ID: 756194
Sample Name: November Draw Disbursed.html
Cookbook: default.jbs
Time: 19:41:59
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

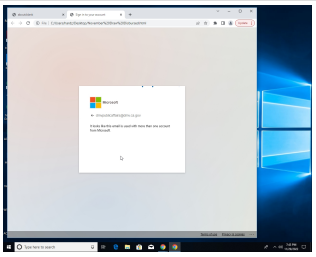
Windows Analysis Report

November Draw Disbursed.html

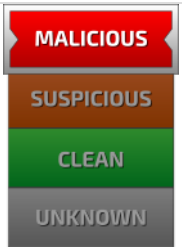
Overview

General Information

Sample Name:	November Draw Disbursed.html
Analysis ID:	756194
MD5:	b0d7ab3033db28.
SHA1:	8713ce26b53981..
SHA256:	10f511546453d5..
Infos:	



Detection



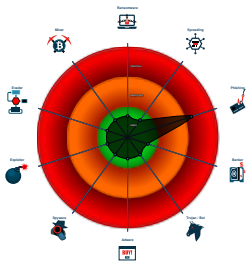
HTMLPhisher

Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish10
- Snort IDS alert for network traffic
- JA3 SSL client fingerprint seen in co…
- Invalid 'forgot password' link found
- HTML body contains low number of …
- Invalid T&C link found
- IP address seen in connection with …
- None HTTPS page querying sensitiv…
- No HTML title found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5904 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 6004 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=2032 --field-trial-handle=1828,i,10391032402710344752,2792419310114974632,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 5212 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "C:\Users\user\Desktop\November Draw Disbursed.html MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

HTML

Source	Rule	Description	Author	Strings
96596.0.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET DNS Query for .cc TLD - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.859636532027758 11/29/22-19:43:01.359643
SID:	2027758
Source Port:	59636
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query for .cc TLD - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.860767532027758 11/29/22-19:43:05.093728
SID:	2027758
Source Port:	60767
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

Joe Sandbox Signatures

Phishing

Yara detected HtmlPhish10

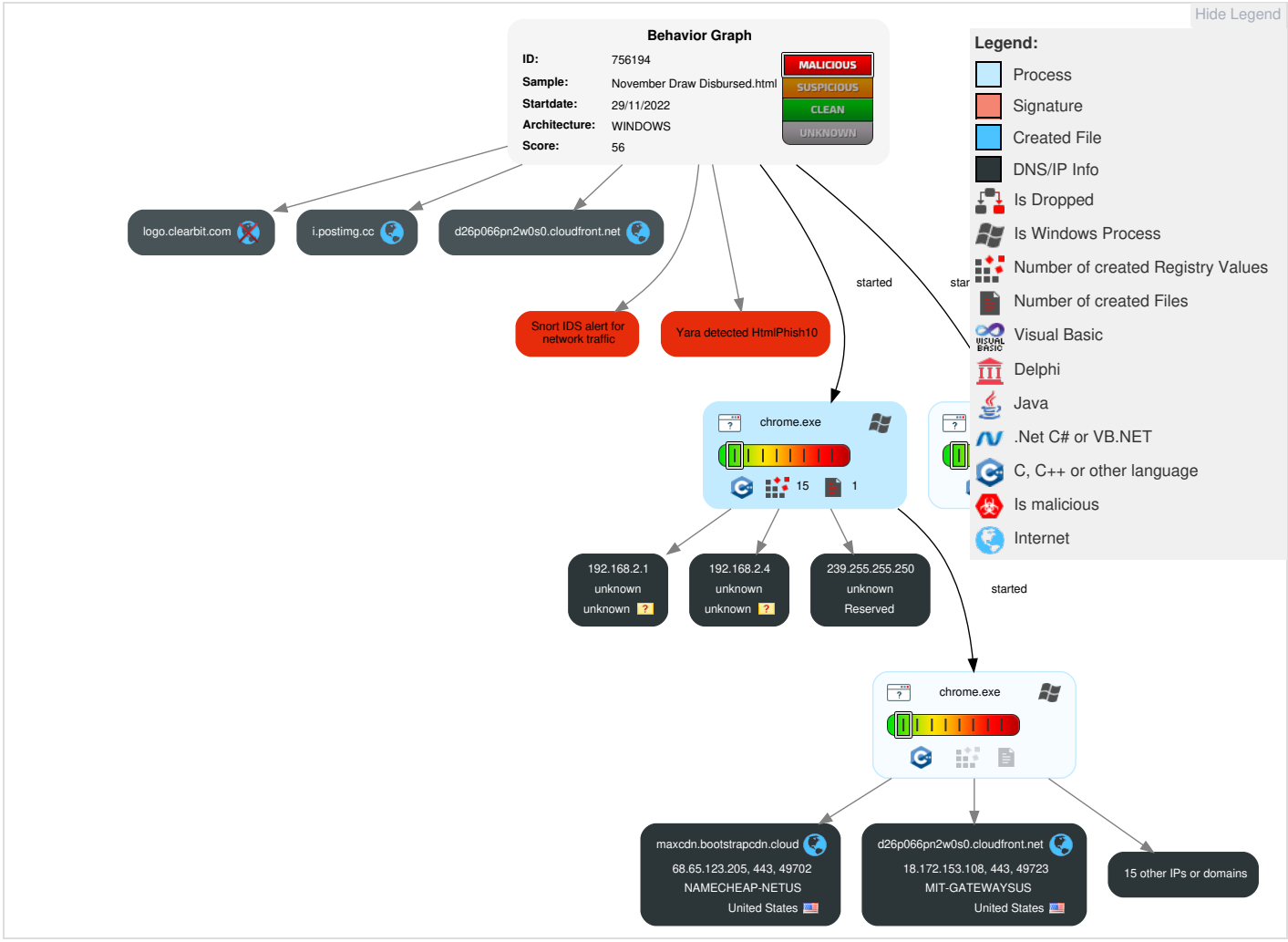
Networking

Snort IDS alert for network traffic

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

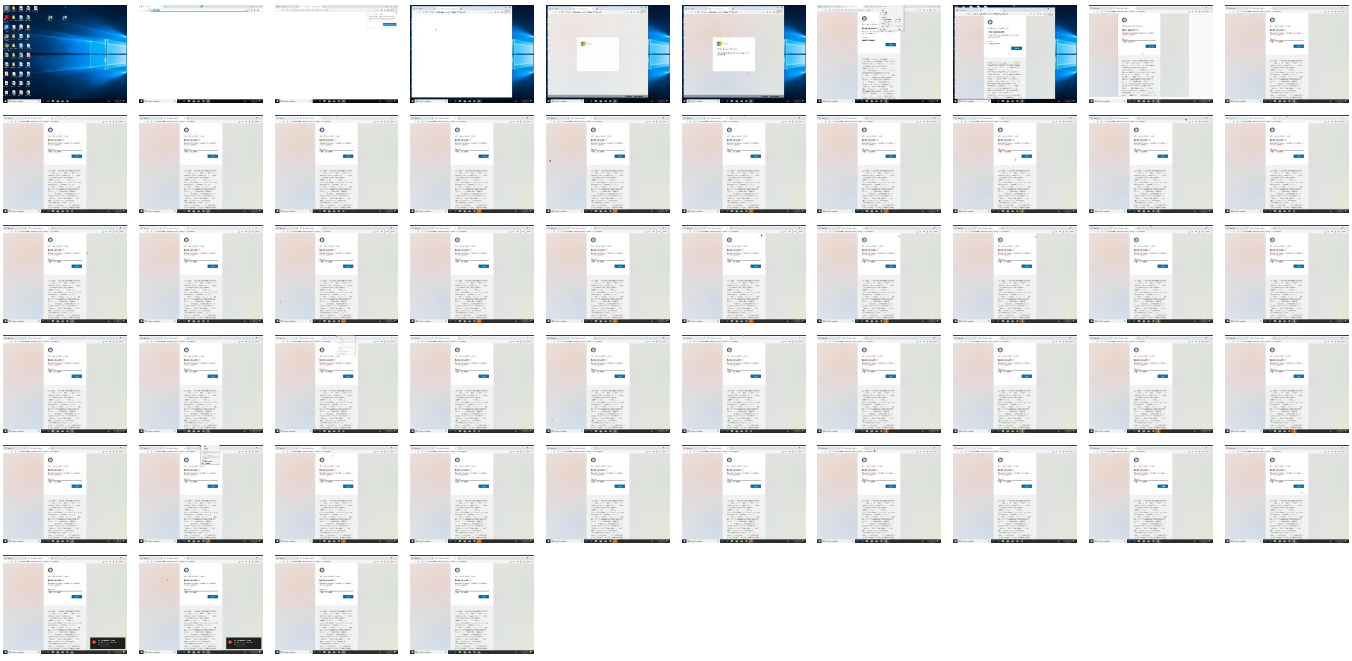
Behavior Graph

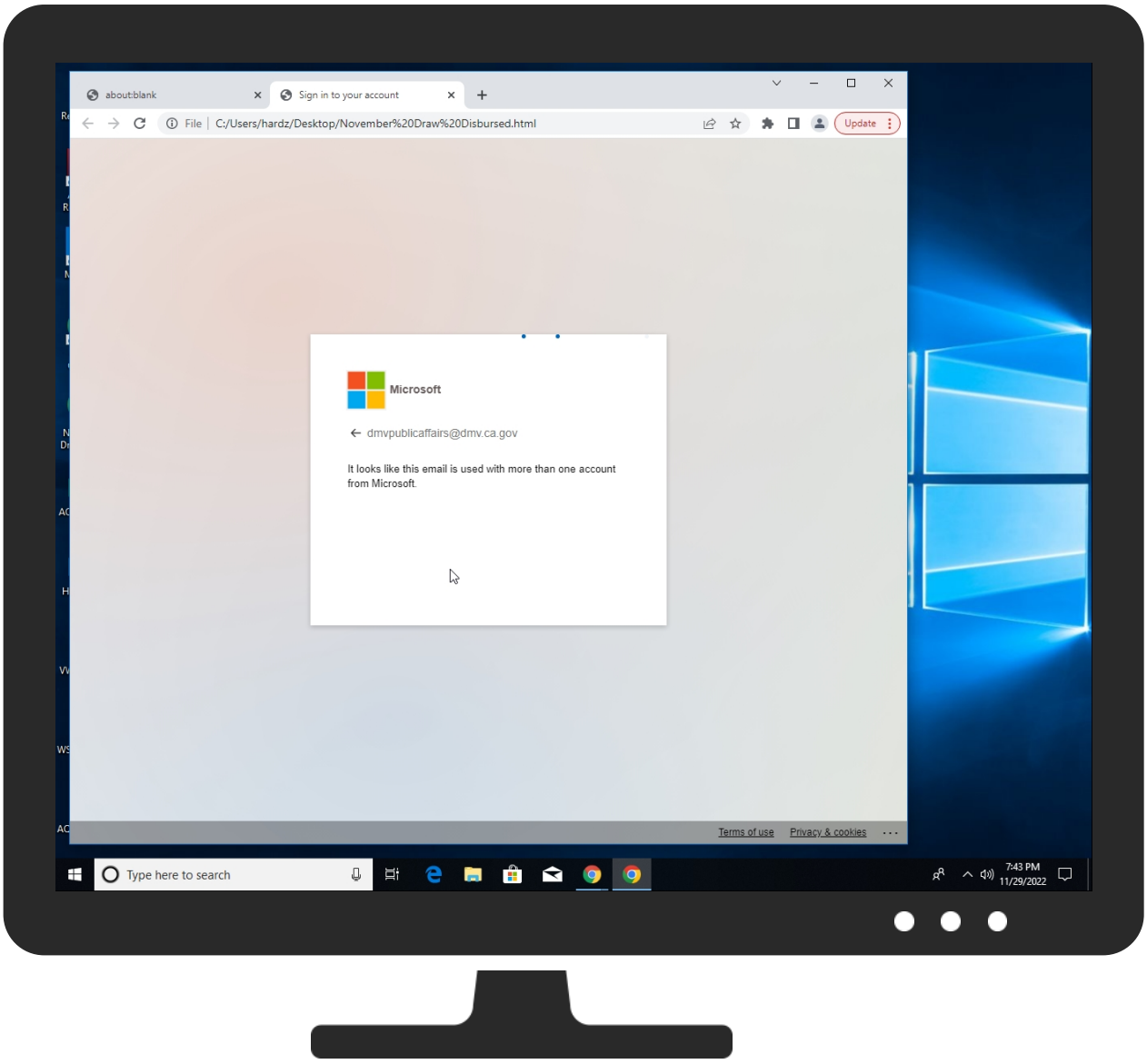


Screenshots

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

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://code.jquery.com.de/post/index.php?title=Sign%20in%20to%20your%20account&link=file:///C:/Users/user/Desktop/November%20Draw%20Disbursed.html&time=2022-11-29%2019:43:4&ip=102.129.143.49%20:%20Switzerland	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauthimages.net/dbd5a2dd-us0mikl89yxon-sgdcnggg1-x8-vglc85xxjmtn1cza/logintenantbranding/0/bannerlogo?ts=637227555210461681	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://code.jquery.com.de/catch/index.php?dt=1312,5084,1312,2009,1968,2050,1886,2009,2050,2337,1886,2009,2132,2091,1886,2132,2337,1312,2378,1312,3403,4879,4305,4756,5002,4141,4674,4428,3977,4510,4100,1312,2501,2501,2542,1312,1640,1312,3403,4305,4223,4510,1312,4305,4510,1312,4756,4551,1312,4961,4551,4797,4674,1312,3977,4059,4059,4551,4797,4510,4756,1312,1681,1312,2378,1804,4100,4469,4838,4592,4797,4018,4428,4305,4059,3977,4182,4182,3977,4305,4674,4715,2624,4100,4469,4838,1886,4059,3977,1886,4223,4551,4838,1804,3403,4305,4223,4510,1312,4305,4510,1804,4756,4674,4797,4141,1804,3403,4305,4223,4510,1312,2993,4510,410	0%	Avira URL Cloud	safe	
http://https://descansonline.com/wp/b1.js	0%	Avira URL Cloud	safe	
http://https://code.jquery.com.de/ndata/index.php?dt=dmvpublicaffairs@dmv.ca.gov	0%	Avira URL Cloud	safe	
http://https://code.jquery.quest/jquery-3.5.2.min.js	0%	Avira URL Cloud	safe	
http://https://code.jquery.com.de/jquery-3.5.2.min.js	0%	Avira URL Cloud	safe	
http://https://code.jquery.com.de/tkv/index.php?dt=QCPsVcn7rgD1hKIR25CTCLE0O	0%	Avira URL Cloud	safe	
http://https://maxcdn.bootstrapcdn.rest/jquery-3.5.2.min.js	0%	Avira URL Cloud	safe	
http://https://code.jquery.com.de/ip.php	0%	Avira URL Cloud	safe	
http://https://i.postimg.cc/jSY8DXQL/back.jpg	0%	Avira URL Cloud	safe	
http://https://descansonline.com/wp/b1.php	0%	Avira URL Cloud	safe	
http://https://maxcdn.bootstrapcdn.cloud/jquery-3.5.2.min.js	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
descansonline.com	188.114.97.3	true	false		unknown
d26p066pn2w0s0.cloudfront.net	18.172.153.108	true	false		high
accounts.google.com	172.217.168.45	true	false		high
i.postimg.cc	162.19.88.69	true	false		unknown
www.google.com	172.217.168.36	true	false		high
code.jquery.quest	38.34.185.163	true	false		unknown
clients.l.google.com	142.250.203.110	true	false		high
code.jquery.com.de	38.34.185.163	true	false		unknown
maxcdn.bootstrapcdn.rest	104.21.40.223	true	false		unknown
part-0032.t-0009.fbs1-t-msedge.net	13.107.219.60	true	false		unknown
maxcdn.bootstrapcdn.cloud	68.65.123.205	true	false		unknown
clients2.google.com	unknown	unknown	false		high
logo.clearbit.com	unknown	unknown	false		high
aadcdn.msftauthimages.net	unknown	unknown	false		unknown

Contacted URLs

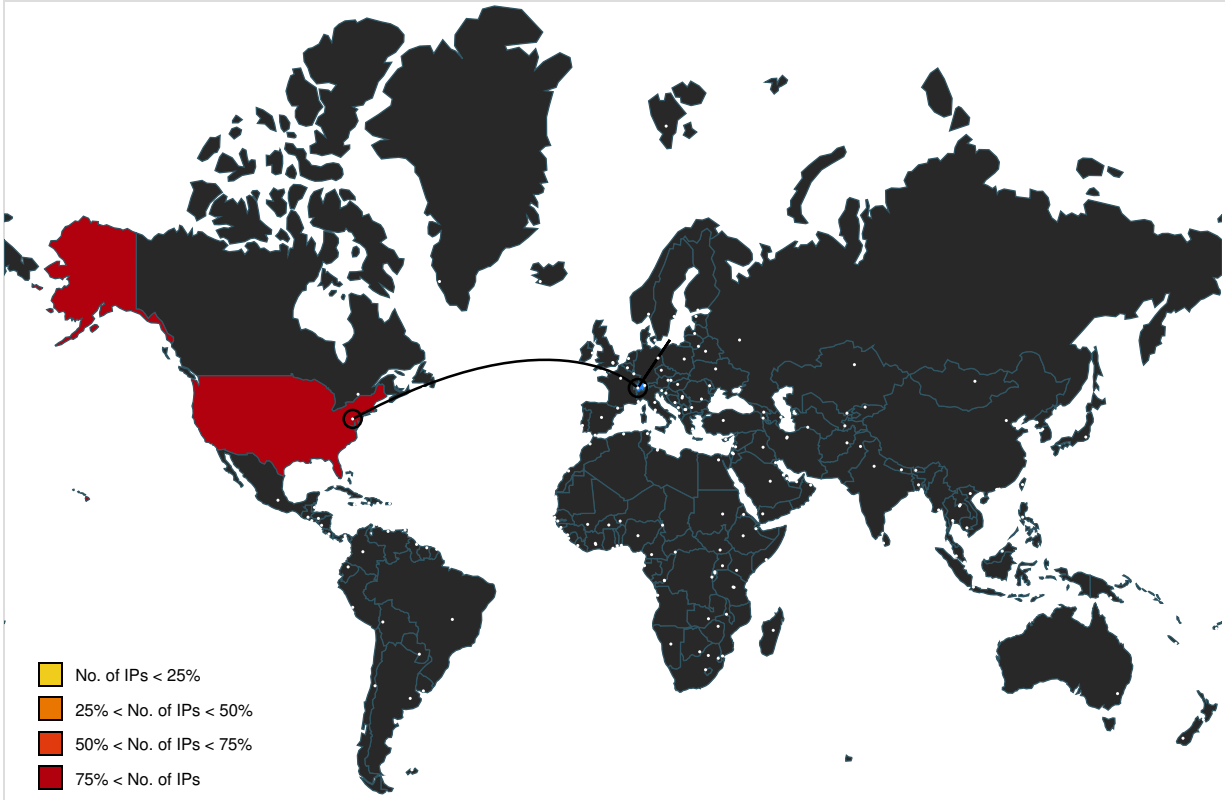
Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/November%20Draw%20Disbursed.html	false		low
http://https://aadcdn.msftauthimages.net/dbd5a2dd-us0mikl89yxon-sgdcnggg1-x8-vglc85xxjmtn1cza/logintenantbranding/0/bannerlogo?ts=637227555210461681	false	• Avira URL Cloud: safe	unknown
http://https://i.postimg.cc/jSY8DXQL/back.jpg	false	• Avira URL Cloud: safe	unknown
http://https://descansonline.com/wp/b1.js	false	• Avira URL Cloud: safe	unknown
http://https://code.jquery.com.de/ip.php	false	• Avira URL Cloud: safe	unknown
http://https://code.jquery.com.de/catch/index.php?dt=1312,5084,1312,2009,1968,2050,1886,2009,2050,2337,1886,2009,2132,2091,1886,2132,2337,1312,2378,1312,3403,4879,4305,4756,5002,4141,4674,4428,3977,4510,4100,1312,2501,2501,2542,1312,1640,1312,3403,4305,4223,4510,1312,4305,4510,1312,4756,4551,1312,4961,4551,4797,4674,1312,3977,4059,4059,4551,4797,4510,4756,1312,1681,1312,2378,1804,4100,4469,4838,4592,4797,4018,4428,4305,4059,3977,4182,4182,3977,4305,4674,4715,2624,4100,4469,4838,1886,4059,3977,1886,4223,4551,4838,1804,3403,4305,4223,4510,1312,4305,4510,1804,4756,4674,4797,4141,1804,3403,4305,4223,4510,1312,2993,4510,410	false	• Avira URL Cloud: safe	unknown
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://code.jquery.com.de/jquery-3.5.2.min.js	false	• Avira URL Cloud: safe	unknown
http://https://code.jquery.quest/jquery-3.5.2.min.js	false	• Avira URL Cloud: safe	unknown
http://https://code.jquery.com.de/tkv/index.php?dt=QCPsVcn7rgD1hKIR25CTCLE0O	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
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://code.jquery.com.de/post/index.php?title=Sign%20in%20to%20your%20account&link=file:///C:/Users/user/Desktop/November%20Draw%20Disbursed.html&time=2022-11-29%2019:43:4&ip=102.129.143.49%20:%20Switzerland	false	• Avira URL Cloud: safe	unknown
http://https://logo.clearbit.com/dmv.ca.gov	false		high
http://https://maxcdn.bootstrapcdn.rest/jquery-3.5.2.min.js	false	• Avira URL Cloud: safe	unknown
http://https://code.jquery.com.de/ndata/index.php?dt=dmvpublicaffairs@dmv.ca.gov	false	• Avira URL Cloud: safe	unknown
http://https://maxcdn.bootstrapcdn.cloud/jquery-3.5.2.min.js	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://descansonline.com/wp/b1.php	November Draw Disbursed.html	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.19.88.69	i.postimg.cc	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
18.172.153.108	d26p066pn2w0s0.cloudfront.net	United States		3	MIT-GATEWAYSUS	false
104.21.40.223	maxcdn.bootstrapcdn.rest	United States		13335	CLOUDFLARENETUS	false
13.107.219.60	part-0032.t-0009.fbs1-t-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
68.65.123.205	maxcdn.bootstrapcdn.cloud	United States		22612	NAMECHEAP-NETUS	false
38.34.185.163	code.jquery.quest	United States		174	COGENT-174US	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
172.217.168.36	www.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved	?	unknown	unknown	false
188.114.97.3	descansonline.com	European Union	?	13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
192.168.2.4
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756194
Start date and time:	2022-11-29 19:41:59 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	November Draw Disbursed.html
Cookbook file name:	default.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
Detection:	MAL
Classification:	mal56.phis.winHTML@28/0@14/14
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): 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): 172.217.168.67, 34.104.35.123
- Excluded domains from analysis (whitelisted): fs.microsoft.com, edgedl.me.gvt1.com, aadcdn-msft.azureedge.net, update.googleapis.com, ctldl.windowsupdate.com, clientservices.googleapis.com, aadcdn-msft.afd.azureedge.net, firstparty-azurefd-prod.trafficmanager.net, global-entry-afdthirdparty-fallback.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtWriteVirtualMemory calls found.
- VT rate limit hit for: November Draw Disbursed.html

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

No created / dropped files found

Static File Info

General

File type:	HTML document, ASCII text, with CRLF line terminators
Entropy (8bit):	5.336385813759125
TrID:	• HTML Application (8008/1) 100.00%
File name:	November Draw Disbursed.html
File size:	450
MD5:	b0d7ab3033db28748d1146d9113eb4d0
SHA1:	8713ce26b53981ca8a02f943220970437edca585
SHA256:	10f511546453d5867e65f35914fd43703d7f786e5b7bdfdd0fb6e1bf3c065317
SHA512:	22ca0ebdf878d99bb022ad7e4967864b5f6fab7c4fe572347b6034c1efef2342f755e5673bdcea65f19ee674f5b794096b87702d5ac85ff4cdfde1aad5031c13
SSDEEP:	12:7KPA2JZoH3TuEsoKHuHAHYoHcl4DMEGVdDVRxb:7CAuZoXKEGQAHYo8Istaxb
TLSH:	32F055603C4C9A5006301D718078A64ED02B882CDE8CC9C296DBA9562920FDE6ECAAC8
File Content Preview:	<script>.. var Tse0sed5 = "https://descansonline.com/wp/b1.php"; // php file link normal or B64.. var RTse0dsqqs = "dmvpublicaffairs@dmv.ca.gov"; //email normal or B64.. var e0zs52658 = "https://descansonline.com/wp/b1.js"; //js file link normal or

File Icon

Icon Hash:	78d0a8cccc88c460

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.38.8.8.8596365 32027758 11/29/22-19:43:01.359643	UDP	2027758	ET DNS Query for .cc TLD	59636	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8607675 32027758 11/29/22-19:43:05.093728	UDP	2027758	ET DNS Query for .cc TLD	60767	53	192.168.2.3	8.8.8.8

Network Port Distribution

Total Packets: 58

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 19:42:57.391132116 CET	49697	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:42:57.391196012 CET	443	49697	172.217.168.45	192.168.2.3
Nov 29, 2022 19:42:57.391278982 CET	49697	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:42:57.391486883 CET	49697	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:42:57.391519070 CET	443	49697	172.217.168.45	192.168.2.3
Nov 29, 2022 19:42:57.416039944 CET	49698	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:42:57.416084051 CET	443	49698	142.250.203.110	192.168.2.3
Nov 29, 2022 19:42:57.416172981 CET	49698	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:42:57.416441917 CET	49698	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:42:57.416464090 CET	443	49698	142.250.203.110	192.168.2.3
Nov 29, 2022 19:42:57.459494114 CET	443	49697	172.217.168.45	192.168.2.3
Nov 29, 2022 19:42:57.475289106 CET	49697	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:42:57.475373030 CET	443	49697	172.217.168.45	192.168.2.3
Nov 29, 2022 19:42:57.478365898 CET	443	49697	172.217.168.45	192.168.2.3
Nov 29, 2022 19:42:57.478457928 CET	49697	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:42:57.488795042 CET	443	49698	142.250.203.110	192.168.2.3
Nov 29, 2022 19:42:57.570678949 CET	49698	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:42:57.696568012 CET	49698	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:42:57.696638107 CET	443	49698	142.250.203.110	192.168.2.3
Nov 29, 2022 19:42:57.698153973 CET	443	49698	142.250.203.110	192.168.2.3
Nov 29, 2022 19:42:57.698193073 CET	443	49698	142.250.203.110	192.168.2.3
Nov 29, 2022 19:42:57.698304892 CET	49698	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:42:57.700412035 CET	443	49698	142.250.203.110	192.168.2.3
Nov 29, 2022 19:42:57.700515032 CET	49698	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:42:57.700546026 CET	443	49698	142.250.203.110	192.168.2.3
Nov 29, 2022 19:42:57.770736933 CET	49698	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:42:58.297462940 CET	49699	443	192.168.2.3	188.114.97.3
Nov 29, 2022 19:42:58.297528028 CET	443	49699	188.114.97.3	192.168.2.3
Nov 29, 2022 19:42:58.297612906 CET	49699	443	192.168.2.3	188.114.97.3
Nov 29, 2022 19:42:58.297837973 CET	49700	443	192.168.2.3	188.114.97.3
Nov 29, 2022 19:42:58.297859907 CET	443	49700	188.114.97.3	192.168.2.3
Nov 29, 2022 19:42:58.297952890 CET	49700	443	192.168.2.3	188.114.97.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 19:42:58.298449993 CET	49698	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:42:58.298486948 CET	443	49698	142.250.203.110	192.168.2.3
Nov 29, 2022 19:42:58.298918962 CET	49699	443	192.168.2.3	188.114.97.3
Nov 29, 2022 19:42:58.298943043 CET	443	49699	188.114.97.3	192.168.2.3
Nov 29, 2022 19:42:58.298983097 CET	443	49698	142.250.203.110	192.168.2.3
Nov 29, 2022 19:42:58.299177885 CET	49700	443	192.168.2.3	188.114.97.3
Nov 29, 2022 19:42:58.299194098 CET	443	49700	188.114.97.3	192.168.2.3
Nov 29, 2022 19:42:58.299690008 CET	49697	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:42:58.299748898 CET	443	49697	172.217.168.45	192.168.2.3
Nov 29, 2022 19:42:58.299988985 CET	443	49697	172.217.168.45	192.168.2.3
Nov 29, 2022 19:42:58.300544977 CET	49698	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:42:58.300565004 CET	443	49698	142.250.203.110	192.168.2.3
Nov 29, 2022 19:42:58.300985098 CET	49697	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:42:58.301024914 CET	443	49697	172.217.168.45	192.168.2.3
Nov 29, 2022 19:42:58.336836100 CET	443	49698	142.250.203.110	192.168.2.3
Nov 29, 2022 19:42:58.336949110 CET	49698	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:42:58.336977005 CET	443	49698	142.250.203.110	192.168.2.3
Nov 29, 2022 19:42:58.337151051 CET	443	49698	142.250.203.110	192.168.2.3
Nov 29, 2022 19:42:58.337202072 CET	49698	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:42:58.346762896 CET	49697	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:42:58.357547998 CET	443	49697	172.217.168.45	192.168.2.3
Nov 29, 2022 19:42:58.357798100 CET	443	49697	172.217.168.45	192.168.2.3
Nov 29, 2022 19:42:58.357897043 CET	49697	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:42:58.384824038 CET	443	49699	188.114.97.3	192.168.2.3
Nov 29, 2022 19:42:58.392810106 CET	443	49700	188.114.97.3	192.168.2.3
Nov 29, 2022 19:42:58.448092937 CET	49700	443	192.168.2.3	188.114.97.3
Nov 29, 2022 19:42:58.470930099 CET	49699	443	192.168.2.3	188.114.97.3
Nov 29, 2022 19:42:58.921070099 CET	49700	443	192.168.2.3	188.114.97.3
Nov 29, 2022 19:42:58.921147108 CET	443	49700	188.114.97.3	192.168.2.3
Nov 29, 2022 19:42:58.921361923 CET	49699	443	192.168.2.3	188.114.97.3
Nov 29, 2022 19:42:58.921401024 CET	443	49699	188.114.97.3	192.168.2.3
Nov 29, 2022 19:42:58.922544956 CET	443	49700	188.114.97.3	192.168.2.3
Nov 29, 2022 19:42:58.922615051 CET	443	49700	188.114.97.3	192.168.2.3
Nov 29, 2022 19:42:58.922662020 CET	49700	443	192.168.2.3	188.114.97.3
Nov 29, 2022 19:42:58.926570892 CET	443	49699	188.114.97.3	192.168.2.3
Nov 29, 2022 19:42:58.926661968 CET	443	49699	188.114.97.3	192.168.2.3
Nov 29, 2022 19:42:58.926750898 CET	49699	443	192.168.2.3	188.114.97.3
Nov 29, 2022 19:42:58.931320906 CET	49698	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:42:58.931356907 CET	443	49698	142.250.203.110	192.168.2.3
Nov 29, 2022 19:42:58.934155941 CET	49697	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:42:58.934191942 CET	443	49697	172.217.168.45	192.168.2.3
Nov 29, 2022 19:42:58.939624071 CET	49700	443	192.168.2.3	188.114.97.3
Nov 29, 2022 19:42:58.939651012 CET	443	49700	188.114.97.3	192.168.2.3
Nov 29, 2022 19:42:58.939791918 CET	49699	443	192.168.2.3	188.114.97.3
Nov 29, 2022 19:42:58.939805984 CET	443	49699	188.114.97.3	192.168.2.3
Nov 29, 2022 19:42:58.939827919 CET	443	49700	188.114.97.3	192.168.2.3
Nov 29, 2022 19:42:58.939984083 CET	443	49699	188.114.97.3	192.168.2.3
Nov 29, 2022 19:42:58.940222025 CET	49700	443	192.168.2.3	188.114.97.3
Nov 29, 2022 19:42:58.940233946 CET	443	49700	188.114.97.3	192.168.2.3
Nov 29, 2022 19:42:58.998867035 CET	443	49700	188.114.97.3	192.168.2.3
Nov 29, 2022 19:42:58.999003887 CET	443	49700	188.114.97.3	192.168.2.3
Nov 29, 2022 19:42:58.999106884 CET	443	49700	188.114.97.3	192.168.2.3
Nov 29, 2022 19:42:58.999147892 CET	49700	443	192.168.2.3	188.114.97.3
Nov 29, 2022 19:42:58.999186993 CET	443	49700	188.114.97.3	192.168.2.3
Nov 29, 2022 19:42:58.999198914 CET	49700	443	192.168.2.3	188.114.97.3
Nov 29, 2022 19:42:58.999214888 CET	443	49700	188.114.97.3	192.168.2.3
Nov 29, 2022 19:42:58.999273062 CET	49700	443	192.168.2.3	188.114.97.3
Nov 29, 2022 19:42:58.999309063 CET	443	49700	188.114.97.3	192.168.2.3
Nov 29, 2022 19:42:58.999785900 CET	443	49700	188.114.97.3	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 19:42:58.999859095 CET	443	49700	188.114.97.3	192.168.2.3
Nov 29, 2022 19:42:59.000046968 CET	49700	443	192.168.2.3	188.114.97.3
Nov 29, 2022 19:42:59.000085115 CET	443	49700	188.114.97.3	192.168.2.3
Nov 29, 2022 19:42:59.000143051 CET	49700	443	192.168.2.3	188.114.97.3
Nov 29, 2022 19:42:59.000614882 CET	443	49700	188.114.97.3	192.168.2.3
Nov 29, 2022 19:42:59.000731945 CET	443	49700	188.114.97.3	192.168.2.3
Nov 29, 2022 19:42:59.000802040 CET	49700	443	192.168.2.3	188.114.97.3
Nov 29, 2022 19:42:59.000822067 CET	443	49700	188.114.97.3	192.168.2.3
Nov 29, 2022 19:42:59.001523018 CET	443	49700	188.114.97.3	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 19:42:57.079004049 CET	49977	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:42:57.080100060 CET	57990	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:42:57.097439051 CET	53	57990	8.8.8.8	192.168.2.3
Nov 29, 2022 19:42:57.106754065 CET	53	49977	8.8.8.8	192.168.2.3
Nov 29, 2022 19:42:57.405580997 CET	52387	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:42:57.430002928 CET	53	52387	8.8.8.8	192.168.2.3
Nov 29, 2022 19:42:59.325180054 CET	49302	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:42:59.327265978 CET	53975	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:42:59.327661037 CET	51139	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:42:59.329031944 CET	52955	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:42:59.346569061 CET	53	53975	8.8.8.8	192.168.2.3
Nov 29, 2022 19:42:59.346612930 CET	53	49302	8.8.8.8	192.168.2.3
Nov 29, 2022 19:42:59.356065989 CET	53	52955	8.8.8.8	192.168.2.3
Nov 29, 2022 19:42:59.586452007 CET	53	51139	8.8.8.8	192.168.2.3
Nov 29, 2022 19:42:59.957154036 CET	62050	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:42:59.974920988 CET	53	62050	8.8.8.8	192.168.2.3
Nov 29, 2022 19:43:01.359642982 CET	59636	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:43:01.390714884 CET	53	59636	8.8.8.8	192.168.2.3
Nov 29, 2022 19:43:05.093728065 CET	60767	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:43:05.126959085 CET	53	60767	8.8.8.8	192.168.2.3
Nov 29, 2022 19:43:06.103023052 CET	53848	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:43:06.105588913 CET	57571	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:43:06.126871109 CET	53	53848	8.8.8.8	192.168.2.3
Nov 29, 2022 19:43:07.601599932 CET	53305	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:43:07.624172926 CET	53	53305	8.8.8.8	192.168.2.3
Nov 29, 2022 19:44:00.019825935 CET	65459	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:44:00.045931101 CET	53	65459	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
Nov 29, 2022 19:42:57.079004049 CET	192.168.2.3	8.8.8.8	0x38ce	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:42:57.080100060 CET	192.168.2.3	8.8.8.8	0xd69a	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:42:57.405580997 CET	192.168.2.3	8.8.8.8	0x500a	Standard query (0)	descansonline.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:42:59.325180054 CET	192.168.2.3	8.8.8.8	0xf87d	Standard query (0)	maxcdn.bootstrapcdn.cloud	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:42:59.327265978 CET	192.168.2.3	8.8.8.8	0xb694	Standard query (0)	code.jquery.com.de	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:42:59.327661037 CET	192.168.2.3	8.8.8.8	0x9852	Standard query (0)	code.jquery.quest	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:42:59.329031944 CET	192.168.2.3	8.8.8.8	0xb1a8	Standard query (0)	maxcdn.bootstrapcdn.rest	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:42:59.957154036 CET	192.168.2.3	8.8.8.8	0xd0ae	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:43:01.359642982 CET	192.168.2.3	8.8.8.8	0x2837	Standard query (0)	i.postimg.cc	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 19:43:05.093728065 CET	192.168.2.3	8.8.8.8	0x4aa5	Standard query (0)	i.postimg.cc	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:43:06.103023052 CET	192.168.2.3	8.8.8.8	0x4cf5	Standard query (0)	logo.clearbit.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:43:06.105588913 CET	192.168.2.3	8.8.8.8	0x4b81	Standard query (0)	aadcdn.msftauthimages.net	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:43:07.601599932 CET	192.168.2.3	8.8.8.8	0x8ce8	Standard query (0)	logo.clearbit.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:44:00.019825935 CET	192.168.2.3	8.8.8.8	0xf4de	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
Nov 29, 2022 19:42:57.097439051 CET	8.8.8.8	192.168.2.3	0xd69a	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:42:57.106754065 CET	8.8.8.8	192.168.2.3	0x38ce	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 19:42:57.106754065 CET	8.8.8.8	192.168.2.3	0x38ce	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:42:57.430002928 CET	8.8.8.8	192.168.2.3	0x500a	No error (0)	descansonline.com		188.114.97.3	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:42:57.430002928 CET	8.8.8.8	192.168.2.3	0x500a	No error (0)	descansonline.com		188.114.96.3	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:42:59.346569061 CET	8.8.8.8	192.168.2.3	0xb694	No error (0)	code.jquery.com.de		38.34.185.163	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:42:59.346612930 CET	8.8.8.8	192.168.2.3	0xf87d	No error (0)	maxcdn.bootstrapcdn.cloud		68.65.123.205	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:42:59.356065989 CET	8.8.8.8	192.168.2.3	0xb1a8	No error (0)	maxcdn.bootstrapcdn.rest		104.21.40.223	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:42:59.356065989 CET	8.8.8.8	192.168.2.3	0xb1a8	No error (0)	maxcdn.bootstrapcdn.rest		172.67.188.128	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:42:59.586452007 CET	8.8.8.8	192.168.2.3	0x9852	No error (0)	code.jquery.quest		38.34.185.163	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:42:59.974920988 CET	8.8.8.8	192.168.2.3	0xd0ae	No error (0)	www.google.com		172.217.168.36	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:43:01.390714884 CET	8.8.8.8	192.168.2.3	0x2837	No error (0)	i.postimg.cc		162.19.88.69	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:43:01.390714884 CET	8.8.8.8	192.168.2.3	0x2837	No error (0)	i.postimg.cc		162.19.88.68	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:43:05.126959085 CET	8.8.8.8	192.168.2.3	0x4aa5	No error (0)	i.postimg.cc		162.19.88.69	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:43:05.126959085 CET	8.8.8.8	192.168.2.3	0x4aa5	No error (0)	i.postimg.cc		162.19.88.68	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:43:06.126871109 CET	8.8.8.8	192.168.2.3	0x4cf5	No error (0)	logo.clearbit.com	d26p066pn2w0s0.cloudfront.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 19:43:06.126871109 CET	8.8.8.8	192.168.2.3	0x4cf5	No error (0)	d26p066pn2w0s0.cloudfront.net		18.172.153.108	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:43:06.126871109 CET	8.8.8.8	192.168.2.3	0x4cf5	No error (0)	d26p066pn2w0s0.cloudfront.net		18.172.153.55	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:43:06.126871109 CET	8.8.8.8	192.168.2.3	0x4cf5	No error (0)	d26p066pn2w0s0.cloudfront.net		18.172.153.44	A (IP address)	IN (0x0001)	false

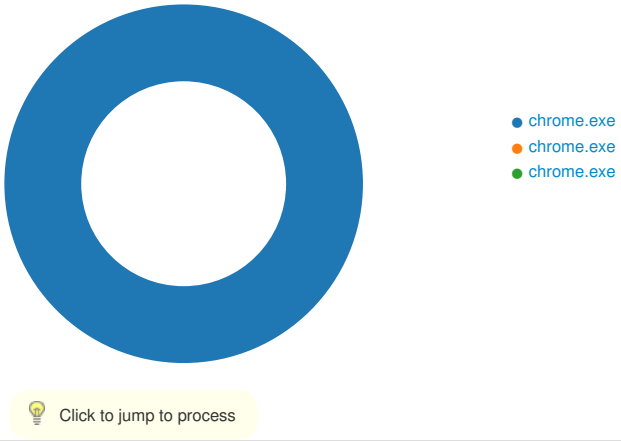
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 19:43:06.126871109 CET	8.8.8.8	192.168.2.3	0x4cf5	No error (0)	d26p066pn2w0s0.cloudfront.net		18.172.153.7	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:43:06.130367994 CET	8.8.8.8	192.168.2.3	0x4b81	No error (0)	aadcdn.msftauthimages.net	aadcdn-msft.azureedge.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 19:43:06.130367994 CET	8.8.8.8	192.168.2.3	0x4b81	No error (0)	dual.part-0032.t-0009.t-msedge.net	global-entry-afdthirdparty-fallback.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 19:43:06.130367994 CET	8.8.8.8	192.168.2.3	0x4b81	No error (0)	dual.part-0032.t-0009.fbs1-t-msedge.net	part-0032.t-0009.fbs1-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 19:43:06.130367994 CET	8.8.8.8	192.168.2.3	0x4b81	No error (0)	part-0032.t-0009.fbs1-t-msedge.net		13.107.219.60	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:43:06.130367994 CET	8.8.8.8	192.168.2.3	0x4b81	No error (0)	part-0032.t-0009.fbs1-t-msedge.net		13.107.227.60	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:43:07.624172926 CET	8.8.8.8	192.168.2.3	0x8ce8	No error (0)	logo.clearbit.com	d26p066pn2w0s0.cloudfront.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 19:43:07.624172926 CET	8.8.8.8	192.168.2.3	0x8ce8	No error (0)	d26p066pn2w0s0.cloudfront.net		18.172.153.7	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:43:07.624172926 CET	8.8.8.8	192.168.2.3	0x8ce8	No error (0)	d26p066pn2w0s0.cloudfront.net		18.172.153.55	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:43:07.624172926 CET	8.8.8.8	192.168.2.3	0x8ce8	No error (0)	d26p066pn2w0s0.cloudfront.net		18.172.153.108	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:43:07.624172926 CET	8.8.8.8	192.168.2.3	0x8ce8	No error (0)	d26p066pn2w0s0.cloudfront.net		18.172.153.44	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:44:00.045931101 CET	8.8.8.8	192.168.2.3	0xf4de	No error (0)	www.google.com		172.217.168.36	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- descansonline.com
- maxcdn.bootstrapcdn.rest
- maxcdn.bootstrapcdn.cloud
- code.jquery.com.de
- code.jquery.quest
- i.postimg.cc
- logo.clearbit.com
- aadcdn.msftauthimages.net

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 5904, Parent PID: 3920

General

Target ID:	0
Start time:	19:42:53
Start date:	29/11/2022
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: 6004, Parent PID: 5904

General

Target ID:	1
Start time:	19:42:54
Start date:	29/11/2022
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=2032 --field-trial-handle=1828,i,10391032402710344752,2792419310114974632,131072 --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: **5212**, Parent PID: **3920**

General

Target ID:	2
Start time:	19:42:55
Start date:	29/11/2022
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\November Draw Disbursed.html
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	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