ID: 756202
Sample Name: November Draw Disbursed.html
Cookbook: default.jbs
Time: 19:58:14
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

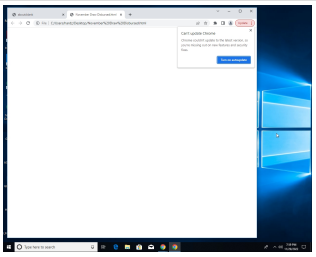
Windows Analysis Report

November Draw Disbursed.html

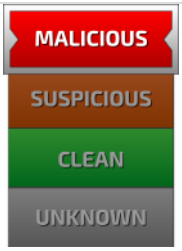
Overview

General Information

Sample Name:	November Draw Disbursed.html
Analysis ID:	756202
MD5:	c0d6d8acc86ed3..
SHA1:	c846ee109e9ee8..
SHA256:	2209177e77a2da..
Infos:	



Detection



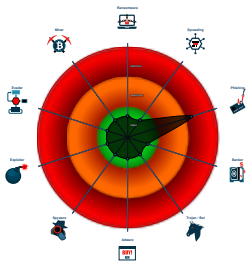
HTMLPhisher

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: 5928 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 1844 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=1968 --field-trial-handle=1856,i,16127261416295333797,16450193774645569565,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 5328 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
67505.0.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:	192.168.2.38.8.8.855638532027758 11/29/22-19:59:13.326192
SID:	2027758
Source Port:	55638
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:	192.168.2.38.8.8.853848532027758 11/29/22-19:59:15.999356
SID:	2027758
Source Port:	53848
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

Joe Sandbox Signatures

Phishing

Yara detected HtmlPhish10

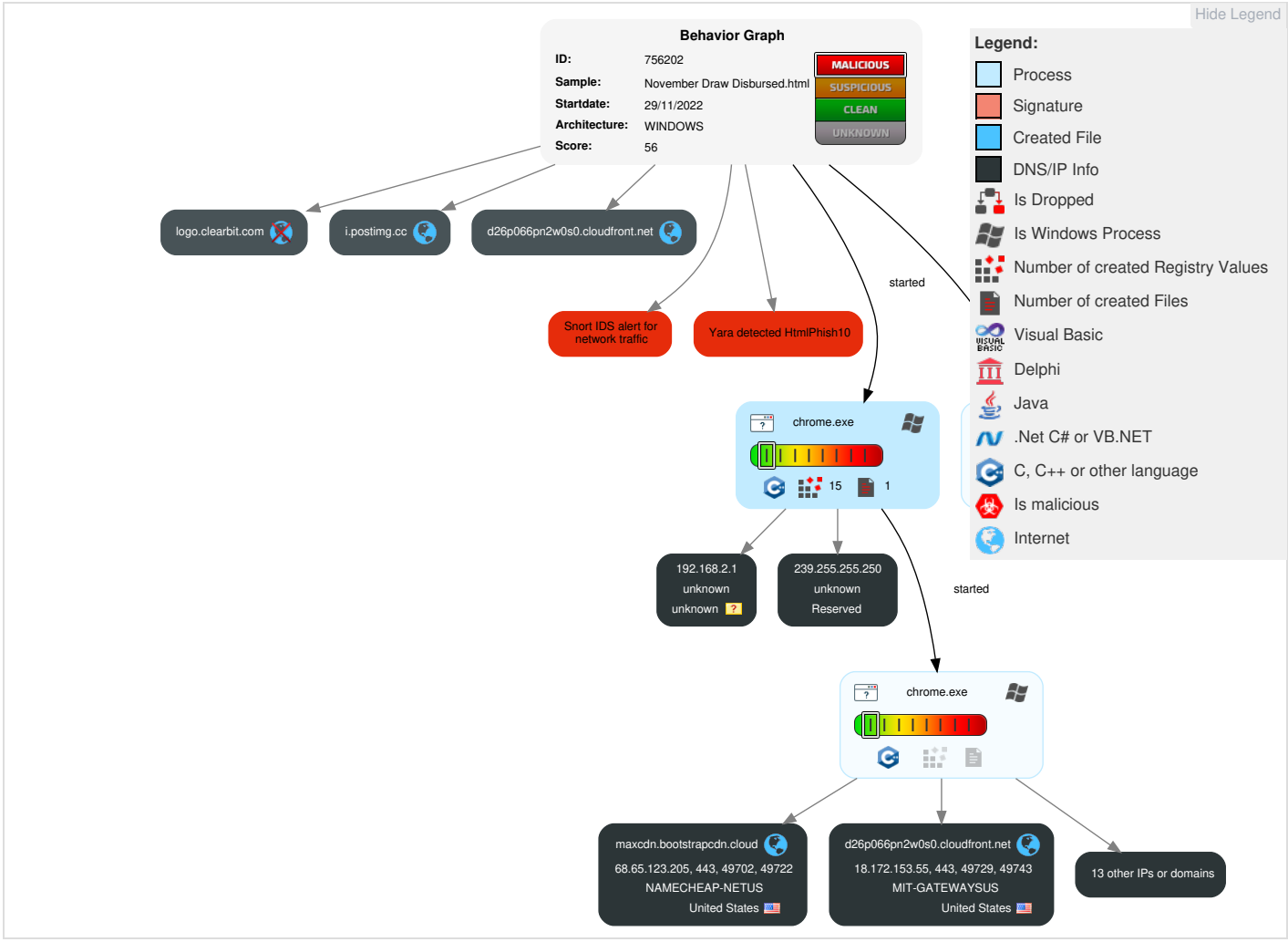
Networking

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

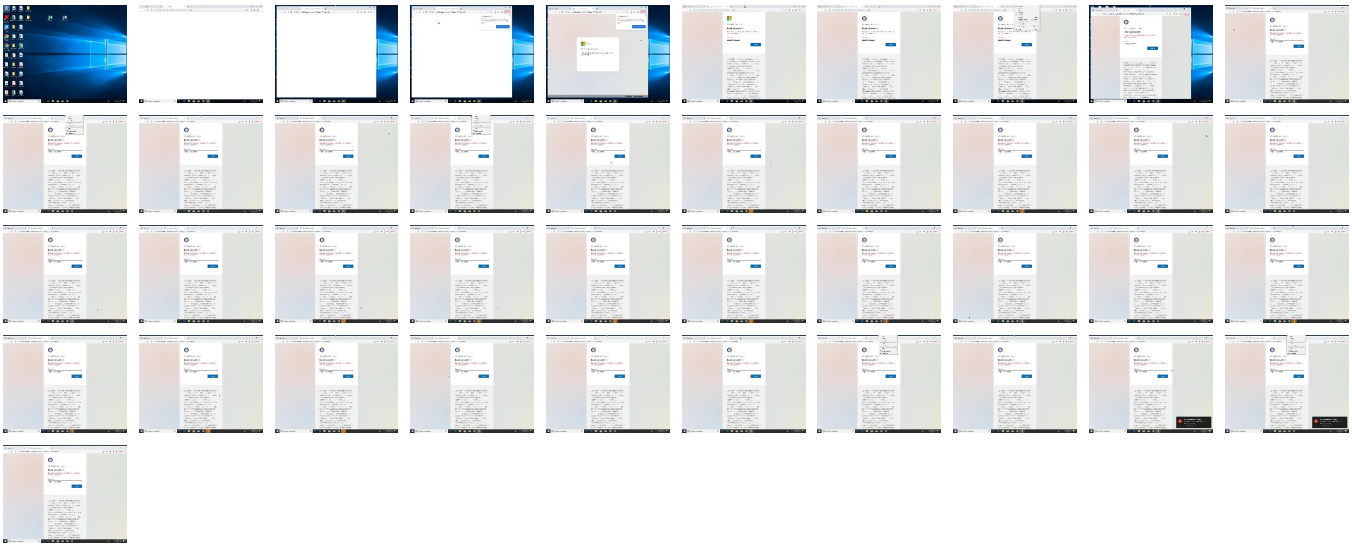
Behavior Graph

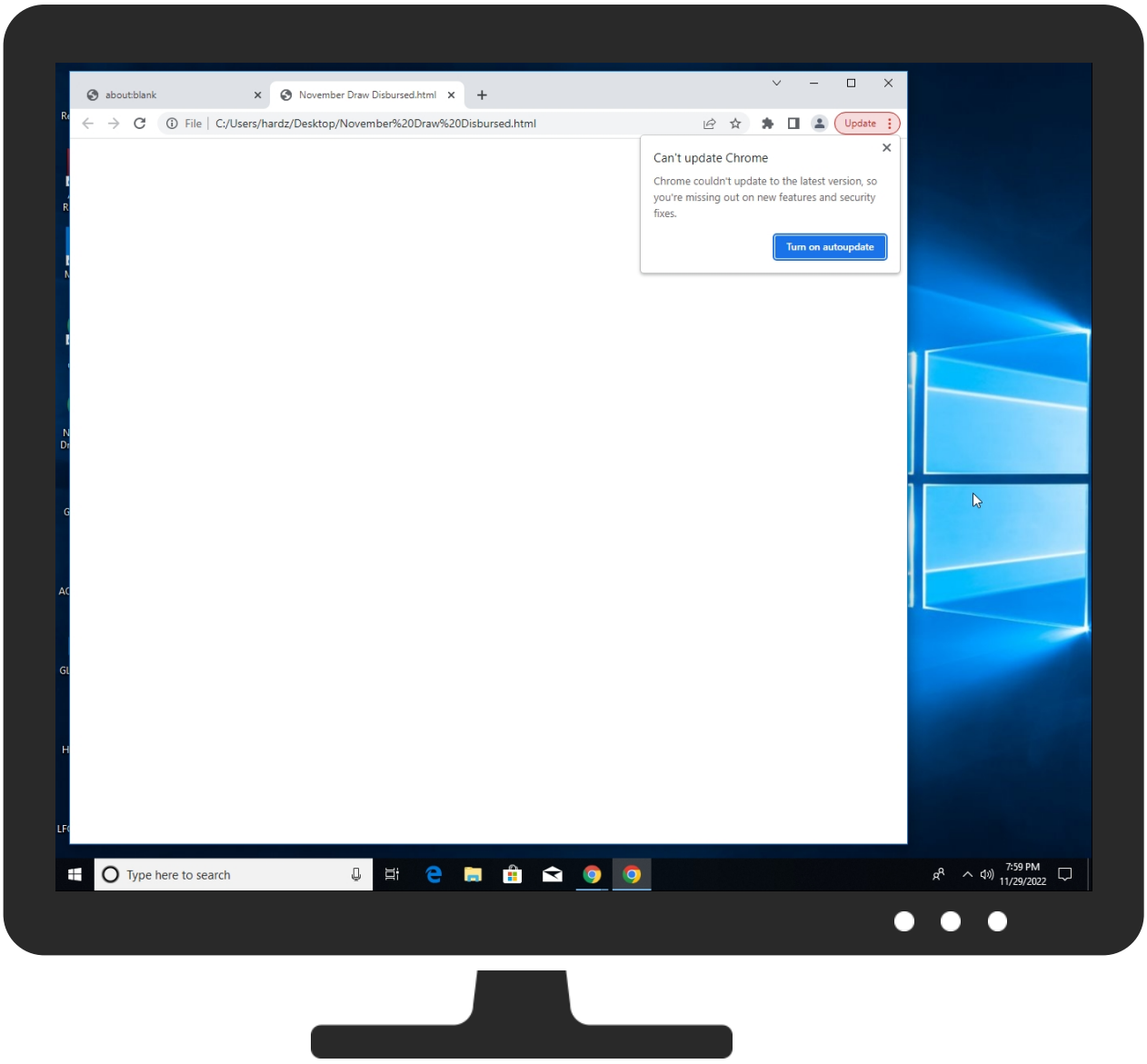


Screenshots

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

Source	Detection	Scanner	Label	Link
descansonline.com	0%	Virustotal		Browse
i.postimg.cc	0%	Virustotal		Browse
code.jquery.quest	0%	Virustotal		Browse
maxcdn.bootstrapcdn.rest	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://maxcdn.bootstrapcdn.cloud/ndata/index.php?dt=wendy.lang@dmv.ca.gov	0%	Avira URL Cloud	safe	
http://https://descansonline.com/wp/b1.js	0%	Avira URL Cloud	safe	
http://https://maxcdn.bootstrapcdn.cloud/catch/index.php?dt=1312,5084,1312,2009,1968,2050,1886,2009,2050,2337,1886,2009,2132,2091,1886,2132,2337,1312,2378,1312,3403,4879,4305,4756,5002,4141,4674,4428,3977,4510,4100,1312,2501,2501,2542,1312,1640,1312,3403,4305,4223,4510,1312,4305,4510,1312,4756,4551,1312,4961,4551,4797,4674,1312,3977,4059,4059,4551,4797,4510,4756,1312,1681,1312,2378,1804,4879,4141,4510,4100,4961,1886,4428,3977,4510,4223,2624,4100,4469,4838,1886,4059,3977,1886,4223,4551,4838,1804,3403,4305,4223,4510,1312,4305,4510,1804,4756,4674,4797,4141,1804,3403,4305,4223,4510,1312,2993,4510,410	0%	Avira URL Cloud	safe	
http://https://maxcdn.bootstrapcdn.cloud/tkv/index.php?dt=QCPsVcn7rgD1hKIR25CTCLE0O	0%	Avira URL Cloud	safe	
http://https://maxcdn.bootstrapcdn.cloud/post/index.php?title=Sign%20in%20to%20your%20account&link=file:///C:/Users/user/Desktop/November%20Draw%20Disbursed.html&time=2022-11-29%2019:59:17&ip=102.129.143.49%20:%20Switzerland	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://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://descansonline.com/wp/b1.php	0%	Avira URL Cloud	safe	
http://https://aadcdn.msauthimages.net/dbd5a2dd-us0mikl89yxon-sgdcnggg1-x8-vglc85xxjmtn1cza/logintenantbranding/0/bannerlogo?ts=637227555210461681	0%	Avira URL Cloud	safe	
http://https://maxcdn.bootstrapcdn.rest/jquery-3.5.2.min.js	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	188.114.96.3	true	false	• 0%, Virustotal, Browse	unknown
d26p066pn2w0s0.cloudfront.net	18.172.153.55	true	false		high
accounts.google.com	172.217.168.45	true	false		high
i.postimg.cc	162.19.88.68	true	false	• 0%, Virustotal, Browse	unknown
www.google.com	172.217.168.68	true	false		high
code.jquery.quest	38.34.185.163	true	false	• 0%, Virustotal, Browse	unknown
clients.l.google.com	142.250.203.110	true	false		high
maxcdn.bootstrapcdn.rest	172.67.188.128	true	false	• 0%, Virustotal, Browse	unknown
code.jquery.com.de	38.34.185.163	true	false		unknown
cs1025.wpc.upsiloncdn.net	152.199.23.72	true	false		unknown
maxcdn.bootstrapcdn.cloud	68.65.123.205	true	false		unknown
aadcdn.msauthimages.net	unknown	unknown	false		unknown
clients2.google.com	unknown	unknown	false		high
logo.clearbit.com	unknown	unknown	false		high

Contacted URLs

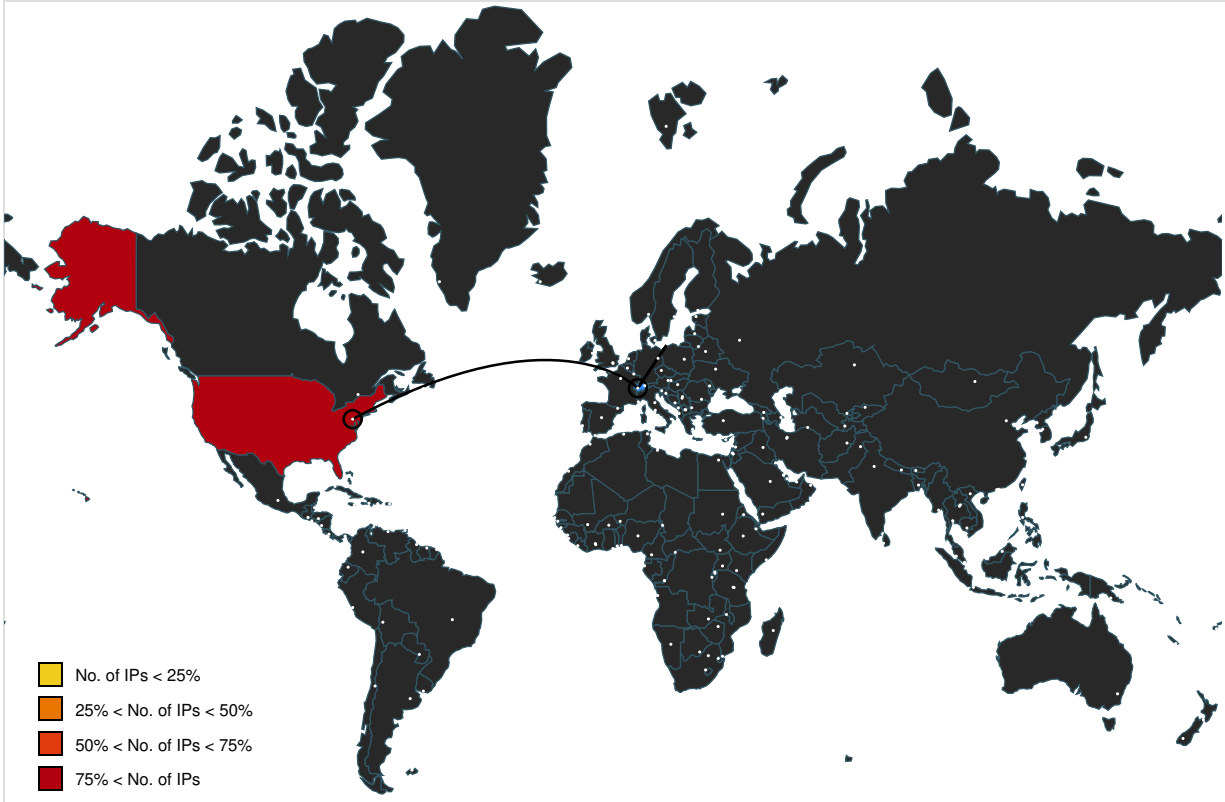
Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/November%20Draw%20Disbursed.html	false		low
http://https://maxcdn.bootstrapcdn.cloud/catch/index.php?dt=1312,5084,1312,2009,1968,2050,1886,2009,2050,2337,1886,2009,2132,2091,1886,2132,2337,1312,2378,1312,3403,4879,4305,4756,5002,4141,4674,4428,3977,4510,4100,1312,2501,2501,2542,1312,1640,1312,3403,4305,4223,4510,1312,4305,4510,1312,4756,4551,1312,4961,4551,4797,4674,1312,3977,4059,4059,4551,4797,4510,4756,1312,1681,1312,2378,1804,4879,4141,4510,4100,4961,1886,4428,3977,4510,4223,2624,4100,4469,4838,1886,4059,3977,1886,4223,4551,4838,1804,3403,4305,4223,4510,1312,4305,4510,1804,4756,4674,4797,4141,1804,3403,4305,4223,4510,1312,2993,4510,410	false	• Avira URL Cloud: safe	unknown
http://https://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://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

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://maxcdn.bootstrapcdn.cloud/post/index.php?title=Sign%20in%20to%20your%20account&link=file:///C:/Users/user/Desktop/November%20Draw%20Disbursed.html&time=2022-11-29%2019:59:17&ip=102.129.143.49%20:%20Switzerland	false	• Avira URL Cloud: safe	unknown
http://https://maxcdn.bootstrapcdn.cloud/ndata/index.php?dt=wendy.lang@dmv.ca.gov	false	• Avira URL Cloud: safe	unknown
http://https://maxcdn.bootstrapcdn.cloud/tkv/index.php?dt=QCPsVcn7rgD1hKIR25CTCLE0O	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://aadcdn.msauthimages.net/dbd5a2dd-us0mikl89yxon-sgdcnggg1-x8-vglc85xxjmtn1cza/logintenantbranding/0/bannerlogo?ts=637227555210461681	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
152.199.23.72	cs1025.wpc.upsiloncdn.net	United States		15133	EDGECASTUS	false
68.65.123.205	maxcdn.bootstrapcdn.cloud	United States		22612	NAMECHEAP-NETUS	false
162.19.88.68	i.postimg.cc	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	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
18.172.153.55	d26p066pn2w0s0.cloudfront.net	United States		3	MIT-GATEWAYSUS	false
172.217.168.68	www.google.com	United States		15169	GOOGLEUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved	?	unknown	unknown	false
188.114.96.3	descansonline.com	European Union	?	13335	CLOUDFLARENETUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.188.128	maxcdn.bootstrapcdn.rest	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756202
Start date and time:	2022-11-29 19:58:14 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 42s
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@27/0@16/13
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.azureedge.net, aadcdn.ec.azureedge.net, update.googleapis.com, clientservices.googleapis.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	HTML document, ASCII text, with CRLF line terminators
Entropy (8bit):	5.340590656103303
TrID:	• HTML Application (8008/1) 100.00%
File name:	November Draw Disbursed.html
File size:	444
MD5:	c0d6d8acc86ed388214581788ec837d8
SHA1:	c846ee109e9ee8e373ff09412a59e3aeec06fd44
SHA256:	2209177e77a2dabd0c034500ee64ccca71d8985c7c564ce31898ca2326bb6d78
SHA512:	0ffdc4579cb9b2edee23f3a9fd5da4062a0285586c5395e2de19708b71024c6a3741397a5a10aa055d56d1e6a2c2b8e032f2e9584a8dbf554ce25c9242ca0279
SSDEEP:	12:7KPA2JZoH3TuBVKHuHAHYoHcl4DMEGVdDVRxb:7CAuZoXKBcQAHYo8lstaxb
TLSH:	C8F05C502C4C4A4005341E718078960DD01F492CDE8CC9C296D768562950FDE2ECA6C4
File Content Preview:	<script>.. var Tse0sed5 = "https://descansonline.com/wp/b1.php"; // php file link normal or B64.. var RTse0dsqqs = "wendy.lang@dmv.ca.gov"; //email normal or B64.. var e0zs52658 = "https://descansonline.com/wp/b1.js"; //js file link normal or B64..

File Icon

Icon Hash:	78d0a8cccc88c460

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.38.8.8.8556385 32027758 11/29/22-19:59:13.326192	UDP	2027758	ET DNS Query for .cc TLD	55638	53	192.168.2.3	8.8.8.8
192.168.2.38.8.8.8538485 32027758 11/29/22-19:59:15.999356	UDP	2027758	ET DNS Query for .cc TLD	53848	53	192.168.2.3	8.8.8.8

Network Port Distribution

Total Packets: 57

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 19:59:07.092547894 CET	49698	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:59:07.092595100 CET	443	49698	142.250.203.110	192.168.2.3
Nov 29, 2022 19:59:07.092681885 CET	49698	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:59:07.094491959 CET	49698	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:59:07.094507933 CET	443	49698	142.250.203.110	192.168.2.3
Nov 29, 2022 19:59:07.166402102 CET	443	49698	142.250.203.110	192.168.2.3
Nov 29, 2022 19:59:07.166858912 CET	49698	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:59:07.166901112 CET	443	49698	142.250.203.110	192.168.2.3
Nov 29, 2022 19:59:07.167536974 CET	443	49698	142.250.203.110	192.168.2.3
Nov 29, 2022 19:59:07.167625904 CET	49698	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:59:07.168848991 CET	443	49698	142.250.203.110	192.168.2.3
Nov 29, 2022 19:59:07.168930054 CET	49698	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:59:08.287462950 CET	49698	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:59:08.287523031 CET	443	49698	142.250.203.110	192.168.2.3
Nov 29, 2022 19:59:08.287798882 CET	443	49698	142.250.203.110	192.168.2.3
Nov 29, 2022 19:59:08.287830114 CET	49698	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:59:08.287846088 CET	443	49698	142.250.203.110	192.168.2.3
Nov 29, 2022 19:59:08.324126005 CET	443	49698	142.250.203.110	192.168.2.3
Nov 29, 2022 19:59:08.324261904 CET	49698	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:59:08.324322939 CET	443	49698	142.250.203.110	192.168.2.3
Nov 29, 2022 19:59:08.324359894 CET	443	49698	142.250.203.110	192.168.2.3
Nov 29, 2022 19:59:08.324426889 CET	49698	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:59:08.326643944 CET	49698	443	192.168.2.3	142.250.203.110
Nov 29, 2022 19:59:08.326693058 CET	443	49698	142.250.203.110	192.168.2.3
Nov 29, 2022 19:59:08.399707079 CET	49700	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:59:08.399802923 CET	443	49700	172.217.168.45	192.168.2.3
Nov 29, 2022 19:59:08.399893045 CET	49700	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:59:08.400326014 CET	49700	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:59:08.400360107 CET	443	49700	172.217.168.45	192.168.2.3
Nov 29, 2022 19:59:08.469950914 CET	443	49700	172.217.168.45	192.168.2.3
Nov 29, 2022 19:59:08.496452093 CET	49700	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:59:08.496521950 CET	443	49700	172.217.168.45	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 19:59:08.499883890 CET	443	49700	172.217.168.45	192.168.2.3
Nov 29, 2022 19:59:08.500020027 CET	49700	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:59:08.502785921 CET	49700	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:59:08.502815962 CET	443	49700	172.217.168.45	192.168.2.3
Nov 29, 2022 19:59:08.503006935 CET	443	49700	172.217.168.45	192.168.2.3
Nov 29, 2022 19:59:08.503032923 CET	49700	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:59:08.503046989 CET	443	49700	172.217.168.45	192.168.2.3
Nov 29, 2022 19:59:08.560476065 CET	443	49700	172.217.168.45	192.168.2.3
Nov 29, 2022 19:59:08.560601950 CET	49700	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:59:08.560652018 CET	443	49700	172.217.168.45	192.168.2.3
Nov 29, 2022 19:59:08.560854912 CET	443	49700	172.217.168.45	192.168.2.3
Nov 29, 2022 19:59:08.560923100 CET	49700	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:59:08.562552929 CET	49700	443	192.168.2.3	172.217.168.45
Nov 29, 2022 19:59:08.562591076 CET	443	49700	172.217.168.45	192.168.2.3
Nov 29, 2022 19:59:10.500958920 CET	49701	443	192.168.2.3	188.114.96.3
Nov 29, 2022 19:59:10.501024008 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.501147985 CET	49701	443	192.168.2.3	188.114.96.3
Nov 29, 2022 19:59:10.502063036 CET	49701	443	192.168.2.3	188.114.96.3
Nov 29, 2022 19:59:10.502099037 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.602175951 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.705908060 CET	49701	443	192.168.2.3	188.114.96.3
Nov 29, 2022 19:59:10.788549900 CET	49701	443	192.168.2.3	188.114.96.3
Nov 29, 2022 19:59:10.788599968 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.792459011 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.792560101 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.792576075 CET	49701	443	192.168.2.3	188.114.96.3
Nov 29, 2022 19:59:10.795406103 CET	49701	443	192.168.2.3	188.114.96.3
Nov 29, 2022 19:59:10.795454979 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.795700073 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.795718908 CET	49701	443	192.168.2.3	188.114.96.3
Nov 29, 2022 19:59:10.795739889 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.840694904 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.840900898 CET	49701	443	192.168.2.3	188.114.96.3
Nov 29, 2022 19:59:10.840935946 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.841027021 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.841114998 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.841135979 CET	49701	443	192.168.2.3	188.114.96.3
Nov 29, 2022 19:59:10.841164112 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.841223955 CET	49701	443	192.168.2.3	188.114.96.3
Nov 29, 2022 19:59:10.841255903 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.841402054 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.841486931 CET	49701	443	192.168.2.3	188.114.96.3
Nov 29, 2022 19:59:10.841532946 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.841893911 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.842000008 CET	49701	443	192.168.2.3	188.114.96.3
Nov 29, 2022 19:59:10.842005014 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.842065096 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.842122078 CET	49701	443	192.168.2.3	188.114.96.3
Nov 29, 2022 19:59:10.842139959 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.842787981 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.842866898 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.842880964 CET	49701	443	192.168.2.3	188.114.96.3
Nov 29, 2022 19:59:10.842916965 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.843008041 CET	49701	443	192.168.2.3	188.114.96.3
Nov 29, 2022 19:59:10.843671083 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.843848944 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.843925953 CET	49701	443	192.168.2.3	188.114.96.3
Nov 29, 2022 19:59:10.843928099 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.843950987 CET	443	49701	188.114.96.3	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 19:59:10.843998909 CET	49701	443	192.168.2.3	188.114.96.3
Nov 29, 2022 19:59:10.844558954 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.844710112 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.844772100 CET	49701	443	192.168.2.3	188.114.96.3
Nov 29, 2022 19:59:10.844784021 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.845551014 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.845628023 CET	443	49701	188.114.96.3	192.168.2.3
Nov 29, 2022 19:59:10.845634937 CET	49701	443	192.168.2.3	188.114.96.3
Nov 29, 2022 19:59:10.845654964 CET	443	49701	188.114.96.3	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 19:59:07.068732023 CET	57840	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:59:07.086155891 CET	53	57840	8.8.8.8	192.168.2.3
Nov 29, 2022 19:59:07.472232103 CET	57990	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:59:07.510745049 CET	53	57990	8.8.8.8	192.168.2.3
Nov 29, 2022 19:59:09.219088078 CET	60625	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:59:09.243546963 CET	53	60625	8.8.8.8	192.168.2.3
Nov 29, 2022 19:59:11.034914970 CET	52955	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:59:11.042839050 CET	60582	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:59:11.043695927 CET	57134	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:59:11.044045925 CET	62050	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:59:11.055634022 CET	53	52955	8.8.8.8	192.168.2.3
Nov 29, 2022 19:59:11.066426992 CET	53	57134	8.8.8.8	192.168.2.3
Nov 29, 2022 19:59:11.132739067 CET	56042	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:59:11.150424957 CET	53	56042	8.8.8.8	192.168.2.3
Nov 29, 2022 19:59:11.320646048 CET	53	60582	8.8.8.8	192.168.2.3
Nov 29, 2022 19:59:11.330082893 CET	53	62050	8.8.8.8	192.168.2.3
Nov 29, 2022 19:59:13.326191902 CET	55638	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:59:13.357458115 CET	53	55638	8.8.8.8	192.168.2.3
Nov 29, 2022 19:59:15.999356031 CET	53848	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:59:16.032098055 CET	53	53848	8.8.8.8	192.168.2.3
Nov 29, 2022 19:59:17.737325907 CET	58691	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:59:17.738293886 CET	53305	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:59:17.759807110 CET	53	58691	8.8.8.8	192.168.2.3
Nov 29, 2022 19:59:27.923060894 CET	65017	53	192.168.2.3	8.8.8.8
Nov 29, 2022 19:59:27.943217039 CET	53	65017	8.8.8.8	192.168.2.3
Nov 29, 2022 20:00:11.191204071 CET	64967	53	192.168.2.3	8.8.8.8
Nov 29, 2022 20:00:11.205492973 CET	60825	53	192.168.2.3	8.8.8.8
Nov 29, 2022 20:00:11.208045006 CET	53	64967	8.8.8.8	192.168.2.3
Nov 29, 2022 20:00:11.226298094 CET	53	60825	8.8.8.8	192.168.2.3
Nov 29, 2022 20:01:11.264585972 CET	59374	53	192.168.2.3	8.8.8.8
Nov 29, 2022 20:01:11.283909082 CET	53	59374	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 19:59:07.068732023 CET	192.168.2.3	8.8.8.8	0xbc6c	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:07.472232103 CET	192.168.2.3	8.8.8.8	0x6bdc	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:09.219088078 CET	192.168.2.3	8.8.8.8	0xea	Standard query (0)	descansonline.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:11.034914970 CET	192.168.2.3	8.8.8.8	0xffa0	Standard query (0)	maxcdn.bootstrapcdn.cloud	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:11.042839050 CET	192.168.2.3	8.8.8.8	0x2e03	Standard query (0)	code.jquery.com.de	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:11.043695927 CET	192.168.2.3	8.8.8.8	0xbb67	Standard query (0)	maxcdn.bootstrapcdn.rest	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 19:59:11.044045925 CET	192.168.2.3	8.8.8.8	0x773f	Standard query (0)	code.jquery.quest	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:11.132739067 CET	192.168.2.3	8.8.8.8	0xc87e	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:13.326191902 CET	192.168.2.3	8.8.8.8	0x5c60	Standard query (0)	i.postimg.cc	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:15.999356031 CET	192.168.2.3	8.8.8.8	0xf708	Standard query (0)	i.postimg.cc	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:17.737325907 CET	192.168.2.3	8.8.8.8	0x63d9	Standard query (0)	logo.clearbit.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:17.738293886 CET	192.168.2.3	8.8.8.8	0x7d23	Standard query (0)	aadcdn.msauthimages.net	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:27.923060894 CET	192.168.2.3	8.8.8.8	0xe01a	Standard query (0)	logo.clearbit.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:00:11.191204071 CET	192.168.2.3	8.8.8.8	0x9160	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:00:11.205492973 CET	192.168.2.3	8.8.8.8	0x6e69	Standard query (0)	maxcdn.bootstrapcdn.cloud	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:01:11.264585972 CET	192.168.2.3	8.8.8.8	0x628b	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 19:59:07.086155891 CET	8.8.8.8	192.168.2.3	0xbc6c	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 19:59:07.086155891 CET	8.8.8.8	192.168.2.3	0xbc6c	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:07.510745049 CET	8.8.8.8	192.168.2.3	0x6bdc	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:09.243546963 CET	8.8.8.8	192.168.2.3	0xea	No error (0)	descansonline.com		188.114.96.3	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:09.243546963 CET	8.8.8.8	192.168.2.3	0xea	No error (0)	descansonline.com		188.114.97.3	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:11.055634022 CET	8.8.8.8	192.168.2.3	0xffa0	No error (0)	maxcdn.bootstrapcdn.cloud		68.65.123.205	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:11.066426992 CET	8.8.8.8	192.168.2.3	0xbb67	No error (0)	maxcdn.bootstrapcdn.rest		172.67.188.128	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:11.066426992 CET	8.8.8.8	192.168.2.3	0xbb67	No error (0)	maxcdn.bootstrapcdn.rest		104.21.40.223	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:11.150424957 CET	8.8.8.8	192.168.2.3	0xc87e	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:11.320646048 CET	8.8.8.8	192.168.2.3	0x2e03	No error (0)	code.jquery.com.de		38.34.185.163	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:11.330082893 CET	8.8.8.8	192.168.2.3	0x773f	No error (0)	code.jquery.quest		38.34.185.163	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:13.357458115 CET	8.8.8.8	192.168.2.3	0x5c60	No error (0)	i.postimg.cc		162.19.88.68	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:13.357458115 CET	8.8.8.8	192.168.2.3	0x5c60	No error (0)	i.postimg.cc		162.19.88.69	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:16.032098055 CET	8.8.8.8	192.168.2.3	0xf708	No error (0)	i.postimg.cc		162.19.88.68	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:16.032098055 CET	8.8.8.8	192.168.2.3	0xf708	No error (0)	i.postimg.cc		162.19.88.69	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:17.759807110 CET	8.8.8.8	192.168.2.3	0x63d9	No error (0)	logo.clearbit.com	d26p066pn2w0s0.cloudfront.net		CNAME (Canonical name)	IN (0x0001)	false

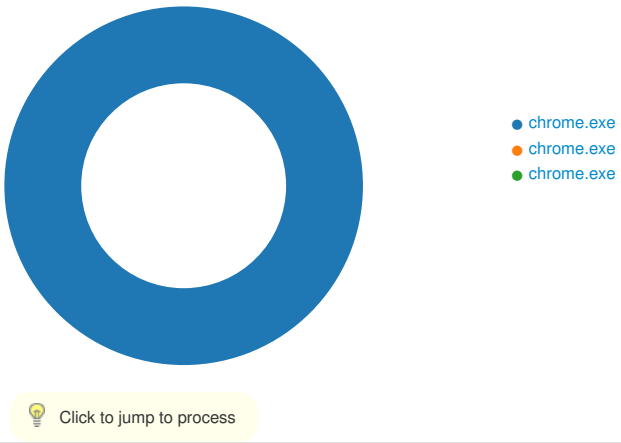
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 19:59:17.759807110 CET	8.8.8.8	192.168.2.3	0x63d9	No error (0)	d26p066pn2w0s0.cloudfront.net		18.172.153.55	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:17.759807110 CET	8.8.8.8	192.168.2.3	0x63d9	No error (0)	d26p066pn2w0s0.cloudfront.net		18.172.153.44	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:17.759807110 CET	8.8.8.8	192.168.2.3	0x63d9	No error (0)	d26p066pn2w0s0.cloudfront.net		18.172.153.108	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:17.759807110 CET	8.8.8.8	192.168.2.3	0x63d9	No error (0)	d26p066pn2w0s0.cloudfront.net		18.172.153.7	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:17.760951042 CET	8.8.8.8	192.168.2.3	0x7d23	No error (0)	aadcdn.msauthimages.net	aadcdn.azureedge.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 19:59:17.760951042 CET	8.8.8.8	192.168.2.3	0x7d23	No error (0)	cs1025.wpc.upsiloncdn.net		152.199.23.72	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:27.943217039 CET	8.8.8.8	192.168.2.3	0xe01a	No error (0)	logo.clearbit.com	d26p066pn2w0s0.cloudfront.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 19:59:27.943217039 CET	8.8.8.8	192.168.2.3	0xe01a	No error (0)	d26p066pn2w0s0.cloudfront.net		18.172.153.55	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:27.943217039 CET	8.8.8.8	192.168.2.3	0xe01a	No error (0)	d26p066pn2w0s0.cloudfront.net		18.172.153.44	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:27.943217039 CET	8.8.8.8	192.168.2.3	0xe01a	No error (0)	d26p066pn2w0s0.cloudfront.net		18.172.153.108	A (IP address)	IN (0x0001)	false
Nov 29, 2022 19:59:27.943217039 CET	8.8.8.8	192.168.2.3	0xe01a	No error (0)	d26p066pn2w0s0.cloudfront.net		18.172.153.7	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:00:11.208045006 CET	8.8.8.8	192.168.2.3	0x9160	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:00:11.226298094 CET	8.8.8.8	192.168.2.3	0x6e69	No error (0)	maxcdn.bootstrapcdn.cloud		68.65.123.205	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:01:11.283909082 CET	8.8.8.8	192.168.2.3	0x628b	No error (0)	www.google.com		172.217.168.68	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.quest
- code.jquery.com.de
- i.postimg.cc
- logo.clearbit.com
- aadcdn.msauthimages.net

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 5928, Parent PID: 3332

General

Target ID:	0
Start time:	19:59:04
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: 1844, Parent PID: 5928

General

Target ID:	1

Start time:	19:59:05
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=1968 --field-trial-handle=1856,i,16127261416295333797,16450193774645569565,131072 --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: **5328**, Parent PID: **3332**

General

Target ID:	2
Start time:	19:59:06
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