ID: 877003
Cookbook: browseurl.jbs
Time: 10:55:58
Date: 28/05/2023
Version: 37.1.0 Beryl

Table of Contents

Table of Contents 2
Windows Analysis Report https://ipg.vendorreg.com/Default.asp. 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Signatures 3
Sigma Signatures 3
Snort Signatures 4
Joe Sandbox Signatures 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
Contacted URLs 7
World Map of Contacted IPs 7
Public IPs 7
Private 8
General Information 8
Warnings 8
Simulations 8
Behavior and APIs 8
Joe Sandbox View / Context 8
IPs 9
Domains 9
ASNs 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Chrome Cache Entry: 101 9
Chrome Cache Entry: 102 9
Static File Info 10
Network Behavior 10
Network Port Distribution 10
TCP Packets 10
UDP Packets 12
DNS Queries 12
DNS Answers 12
HTTP Request Dependency Graph 13
Statistics 13
Behavior 13
System Behavior 13
Analysis Process: chrome.exePID: 6140, Parent PID: 2108 13
General 13
File Activities 14
Analysis Process: chrome.exePID: 5984, Parent PID: 6140 14
General 14
File Activities 14
Analysis Process: chrome.exePID: 6340, Parent PID: 2108 14
General 14
Disassembly 15

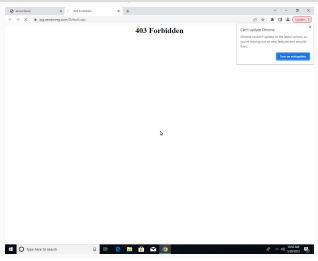
Windows Analysis Report

https://ipg.vendorreg.com/Default.asp.

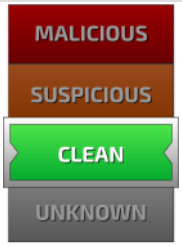
Overview

General Information

Sample URL:	http://https://ipg.vendorreg.com/Default.asp.
Analysis ID:	877003
Infos:	



Detection

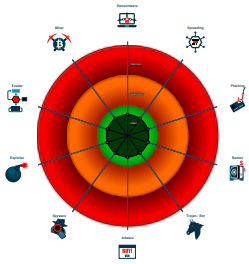


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64
- chrome.exe (PID: 6140 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 5984 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=1612 --field-trial-handle=1760,i,16128215241196653397,1351737748157124362,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 6340 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://ipg.vendorreg.com/Default.asp. 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

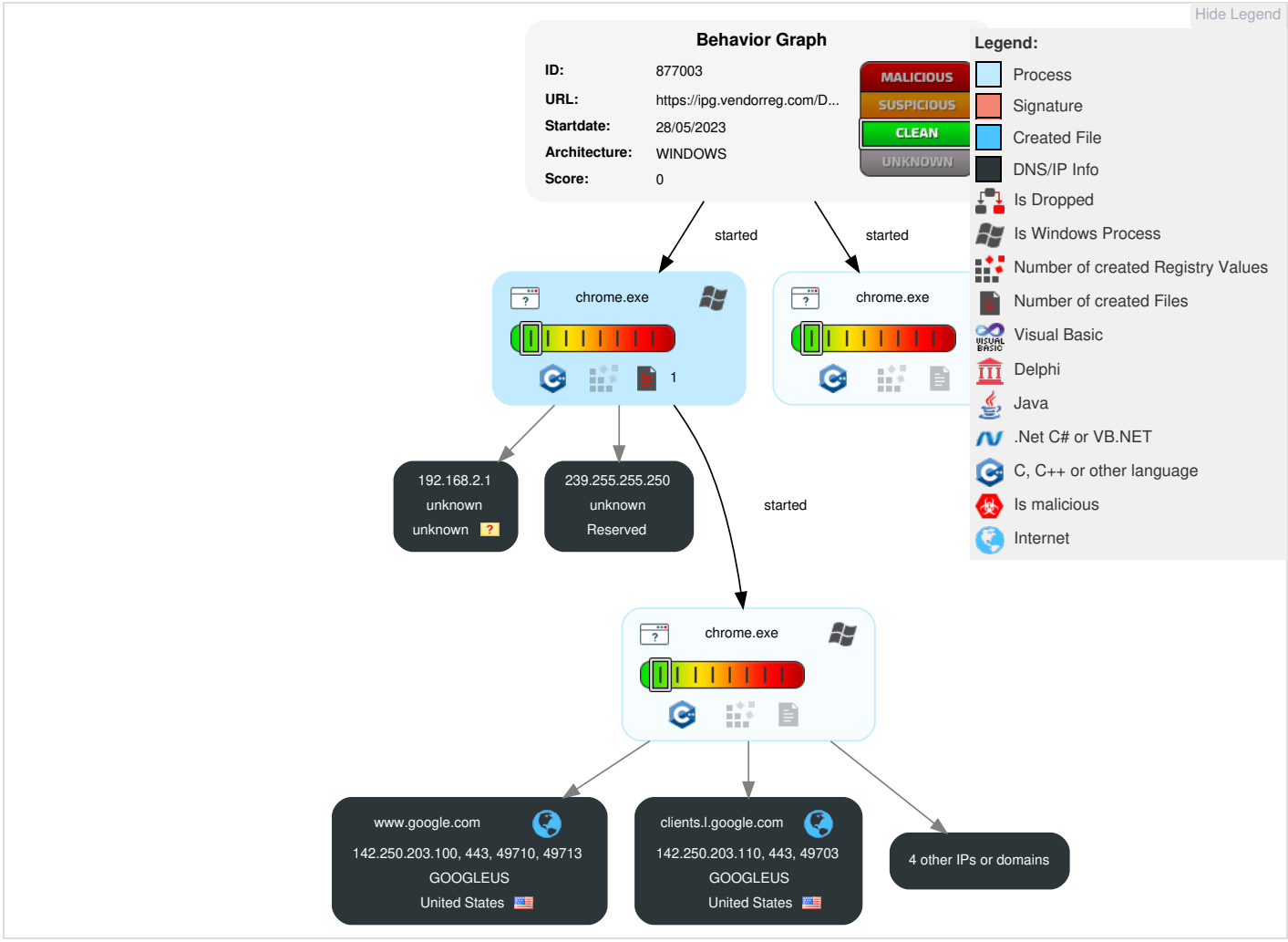
Joe Sandbox Signatures

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	4 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	5 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	3 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

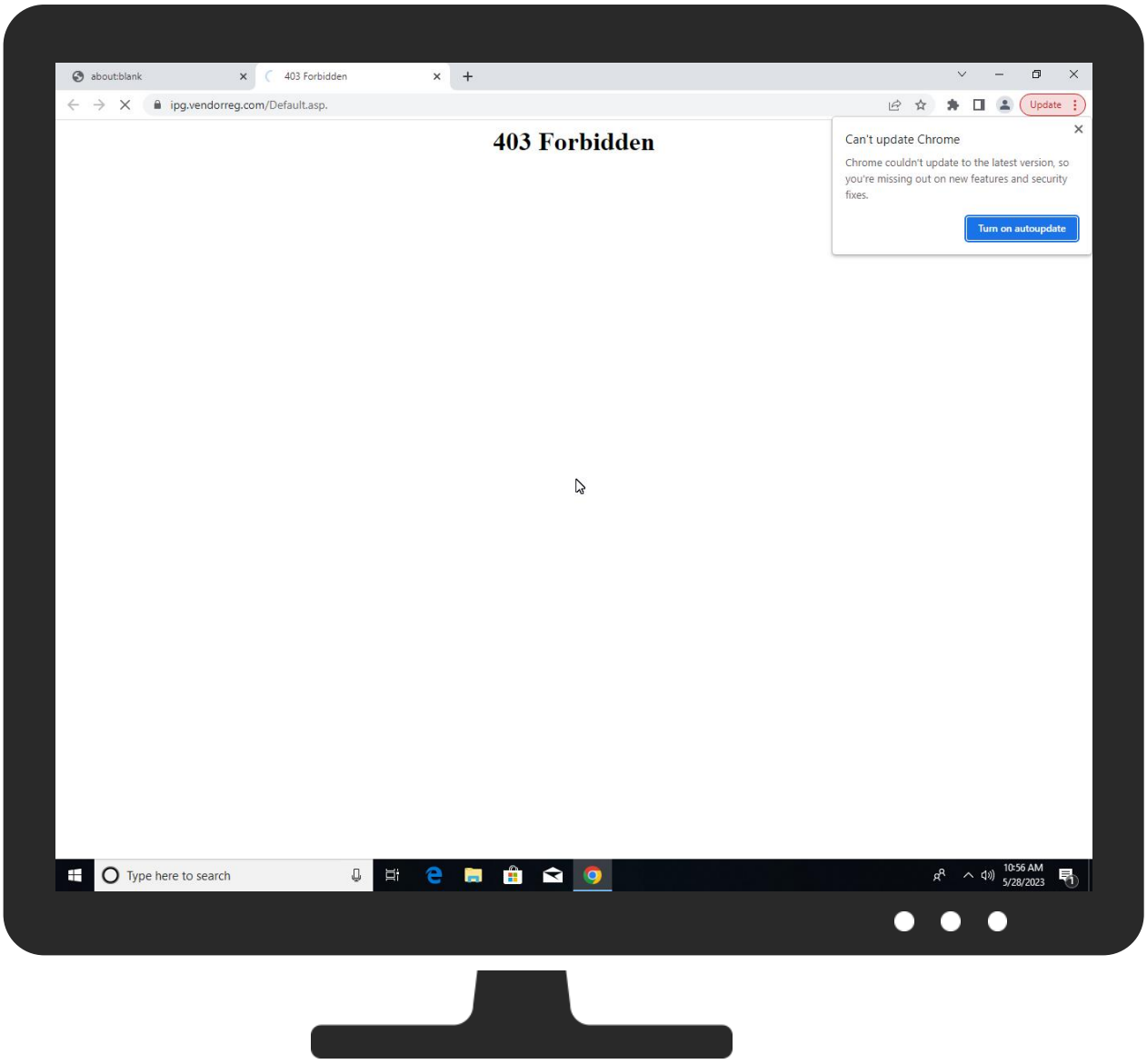
Behavior Graph



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://https://ipg.vendorreg.com/Default.asp.	0%	Virustotal		Browse
http://https://ipg.vendorreg.com/Default.asp.	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://ipg.vendorreg.com/favicon.ico	0%	Avira URL Cloud	safe	
http://https://ipg.vendorreg.com/Default.asp.	0%	Virustotal		Browse

Domains and IPs

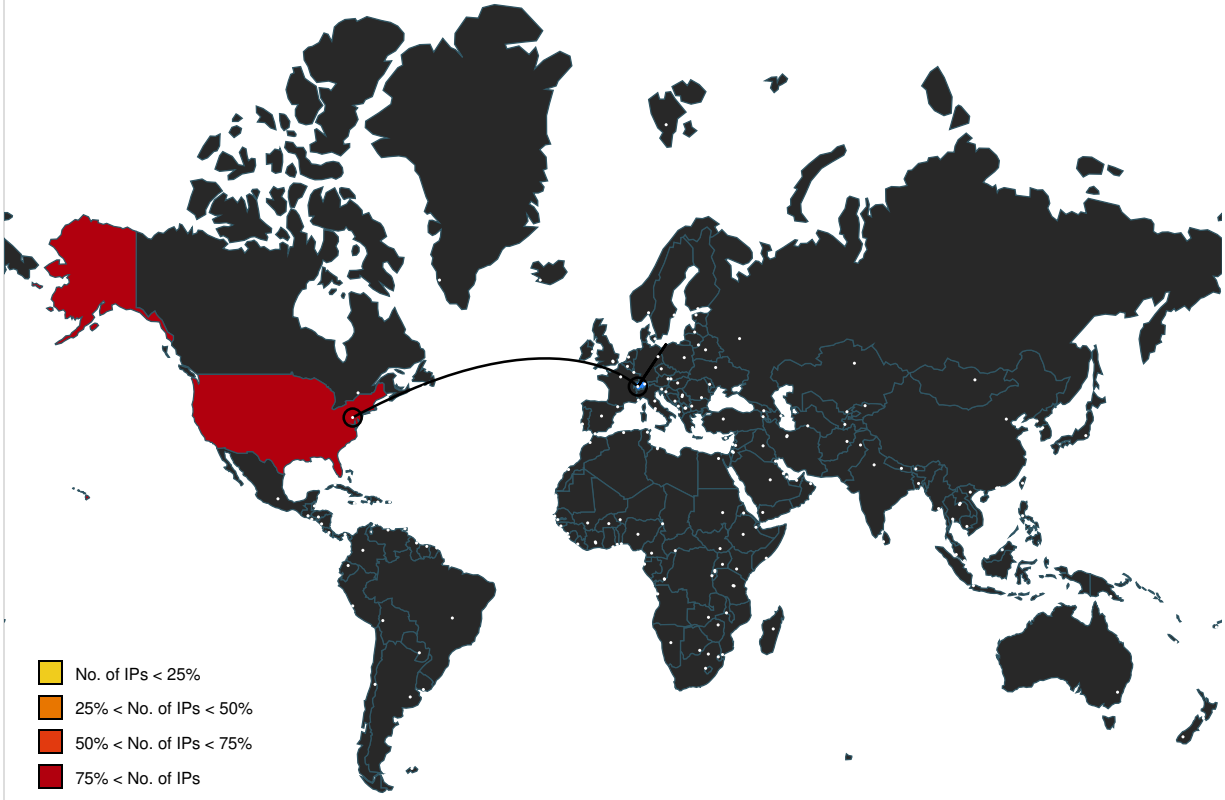
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
multi-domain-loadbalancer-b2gnow-1087660409.us-east-1.elb.amazonaws.com	34.231.91.0	true	false		high
accounts.google.com	216.58.215.237	true	false		high
www.google.com	142.250.203.100	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
ipg.vendorreg.com	unknown	unknown	false		unknown
clients2.google.com	unknown	unknown	false		high

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://ipg.vendorreg.com/Default.asp.	false	• 0%, Virustotal, Browse	unknown
http://https://ipg.vendorreg.com/Default.asp.	false	• 0%, Virustotal, Browse	unknown
http://https://ipg.vendorreg.com/favicon.ico	false	• Avira URL Cloud: safe	unknown
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
216.58.215.237	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.203.100	www.google.com	United States		15169	GOOGLEUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.231.91.0	multi-domain-loadbalancer-b2gnow-1087660409.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	877003
Start date and time:	2023-05-28 10:55:58 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://ipg.vendorreg.com/Default.asp.
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@24/2@5/6
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): 142.250.203.99, 34.104.35.123
- Excluded domains from analysis (whitelisted): edgedl.me.gvt1.com, update.googleapis.com, clientservices.googleapis.com
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

Chrome Cache Entry: 101

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	520
Entropy (8bit):	4.639855426580243
Encrypted:	false
SSDEEP:	12:TvgsoCVlogs01IlNGlTF5TF5TF5TF5TF5TFK:cEQtn7TPTPTPTPTPTc
MD5:	2E40045EFE5134ADA9942798C090D269
SHA1:	76F70F10F6B6A17B7CEC2D17C689F92C80F8BD56
SHA-256:	8B73B6CCD7091D6D9D23ADAAB2BAAE3C4ABF6DE06DF8EFDD03215EE9376FA035
SHA-512:	F603D4DDA62344EF797DE8DE82101EEBF8BF3DAD87E1BC8F840D20A4ED5BFE24434AA8B5B3DFBF287C1AC6A2D568F5E85F943CADED868E21C97EE70E9705 E63
Malicious:	false
Reputation:	low
URL:	http://https://ipg.vendorreg.com/Default.asp.
Preview:	<html>..<head><title>403 Forbidden</title></head>..<body>.. 403 Forbidden ..</body>..</html>.. a padding to disable MSIE and Chrome fr iendly error page -->.. a padding to disable MSIE and Chrome friendly error page -->.. a padding to disable MSIE and Chrome friendly error page -->.. a padding to d isable MSIE and Chrome friendly error page -->.. a padding to disable MSIE and Chrome friendly error page -->.. a padding to disable MSIE and Chrome friendly error page -->..

Chrome Cache Entry: 102

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	520
Entropy (8bit):	4.639855426580243
Encrypted:	false
SSDEEP:	12:TvgsoCVlogs01IlNGlTF5TF5TF5TF5TF5TFK:cEQtn7TPTPTPTPTPTc
MD5:	2E40045EFE5134ADA9942798C090D269
SHA1:	76F70F10F6B6A17B7CEC2D17C689F92C80F8BD56
SHA-256:	8B73B6CCD7091D6D9D23ADAAB2BAAE3C4ABF6DE06DF8EFDD03215EE9376FA035
SHA-512:	F603D4DDA62344EF797DE8DE82101EEBF8BF3DAD87E1BC8F840D20A4ED5BFE24434AA8B5B3DFBF287C1AC6A2D568F5E85F943CADED868E21C97EE70E9705 E63
Malicious:	false
Reputation:	low
URL:	http://https://ipg.vendorreg.com/favicon.ico

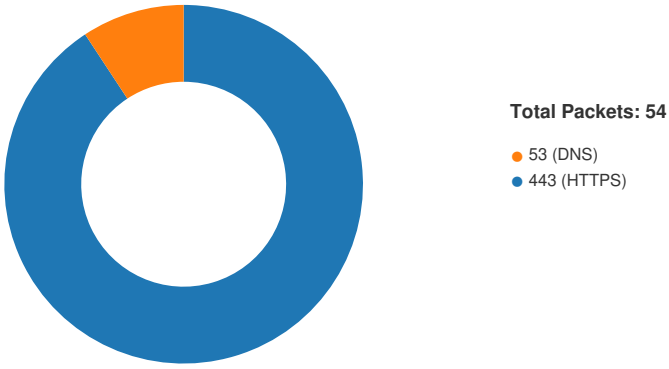
Preview:	<html>..<head><title>403 Forbidden</title></head>..<body>.. 403 Forbidden ..</body>..</html>.. a padding to disable MSIE and Chrome friendly error page -->.. a padding to disable MSIE and Chrome friendly error page -->.. a padding to disable MSIE and Chrome friendly error page -->.. a padding to disable MSIE and Chrome friendly error page -->.. a padding to disable MSIE and Chrome friendly error page -->.. a padding to disable MSIE and Chrome friendly error page -->..

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 28, 2023 10:56:52.296796083 CEST	49701	443	192.168.2.3	216.58.215.237
May 28, 2023 10:56:52.296849966 CEST	443	49701	216.58.215.237	192.168.2.3
May 28, 2023 10:56:52.296931982 CEST	49701	443	192.168.2.3	216.58.215.237
May 28, 2023 10:56:52.297379017 CEST	49703	443	192.168.2.3	142.250.203.110
May 28, 2023 10:56:52.297518969 CEST	443	49703	142.250.203.110	192.168.2.3
May 28, 2023 10:56:52.297611952 CEST	49703	443	192.168.2.3	142.250.203.110
May 28, 2023 10:56:52.297930956 CEST	49701	443	192.168.2.3	216.58.215.237
May 28, 2023 10:56:52.297967911 CEST	443	49701	216.58.215.237	192.168.2.3
May 28, 2023 10:56:52.298296928 CEST	49703	443	192.168.2.3	142.250.203.110
May 28, 2023 10:56:52.298341990 CEST	443	49703	142.250.203.110	192.168.2.3
May 28, 2023 10:56:52.415628910 CEST	443	49701	216.58.215.237	192.168.2.3
May 28, 2023 10:56:52.417831898 CEST	443	49703	142.250.203.110	192.168.2.3
May 28, 2023 10:56:52.421081066 CEST	49701	443	192.168.2.3	216.58.215.237
May 28, 2023 10:56:52.421143055 CEST	443	49701	216.58.215.237	192.168.2.3
May 28, 2023 10:56:52.421304941 CEST	49703	443	192.168.2.3	142.250.203.110
May 28, 2023 10:56:52.421349049 CEST	443	49703	142.250.203.110	192.168.2.3
May 28, 2023 10:56:52.422038078 CEST	443	49703	142.250.203.110	192.168.2.3
May 28, 2023 10:56:52.422123909 CEST	49703	443	192.168.2.3	142.250.203.110
May 28, 2023 10:56:52.423613071 CEST	443	49703	142.250.203.110	192.168.2.3
May 28, 2023 10:56:52.423615932 CEST	443	49701	216.58.215.237	192.168.2.3
May 28, 2023 10:56:52.423741102 CEST	49701	443	192.168.2.3	216.58.215.237
May 28, 2023 10:56:52.423789978 CEST	49703	443	192.168.2.3	142.250.203.110
May 28, 2023 10:56:52.838762045 CEST	49701	443	192.168.2.3	216.58.215.237
May 28, 2023 10:56:52.838856936 CEST	49701	443	192.168.2.3	216.58.215.237
May 28, 2023 10:56:52.838880062 CEST	443	49701	216.58.215.237	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 28, 2023 10:56:52.839061975 CEST	49703	443	192.168.2.3	142.250.203.110
May 28, 2023 10:56:52.839198112 CEST	49703	443	192.168.2.3	142.250.203.110
May 28, 2023 10:56:52.839200020 CEST	443	49701	216.58.215.237	192.168.2.3
May 28, 2023 10:56:52.839226961 CEST	443	49703	142.250.203.110	192.168.2.3
May 28, 2023 10:56:52.839390039 CEST	443	49703	142.250.203.110	192.168.2.3
May 28, 2023 10:56:52.875277042 CEST	443	49703	142.250.203.110	192.168.2.3
May 28, 2023 10:56:52.875365019 CEST	49703	443	192.168.2.3	142.250.203.110
May 28, 2023 10:56:52.875402927 CEST	443	49703	142.250.203.110	192.168.2.3
May 28, 2023 10:56:52.875581980 CEST	443	49703	142.250.203.110	192.168.2.3
May 28, 2023 10:56:52.875699997 CEST	49703	443	192.168.2.3	142.250.203.110
May 28, 2023 10:56:52.876343966 CEST	49703	443	192.168.2.3	142.250.203.110
May 28, 2023 10:56:52.876385927 CEST	443	49703	142.250.203.110	192.168.2.3
May 28, 2023 10:56:52.884418011 CEST	49701	443	192.168.2.3	216.58.215.237
May 28, 2023 10:56:52.884443045 CEST	443	49701	216.58.215.237	192.168.2.3
May 28, 2023 10:56:52.889959097 CEST	443	49701	216.58.215.237	192.168.2.3
May 28, 2023 10:56:52.890038967 CEST	49701	443	192.168.2.3	216.58.215.237
May 28, 2023 10:56:52.890064001 CEST	443	49701	216.58.215.237	192.168.2.3
May 28, 2023 10:56:52.890361071 CEST	443	49701	216.58.215.237	192.168.2.3
May 28, 2023 10:56:52.890433073 CEST	49701	443	192.168.2.3	216.58.215.237
May 28, 2023 10:56:52.891948938 CEST	49701	443	192.168.2.3	216.58.215.237
May 28, 2023 10:56:52.891978025 CEST	443	49701	216.58.215.237	192.168.2.3
May 28, 2023 10:56:53.930038929 CEST	49705	443	192.168.2.3	34.231.91.0
May 28, 2023 10:56:53.930102110 CEST	443	49705	34.231.91.0	192.168.2.3
May 28, 2023 10:56:53.930246115 CEST	49705	443	192.168.2.3	34.231.91.0
May 28, 2023 10:56:53.931158066 CEST	49706	443	192.168.2.3	34.231.91.0
May 28, 2023 10:56:53.931211948 CEST	443	49706	34.231.91.0	192.168.2.3
May 28, 2023 10:56:53.931288958 CEST	49706	443	192.168.2.3	34.231.91.0
May 28, 2023 10:56:53.931405067 CEST	49705	443	192.168.2.3	34.231.91.0
May 28, 2023 10:56:53.931458950 CEST	443	49705	34.231.91.0	192.168.2.3
May 28, 2023 10:56:53.931672096 CEST	49706	443	192.168.2.3	34.231.91.0
May 28, 2023 10:56:53.931704044 CEST	443	49706	34.231.91.0	192.168.2.3
May 28, 2023 10:56:54.404093027 CEST	443	49705	34.231.91.0	192.168.2.3
May 28, 2023 10:56:54.404103994 CEST	443	49706	34.231.91.0	192.168.2.3
May 28, 2023 10:56:54.410346985 CEST	49705	443	192.168.2.3	34.231.91.0
May 28, 2023 10:56:54.410403967 CEST	443	49705	34.231.91.0	192.168.2.3
May 28, 2023 10:56:54.410517931 CEST	49706	443	192.168.2.3	34.231.91.0
May 28, 2023 10:56:54.410563946 CEST	443	49706	34.231.91.0	192.168.2.3
May 28, 2023 10:56:54.411818981 CEST	443	49705	34.231.91.0	192.168.2.3
May 28, 2023 10:56:54.411895990 CEST	49705	443	192.168.2.3	34.231.91.0
May 28, 2023 10:56:54.411899090 CEST	443	49706	34.231.91.0	192.168.2.3
May 28, 2023 10:56:54.411967993 CEST	49706	443	192.168.2.3	34.231.91.0
May 28, 2023 10:56:54.443233013 CEST	49705	443	192.168.2.3	34.231.91.0
May 28, 2023 10:56:54.443480015 CEST	49705	443	192.168.2.3	34.231.91.0
May 28, 2023 10:56:54.443501949 CEST	443	49705	34.231.91.0	192.168.2.3
May 28, 2023 10:56:54.443608046 CEST	443	49705	34.231.91.0	192.168.2.3
May 28, 2023 10:56:54.443783045 CEST	49706	443	192.168.2.3	34.231.91.0
May 28, 2023 10:56:54.444367886 CEST	443	49706	34.231.91.0	192.168.2.3
May 28, 2023 10:56:54.539367914 CEST	49706	443	192.168.2.3	34.231.91.0
May 28, 2023 10:56:54.539400101 CEST	443	49706	34.231.91.0	192.168.2.3
May 28, 2023 10:56:54.584415913 CEST	443	49705	34.231.91.0	192.168.2.3
May 28, 2023 10:56:54.584511042 CEST	49705	443	192.168.2.3	34.231.91.0
May 28, 2023 10:56:54.587491035 CEST	49705	443	192.168.2.3	34.231.91.0
May 28, 2023 10:56:54.587524891 CEST	443	49705	34.231.91.0	192.168.2.3
May 28, 2023 10:56:54.639452934 CEST	49706	443	192.168.2.3	34.231.91.0
May 28, 2023 10:56:54.679466009 CEST	49706	443	192.168.2.3	34.231.91.0
May 28, 2023 10:56:54.720299006 CEST	443	49706	34.231.91.0	192.168.2.3
May 28, 2023 10:56:54.819509983 CEST	443	49706	34.231.91.0	192.168.2.3
May 28, 2023 10:56:54.819662094 CEST	443	49706	34.231.91.0	192.168.2.3
May 28, 2023 10:56:54.819756031 CEST	49706	443	192.168.2.3	34.231.91.0

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 28, 2023 10:56:54.821851015 CEST	49706	443	192.168.2.3	34.231.91.0
May 28, 2023 10:56:54.821888924 CEST	443	49706	34.231.91.0	192.168.2.3
May 28, 2023 10:56:54.847786903 CEST	49707	443	192.168.2.3	34.231.91.0
May 28, 2023 10:56:54.847877026 CEST	443	49707	34.231.91.0	192.168.2.3
May 28, 2023 10:56:54.848026037 CEST	49707	443	192.168.2.3	34.231.91.0
May 28, 2023 10:56:54.848063946 CEST	49708	443	192.168.2.3	34.231.91.0
May 28, 2023 10:56:54.848170042 CEST	443	49708	34.231.91.0	192.168.2.3
May 28, 2023 10:56:54.848287106 CEST	49708	443	192.168.2.3	34.231.91.0
May 28, 2023 10:56:54.852104902 CEST	49708	443	192.168.2.3	34.231.91.0
May 28, 2023 10:56:54.852193117 CEST	443	49708	34.231.91.0	192.168.2.3
May 28, 2023 10:56:54.852308989 CEST	49707	443	192.168.2.3	34.231.91.0
May 28, 2023 10:56:54.852356911 CEST	443	49707	34.231.91.0	192.168.2.3
May 28, 2023 10:56:55.190023899 CEST	443	49707	34.231.91.0	192.168.2.3
May 28, 2023 10:56:55.190047026 CEST	443	49708	34.231.91.0	192.168.2.3
May 28, 2023 10:56:55.190507889 CEST	49707	443	192.168.2.3	34.231.91.0
May 28, 2023 10:56:55.190624952 CEST	443	49707	34.231.91.0	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 28, 2023 10:56:52.237941980 CEST	53975	53	192.168.2.3	8.8.8.8
May 28, 2023 10:56:52.238989115 CEST	51139	53	192.168.2.3	8.8.8.8
May 28, 2023 10:56:52.258498907 CEST	53	51139	8.8.8.8	192.168.2.3
May 28, 2023 10:56:52.291738033 CEST	53	53975	8.8.8.8	192.168.2.3
May 28, 2023 10:56:53.802108049 CEST	57134	53	192.168.2.3	8.8.8.8
May 28, 2023 10:56:53.859759092 CEST	53	57134	8.8.8.8	192.168.2.3
May 28, 2023 10:56:56.153454065 CEST	59636	53	192.168.2.3	8.8.8.8
May 28, 2023 10:56:56.176875114 CEST	53	59636	8.8.8.8	192.168.2.3
May 28, 2023 10:57:56.226293087 CEST	58301	53	192.168.2.3	8.8.8.8
May 28, 2023 10:57:56.261471987 CEST	53	58301	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
May 28, 2023 10:56:52.237941980 CEST	192.168.2.3	8.8.8.8	0xe12d	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:56:52.238989115 CEST	192.168.2.3	8.8.8.8	0xaef9	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:56:53.802108049 CEST	192.168.2.3	8.8.8.8	0x43ef	Standard query (0)	ipg.vendorreg.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:56:56.153454065 CEST	192.168.2.3	8.8.8.8	0x8380	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:57:56.226293087 CEST	192.168.2.3	8.8.8.8	0xe237	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
May 28, 2023 10:56:52.258498907 CEST	8.8.8.8	192.168.2.3	0xaef9	No error (0)	accounts.google.com		216.58.215.237	A (IP address)	IN (0x0001)	false
May 28, 2023 10:56:52.291738033 CEST	8.8.8.8	192.168.2.3	0xe12d	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
May 28, 2023 10:56:52.291738033 CEST	8.8.8.8	192.168.2.3	0xe12d	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
May 28, 2023 10:56:53.859759092 CEST	8.8.8.8	192.168.2.3	0x43ef	No error (0)	ipg.vendorreg.com	multi-domain-loadbalancer-b2gnow-1087660409.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)	false

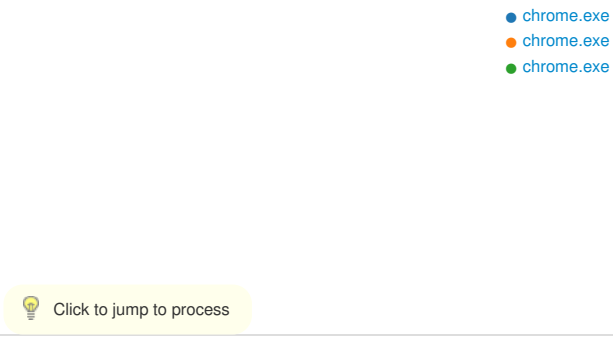
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 28, 2023 10:56:53.859759092 CEST	8.8.8.8	192.168.2.3	0x43ef	No error (0)	multi-domain-loadbalancer-b2gnow-1087660409.us-east-1.elb.amazonaws.com		34.231.91.0	A (IP address)	IN (0x0001)	false
May 28, 2023 10:56:53.859759092 CEST	8.8.8.8	192.168.2.3	0x43ef	No error (0)	multi-domain-loadbalancer-b2gnow-1087660409.us-east-1.elb.amazonaws.com		18.215.95.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:56:56.176875114 CEST	8.8.8.8	192.168.2.3	0x8380	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
May 28, 2023 10:57:56.261471987 CEST	8.8.8.8	192.168.2.3	0xe237	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- accounts.google.com
- clients2.google.com
- ipg.vendorreg.com
- https:

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 6140, Parent PID: 2108

General

Target ID:	0

Start time:	10:56:49
Start date:	28/05/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	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

Analysis Process: chrome.exe PID: **5984**, Parent PID: **6140**

General

Target ID:	1
Start time:	10:56:49
Start date:	28/05/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1612 --field-trial-handle=1760,i,16128215241196653397,1351737748157124362,131072 --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:	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

Analysis Process: chrome.exe PID: **6340**, Parent PID: **2108**

General

Target ID:	2
Start time:	10:56:52
Start date:	28/05/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false

Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "https://ipg.vendorreg.com/Default.asp.
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:	low

Disassembly

No disassembly