)
Category:	downloaded
Size (bytes):	69597
Entropy (8bit):	5.369216080582935
Encrypted:	false
SSDEEP:	1536:qNhEyjjTikEJO4edXXe9J578go6MWX2xkjVe4c4j2ll2Ac7pK3F71QDU8CuT:Exc2yjq4j2uYnQDU8CuT
MD5:	5F48FC77CAC90C4778FA24EC9C57F37D
SHA1:	9E89D1515BC4C371B86F4CB1002FD8E377C1829F
SHA-256:	9365920887B11B33A3DC4BA28A0F93951F200341263E3B9CEFD384798E4BE398
SHA-512:	CAB8C4AFA1D8E3A8B7856EE29AE92566D44CEEAD70C8D533F2C98A976D77D0E1D314719B5C6A473789D8C6B21EBB4B89A6B0EC2E1C9C618FB1437EBC77D3A269
Malicious:	false
Reputation:	low

URL:	http://https://code.jquery.com/jquery-3.2.1.slim.min.js
Preview:	/*! jQuery v3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_evalUrl,-event/ajax,-effects,-effects/Tween,-effects/animatedSelector | (c) JS Foundation and other contributors | jquery.org/license */!function(a,b){"use strict";"object"==typeof module &&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_e

Chrome Cache Entry: 123

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (50758)
Category:	downloaded
Size (bytes):	51039
Entropy (8bit):	5.247253437401007
Encrypted:	false
SSDEEP:	768:E9Yw7GuJM+HV0cen/7Kh5rM7V4RxCKg8FW/xsXQUd+FiID65r48Hgp5HRl+:E9X7PMIM7V4R5LFAxTWyuHHgp5HRl+
MD5:	67176C242E1BDC20603C878DEE836DF3
SHA1:	27A71B00383D61EF3C489326B3564D698FC1227C
SHA-256:	56C12A125B021D21A69E61D7190CEFA168D6C28CE715265CEA1B3B0112D169C4
SHA-512:	9FA75814E1B9F7DB38FE61A503A13E60B82D83DB8F4CE30351BD08A6B48C0D854BAF472D891AF23C443C8293380C2325C7B3361B708AF9971AA0EA09A25CDD(A
Malicious:	false
Reputation:	low
URL:	http://https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/js/bootstrap.min.js
Preview:	/*!. * Bootstrap v4.1.3 (https://getbootstrap.com/). * Copyright 2011-2018 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors). * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquery"),require("popper.js")):"function"==typeof define&&define.amd?define(["exports","jquery","popper.js"],e):e(t.bootstrap={},t.jQuery,t.Popper)}(this,function(t,e,h){"use strict";function i(t,e){for(var n=0;n<e.length;n++){var i=e[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(t,i.key,i)}}function s(t,e,n){return e&&i(t.prototype,e),n&&i(t,n),t}function l(r){for(var t=1;t<arguments.length;t++){var o=null!=arguments[t]?arguments[t]:{},e=Object.keys(o);"function"==typeof Object.getOwnPropertySymbols&&(e=e.concat(Object.getOwnPropertySymbols(o).filter(function(t){return Object.getOwnPropertyDescriptor(o,t).enum

Chrome Cache Entry: 124

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (32065)
Category:	downloaded
Size (bytes):	85578
Entropy (8bit):	5.366055229017455
Encrypted:	false
SSDEEP:	1536:EYE1JVoiB9JqZdXXe2pD3PgoIiulrUndZ6a4tfOR7WpfWBZ2BJda4w9W3qG9a986:v4J+OlfOhWppCW6G9a98Hr2
MD5:	2F6B11A7E914718E0290410E85366FE9
SHA1:	69BB69E25CA7D5EF0935317584E6153F3FD9A88C
SHA-256:	05B85D96F41FFF14D8F608DAD03AB71E2C1017C2DA0914D7C59291BAD7A54F8E
SHA-512:	0D40BCCAA59FEDECF7243D63B33C42592541D0330FEFC78EC81A4C6B9689922D5B211011CA4BE23AE22621CCE4C658F52A1552C92D7AC3615241EB640F8514B
Malicious:	false
Reputation:	low
URL:	http://https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js
Preview:	/*! jQuery v2.2.4 | (c) jQuery Foundation | jquery.org/license */!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProperty,l={},m="2.2.4",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:e.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a){return n.each(this,a)},map:function(a){return this.pushStack(n.map(this,function(b,c){return a.call

Chrome Cache Entry: 125

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (48664)
Category:	downloaded
Size (bytes):	48944
Entropy (8bit):	5.272507874206726
Encrypted:	false
SSDEEP:	768:9VG5R15WbHVKZrycEHSYro34CrSLB6WU/6DqBf4l1B:9VIRuo53XiwWTvl1B
MD5:	14D449EB8876FA55E1EF3C2CC52B0C17
SHA1:	A9545831803B1359CFEED47E3B4D6BAE68E40E99

SHA-256:	E7ED36CEEE5450B4243BBC35188AFABDFB4280C7C57597001DE0ED167299B01B
SHA-512:	00D9069B9BD29AD0DAA0503F341D67549CCE28E888E1AFFD1A2A45B64A4C1BC460D81CFC4751857F991F2F4FB3D2572FD97FCA651BA0C2B0255530209B182F2 2
Malicious:	false
Reputation:	low
URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js
Preview:	/*!. * Bootstrap v4.0.0 (https://getbootstrap.com). * Copyright 2011-2018 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors). * Licensed und er MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquer y"),require("popper.js")):"function"==typeof define&&define.amd?define(["exports","jquery","popper.js"],e):e(t.bootstrap={},t.jQuery,t.Popper)}(this,function(t,e,n){"use strict";function i(t,e){for(var n=0;n<e.length;n++){var i=e[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(t,i.key, i)}}function s(t,e,n){return e&&i(t.prototype,e),n&&i(t,n),t}function r(){return(r=Object.assign||function(t){for(var e=1;e<arguments.length;e++){var n=arguments[e];for(var i in n)Object.prototype.hasOwnProperty.call(n,i)&&(t[i]=n[i])}return t}).apply(this,arguments)}e=e&&e.hasOwnProperty("default")?e.default:e,n=n&&n.hasOwnProp

Chrome Cache Entry: 126	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	28
Entropy (8bit):	4.137537511266052
Encrypted:	false
SSDEEP:	3:G4iC1Y:ziC1Y
MD5:	C41A026A97DFC107025EEC7F45F29C85
SHA1:	B77C8FE6D6A770AF1758FC34B3E716656B8F2485
SHA-256:	8A7130BC862841606D062AC516513B01EB176CEF37D017E18B54E844E8390029
SHA-512:	6DE72788DA933F3DA0D1FB315335B8DE1BD9D4F7B59A0F1D1F6E758AB0D1EC3D7F0B8FFCDE16313B555BFE18832FF8671A2159F5AFCEEA6C45C2A037345ED 17
Malicious:	false
Reputation:	low
URL:	http://https://content-autofill.googleapis.com/v1/pages/ChRDaHJvbWUvMTA0LjAuNTExMi44MRIXCQA2a1JSmA4aEgUNU1WBtRIFDa0JrrE=?alt=proto
Preview:	ChIKBw1TVYG1GgAKBw2tCa6xGgA=

Chrome Cache Entry: 127	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (65325)
Category:	downloaded
Size (bytes):	144877
Entropy (8bit):	5.049937202697915
Encrypted:	false
SSDEEP:	1536:GcoqwrUPyDHU7c7TcDEBi82NcuSELL4d/+oENM6HN26Q:VoPgPard2oENM6HN26Q
MD5:	450FC463B8B1A349DF717056FBB3E078
SHA1:	895125A4522A3B10EE7ADA06EE6503587CBF95C5
SHA-256:	2C0F3DCFE93D7E380C290FE4AB838ED8CADFF1596D62697F5444BE460D1F876D
SHA-512:	93BF1ED5F6D8B34F53413A86EFD4A925D578C97ABC757EA871F3F46F340745E4126C48219D2E8040713605B64A9ECF7AD986AA8102F5EA5ECF9228801D962F5D
Malicious:	false
Reputation:	low
URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css
Preview:	/*!. * Bootstrap v4.0.0 (https://getbootstrap.com). * Copyright 2011-2018 The Bootstrap Authors. * Copyright 2011-2018 Twitter, Inc.. * Licensed under MIT (https://github .com/twbs/bootstrap/blob/master/LICENSE). */:root{--blue:#007bff;--indigo:#6610f2;--purple:#6f42c1;--pink:#e83e8c;--red:#dc3545;--orange:#fd7e14;--yellow:#ffc107;-- green:#28a745;--teal:#20c997;--cyan:#17a2b8;--white:#fff;--gray:#6c757d;--gray-dark:#343a40;--primary:#007bff;--secondary:#6c757d;--success:#28a745;--info:#17a2b8;- -warning:#ffc107;--danger:#dc3545;--light:#f8f9fa;--dark:#343a40;--breakpoint-xs:0;--breakpoint-sm:576px;--breakpoint-md:768px;--breakpoint-lg:992px;--breakpoint- xl:1200px;--font-family-sans-serif:-apple-system,BlinkMacSystemFont,"Segoe UI",Roboto,"Helvetica Neue",Arial,sans-serif,"Apple Color Emoji","Segoe UI Emoji","Segoe UI Symbol";--font-family-monospace:SFMono-Regular,Menlo,Monaco,Consolas,"Liberation Mono","Courier New",monospace}*,::after,::before{box-sizing:border-box}h tml{font-family:sans

Chrome Cache Entry: 128	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	2787
Entropy (8bit):	5.570988829563644
Encrypted:	false
SSDEEP:	48:ZOxMMB9kOJOxMMB9YivFZ8OxMMB9hOxMMB9eOxMMB9odUOxMMB9ZvOxMMB99toQg:ZOxMMBtJOxMMBfvFZ8OxMMBjOxMMBoOq
MD5:	1EFD88F39E1B11D2F6506F4E7C853D60

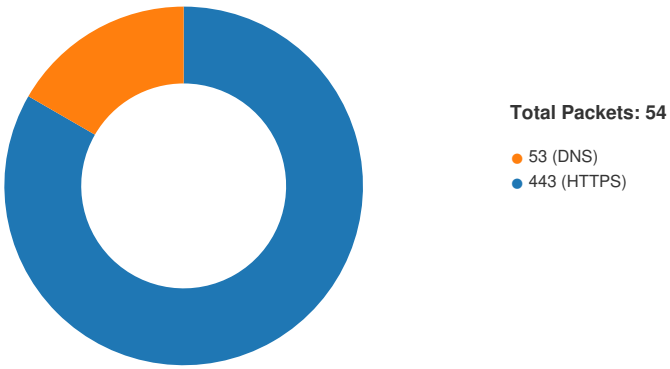
SHA1:	35ADDC2C29544E49BCA30C49CFF776D7CD6805F5
SHA-256:	3262C2BD70D868ED379B89EB25E964BF826721F17189A5170C352D20A7563F94
SHA-512:	18609127E68B33614D9FAA5E3CCB53BC2D5F8F89A1EC3DC6451D6DE90787B1F39CA0F721AE1D9DC85A850681F38E3801A38A998919B95EDDF593CDE132CA69A
Malicious:	false
Reputation:	low
URL:	http://https://fonts.googleapis.com/css?family=Open+Sans:600
Preview:	/* cyrillic-ext */.@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 600;. font-stretch: 100%;. src: url(https://fonts.gstatic.com/s/opensans/v34/memSYaGs126MiZpBA-UvWbX2vVnXBbObj2OVZyOOSr4dVJWUgsgH1x4taVIGxA.woff2) format('woff2');. unicode-range: U+0460-052F, U+1C80-1C88, U+20B4, U+2DE0-2DFF, U+A640-A69F, U+FE2E-FE2F;.}./* cyrillic */.@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 600;. font-stretch: 100%;. src: url(https://fonts.gstatic.com/s/opensans/v34/memSYaGs126MiZpBA-UvWbX2vVnXBbObj2OVZyOOSr4dVJWUgsgH1x4kaVIGxA.woff2) format('woff2');. unicode-range: U+0301, U+0400-045F, U+0490-0491, U+04B0-04B1, U+2116;.}./* greek-ext */.@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 600;. font-stretch: 100%;. src: url(https://fonts.gstatic.com/s/opensans/v34/memSYaGs126MiZpBA-UvWbX2vVnXBbObj2OVZyOOSr4dVJWUgsgH1x4saVIGxA.woff2) format('woff2');. unicode-range: U+1F00-1FFF;.}./* greek */.@font-fa

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 22:34:33.285990953 CET	49696	443	192.168.2.3	142.250.203.109
Mar 20, 2023 22:34:33.286077023 CET	443	49696	142.250.203.109	192.168.2.3
Mar 20, 2023 22:34:33.286183119 CET	49696	443	192.168.2.3	142.250.203.109
Mar 20, 2023 22:34:33.286806107 CET	49696	443	192.168.2.3	142.250.203.109
Mar 20, 2023 22:34:33.286845922 CET	443	49696	142.250.203.109	192.168.2.3
Mar 20, 2023 22:34:33.297059059 CET	49698	443	192.168.2.3	142.250.203.110
Mar 20, 2023 22:34:33.297133923 CET	443	49698	142.250.203.110	192.168.2.3
Mar 20, 2023 22:34:33.297224045 CET	49698	443	192.168.2.3	142.250.203.110
Mar 20, 2023 22:34:33.299969912 CET	49698	443	192.168.2.3	142.250.203.110
Mar 20, 2023 22:34:33.300004959 CET	443	49698	142.250.203.110	192.168.2.3
Mar 20, 2023 22:34:33.361490965 CET	443	49696	142.250.203.109	192.168.2.3
Mar 20, 2023 22:34:33.371572971 CET	443	49698	142.250.203.110	192.168.2.3
Mar 20, 2023 22:34:33.377690077 CET	49698	443	192.168.2.3	142.250.203.110
Mar 20, 2023 22:34:33.377732038 CET	443	49698	142.250.203.110	192.168.2.3
Mar 20, 2023 22:34:33.378070116 CET	49696	443	192.168.2.3	142.250.203.109
Mar 20, 2023 22:34:33.378129959 CET	443	49696	142.250.203.109	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 22:34:33.378335953 CET	443	49698	142.250.203.110	192.168.2.3
Mar 20, 2023 22:34:33.378448963 CET	49698	443	192.168.2.3	142.250.203.110
Mar 20, 2023 22:34:33.379755974 CET	443	49698	142.250.203.110	192.168.2.3
Mar 20, 2023 22:34:33.379889011 CET	49698	443	192.168.2.3	142.250.203.110
Mar 20, 2023 22:34:33.380012035 CET	443	49696	142.250.203.109	192.168.2.3
Mar 20, 2023 22:34:33.380088091 CET	49696	443	192.168.2.3	142.250.203.109
Mar 20, 2023 22:34:34.571316004 CET	49698	443	192.168.2.3	142.250.203.110
Mar 20, 2023 22:34:34.571382046 CET	443	49698	142.250.203.110	192.168.2.3
Mar 20, 2023 22:34:34.571466923 CET	49698	443	192.168.2.3	142.250.203.110
Mar 20, 2023 22:34:34.571499109 CET	443	49698	142.250.203.110	192.168.2.3
Mar 20, 2023 22:34:34.571707964 CET	49696	443	192.168.2.3	142.250.203.109
Mar 20, 2023 22:34:34.571774006 CET	443	49698	142.250.203.110	192.168.2.3
Mar 20, 2023 22:34:34.571779966 CET	443	49696	142.250.203.109	192.168.2.3
Mar 20, 2023 22:34:34.571852922 CET	49696	443	192.168.2.3	142.250.203.109
Mar 20, 2023 22:34:34.571867943 CET	443	49696	142.250.203.109	192.168.2.3
Mar 20, 2023 22:34:34.572096109 CET	443	49696	142.250.203.109	192.168.2.3
Mar 20, 2023 22:34:34.609304905 CET	443	49698	142.250.203.110	192.168.2.3
Mar 20, 2023 22:34:34.609461069 CET	49698	443	192.168.2.3	142.250.203.110
Mar 20, 2023 22:34:34.609496117 CET	443	49698	142.250.203.110	192.168.2.3
Mar 20, 2023 22:34:34.609720945 CET	443	49698	142.250.203.110	192.168.2.3
Mar 20, 2023 22:34:34.609810114 CET	49698	443	192.168.2.3	142.250.203.110
Mar 20, 2023 22:34:34.625536919 CET	443	49696	142.250.203.109	192.168.2.3
Mar 20, 2023 22:34:34.625688076 CET	49696	443	192.168.2.3	142.250.203.109
Mar 20, 2023 22:34:34.625736952 CET	443	49696	142.250.203.109	192.168.2.3
Mar 20, 2023 22:34:34.625962973 CET	443	49696	142.250.203.109	192.168.2.3
Mar 20, 2023 22:34:34.626050949 CET	49696	443	192.168.2.3	142.250.203.109
Mar 20, 2023 22:34:34.643790960 CET	49696	443	192.168.2.3	142.250.203.109
Mar 20, 2023 22:34:34.643824100 CET	443	49696	142.250.203.109	192.168.2.3
Mar 20, 2023 22:34:34.644315958 CET	49698	443	192.168.2.3	142.250.203.110
Mar 20, 2023 22:34:34.644345999 CET	443	49698	142.250.203.110	192.168.2.3
Mar 20, 2023 22:34:35.280416012 CET	49699	443	192.168.2.3	149.137.137.254
Mar 20, 2023 22:34:35.280500889 CET	443	49699	149.137.137.254	192.168.2.3
Mar 20, 2023 22:34:35.280642986 CET	49699	443	192.168.2.3	149.137.137.254
Mar 20, 2023 22:34:35.280951977 CET	49699	443	192.168.2.3	149.137.137.254
Mar 20, 2023 22:34:35.281001091 CET	443	49699	149.137.137.254	192.168.2.3
Mar 20, 2023 22:34:35.533071041 CET	443	49699	149.137.137.254	192.168.2.3
Mar 20, 2023 22:34:35.533456087 CET	49699	443	192.168.2.3	149.137.137.254
Mar 20, 2023 22:34:35.533498049 CET	443	49699	149.137.137.254	192.168.2.3
Mar 20, 2023 22:34:35.534892082 CET	443	49699	149.137.137.254	192.168.2.3
Mar 20, 2023 22:34:35.534992933 CET	49699	443	192.168.2.3	149.137.137.254
Mar 20, 2023 22:34:35.570651054 CET	49699	443	192.168.2.3	149.137.137.254
Mar 20, 2023 22:34:35.570722103 CET	443	49699	149.137.137.254	192.168.2.3
Mar 20, 2023 22:34:35.570909977 CET	49699	443	192.168.2.3	149.137.137.254
Mar 20, 2023 22:34:35.570925951 CET	443	49699	149.137.137.254	192.168.2.3
Mar 20, 2023 22:34:35.571049929 CET	443	49699	149.137.137.254	192.168.2.3
Mar 20, 2023 22:34:35.708223104 CET	49699	443	192.168.2.3	149.137.137.254
Mar 20, 2023 22:34:35.708275080 CET	443	49699	149.137.137.254	192.168.2.3
Mar 20, 2023 22:34:35.779844046 CET	443	49699	149.137.137.254	192.168.2.3
Mar 20, 2023 22:34:35.779900074 CET	443	49699	149.137.137.254	192.168.2.3
Mar 20, 2023 22:34:35.779948950 CET	443	49699	149.137.137.254	192.168.2.3
Mar 20, 2023 22:34:35.779967070 CET	443	49699	149.137.137.254	192.168.2.3
Mar 20, 2023 22:34:35.779985905 CET	443	49699	149.137.137.254	192.168.2.3
Mar 20, 2023 22:34:35.779999018 CET	49699	443	192.168.2.3	149.137.137.254
Mar 20, 2023 22:34:35.780073881 CET	443	49699	149.137.137.254	192.168.2.3
Mar 20, 2023 22:34:35.780121088 CET	49699	443	192.168.2.3	149.137.137.254
Mar 20, 2023 22:34:35.780121088 CET	49699	443	192.168.2.3	149.137.137.254
Mar 20, 2023 22:34:35.780121088 CET	49699	443	192.168.2.3	149.137.137.254
Mar 20, 2023 22:34:35.780148029 CET	443	49699	149.137.137.254	192.168.2.3
Mar 20, 2023 22:34:35.780205011 CET	49699	443	192.168.2.3	149.137.137.254

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 22:34:35.880132914 CET	443	49699	149.137.137.254	192.168.2.3
Mar 20, 2023 22:34:35.880162954 CET	443	49699	149.137.137.254	192.168.2.3
Mar 20, 2023 22:34:35.880254984 CET	49699	443	192.168.2.3	149.137.137.254
Mar 20, 2023 22:34:35.880264997 CET	443	49699	149.137.137.254	192.168.2.3
Mar 20, 2023 22:34:35.880283117 CET	443	49699	149.137.137.254	192.168.2.3
Mar 20, 2023 22:34:35.880297899 CET	443	49699	149.137.137.254	192.168.2.3
Mar 20, 2023 22:34:35.880302906 CET	49699	443	192.168.2.3	149.137.137.254
Mar 20, 2023 22:34:35.880330086 CET	49699	443	192.168.2.3	149.137.137.254
Mar 20, 2023 22:34:35.880371094 CET	443	49699	149.137.137.254	192.168.2.3
Mar 20, 2023 22:34:35.880405903 CET	49699	443	192.168.2.3	149.137.137.254
Mar 20, 2023 22:34:35.880405903 CET	49699	443	192.168.2.3	149.137.137.254
Mar 20, 2023 22:34:35.880428076 CET	443	49699	149.137.137.254	192.168.2.3
Mar 20, 2023 22:34:35.880462885 CET	49699	443	192.168.2.3	149.137.137.254
Mar 20, 2023 22:34:35.929647923 CET	443	49699	149.137.137.254	192.168.2.3
Mar 20, 2023 22:34:35.929677010 CET	443	49699	149.137.137.254	192.168.2.3
Mar 20, 2023 22:34:35.929835081 CET	49699	443	192.168.2.3	149.137.137.254
Mar 20, 2023 22:34:35.929835081 CET	49699	443	192.168.2.3	149.137.137.254
Mar 20, 2023 22:34:35.929838896 CET	443	49699	149.137.137.254	192.168.2.3
Mar 20, 2023 22:34:35.929886103 CET	443	49699	149.137.137.254	192.168.2.3
Mar 20, 2023 22:34:35.929908991 CET	443	49699	149.137.137.254	192.168.2.3
Mar 20, 2023 22:34:35.929955959 CET	443	49699	149.137.137.254	192.168.2.3
Mar 20, 2023 22:34:35.930001020 CET	49699	443	192.168.2.3	149.137.137.254
Mar 20, 2023 22:34:35.930001020 CET	49699	443	192.168.2.3	149.137.137.254
Mar 20, 2023 22:34:35.930001020 CET	49699	443	192.168.2.3	149.137.137.254
Mar 20, 2023 22:34:35.930006027 CET	443	49699	149.137.137.254	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 22:34:33.231920004 CET	49977	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:34:33.233052969 CET	57840	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:34:33.258387089 CET	53	49977	8.8.8.8	192.168.2.3
Mar 20, 2023 22:34:33.261249065 CET	53	57840	8.8.8.8	192.168.2.3
Mar 20, 2023 22:34:33.797461033 CET	57990	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:34:33.818470955 CET	53	57990	8.8.8.8	192.168.2.3
Mar 20, 2023 22:34:36.329946041 CET	52955	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:34:36.334986925 CET	60582	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:34:36.349397898 CET	53	52955	8.8.8.8	192.168.2.3
Mar 20, 2023 22:34:36.379159927 CET	57134	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:34:36.397258997 CET	56042	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:34:36.401427031 CET	53	57134	8.8.8.8	192.168.2.3
Mar 20, 2023 22:34:36.419397116 CET	53	56042	8.8.8.8	192.168.2.3
Mar 20, 2023 22:34:36.420403004 CET	59636	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:34:36.451076031 CET	53	59636	8.8.8.8	192.168.2.3
Mar 20, 2023 22:35:36.486462116 CET	51992	53	192.168.2.3	8.8.8.8
Mar 20, 2023 22:35:36.514359951 CET	53	51992	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 22:34:33.231920004 CET	192.168.2.3	8.8.8.8	0x8610	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:34:33.233052969 CET	192.168.2.3	8.8.8.8	0xa57f	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:34:33.797461033 CET	192.168.2.3	8.8.8.8	0xe2c	Standard query (0)	dfsfsfsd.s3.us-east-005.backblazeb2.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:34:36.329946041 CET	192.168.2.3	8.8.8.8	0x3897	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:34:36.334986925 CET	192.168.2.3	8.8.8.8	0x5894	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 22:34:36.379159927 CET	192.168.2.3	8.8.8.8	0x9a7b	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:34:36.397258997 CET	192.168.2.3	8.8.8.8	0x3dc	Standard query (0)	stackpath.bootstrapcdn.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:34:36.420403004 CET	192.168.2.3	8.8.8.8	0x5087	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:35:36.486462116 CET	192.168.2.3	8.8.8.8	0x72b5	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

DNS Answers

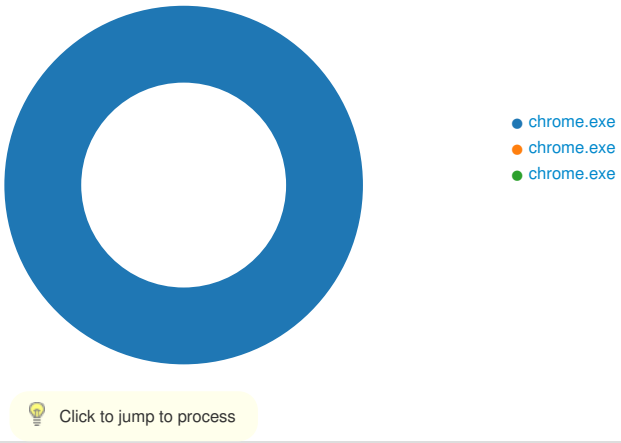
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 22:34:22.546449900 CET	8.8.8.8	192.168.2.3	0xb105	No error (0)	au.c-0001.c-msedge.net	c-0001.c-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:34:22.546449900 CET	8.8.8.8	192.168.2.3	0xb105	No error (0)	c-0001.c-msedge.net		13.107.4.50	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:34:22.962954998 CET	8.8.8.8	192.168.2.3	0x6420	No error (0)	au.c-0001.c-msedge.net	c-0001.c-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:34:22.962954998 CET	8.8.8.8	192.168.2.3	0x6420	No error (0)	c-0001.c-msedge.net		13.107.4.50	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:34:33.258387089 CET	8.8.8.8	192.168.2.3	0x8610	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:34:33.258387089 CET	8.8.8.8	192.168.2.3	0x8610	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:34:33.261249065 CET	8.8.8.8	192.168.2.3	0xa57f	No error (0)	accounts.google.com		142.250.203.109	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:34:33.818470955 CET	8.8.8.8	192.168.2.3	0xe2c	No error (0)	dfsfsfsd.s3.us-east-005.backblazeb2.com		149.137.137.254	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:34:36.349397898 CET	8.8.8.8	192.168.2.3	0x3897	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:34:36.349397898 CET	8.8.8.8	192.168.2.3	0x3897	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:34:36.357712030 CET	8.8.8.8	192.168.2.3	0x5894	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:34:36.401427031 CET	8.8.8.8	192.168.2.3	0x9a7b	No error (0)	cdnjs.cloudflare.com		104.17.25.14	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:34:36.401427031 CET	8.8.8.8	192.168.2.3	0x9a7b	No error (0)	cdnjs.cloudflare.com		104.17.24.14	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:34:36.419397116 CET	8.8.8.8	192.168.2.3	0x3dc	No error (0)	stackpath.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:34:36.419397116 CET	8.8.8.8	192.168.2.3	0x3dc	No error (0)	stackpath.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:34:36.451076031 CET	8.8.8.8	192.168.2.3	0x5087	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:35:36.514359951 CET	8.8.8.8	192.168.2.3	0x72b5	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- dfsfsfsd.s3.us-east-005.backblazeb2.com
- https:
  - maxcdn.bootstrapcdn.com
  - cdnjs.cloudflare.com
  - stackpath.bootstrapcdn.com

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **3176**, Parent PID: **4908**

General

Target ID:	0
Start time:	22:34:29
Start date:	20/03/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: chrome.exe PID: **848**, Parent PID: **3176**

General

Target ID:	1
Start time:	22:34:30
Start date:	20/03/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1928 --field-trial-handle=1644,i,2101607640442121641,12480239808714859300,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **4900**, Parent PID: **4908**

General

Target ID:	2
Start time:	22:34:31
Start date:	20/03/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "https://dfsfsfsd.s3.us-east-005.backblazeb2.com/index+(44).html
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

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

Disassembly

No disassembly