ID: 831012
Sample Name: Copy.shtml
Cookbook:
defaultwindowshtmlcookbook.jbs
Time: 00:28:29
Date: 21/03/2023
Version: 37.0.0 Beryl

Table of Contents

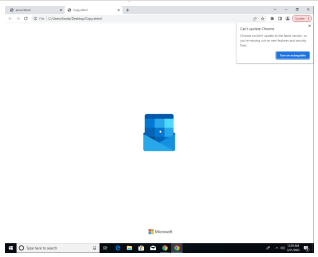
Windows Analysis Report

Copy.shtml

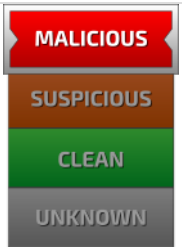
Overview

General Information

Sample Name:	Copy.shtml
Analysis ID:	831012
MD5:	2c83c8c06097…
SHA1:	6df38d5b9ce2d..
SHA256:	84af4fc733abb…
Infos:	



Detection



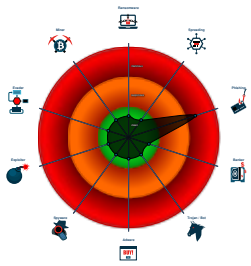
HTMLPhisher

Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish48
- Phishing site detected (based on im…
- IP address seen in connection with …

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 6052 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 3312 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=1692 --field-trial-handle=1788,i,8236339667510414405,2185392968241344403,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 5376 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "C:\Users\user\Desktop\Copy.shtml MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

HTML

Source	Rule	Description	Author	Strings
99254.0.pages.csv	JoeSecurity_HtmlPhish_48	Yara detected HtmlPhish_48	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Phishing

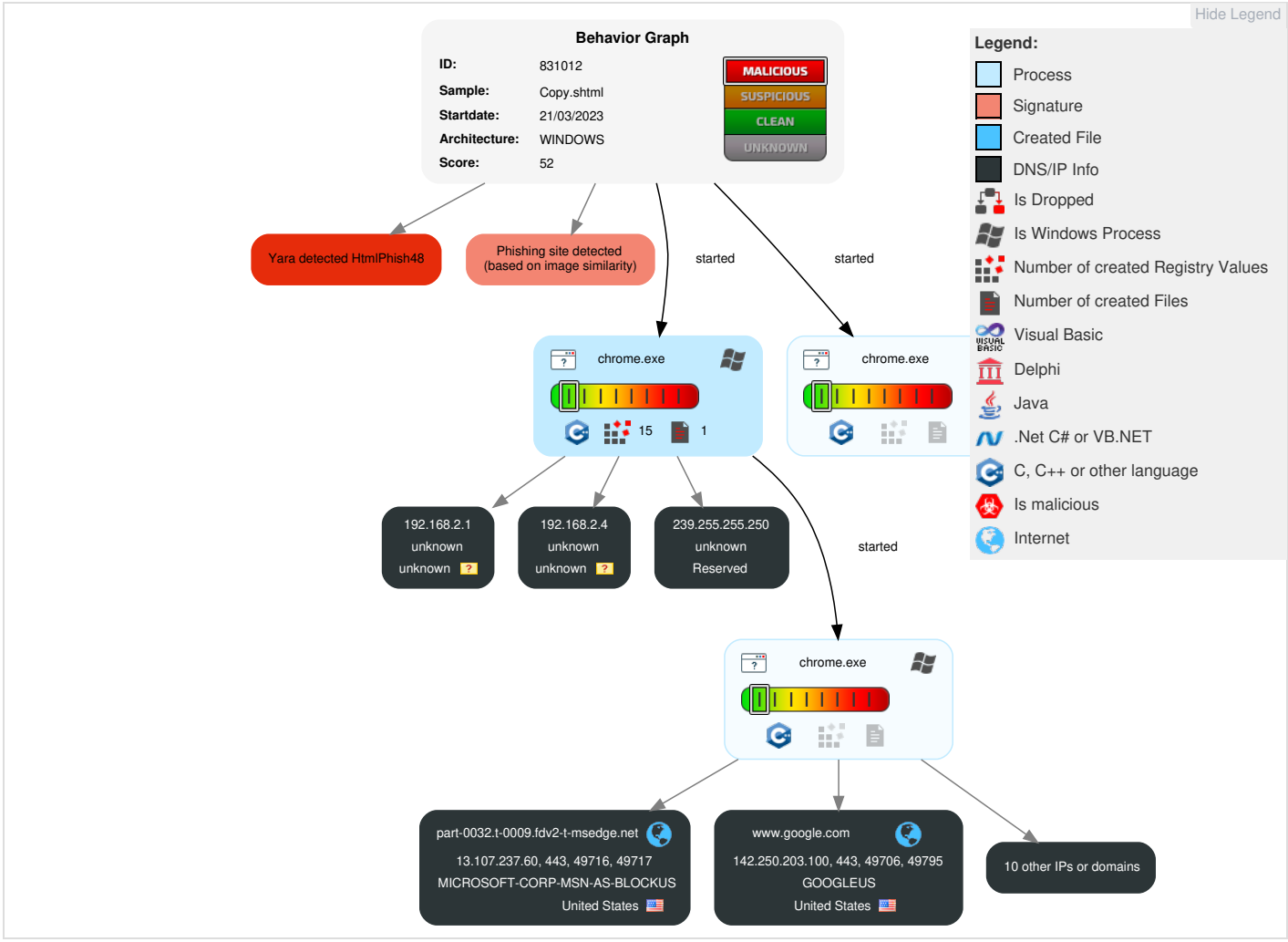
Yara detected HtmlPhish48

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

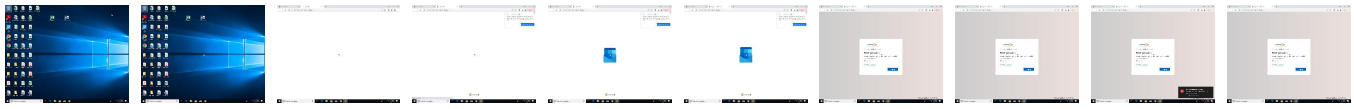
Behavior Graph

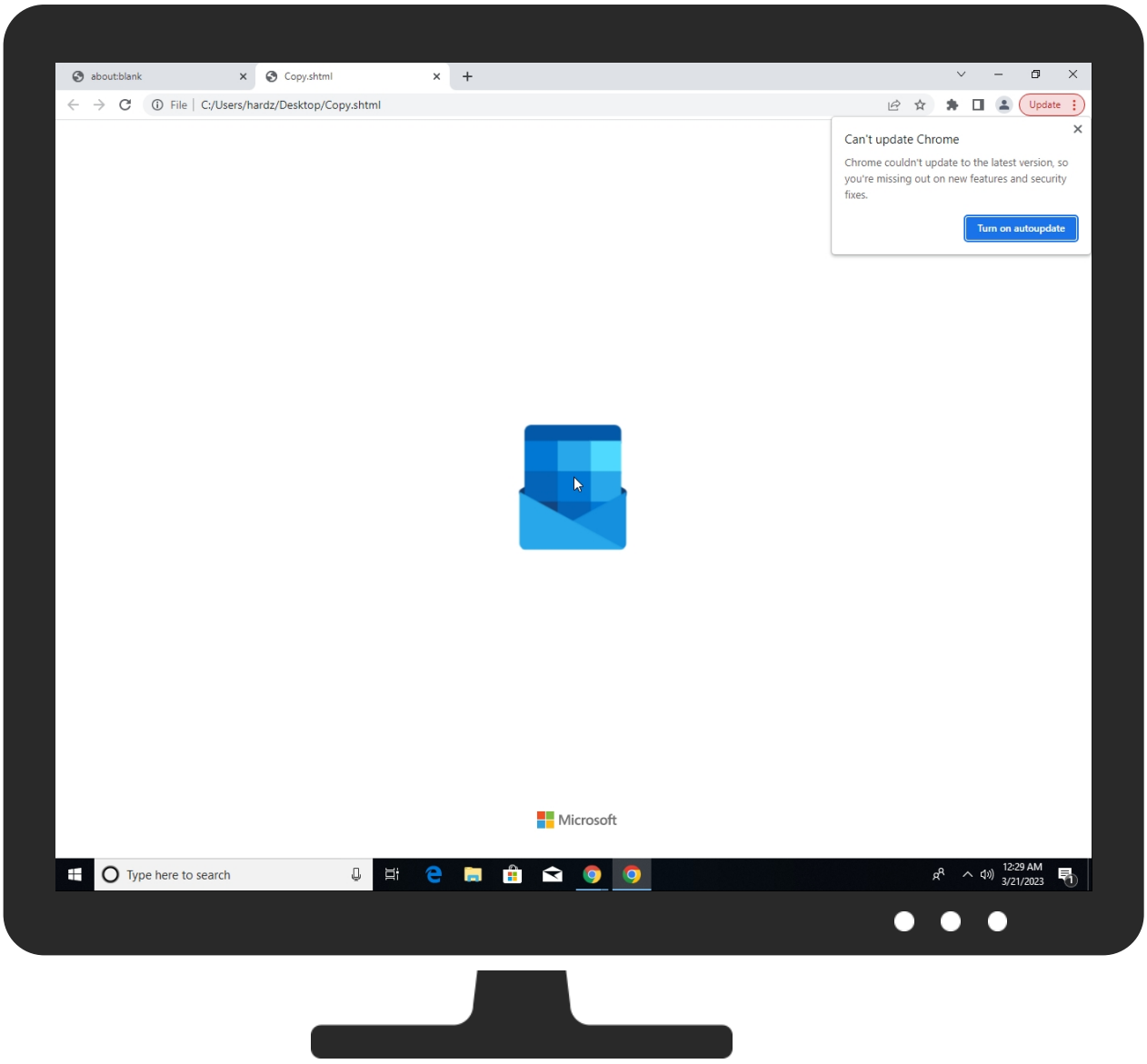


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
part-0032.t-0009.fdv2-t-msedge.net	0%	Virustotal		Browse
aadcdn.msauthimages.net	0%	Virustotal		Browse
cs1025.wpc.upsiloncdn.net	0%	Virustotal		Browse
ahg1.co	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://aadcdn.msauthimages.net/dbd5a2dd-nlfbwdmmtwey3bmysqci40atk0x2ttpxcb1c-eutnqu/logintenantbranding/0/bannerlogo?ts=637594497510297324	0%	Avira URL Cloud	safe	
http://https://ahg1.co/q/dd50b59.php	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.250.203.109	true	false		high
cdnjs.cloudflare.com	104.17.25.14	true	false		high
www.google.com	142.250.203.100	true	false		high
part-0032.t-0009.fdv2-t-msedge.net	13.107.237.60	true	false	• 0%, Virustotal, Browse	unknown
clients.l.google.com	142.250.203.110	true	false		high
cs1025.wpc.upsiloncdn.net	152.199.23.72	true	false	• 0%, Virustotal, Browse	unknown
ahg1.co	52.11.128.180	true	false	• 0%, Virustotal, Browse	unknown
aadcdn.msauthimages.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
clients2.google.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high

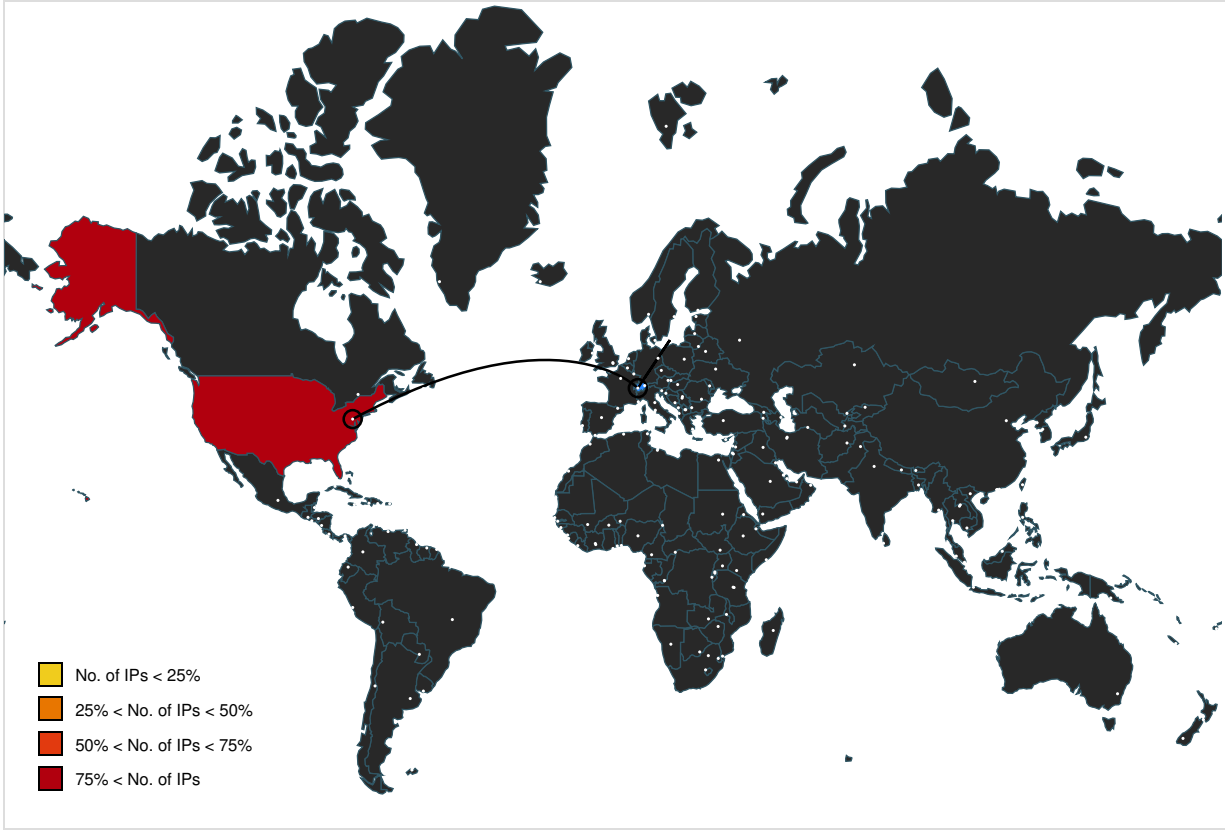
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://ahg1.co/q/dd50b59.php	false	• Avira URL Cloud: safe	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://aadcdn.msauthimages.net/dbd5a2dd-nlfbwdmmtwey3bmysqci40atk0x2ttpxcb1c-eutnqu/logintenantbranding/0/bannerlogo?ts=637594497510297324	false	• Avira URL Cloud: safe	unknown
http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.css	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
file:///C:/Users/user/Desktop/Copy.shtml	true		low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontawesome.io	chromecache_142.1.dr	false		high
http://fontawesome.io/license	chromecache_142.1.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.11.128.180	ahg1.co	United States		16509	AMAZON-02US	false
152.199.23.72	cs1025.wpc.upsiloncdn.net	United States		15133	EDGECASTUS	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
239.255.255.250	unknown	Reserved		unknown	unknown	false
13.107.237.60	part-0032.t-0009.fdv2-t-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	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
192.168.2.4
127.0.0.1

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	831012
Start date and time:	2023-03-21 00:28:29 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowshtmlcookbook.jbs
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:	17
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
Sample file name:	Copy.shtml
Detection:	MAL
Classification:	mal52.phis.winSHTML@29/10@8/11
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .shtml

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 93.184.221.240, 142.250.203.99, 69.16.175.42, 69.16.175.10, 34.104.35.123
- Excluded domains from analysis (whitelisted): cds.s5x3j6q5.hwcdn.net, fs.microsoft.com, aadcdnoriginwus2.azureedge.net, wu.ec.azureedge.net, ctldl.windowsupdate.com, clientservices.googleapis.com, aadcdn.msauth.net, wu-bg-shim.trafficmanager.net, wu.azureedge.net, firstparty-azurefd-prod.trafficmanager.net, edgedl.me.gvt1.com, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, aadcdn.azureedge.net, aadcdn.ec.azureedge.net, hlb.apr-52dd2-0.edgecastdns.net, update.googleapis.com, aadcdnoriginwus2.afd.azureedge.net
- 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: 141

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, max speed, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 2905
Category:	downloaded
Size (bytes):	1173
Entropy (8bit):	7.811199816788843
Encrypted:	false
SSDEEP:	24:XuByTjb3w436CJvnuI5wTGPjl2kGKvu3pufqOdyq3/VYHjyK5AXn:X8yz1qCkUYo1ozgt9YHGKe
MD5:	5C7ACF60A2ACAA5C54BF2B2EC6D484D8
SHA1:	F1837FD5DB6DAD498148D7D77438DE693114B042
SHA-256:	EE21196A4F5EF64135B7998E58F1E7210608674E3FDF97B328C1C237E3B184DB
SHA-512:	11516935B1C777D6457B7FB44235F8C8A73BA1313AC8607C16D342EECAE22AE5BFD702CE01DBB2DC63C3D480E89A689C7AA6CAC8D822E306B413534FEE770A77
Malicious:	false
Reputation:	moderate, very likely benign file
URL:	http://https://aadcdn.msauth.net/shared/1.0/content/images/picker_verify_call_fe87496cc7a44412f7893a72099c120a.svg
Preview:	.....uV.n$7.....iR.+..LN9.oA..5.....nx..S...I..%[.*.)..=.....z.?/._.....\|{8.4M.....^.~w>=>.....t.....~.M;.....,...n~}=-.7.....U.<>=.._.O.....y9.>.....y...wR.`8..r..q$.....KR...X.....W.....$g'". W<..$..-.2.....h04.O...|._../.6.)..ax..X...wzT.....2..7....1....C.@8B....d.M..KS8..>... .%=...q....yWF....\..kM.H....<..&.mM..s...%.'G.n..(..h.-.I.S.K...1;..:7.xdvP..y.]....Q$..4.@.2Fp ..Oe.....=.I.....F.....{....`.....uC..G.....'..E.....dR..g.(.+K.q...?...O.%.@.i..."n...1 .JTm.*S..wM.,../.\|H..s.....C.=.B1(.B.f..:K.\.T....c..N...sT..D....T.=..Zt..M2.).FP.h.:.*+A.. ^N-$..U.K..n.u.DZ...d.C....s.n.PI..@.4.pi....G..j.5.7I6....Q$...fs....uD.....F...e%..}5.S.s.n".9...e&(_.=..oq..F%L...G].....b.`..hi.S.I.8..Y%hM.|..W....jC.-a..'..%.r..W?...a...H...5.c.....v.G..v.G.a....a/.LT.Fv.....7.A...@.OcV.....6xcy,\[.wkP..-E...U..J.....*1j....2....C+...?.I.Q.C.kM.n...j..5{HV)I...M.G2o.....5.....E_..j.....D...^b..+.U..,K2

Chrome Cache Entry: 142

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	troff or preprocessor input, ASCII text, with very long lines (372)
Category:	downloaded
Size (bytes):	37414
Entropy (8bit):	4.82325822639402
Encrypted:	false
SSDEEP:	768:mmMtI+A4CSIDqvnI+YTBrFPvVrJjhiRAiiEL:mXtI+A4GDUI+Y9rpVljhiIEL
MD5:	C495654869785BC3DF60216616814AD1
SHA1:	0140952C64E3F2B74EF64E050F2FE86EAB6624C8
SHA-256:	36E0A7E08BEE65774168528938072C536437669C1B7458AC77976EC788E4439C
SHA-512:	E40F27C1D30E5AB4B3DB47C3B2373381489D50147C9623D853E5B299364FD65998F46E8E73B1E566FD79E97AA7B20354CD3C8C79F15372C147FED9C913FFB10
Malicious:	false
Reputation:	moderate, very likely benign file
URL:	http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.css
Preview:	/*!. * Font Awesome 4.7.0 by @davegandy - http://fontawesome.io - @fontawesome. * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License). */./* FONT PATH. * ---------- */.@font-face {. font-family: 'FontAwesome';. src: url('../fonts/fontawesome-webfont.eot?v=4.7.0');. src: url('../fonts/fontawesome-webfont.eot?#iefix&v=4.7.0') format('embedded-opentype'), url('../fonts/fontawesome-webfont.woff2?v=4.7.0') format('woff2'), url('../fonts/fontawesome-webfont.woff?v=4.7.0') format('woff'), url('../fonts/fontawesome-webfont.ttf?v=4.7.0') format('truetype'), url('../fonts/fontawesome-webfont.svg?v=4.7.0#fontawesomeregular') format('svg');. font-weight: normal;. font-style: normal;.}..fa {. display: inline-block;. font: normal normal normal 14px/1 FontAwesome;. font-size: inherit;. text-rendering: auto;. -webkit-font-smoothing: antialiased;. -moz-osx-font-smoothing: grayscale;.}./* makes the font 33% larger relative to the icon container */..

Chrome Cache Entry: 143

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, max speed, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 7390
Category:	downloaded
Size (bytes):	2407
Entropy (8bit):	7.900400471609788
Encrypted:	false
SSDEEP:	48:XVBUIsjnR4Zg0ddZ8E5EyQk7J0e+r/9lifUUuHDM3oOY+:XUIIKZg0ddZdEzTsfUUmyY+
MD5:	9D372E951D45A26EDE2DC8B417AAE4F8
SHA1:	84F97A777B6C33E2947E6D0BD2BFCFFEC601785A
SHA-256:	4E9C9141705E9A4D83514CEE332148E1E92126376D049DAED9079252FA9F9212
SHA-512:	78F5AA71EA44FF18BA081288F13AD118DB0E1B9C8D4D321ED40DCAB29277BD171BBB25BA7514566BBD4E25EA416C066019077FAA43E6ED781A29ADB683D218E2
Malicious:	false
Reputation:	moderate, very likely benign file
URL:	http://https://aadcdn.msauth.net/shared/1.0/content/images/picker_verify_fluent_authenticator_b59c16ca9bf156438a8a96d45e33db64.svg

Preview:	.....Y=s.8.....mr...f.y....8.R...l.Nk.l..?....{$.l\|e'zM.3.....S(.....O./.....Mn.e..O..7.O.?=..?...../...~yy._t....8.a.....~.....+..$..*..z..\....~..Jx|.....|y...=...../.3....kN2...H...;<sy....H..?2..q5.0.0....f.....L.^..v.W.L..7XCm8.I...6\.p.....O/%sX..I.....u.....yE.....$q....1/.....W....Zg...w..-..v....x...N).....R....c.W5.=...{_1_...+.#.....e...K..:..b.Ec...!...".I1../2X.....].i.sAF;^.1....1/UM.[r..d...>RX..U...<..1...V.\|.....X.jX:..0...9..F.KsT...{.6,..._Q..9.b...Q)..0.R.t.u.JN..u$V.%X.9k..t.."..Q.....y.V.Z$7.q.{.....k.....W..5.x..K..'y...=.....4...h\|!....r.."\f`..c+.....b..hc.jn....0.&G..m.=.@..6../.....6....tM^.&3.$.....~.....m2...wFs..#5.Hy..?...r.p.O.X.'n...Z8L.....7.;..QWGnr.sY..n...3.Jfq..+{m....\...X.q...0...0...........}}d...33.....Q...F$.8..v..UH&.H.....0.q..n...q...F.Y7...u..B>..J.A.....$.,....w.....Z..oe..w..%....$[+.....d...

Chrome Cache Entry: 144

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 280 x 60, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	9758
Entropy (8bit):	7.539935161666618
Encrypted:	false
SSDEEP:	192:f0Sbkn0A8lVOJN+T5d2v3H43hDZTFY6YFrjGFWOQ81fgpVqJtD3z:fzwn0AAT5s3H4xDxFIjGFWOQAfg+JtTz
MD5:	EA359CDF8AB9BCC8050F5598AEB32259
SHA1:	D8C383AC219E39BB4BBB86BE21036970CEB104B4
SHA-256:	69DDFE453E61D696267ADD7F6F0C44617E8FBB5748C0BBFE3D645285DFCDFC75
SHA-512:	C48E55C76ACDE771A2D3A1D5402183F321DB8237A71077FB91B7C3AAEE05BD8E61F7D2557A1008977E65D93A034A002A937FCEDCA9F516D17E2FE8026038304D
Malicious:	false
Preview:	.PNG.....IHDR.....<.....pHYs.....iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 6.0-c006 79.dabacbb, 2021/04/14-00:39:44 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpTPg="http://ns.adobe.com/xap/1.0/t/pg/" xmlns:stDim="http://ns.adobe.com/xap/1.0/sType/Dimensions#" xmlns:xmpG="http://ns.adobe.com/xap/1.0/g/" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/" xmp:CreatorTool="Adobe Illustrator CS5" xmp:CreateDate="2011-05-18T11:26:06-06:00" xmp:ModifyDate="2021-06-15T16:32:42-06:00" xmp:MetadataDate="2021-06-15T16:32:42-06:00" xmpTPg:NPages="1" xmpTP

Chrome Cache Entry: 145

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, max speed, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 250
Category:	dropped
Size (bytes):	199
Entropy (8bit):	6.766983163126765
Encrypted:	false
SSDEEP:	6:XtkhhsKHWpSiKPjPOeNWo6Rs7J1TxODwpV:X8hsKHDTPyeNSRs7vV0aV
MD5:	21B761F2B1FD37F587D7222023B09276
SHA1:	F7A416C8907424F9A9644753E3A93D4D63AE640E
SHA-256:	72D4161C18A46D85C5566273567F791976431EFEF49510A0E3DD76FEC92D9393
SHA-512:	77745F60804D421B34DE26F8A216CEE27C440E469FD786A642757CCEDBC4875D5196431897D80137BD3E20B01104BA76DEC7D8E75771D8A9B5F14B66F2A9B7C
Malicious:	false
Preview:	.....u....0.._%2k.8?....w..k..!.M.."b5<.M.bD..c..l.:..}...@.8p.sn.j...%".B...J..6...c..^..?...2d...R..w.<%..}..}s..ir0/.....:8).(.....^u...0..U..I.F....{]...[-.....~..F.P_.....G.....

Chrome Cache Entry: 146

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, max speed, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 2905
Category:	dropped
Size (bytes):	1173
Entropy (8bit):	7.811199816788843
Encrypted:	false
SSDEEP:	24:XuByTjb3w436CJvnuI5wTGPjI2kGKvu3pufqOdyq3/VYHjyK5AXn:X8yz1qCkUYo1ozgt9YHGKe
MD5:	5C7ACF60A2ACAA5C54BF2B2EC6D484D8
SHA1:	F1837FD5DB6DAD498148D7D77438DE693114B042
SHA-256:	EE21196A4F5EF64135B7998E58F1E7210608674E3FDF97B328C1C237E3B184DB
SHA-512:	11516935B1C777D6457B7FB44235F8C8A73BA1313AC8607C16D342EECAE22AE5BFD702CE01DBB2DC63C3D480E89A689C7AA6CAC8D822E306B413534FEE770A77
Malicious:	false
Preview:	.....uV.n$7.....iR.+..LN9.oA..5.....nx..S...l..%[.*.)..=.....z.?/._.....\|{8.4M.....^.~w>=>.....t.....~.M;.....,....n~}=-.7.....U.<>=.._.O.....y9.>.....y...wR.`8..r..q$.....KR...X.....W.....$g'". W<..$..-.2.....h04.O...|._../.6.)..ax..X...wzT.....2..7....1....C.@8B....d.M..KS8..>... .%=...q....yWF....\..kM.H....<..&.mM..s...%.'G.n..(..h.-.I.S.K...1;..:7.xdvP..y.]....Q$..4.@.2Fp ..Oe.....=.I.....F.....{....`.....uC..G....'..E.....dR..g.(.+K.q...?...O.%.@.i..."n...1 .JTm.*S..wM.,../.\|H..s.....C.=.B1(.B.f...:K.\.T....c..N...sT..D....T.=..Zt..M2.).FP.h.:.*+A.. ^N-$..U.K..n.u.DZ...d.C....s.n.PI..@.4.pi....G..j.5.7I6....Q$...fs....uD.....F...e%..}5.S.s.n".9...e&(_.=..oq..F%L...G].....b.`..hi.S.I.8..Y%hM.|..W....jC.-a..'..%.r..W?...a...H...5.c.....v.G..v.G.a....a/.LT.Fv.....7.A...@.OcV.....6xcy,I[.wkP..-E...U..J.....*1j....2....C+...?.I.Q.C.kM.n...j..5{HV)I...M.G2o.....5.....E_..j.....D...^b..+.U..,K2

Chrome Cache Entry: 147	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, max speed, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 7390
Category:	dropped
Size (bytes):	2407
Entropy (8bit):	7.900400471609788
Encrypted:	false
SSDEEP:	48:XVBUIsjnR4Zg0ddZ8E5EyQk7J0e+r/9lifUUuHDM3oOY+:XUIIKZg0ddZdEzTsfUUmyY+
MD5:	9D372E951D45A26EDE2DC8B417AAE4F8
SHA1:	84F97A777B6C33E2947E6D0BD2BFCFFEC601785A
SHA-256:	4E9C9141705E9A4D83514CEE332148E1E92126376D049DAED9079252FA9F9212
SHA-512:	78F5AA71EA44FF18BA081288F13AD118DB0E1B9C8D4D321ED40DCAB29277BD171BBB25BA7514566BBD4E25EA416C066019077FAA43E6ED781A29ADB683D218E2
Malicious:	false
Preview:	.....Y=s.8.....mr...f.y....8.R...I.Nk.I..?....{$.I\|e'zM.3.....S(.....O./.....Mn.e..O..7.O.?=..?...../...~yy._t....8.a.....~.....+..$..*..z..\....~..Jx|.....|y...=...../.3....kN2...H...;<sy....H..?2..q5.0.0....f.....L.^..v.W.L..7XCm8.I...6\.p.....O/%sX..I.....u.....yE.....$q....1/.....W....Zg...w..-..v....x...N).....R....c.W5.=...{_1_...+.#.....e...K..:..b.Ec...!...".I1../2X.....}.i.sAF;^.1....1/UM.[r..d...>RX..U...<..1...V.\|.....X.jX:..0...9..F.KsT...{.6,.._Q..9.b...Q)..0.R.t.u.JN..u$V.%X.9k..t.."..Q.....y.V.Z$7.q.{.....k.....W..5.x..K.."y...=.....4...h\|!....r.."v\f`..c+.....b..hc.jn....0.&G..m.=.@..6../.....6....tM^.&3.$.....~.....m2...wFs..#5.Hy..?...r.p.O.X.'n...Z8L.....7.;..QWGnr.sY..n...3.Jfq..+{m....\...X.q...0...0...........}}d...33.....Q...F$.8..v..UH&.H.....0.q..n...q...F.Y7...u..B>..J.A.....$.,....w.....Z..oe..w..%....$[+.....d...

Chrome Cache Entry: 148	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 280 x 60, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	9758
Entropy (8bit):	7.539935161666618
Encrypted:	false
SSDEEP:	192:f0Sbkn0A8lVOJN+T5d2v3H43hDZTFY6YFrjGFWOQ81fgpVqJtD3z:fzwn0AAT5s3H4xDxFljGFWOQAfg+JtTz
MD5:	EA359CDF8AB9BCC8050F5598AEB32259
SHA1:	D8C383AC219E39BB4BBB86BE21036970CEB104B4
SHA-256:	69DDFE453E61D696267ADD7F6F0C44617E8FBB5748C0BBFE3D645285DFCDFC75
SHA-512:	C48E55C76ACDE771A2D3A1D5402183F321DB8237A71077FB91B7C3AAEE05BD8E61F7D2557A1008977E65D93A034A002A937FCEDCA9F516D17E2FE8026038304D
Malicious:	false
URL:	http://https://aadcdn.msauthimages.net/dbd5a2dd-nlfbwdmmtwey3bmysqci40atk0x2ttpxcb1c-eutnqu/logintenantbranding/0/bannerlogo?ts=637594497510297324
Preview:	.PNG.....IHDR.....<.....pHYs.....iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 6.0-c006 79.dabacbb, 2021/04/14-00:39:44 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpTPg="http://ns.adobe.com/xap/1.0/t/pg/" xmlns:stDim="http://ns.adobe.com/xap/1.0/sType/Dimensions#" xmlns:xmpG="http://ns.adobe.com/xap/1.0/g/" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/" xmp:CreatorTool="Adobe Illustrator CS5" xmp:CreateDate="2011-05-18T11:26:06-06:00" xmp:ModifyDate="2021-06-15T16:32:42-06:00" xmp:MetadataDate="2021-06-15T16:32:42-06:00" xmpTPg:NPages="1" xmpTP

Chrome Cache Entry: 149	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	gzip compressed data, max speed, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 250
Category:	downloaded
Size (bytes):	199
Entropy (8bit):	6.766983163126765
Encrypted:	false
SSDEEP:	6:XtkhhsKHWpSiKPjPOeNWo6Rs7J1TxODwpV:X8hsKHDTPyeNSRs7vV0aV
MD5:	21B761F2B1FD37F587D7222023B09276
SHA1:	F7A416C8907424F9A9644753E3A93D4D63AE640E
SHA-256:	72D4161C18A46D85C5566273567F791976431EFEF49510A0E3DD76FEC92D9393
SHA-512:	77745F60804D421B34DE26F8A216CEE27C440E469FD786A642757CCEDBC4875D5196431897D80137BD3E20B01104BA76DEC7D8E75771D8A9B5F14B66F2A9B7C
Malicious:	false
URL:	http://https://aadcdn.msauth.net/shared/1.0/content/images/picker_verify_sms_27a6d18b56f46818420e60a773c36d4e.svg
Preview:	.....u....0._%2k.8?....w..k..!.M.."b5<.M.bD..c..I.:..}...@.8p.sn.j...%".B...J..6...c..^..?...2d...R..w.<%..}..}s..ir0/.....:8).(.....^u...0..U..I.F....{}...[-.....~..F.P_.....G.....

Chrome Cache Entry: 150	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (32030)

Category:	downloaded
Size (bytes):	86709
Entropy (8bit):	5.367391365596119
Encrypted:	false
SSDEEP:	1536:9NhEyjjTikEJO4edXXe9J578go6MWXqcVhrLyB4Lw13sh2bzrl1+iuH7U3gBORDT:jxcq0hrLZwpsYbmzORDU8Cu5
MD5:	E071ABDA8FE61194711CFC2AB99FE104
SHA1:	F647A6D37DC4CA055CED3CF64BBC1F490070ACBA
SHA-256:	85556761A8800D14CED8FCD41A6B8B26BF012D44A318866C0D81A62092EFD9BF
SHA-512:	53A2B560B20551672FBB0E6E72632D4FD1C7E2DD2ECF7337EBAAAB179CB8BE7C87E9D803CE7765706BC7FCBCF993C34587CD1237DE5A279AEA19911D69067I 65
Malicious:	false
URL:	http://https://code.jquery.com/jquery-3.1.1.min.js
Preview:	/*! jQuery v3.1.1 | (c) jQuery Foundation | 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="3.1.1",r=function(a,b){return new r.fn.init(a,b)},s=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,t=/^-ms-/,u=/-([a-z])/g,v=function(a,b){return b.toUpperCase()};r.fn=r.prototype={jquery:q,constructor:r, length:0,toArray:function(){return f.call(this)},get:function(a){return null==a?f.call(this):a<0?this[a+this.length]:this[a]},pushStack:function(a){var b=r.merge(this.con

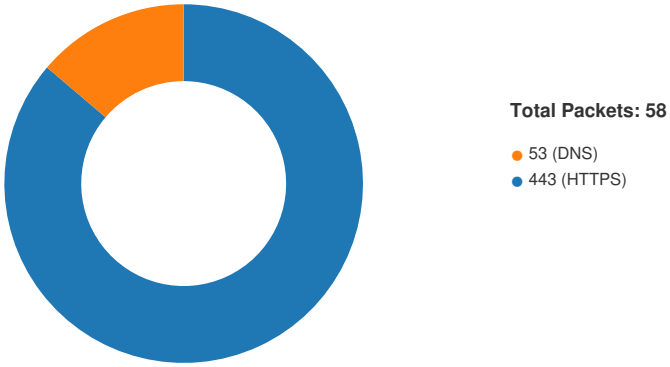
Static File Info

General

File type:	HTML document, ASCII text, with very long lines (35303), with no line terminators
Entropy (8bit):	5.585873948412507
TrID:	• HyperText Markup Language (12001/1) 66.65% • HyperText Markup Language (6006/1) 33.35%
File name:	Copy.shtml
File size:	35303
MD5:	2c83c8c060976da8bc9380954131b257
SHA1:	6df38d5b9ce2dfe3116cb249de6c33ba88d92eb9
SHA256:	84af4fc733abb652f03462fb9c55b134124dff940476e791dda22e8aac7cf3e6
SHA512:	24362593c580370f0fe9fe24f9fea9963c04dc17cf666a9f8d4b53daf61418ac778893dfe47716ab141745dada21a872ff6c63d9aca7df1d453e8e14516269c8
SSDEEP:	768:wmZYg2Q9Q+bHF5ZaVcVkOiDbYJ/oVWWtlzp:wfwm+7fUWVF2YJ/okWy1
TLSH:	C3F24BADBBAC58DE86AA1476D8314A4D8772D706DFC93488B7D9B80A11CFFB1DC08419
File Content Preview:	<html><head></head><body><span """""""""><span """""""""""""" id="dat1" class="PC9ib2R5PjxzY3JpcHQ+dmFyIGxvYWRlciA9ICJQSE4yWnlCcFpEMGliRzloWkdsdVoweHZaMjhpSUhodGJHNXpQU0pvZEhSd09pOHZkM2QzTG5jekxtOXlaeTh5TURBd0wzTjJaeUlnZUcxc2JuTTZlR3hwYm1zOUltaDBkSEE2T

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2023 00:29:26.053328991 CET	49701	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:29:26.053381920 CET	443	49701	142.250.203.109	192.168.2.3
Mar 21, 2023 00:29:26.053464890 CET	49701	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:29:26.053736925 CET	49701	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:29:26.053757906 CET	443	49701	142.250.203.109	192.168.2.3
Mar 21, 2023 00:29:26.054647923 CET	49702	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:29:26.054686069 CET	443	49702	142.250.203.110	192.168.2.3
Mar 21, 2023 00:29:26.054790020 CET	49702	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:29:26.055063963 CET	49702	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:29:26.055089951 CET	443	49702	142.250.203.110	192.168.2.3
Mar 21, 2023 00:29:26.154863119 CET	443	49701	142.250.203.109	192.168.2.3
Mar 21, 2023 00:29:26.156584978 CET	443	49702	142.250.203.110	192.168.2.3
Mar 21, 2023 00:29:26.270648003 CET	49702	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:29:26.291630030 CET	49701	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:29:26.508486986 CET	49702	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:29:26.508537054 CET	443	49702	142.250.203.110	192.168.2.3
Mar 21, 2023 00:29:26.510006905 CET	443	49702	142.250.203.110	192.168.2.3
Mar 21, 2023 00:29:26.510044098 CET	443	49702	142.250.203.110	192.168.2.3
Mar 21, 2023 00:29:26.510128021 CET	49702	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:29:26.513442993 CET	443	49702	142.250.203.110	192.168.2.3
Mar 21, 2023 00:29:26.513542891 CET	49702	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:29:26.513588905 CET	443	49702	142.250.203.110	192.168.2.3
Mar 21, 2023 00:29:26.537899017 CET	49701	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:29:26.537957907 CET	443	49701	142.250.203.109	192.168.2.3
Mar 21, 2023 00:29:26.541482925 CET	443	49701	142.250.203.109	192.168.2.3
Mar 21, 2023 00:29:26.541569948 CET	443	49701	142.250.203.109	192.168.2.3
Mar 21, 2023 00:29:26.541641951 CET	49701	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:29:26.570640087 CET	49702	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:29:26.591773033 CET	49701	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:29:26.838785887 CET	49701	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:29:26.838845015 CET	443	49701	142.250.203.109	192.168.2.3
Mar 21, 2023 00:29:26.839117050 CET	443	49701	142.250.203.109	192.168.2.3
Mar 21, 2023 00:29:26.839360952 CET	49701	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:29:26.839437962 CET	443	49701	142.250.203.109	192.168.2.3
Mar 21, 2023 00:29:26.839555025 CET	49702	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:29:26.839606047 CET	443	49702	142.250.203.110	192.168.2.3
Mar 21, 2023 00:29:26.839813948 CET	49702	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:29:26.839834929 CET	443	49702	142.250.203.110	192.168.2.3
Mar 21, 2023 00:29:26.839934111 CET	443	49702	142.250.203.110	192.168.2.3
Mar 21, 2023 00:29:26.880734921 CET	443	49702	142.250.203.110	192.168.2.3
Mar 21, 2023 00:29:26.880851984 CET	49702	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:29:26.880893946 CET	443	49702	142.250.203.110	192.168.2.3
Mar 21, 2023 00:29:26.881016970 CET	443	49702	142.250.203.110	192.168.2.3
Mar 21, 2023 00:29:26.881117105 CET	49702	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:29:26.887022018 CET	49702	443	192.168.2.3	142.250.203.110
Mar 21, 2023 00:29:26.887056112 CET	443	49702	142.250.203.110	192.168.2.3
Mar 21, 2023 00:29:26.891710997 CET	49701	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:29:26.893688917 CET	443	49701	142.250.203.109	192.168.2.3
Mar 21, 2023 00:29:26.893858910 CET	49701	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:29:26.893902063 CET	443	49701	142.250.203.109	192.168.2.3
Mar 21, 2023 00:29:26.894099951 CET	443	49701	142.250.203.109	192.168.2.3
Mar 21, 2023 00:29:26.894191027 CET	49701	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:29:26.898833036 CET	49701	443	192.168.2.3	142.250.203.109
Mar 21, 2023 00:29:26.898879051 CET	443	49701	142.250.203.109	192.168.2.3
Mar 21, 2023 00:29:27.056014061 CET	49703	443	192.168.2.3	52.11.128.180
Mar 21, 2023 00:29:27.056078911 CET	443	49703	52.11.128.180	192.168.2.3
Mar 21, 2023 00:29:27.056262970 CET	49703	443	192.168.2.3	52.11.128.180

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2023 00:29:27.056689024 CET	49703	443	192.168.2.3	52.11.128.180
Mar 21, 2023 00:29:27.056715965 CET	443	49703	52.11.128.180	192.168.2.3
Mar 21, 2023 00:29:27.447482109 CET	443	49703	52.11.128.180	192.168.2.3
Mar 21, 2023 00:29:27.448061943 CET	49703	443	192.168.2.3	52.11.128.180
Mar 21, 2023 00:29:27.448123932 CET	443	49703	52.11.128.180	192.168.2.3
Mar 21, 2023 00:29:27.449451923 CET	443	49703	52.11.128.180	192.168.2.3
Mar 21, 2023 00:29:27.449738026 CET	49703	443	192.168.2.3	52.11.128.180
Mar 21, 2023 00:29:27.451663017 CET	49703	443	192.168.2.3	52.11.128.180
Mar 21, 2023 00:29:27.451699972 CET	443	49703	52.11.128.180	192.168.2.3
Mar 21, 2023 00:29:27.451833010 CET	443	49703	52.11.128.180	192.168.2.3
Mar 21, 2023 00:29:27.461994886 CET	49703	443	192.168.2.3	52.11.128.180
Mar 21, 2023 00:29:27.462055922 CET	443	49703	52.11.128.180	192.168.2.3
Mar 21, 2023 00:29:27.570720911 CET	49703	443	192.168.2.3	52.11.128.180
Mar 21, 2023 00:29:27.762239933 CET	49703	443	192.168.2.3	52.11.128.180
Mar 21, 2023 00:29:27.762444973 CET	443	49703	52.11.128.180	192.168.2.3
Mar 21, 2023 00:29:27.762533903 CET	49703	443	192.168.2.3	52.11.128.180
Mar 21, 2023 00:29:27.812113047 CET	49705	443	192.168.2.3	52.11.128.180
Mar 21, 2023 00:29:27.812199116 CET	443	49705	52.11.128.180	192.168.2.3
Mar 21, 2023 00:29:27.812283993 CET	49705	443	192.168.2.3	52.11.128.180
Mar 21, 2023 00:29:27.813621998 CET	49705	443	192.168.2.3	52.11.128.180
Mar 21, 2023 00:29:27.813684940 CET	443	49705	52.11.128.180	192.168.2.3
Mar 21, 2023 00:29:27.905401945 CET	49706	443	192.168.2.3	142.250.203.100
Mar 21, 2023 00:29:27.905467033 CET	443	49706	142.250.203.100	192.168.2.3
Mar 21, 2023 00:29:27.905564070 CET	49706	443	192.168.2.3	142.250.203.100
Mar 21, 2023 00:29:27.905900955 CET	49706	443	192.168.2.3	142.250.203.100
Mar 21, 2023 00:29:27.905935049 CET	443	49706	142.250.203.100	192.168.2.3
Mar 21, 2023 00:29:27.974102020 CET	443	49706	142.250.203.100	192.168.2.3
Mar 21, 2023 00:29:27.974560022 CET	49706	443	192.168.2.3	142.250.203.100
Mar 21, 2023 00:29:27.974631071 CET	443	49706	142.250.203.100	192.168.2.3
Mar 21, 2023 00:29:27.976178885 CET	443	49706	142.250.203.100	192.168.2.3
Mar 21, 2023 00:29:27.976291895 CET	49706	443	192.168.2.3	142.250.203.100
Mar 21, 2023 00:29:27.978246927 CET	49706	443	192.168.2.3	142.250.203.100
Mar 21, 2023 00:29:27.978266954 CET	443	49706	142.250.203.100	192.168.2.3
Mar 21, 2023 00:29:27.978373051 CET	443	49706	142.250.203.100	192.168.2.3
Mar 21, 2023 00:29:28.091753960 CET	49706	443	192.168.2.3	142.250.203.100
Mar 21, 2023 00:29:28.091797113 CET	443	49706	142.250.203.100	192.168.2.3
Mar 21, 2023 00:29:28.191770077 CET	49706	443	192.168.2.3	142.250.203.100
Mar 21, 2023 00:29:28.209615946 CET	443	49705	52.11.128.180	192.168.2.3
Mar 21, 2023 00:29:28.210545063 CET	49705	443	192.168.2.3	52.11.128.180
Mar 21, 2023 00:29:28.210623980 CET	443	49705	52.11.128.180	192.168.2.3
Mar 21, 2023 00:29:28.212119102 CET	443	49705	52.11.128.180	192.168.2.3
Mar 21, 2023 00:29:28.212183952 CET	49705	443	192.168.2.3	52.11.128.180
Mar 21, 2023 00:29:28.213929892 CET	49705	443	192.168.2.3	52.11.128.180

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2023 00:29:26.017853022 CET	57840	53	192.168.2.3	8.8.8.8
Mar 21, 2023 00:29:26.019983053 CET	57990	53	192.168.2.3	8.8.8.8
Mar 21, 2023 00:29:26.021302938 CET	52387	53	192.168.2.3	8.8.8.8
Mar 21, 2023 00:29:26.046299934 CET	53	57840	8.8.8.8	192.168.2.3
Mar 21, 2023 00:29:26.046518087 CET	53	52387	8.8.8.8	192.168.2.3
Mar 21, 2023 00:29:26.992461920 CET	60625	53	192.168.2.3	8.8.8.8
Mar 21, 2023 00:29:27.010097980 CET	53	60625	8.8.8.8	192.168.2.3
Mar 21, 2023 00:29:27.881305933 CET	53975	53	192.168.2.3	8.8.8.8
Mar 21, 2023 00:29:27.900943041 CET	53	53975	8.8.8.8	192.168.2.3
Mar 21, 2023 00:29:30.709736109 CET	62050	53	192.168.2.3	8.8.8.8
Mar 21, 2023 00:29:30.733890057 CET	53	62050	8.8.8.8	192.168.2.3
Mar 21, 2023 00:29:32.322016001 CET	55638	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2023 00:30:27.951232910 CET	64823	53	192.168.2.3	8.8.8.8
Mar 21, 2023 00:30:27.978580952 CET	53	64823	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 21, 2023 00:29:26.017853022 CET	192.168.2.3	8.8.8.8	0xa959	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:29:26.019983053 CET	192.168.2.3	8.8.8.8	0xe48a	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:29:26.021302938 CET	192.168.2.3	8.8.8.8	0x3b2c	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:29:26.992461920 CET	192.168.2.3	8.8.8.8	0xfc86	Standard query (0)	ahg1.co	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:29:27.881305933 CET	192.168.2.3	8.8.8.8	0x8bf9	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:29:30.709736109 CET	192.168.2.3	8.8.8.8	0x7949	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:29:32.322016001 CET	192.168.2.3	8.8.8.8	0x527f	Standard query (0)	aadcdn.msauthimages.net	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:30:27.951232910 CET	192.168.2.3	8.8.8.8	0xe534	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

DNS Answers

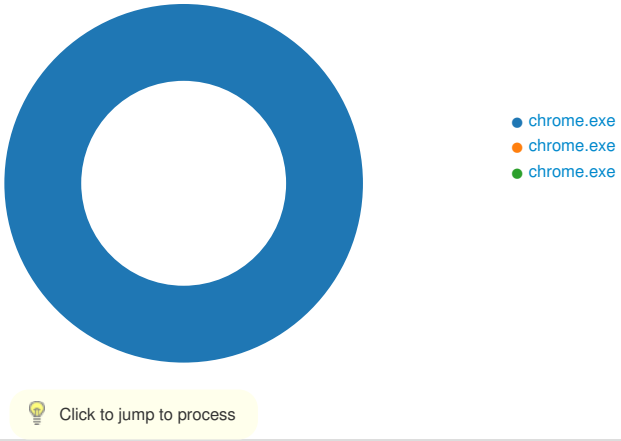
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 21, 2023 00:29:26.041548967 CET	8.8.8.8	192.168.2.3	0xe48a	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 21, 2023 00:29:26.046299934 CET	8.8.8.8	192.168.2.3	0xa959	No error (0)	accounts.google.com		142.250.203.109	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:29:26.046518087 CET	8.8.8.8	192.168.2.3	0x3b2c	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 21, 2023 00:29:26.046518087 CET	8.8.8.8	192.168.2.3	0x3b2c	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:29:27.010097980 CET	8.8.8.8	192.168.2.3	0xfc86	No error (0)	ahg1.co		52.11.128.180	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:29:27.900943041 CET	8.8.8.8	192.168.2.3	0x8bf9	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:29:30.733890057 CET	8.8.8.8	192.168.2.3	0x7949	No error (0)	cdnjs.cloudflare.com		104.17.25.14	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:29:30.733890057 CET	8.8.8.8	192.168.2.3	0x7949	No error (0)	cdnjs.cloudflare.com		104.17.24.14	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:29:30.750484943 CET	8.8.8.8	192.168.2.3	0xb591	No error (0)	shed.dual-low.part-0032.t-0009.fdv2-t-msedge.net	part-0032.t-0009.fdv2-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 21, 2023 00:29:30.750484943 CET	8.8.8.8	192.168.2.3	0xb591	No error (0)	part-0032.t-0009.fdv2-t-msedge.net		13.107.237.60	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:29:30.750484943 CET	8.8.8.8	192.168.2.3	0xb591	No error (0)	part-0032.t-0009.fdv2-t-msedge.net		13.107.238.60	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:29:32.343153000 CET	8.8.8.8	192.168.2.3	0x527f	No error (0)	aadcdn.msauthimages.net	aadcdn.azureedge.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 21, 2023 00:29:32.343153000 CET	8.8.8.8	192.168.2.3	0x527f	No error (0)	cs1025.wpc.upsiloncdn.net		152.199.23.72	A (IP address)	IN (0x0001)	false
Mar 21, 2023 00:30:27.978580952 CET	8.8.8.8	192.168.2.3	0xe534	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- accounts.google.com
- clients2.google.com
- ahg1.co
- cdnjs.cloudflare.com
- aadcdn.msauth.net
- aadcdn.msauthimages.net

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **6052**, Parent PID: **1832**

General

Target ID:	0
Start time:	00:29:20
Start date:	21/03/2023
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:	high

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: **3312**, Parent PID: **6052**

General

Target ID:	1
Start time:	00:29:21
Start date:	21/03/2023
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=1692 --field-trial-handle=1788,i,8236339667510414405,218539296824134440 3,131072 --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:	high

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: **5376**, Parent PID: **1832**

General

Target ID:	2
Start time:	00:29:22
Start date:	21/03/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "C:\Users\user\Desktop\Copy.shtml
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:	high

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