ID: 736952
Cookbook: browseurl.jbs
Time: 12:24:48
Date: 03/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

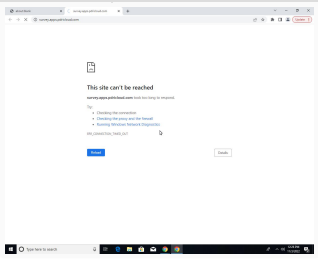
Windows Analysis Report

http://survey.apps.pdricloud.com

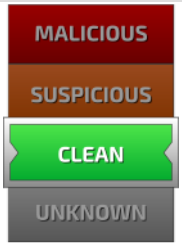
Overview

General Information

Sample URL:	http://survey.apps.pdricloud.com
Analysis ID:	736952
Infos:	



Detection

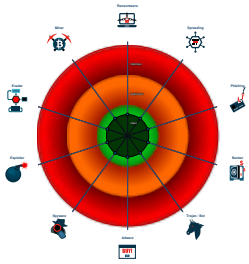


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 1796 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 2880 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=1952 --field-trial-handle=1724,i,4850779736149216259,13576850689647810483,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 5984 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "http://survey.apps.pdricloud.com MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

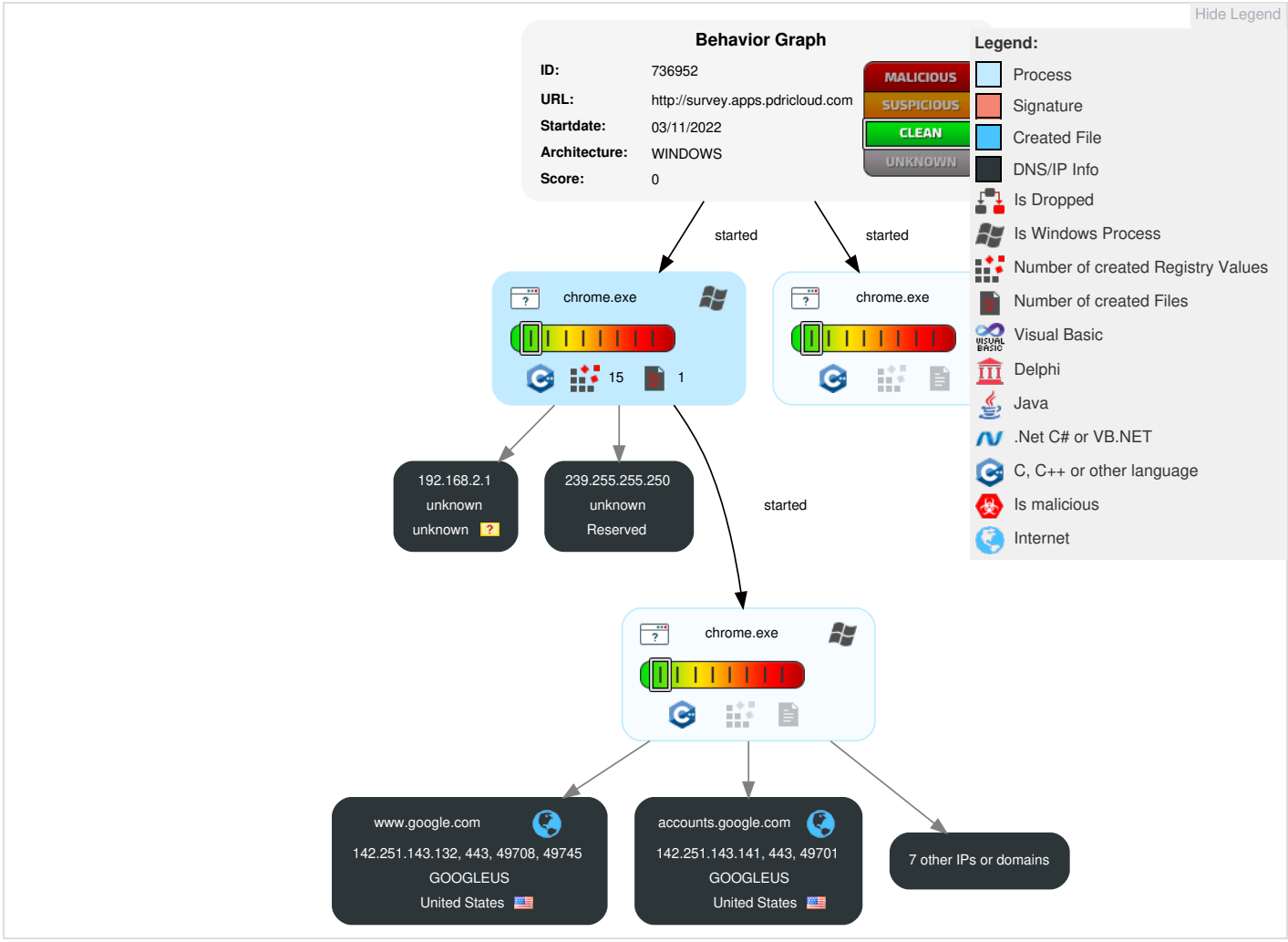
Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	2 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	4 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

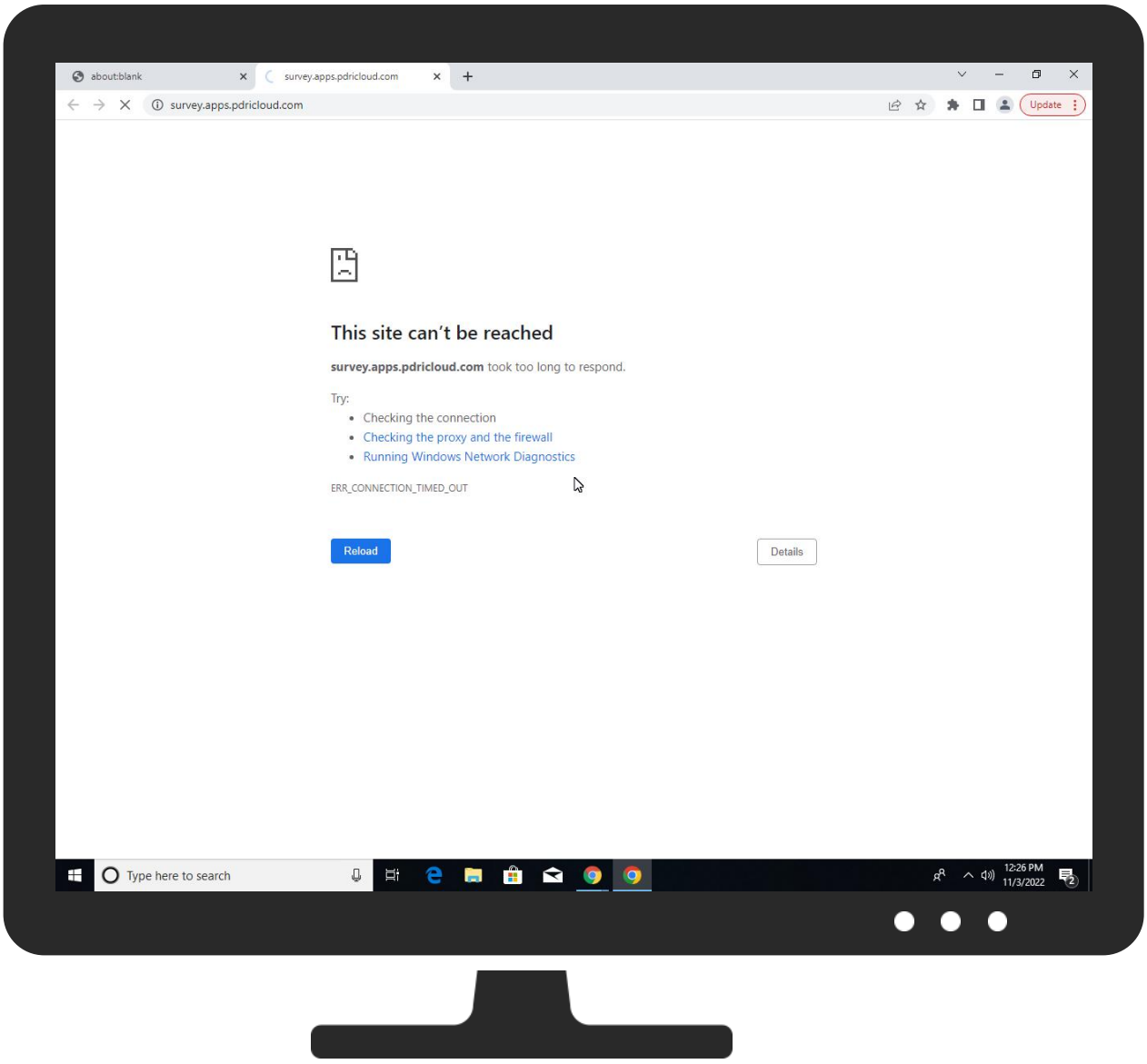
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://survey.apps.pdricloud.com	0%	Virustotal		Browse
http://survey.apps.pdricloud.com	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

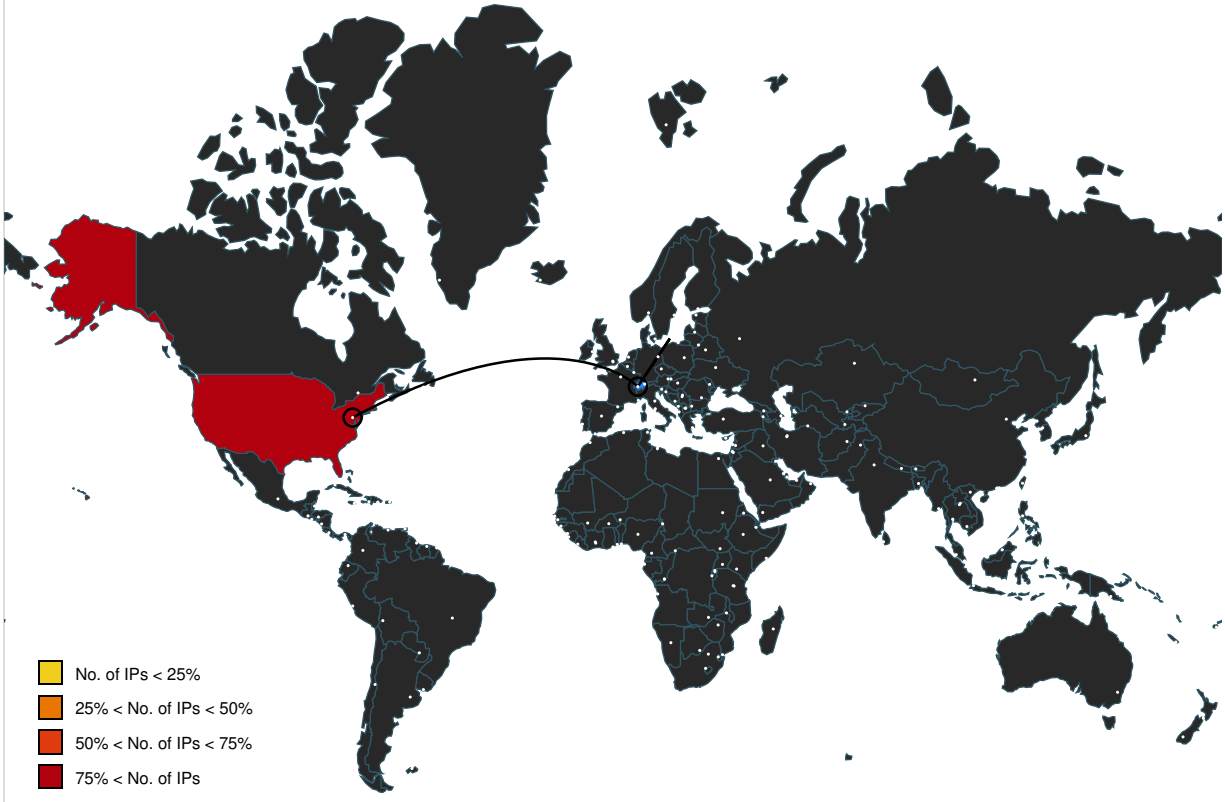
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.251.143.141	true	false		high
www.google.com	142.251.143.132	true	false		high
clients.l.google.com	142.251.143.174	true	false		high
prod-app-964824229.us-east-1.elb.amazonaws.com	54.173.73.112	true	false		high
clients2.google.com	unknown	unknown	false		high
survey.apps.pdricloud.com	unknown	unknown	false		unknown

Contacted URLs

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://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
239.255.255.250	unknown	Reserved	?	unknown	unknown	false
54.173.73.112	prod-app-964824229.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
52.72.68.102	unknown	United States		14618	AMAZON-AESUS	false
142.251.143.132	www.google.com	United States		15169	GOOGLEUS	false
142.251.143.141	accounts.google.com	United States		15169	GOOGLEUS	false
142.251.143.174	clients.l.google.com	United States		15169	GOOGLEUS	false
54.196.226.234	unknown	United States		14618	AMAZON-AESUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	736952
Start date and time:	2022-11-03 12:24:48 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://survey.apps.pdricloud.com
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:	5
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:	CLEAN
Classification:	clean0.win@27/0@5/9
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.251.143.163, 34.104.35.123
- Excluded domains from analysis (whitelisted): edgedl.me.gvt1.com, update.googleapis.com, ctldl.windowsupdate.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

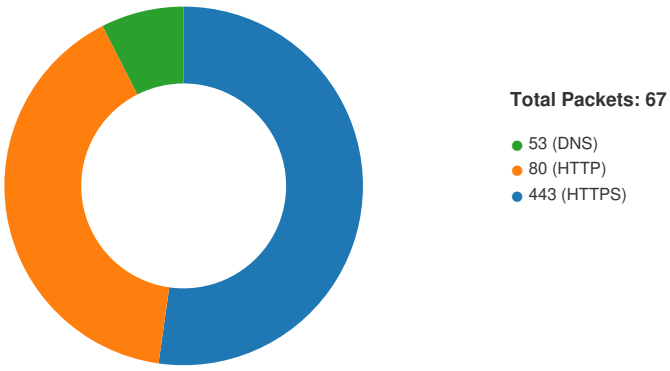
No created / dropped files found

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:25:48.802701950 CET	49701	443	192.168.2.5	142.251.143.141
Nov 3, 2022 12:25:48.802755117 CET	443	49701	142.251.143.141	192.168.2.5
Nov 3, 2022 12:25:48.802844048 CET	49701	443	192.168.2.5	142.251.143.141
Nov 3, 2022 12:25:48.803380013 CET	49702	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:25:48.803431988 CET	443	49702	142.251.143.174	192.168.2.5
Nov 3, 2022 12:25:48.803505898 CET	49702	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:25:48.803925037 CET	49703	80	192.168.2.5	54.173.73.112

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:25:48.805438042 CET	49701	443	192.168.2.5	142.251.143.141
Nov 3, 2022 12:25:48.805475950 CET	443	49701	142.251.143.141	192.168.2.5
Nov 3, 2022 12:25:48.805727005 CET	49702	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:25:48.805757046 CET	443	49702	142.251.143.174	192.168.2.5
Nov 3, 2022 12:25:48.844378948 CET	49704	80	192.168.2.5	54.173.73.112
Nov 3, 2022 12:25:48.898370981 CET	443	49701	142.251.143.141	192.168.2.5
Nov 3, 2022 12:25:48.899574995 CET	49701	443	192.168.2.5	142.251.143.141
Nov 3, 2022 12:25:48.899631977 CET	443	49701	142.251.143.141	192.168.2.5
Nov 3, 2022 12:25:48.901560068 CET	443	49702	142.251.143.174	192.168.2.5
Nov 3, 2022 12:25:48.905193090 CET	443	49701	142.251.143.141	192.168.2.5
Nov 3, 2022 12:25:48.905323029 CET	49701	443	192.168.2.5	142.251.143.141
Nov 3, 2022 12:25:48.907047033 CET	49702	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:25:48.907084942 CET	443	49702	142.251.143.174	192.168.2.5
Nov 3, 2022 12:25:48.908086061 CET	443	49702	142.251.143.174	192.168.2.5
Nov 3, 2022 12:25:48.908185005 CET	49702	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:25:48.909775972 CET	443	49702	142.251.143.174	192.168.2.5
Nov 3, 2022 12:25:48.909842968 CET	49702	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:25:49.074856043 CET	49706	80	192.168.2.5	54.173.73.112
Nov 3, 2022 12:25:49.075782061 CET	49708	443	192.168.2.5	142.251.143.132
Nov 3, 2022 12:25:49.075880051 CET	443	49708	142.251.143.132	192.168.2.5
Nov 3, 2022 12:25:49.075968027 CET	49708	443	192.168.2.5	142.251.143.132
Nov 3, 2022 12:25:49.077219009 CET	49708	443	192.168.2.5	142.251.143.132
Nov 3, 2022 12:25:49.077241898 CET	443	49708	142.251.143.132	192.168.2.5
Nov 3, 2022 12:25:49.181154966 CET	443	49708	142.251.143.132	192.168.2.5
Nov 3, 2022 12:25:49.203989983 CET	49708	443	192.168.2.5	142.251.143.132
Nov 3, 2022 12:25:49.204034090 CET	443	49708	142.251.143.132	192.168.2.5
Nov 3, 2022 12:25:49.206408978 CET	443	49708	142.251.143.132	192.168.2.5
Nov 3, 2022 12:25:49.206577063 CET	49708	443	192.168.2.5	142.251.143.132
Nov 3, 2022 12:25:49.371680021 CET	49702	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:25:49.371748924 CET	443	49702	142.251.143.174	192.168.2.5
Nov 3, 2022 12:25:49.372133970 CET	49702	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:25:49.372145891 CET	443	49702	142.251.143.174	192.168.2.5
Nov 3, 2022 12:25:49.372394085 CET	49708	443	192.168.2.5	142.251.143.132
Nov 3, 2022 12:25:49.372456074 CET	443	49708	142.251.143.132	192.168.2.5
Nov 3, 2022 12:25:49.372601032 CET	443	49702	142.251.143.174	192.168.2.5
Nov 3, 2022 12:25:49.372708082 CET	443	49708	142.251.143.132	192.168.2.5
Nov 3, 2022 12:25:49.373692989 CET	49701	443	192.168.2.5	142.251.143.141
Nov 3, 2022 12:25:49.373733997 CET	443	49701	142.251.143.141	192.168.2.5
Nov 3, 2022 12:25:49.373862982 CET	443	49701	142.251.143.141	192.168.2.5
Nov 3, 2022 12:25:49.374790907 CET	49701	443	192.168.2.5	142.251.143.141
Nov 3, 2022 12:25:49.374839067 CET	443	49701	142.251.143.141	192.168.2.5
Nov 3, 2022 12:25:49.428797007 CET	443	49702	142.251.143.174	192.168.2.5
Nov 3, 2022 12:25:49.428985119 CET	49702	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:25:49.429013014 CET	443	49702	142.251.143.174	192.168.2.5
Nov 3, 2022 12:25:49.429891109 CET	443	49702	142.251.143.174	192.168.2.5
Nov 3, 2022 12:25:49.430006981 CET	49702	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:25:49.435445070 CET	49702	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:25:49.435475111 CET	443	49702	142.251.143.174	192.168.2.5
Nov 3, 2022 12:25:49.443157911 CET	443	49701	142.251.143.141	192.168.2.5
Nov 3, 2022 12:25:49.443341017 CET	49701	443	192.168.2.5	142.251.143.141
Nov 3, 2022 12:25:49.443344116 CET	443	49701	142.251.143.141	192.168.2.5
Nov 3, 2022 12:25:49.443411112 CET	49701	443	192.168.2.5	142.251.143.141
Nov 3, 2022 12:25:49.470700026 CET	49701	443	192.168.2.5	142.251.143.141
Nov 3, 2022 12:25:49.470757008 CET	443	49701	142.251.143.141	192.168.2.5
Nov 3, 2022 12:25:49.485311985 CET	49708	443	192.168.2.5	142.251.143.132
Nov 3, 2022 12:25:49.485356092 CET	443	49708	142.251.143.132	192.168.2.5
Nov 3, 2022 12:25:49.585659981 CET	49708	443	192.168.2.5	142.251.143.132
Nov 3, 2022 12:25:51.878565073 CET	49703	80	192.168.2.5	54.173.73.112
Nov 3, 2022 12:25:51.879978895 CET	49704	80	192.168.2.5	54.173.73.112

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:25:52.085540056 CET	49706	80	192.168.2.5	54.173.73.112
Nov 3, 2022 12:25:57.879961014 CET	49703	80	192.168.2.5	54.173.73.112
Nov 3, 2022 12:25:57.879981041 CET	49704	80	192.168.2.5	54.173.73.112
Nov 3, 2022 12:25:58.085958004 CET	49706	80	192.168.2.5	54.173.73.112
Nov 3, 2022 12:25:59.149203062 CET	443	49708	142.251.143.132	192.168.2.5
Nov 3, 2022 12:25:59.149300098 CET	443	49708	142.251.143.132	192.168.2.5
Nov 3, 2022 12:25:59.149430037 CET	49708	443	192.168.2.5	142.251.143.132
Nov 3, 2022 12:26:02.964536905 CET	49708	443	192.168.2.5	142.251.143.132
Nov 3, 2022 12:26:02.964579105 CET	443	49708	142.251.143.132	192.168.2.5
Nov 3, 2022 12:26:10.074806929 CET	49724	80	192.168.2.5	52.72.68.102
Nov 3, 2022 12:26:10.075242043 CET	49725	80	192.168.2.5	52.72.68.102
Nov 3, 2022 12:26:10.188272953 CET	49726	80	192.168.2.5	52.72.68.102
Nov 3, 2022 12:26:13.087141037 CET	49724	80	192.168.2.5	52.72.68.102
Nov 3, 2022 12:26:13.089790106 CET	49725	80	192.168.2.5	52.72.68.102
Nov 3, 2022 12:26:13.381136894 CET	49726	80	192.168.2.5	52.72.68.102
Nov 3, 2022 12:26:19.087588072 CET	49724	80	192.168.2.5	52.72.68.102
Nov 3, 2022 12:26:19.091315985 CET	49725	80	192.168.2.5	52.72.68.102
Nov 3, 2022 12:26:19.474607944 CET	49726	80	192.168.2.5	52.72.68.102
Nov 3, 2022 12:26:31.089457035 CET	49739	80	192.168.2.5	54.196.226.234
Nov 3, 2022 12:26:31.089732885 CET	49740	80	192.168.2.5	54.196.226.234
Nov 3, 2022 12:26:31.588469982 CET	49741	80	192.168.2.5	54.196.226.234
Nov 3, 2022 12:26:34.276499033 CET	49739	80	192.168.2.5	54.196.226.234
Nov 3, 2022 12:26:34.276540995 CET	49740	80	192.168.2.5	54.196.226.234
Nov 3, 2022 12:26:34.679806948 CET	49741	80	192.168.2.5	54.196.226.234
Nov 3, 2022 12:26:40.339196920 CET	49739	80	192.168.2.5	54.196.226.234
Nov 3, 2022 12:26:40.339270115 CET	49740	80	192.168.2.5	54.196.226.234
Nov 3, 2022 12:26:40.739217997 CET	49741	80	192.168.2.5	54.196.226.234
Nov 3, 2022 12:26:48.876180887 CET	49745	443	192.168.2.5	142.251.143.132
Nov 3, 2022 12:26:48.876341105 CET	443	49745	142.251.143.132	192.168.2.5
Nov 3, 2022 12:26:48.876657009 CET	49745	443	192.168.2.5	142.251.143.132
Nov 3, 2022 12:26:48.909447908 CET	49745	443	192.168.2.5	142.251.143.132
Nov 3, 2022 12:26:48.909512997 CET	443	49745	142.251.143.132	192.168.2.5
Nov 3, 2022 12:26:49.001848936 CET	443	49745	142.251.143.132	192.168.2.5
Nov 3, 2022 12:26:49.044893026 CET	49745	443	192.168.2.5	142.251.143.132

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:25:48.138623953 CET	51441	53	192.168.2.5	8.8.8.8
Nov 3, 2022 12:25:48.140582085 CET	49177	53	192.168.2.5	8.8.8.8
Nov 3, 2022 12:25:48.156235933 CET	53	51441	8.8.8.8	192.168.2.5
Nov 3, 2022 12:25:48.163027048 CET	53	49177	8.8.8.8	192.168.2.5
Nov 3, 2022 12:25:48.737209082 CET	61452	53	192.168.2.5	8.8.8.8
Nov 3, 2022 12:25:48.771136999 CET	53	61452	8.8.8.8	192.168.2.5
Nov 3, 2022 12:25:48.895803928 CET	65323	53	192.168.2.5	8.8.8.8
Nov 3, 2022 12:25:48.916290045 CET	53	65323	8.8.8.8	192.168.2.5
Nov 3, 2022 12:26:53.776024103 CET	60284	53	192.168.2.5	8.8.8.8
Nov 3, 2022 12:26:53.801664114 CET	53	60284	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 3, 2022 12:25:48.138623953 CET	192.168.2.5	8.8.8.8	0x9bc3	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:25:48.140582085 CET	192.168.2.5	8.8.8.8	0x2159	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:25:48.737209082 CET	192.168.2.5	8.8.8.8	0x2bbe	Standard query (0)	survey.apps.pdricloud.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:25:48.895803928 CET	192.168.2.5	8.8.8.8	0xa9e4	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 3, 2022 12:26:53.776024103 CET	192.168.2.5	8.8.8.8	0xbbc9	Standard query (0)	survey.apps.pdricloud.com	A (IP address)	IN (0x0001)	false

DNS Answers

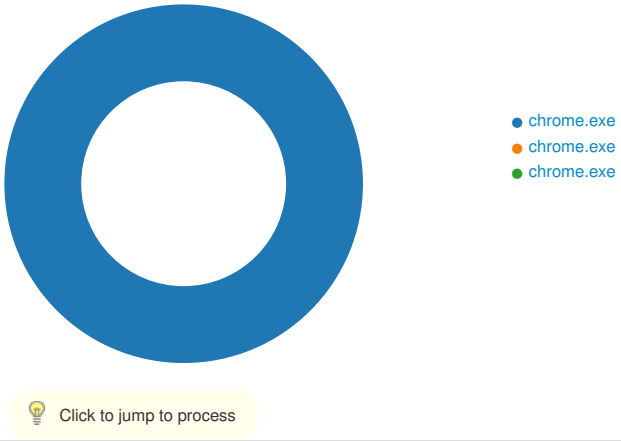
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 3, 2022 12:25:48.156235933 CET	8.8.8.8	192.168.2.5	0x9bc3	No error (0)	accounts.google.com		142.251.143.141	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:25:48.163027048 CET	8.8.8.8	192.168.2.5	0x2159	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 3, 2022 12:25:48.163027048 CET	8.8.8.8	192.168.2.5	0x2159	No error (0)	clients.l.google.com		142.251.143.174	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:25:48.771136999 CET	8.8.8.8	192.168.2.5	0x2bbe	No error (0)	survey.apps.pdricloud.com	prod-app-964824229.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 3, 2022 12:25:48.771136999 CET	8.8.8.8	192.168.2.5	0x2bbe	No error (0)	prod-app-964824229.us-east-1.elb.amazonaws.com		54.173.73.112	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:25:48.771136999 CET	8.8.8.8	192.168.2.5	0x2bbe	No error (0)	prod-app-964824229.us-east-1.elb.amazonaws.com		52.72.68.102	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:25:48.771136999 CET	8.8.8.8	192.168.2.5	0x2bbe	No error (0)	prod-app-964824229.us-east-1.elb.amazonaws.com		54.196.226.234	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:25:48.916290045 CET	8.8.8.8	192.168.2.5	0xa9e4	No error (0)	www.google.com		142.251.143.132	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:26:53.801664114 CET	8.8.8.8	192.168.2.5	0xbbc9	No error (0)	survey.apps.pdricloud.com	prod-app-964824229.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 3, 2022 12:26:53.801664114 CET	8.8.8.8	192.168.2.5	0xbbc9	No error (0)	prod-app-964824229.us-east-1.elb.amazonaws.com		52.72.68.102	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:26:53.801664114 CET	8.8.8.8	192.168.2.5	0xbbc9	No error (0)	prod-app-964824229.us-east-1.elb.amazonaws.com		54.173.73.112	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:26:53.801664114 CET	8.8.8.8	192.168.2.5	0xbbc9	No error (0)	prod-app-964824229.us-east-1.elb.amazonaws.com		54.196.226.234	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **1796**, Parent PID: **2260**

General

Target ID:	0
Start time:	12:25:42
Start date:	03/11/2022
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:	0x7ff7d31b0000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: chrome.exe PID: **2880**, Parent PID: **1796**

General

Target ID:	1
Start time:	12:25:43
Start date:	03/11/2022
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=1952 --field-trial-handle=1724,i,4850779736149216259,13576850689647810483,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff7d31b0000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

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

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **5984**, Parent PID: **2260**

General

Target ID:	2
Start time:	12:25:44
Start date:	03/11/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "http://survey.apps.pdricloud.com
Imagebase:	0x7ff7d31b0000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Registry Activities

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

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

Disassembly

No disassembly