ID: 736958
Cookbook: browseurl.jbs
Time: 12:31:29
Date: 03/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

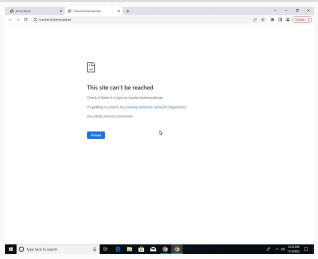
Windows Analysis Report

http://tracker.birkenwald.de

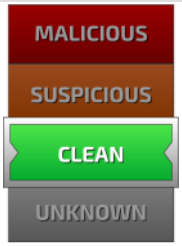
Overview

General Information

Sample URL:	http://tracker.birkenwald.de
Analysis ID:	736958
Infos:	



Detection

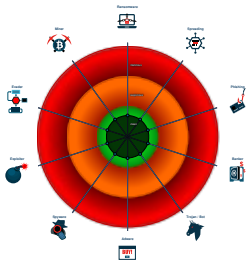


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64
- chrome.exe (PID: 5832 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 1888 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-GB --service-sandbox-type=none --mojo-platform-channel-handle=1948 --field-trial-handle=1724,i,446256194717994275,7506232099030024805,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 3216 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "http://tracker.birkenwald.de 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

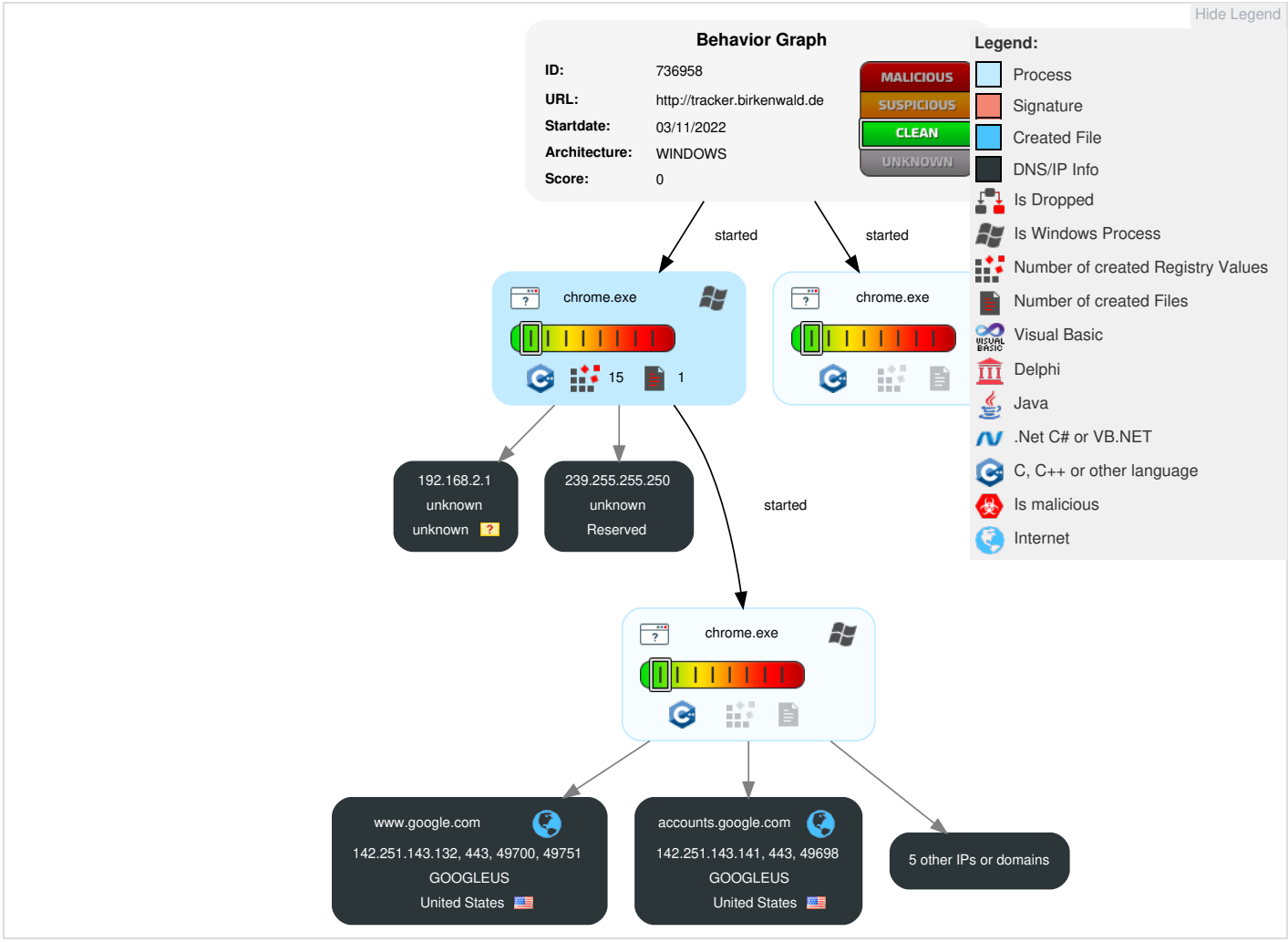
Joe Sandbox Signatures

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

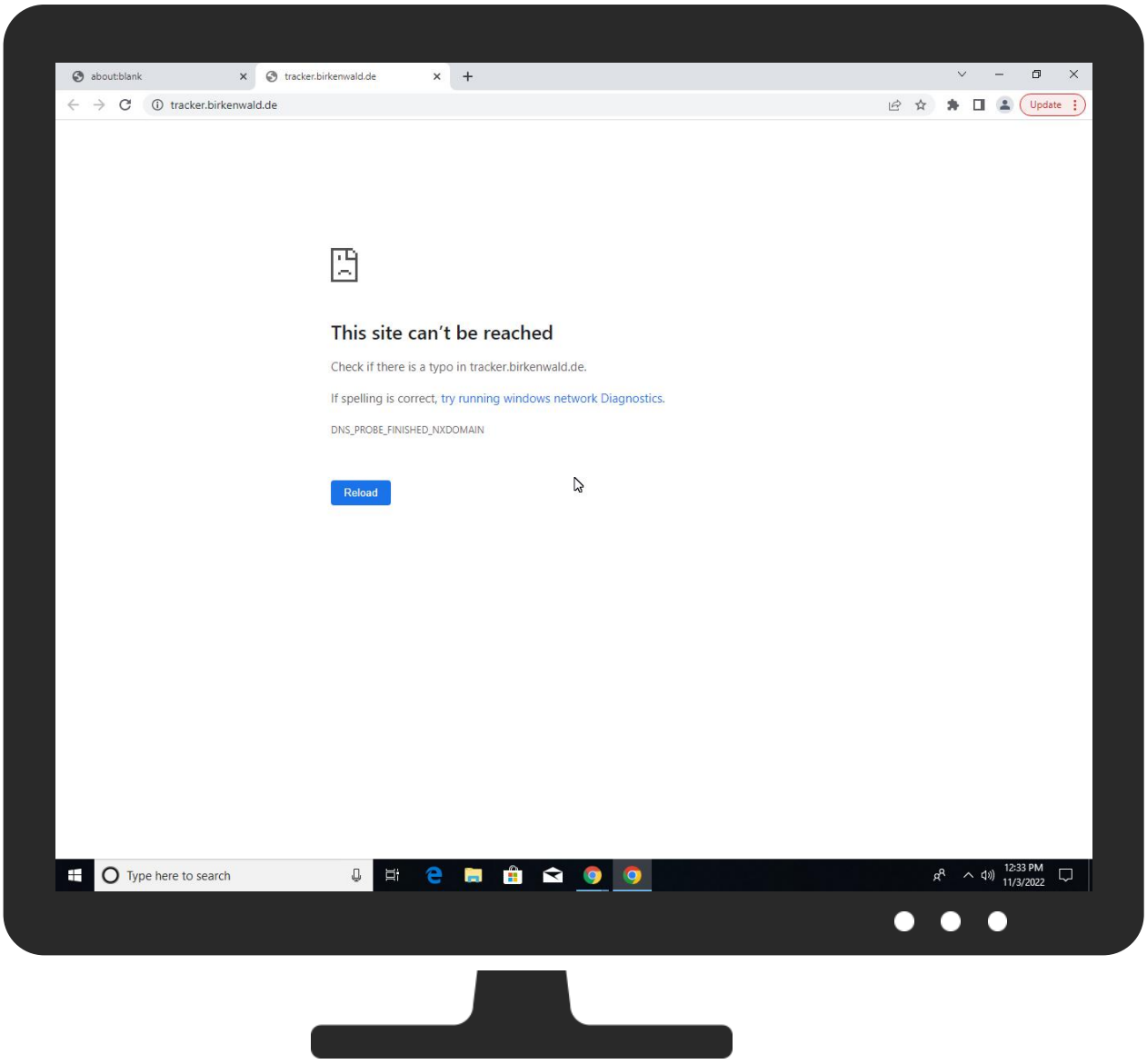
Behavior Graph



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://tracker.birkenwald.de	0%	Virustotal		Browse
http://tracker.birkenwald.de	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

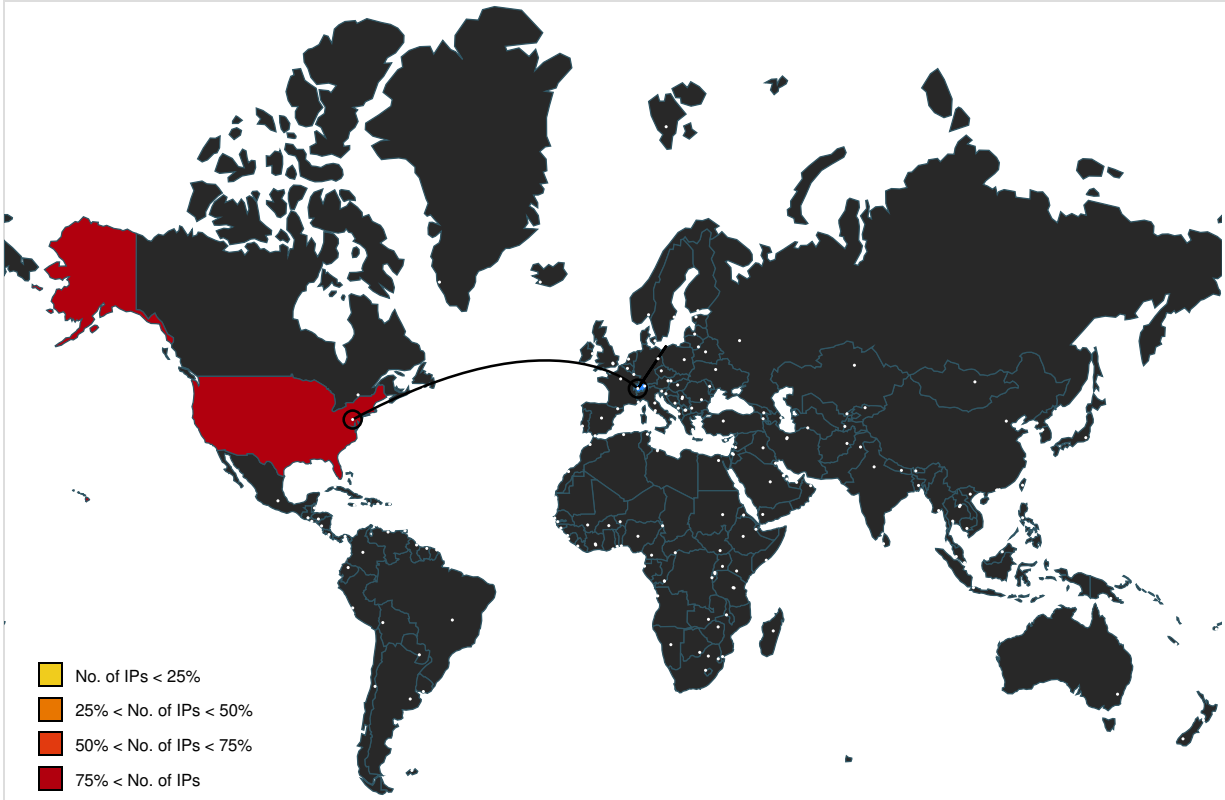
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
google.com	142.251.143.206	true	false		high
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
clients2.google.com	unknown	unknown	false		high
tracker.birkenwald.de	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-GB&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
142.251.143.132	www.google.com	United States		15169	GOOGLEUS	false
142.251.143.174	clients.l.google.com	United States		15169	GOOGLEUS	false
142.251.143.141	accounts.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	736958
Start date and time:	2022-11-03 12:31:29 +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://tracker.birkenwald.de
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@30/0@11/6
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
- Excluded IPs from analysis (whitelisted): 142.251.143.131, 34.104.35.123, 142.251.143.163
- 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
- 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

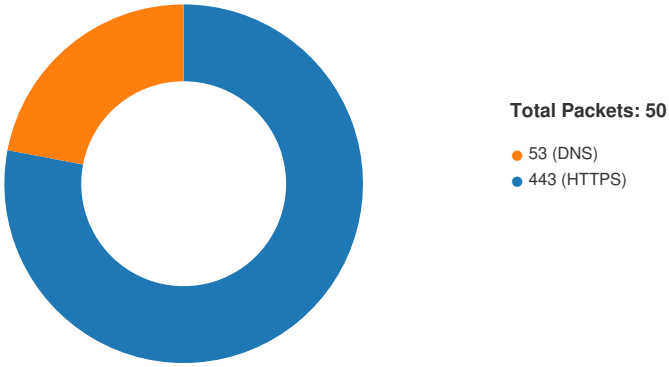
No created / dropped files found

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 12:32:34.848258972 CET	49697	443	192.168.2.4	142.251.143.174
Nov 3, 2022 12:32:34.848320007 CET	443	49697	142.251.143.174	192.168.2.4
Nov 3, 2022 12:32:34.848418951 CET	49697	443	192.168.2.4	142.251.143.174
Nov 3, 2022 12:32:34.848831892 CET	49697	443	192.168.2.4	142.251.143.174
Nov 3, 2022 12:32:34.848875999 CET	443	49697	142.251.143.174	192.168.2.4
Nov 3, 2022 12:32:34.941853046 CET	443	49697	142.251.143.174	192.168.2.4
Nov 3, 2022 12:32:35.008193016 CET	49697	443	192.168.2.4	142.251.143.174
Nov 3, 2022 12:32:35.008227110 CET	443	49697	142.251.143.174	192.168.2.4
Nov 3, 2022 12:32:35.008811951 CET	49698	443	192.168.2.4	142.251.143.141
Nov 3, 2022 12:32:35.008871078 CET	443	49698	142.251.143.141	192.168.2.4
Nov 3, 2022 12:32:35.008976936 CET	49698	443	192.168.2.4	142.251.143.141
Nov 3, 2022 12:32:35.009282112 CET	49698	443	192.168.2.4	142.251.143.141
Nov 3, 2022 12:32:35.009311914 CET	443	49698	142.251.143.141	192.168.2.4
Nov 3, 2022 12:32:35.011080980 CET	443	49697	142.251.143.174	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:32:35.011101007 CET	443	49697	142.251.143.174	192.168.2.4
Nov 3, 2022 12:32:35.011185884 CET	49697	443	192.168.2.4	142.251.143.174
Nov 3, 2022 12:32:35.013556957 CET	443	49697	142.251.143.174	192.168.2.4
Nov 3, 2022 12:32:35.013636112 CET	49697	443	192.168.2.4	142.251.143.174
Nov 3, 2022 12:32:35.013655901 CET	443	49697	142.251.143.174	192.168.2.4
Nov 3, 2022 12:32:35.103030920 CET	443	49698	142.251.143.141	192.168.2.4
Nov 3, 2022 12:32:35.120148897 CET	49698	443	192.168.2.4	142.251.143.141
Nov 3, 2022 12:32:35.120198011 CET	443	49698	142.251.143.141	192.168.2.4
Nov 3, 2022 12:32:35.121865034 CET	443	49698	142.251.143.141	192.168.2.4
Nov 3, 2022 12:32:35.121968985 CET	49698	443	192.168.2.4	142.251.143.141
Nov 3, 2022 12:32:35.127017975 CET	49697	443	192.168.2.4	142.251.143.174
Nov 3, 2022 12:32:35.432127953 CET	49697	443	192.168.2.4	142.251.143.174
Nov 3, 2022 12:32:35.432173967 CET	443	49697	142.251.143.174	192.168.2.4
Nov 3, 2022 12:32:35.432365894 CET	443	49697	142.251.143.174	192.168.2.4
Nov 3, 2022 12:32:35.432419062 CET	49697	443	192.168.2.4	142.251.143.174
Nov 3, 2022 12:32:35.432441950 CET	443	49697	142.251.143.174	192.168.2.4
Nov 3, 2022 12:32:35.433808088 CET	49698	443	192.168.2.4	142.251.143.141
Nov 3, 2022 12:32:35.433852911 CET	443	49698	142.251.143.141	192.168.2.4
Nov 3, 2022 12:32:35.434010029 CET	443	49698	142.251.143.141	192.168.2.4
Nov 3, 2022 12:32:35.434124947 CET	49698	443	192.168.2.4	142.251.143.141
Nov 3, 2022 12:32:35.434144974 CET	443	49698	142.251.143.141	192.168.2.4
Nov 3, 2022 12:32:35.488828897 CET	443	49697	142.251.143.174	192.168.2.4
Nov 3, 2022 12:32:35.488965034 CET	49697	443	192.168.2.4	142.251.143.174
Nov 3, 2022 12:32:35.489017010 CET	443	49697	142.251.143.174	192.168.2.4
Nov 3, 2022 12:32:35.489149094 CET	443	49697	142.251.143.174	192.168.2.4
Nov 3, 2022 12:32:35.489247084 CET	49697	443	192.168.2.4	142.251.143.174
Nov 3, 2022 12:32:35.505986929 CET	49697	443	192.168.2.4	142.251.143.174
Nov 3, 2022 12:32:35.506052971 CET	443	49697	142.251.143.174	192.168.2.4
Nov 3, 2022 12:32:35.513387918 CET	443	49698	142.251.143.141	192.168.2.4
Nov 3, 2022 12:32:35.513516903 CET	49698	443	192.168.2.4	142.251.143.141
Nov 3, 2022 12:32:35.513576031 CET	443	49698	142.251.143.141	192.168.2.4
Nov 3, 2022 12:32:35.513735056 CET	443	49698	142.251.143.141	192.168.2.4
Nov 3, 2022 12:32:35.513900042 CET	49698	443	192.168.2.4	142.251.143.141
Nov 3, 2022 12:32:35.522547960 CET	49698	443	192.168.2.4	142.251.143.141
Nov 3, 2022 12:32:35.522598028 CET	443	49698	142.251.143.141	192.168.2.4
Nov 3, 2022 12:32:37.289654016 CET	49700	443	192.168.2.4	142.251.143.132
Nov 3, 2022 12:32:37.289726973 CET	443	49700	142.251.143.132	192.168.2.4
Nov 3, 2022 12:32:37.289851904 CET	49700	443	192.168.2.4	142.251.143.132
Nov 3, 2022 12:32:37.290338039 CET	49700	443	192.168.2.4	142.251.143.132
Nov 3, 2022 12:32:37.290363073 CET	443	49700	142.251.143.132	192.168.2.4
Nov 3, 2022 12:32:37.367079973 CET	443	49700	142.251.143.132	192.168.2.4
Nov 3, 2022 12:32:37.379189014 CET	49700	443	192.168.2.4	142.251.143.132
Nov 3, 2022 12:32:37.379221916 CET	443	49700	142.251.143.132	192.168.2.4
Nov 3, 2022 12:32:37.380721092 CET	443	49700	142.251.143.132	192.168.2.4
Nov 3, 2022 12:32:37.380795956 CET	49700	443	192.168.2.4	142.251.143.132
Nov 3, 2022 12:32:37.401571989 CET	49700	443	192.168.2.4	142.251.143.132
Nov 3, 2022 12:32:37.401629925 CET	443	49700	142.251.143.132	192.168.2.4
Nov 3, 2022 12:32:37.401850939 CET	443	49700	142.251.143.132	192.168.2.4
Nov 3, 2022 12:32:37.522257090 CET	49700	443	192.168.2.4	142.251.143.132
Nov 3, 2022 12:32:37.522294998 CET	443	49700	142.251.143.132	192.168.2.4
Nov 3, 2022 12:32:37.634299994 CET	49700	443	192.168.2.4	142.251.143.132
Nov 3, 2022 12:32:47.408508062 CET	443	49700	142.251.143.132	192.168.2.4
Nov 3, 2022 12:32:47.408581972 CET	443	49700	142.251.143.132	192.168.2.4
Nov 3, 2022 12:32:47.408736944 CET	49700	443	192.168.2.4	142.251.143.132
Nov 3, 2022 12:32:50.664527893 CET	49700	443	192.168.2.4	142.251.143.132
Nov 3, 2022 12:32:50.664606094 CET	443	49700	142.251.143.132	192.168.2.4
Nov 3, 2022 12:33:37.103055000 CET	49751	443	192.168.2.4	142.251.143.132
Nov 3, 2022 12:33:37.103143930 CET	443	49751	142.251.143.132	192.168.2.4
Nov 3, 2022 12:33:37.103332043 CET	49751	443	192.168.2.4	142.251.143.132

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:33:37.103738070 CET	49751	443	192.168.2.4	142.251.143.132
Nov 3, 2022 12:33:37.103769064 CET	443	49751	142.251.143.132	192.168.2.4
Nov 3, 2022 12:33:37.176470041 CET	443	49751	142.251.143.132	192.168.2.4
Nov 3, 2022 12:33:37.177056074 CET	49751	443	192.168.2.4	142.251.143.132
Nov 3, 2022 12:33:37.177123070 CET	443	49751	142.251.143.132	192.168.2.4
Nov 3, 2022 12:33:37.177563906 CET	443	49751	142.251.143.132	192.168.2.4
Nov 3, 2022 12:33:37.178265095 CET	49751	443	192.168.2.4	142.251.143.132
Nov 3, 2022 12:33:37.178322077 CET	443	49751	142.251.143.132	192.168.2.4
Nov 3, 2022 12:33:37.178410053 CET	443	49751	142.251.143.132	192.168.2.4
Nov 3, 2022 12:33:37.219191074 CET	49751	443	192.168.2.4	142.251.143.132
Nov 3, 2022 12:33:47.198313951 CET	443	49751	142.251.143.132	192.168.2.4
Nov 3, 2022 12:33:47.198463917 CET	443	49751	142.251.143.132	192.168.2.4
Nov 3, 2022 12:33:47.198561907 CET	49751	443	192.168.2.4	142.251.143.132

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:32:34.718369007 CET	64167	53	192.168.2.4	8.8.8.8
Nov 3, 2022 12:32:34.719600916 CET	58565	53	192.168.2.4	8.8.8.8
Nov 3, 2022 12:32:34.720194101 CET	52239	53	192.168.2.4	8.8.8.8
Nov 3, 2022 12:32:34.737428904 CET	53	64167	8.8.8.8	192.168.2.4
Nov 3, 2022 12:32:34.739278078 CET	53	52239	8.8.8.8	192.168.2.4
Nov 3, 2022 12:32:34.746743917 CET	53	58565	8.8.8.8	192.168.2.4
Nov 3, 2022 12:32:35.507956982 CET	56807	53	192.168.2.4	8.8.8.8
Nov 3, 2022 12:32:35.508666992 CET	61007	53	192.168.2.4	8.8.8.8
Nov 3, 2022 12:32:35.525162935 CET	53	56807	8.8.8.8	192.168.2.4
Nov 3, 2022 12:32:35.536830902 CET	53	61007	8.8.8.8	192.168.2.4
Nov 3, 2022 12:32:36.530153990 CET	59444	53	192.168.2.4	8.8.8.8
Nov 3, 2022 12:32:36.549137115 CET	53	59444	8.8.8.8	192.168.2.4
Nov 3, 2022 12:32:37.026036978 CET	55570	53	192.168.2.4	8.8.8.8
Nov 3, 2022 12:32:37.045268059 CET	53	55570	8.8.8.8	192.168.2.4
Nov 3, 2022 12:32:37.218342066 CET	59446	53	192.168.2.4	8.8.8.8
Nov 3, 2022 12:32:37.237991095 CET	53	59446	8.8.8.8	192.168.2.4
Nov 3, 2022 12:32:41.657788038 CET	61088	53	192.168.2.4	8.8.8.8
Nov 3, 2022 12:32:41.674659967 CET	53	61088	8.8.8.8	192.168.2.4
Nov 3, 2022 12:33:12.148623943 CET	49735	53	192.168.2.4	8.8.8.8
Nov 3, 2022 12:33:12.165673018 CET	53	49735	8.8.8.8	192.168.2.4
Nov 3, 2022 12:33:37.081355095 CET	64773	53	192.168.2.4	8.8.8.8
Nov 3, 2022 12:33:37.100749969 CET	53	64773	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 3, 2022 12:32:34.718369007 CET	192.168.2.4	8.8.8.8	0xecf4	Standard query (0)	tracker.bi rkenwald.de	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:32:34.719600916 CET	192.168.2.4	8.8.8.8	0x2432	Standard query (0)	accounts.g oogle.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:32:34.720194101 CET	192.168.2.4	8.8.8.8	0xe387	Standard query (0)	clients2.g oogle.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:32:35.507956982 CET	192.168.2.4	8.8.8.8	0x68	Standard query (0)	google.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:32:35.508666992 CET	192.168.2.4	8.8.8.8	0xe310	Standard query (0)	google.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:32:36.530153990 CET	192.168.2.4	8.8.8.8	0xc3a6	Standard query (0)	tracker.bi rkenwald.de	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:32:37.026036978 CET	192.168.2.4	8.8.8.8	0x2fb9	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:32:37.218342066 CET	192.168.2.4	8.8.8.8	0x69f2	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:32:41.657788038 CET	192.168.2.4	8.8.8.8	0xf0e0	Standard query (0)	tracker.bi rkenwald.de	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 3, 2022 12:33:12.148623943 CET	192.168.2.4	8.8.8.8	0x7bd6	Standard query (0)	tracker.birkenwald.de	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:33:37.081355095 CET	192.168.2.4	8.8.8.8	0xba9	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

DNS Answers

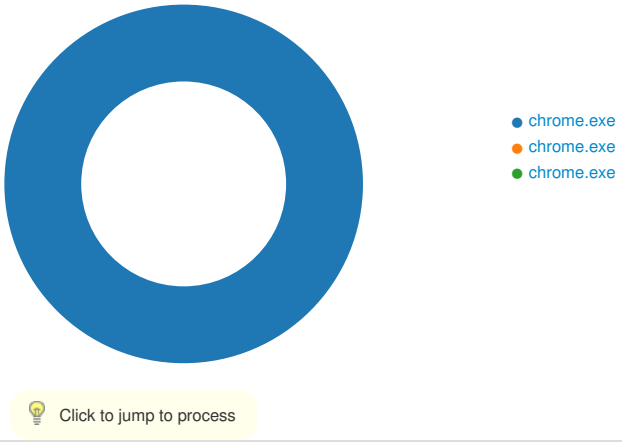
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 3, 2022 12:32:34.739278078 CET	8.8.8.8	192.168.2.4	0xe387	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 3, 2022 12:32:34.739278078 CET	8.8.8.8	192.168.2.4	0xe387	No error (0)	clients.l.google.com		142.251.143.174	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:32:34.746743917 CET	8.8.8.8	192.168.2.4	0x2432	No error (0)	accounts.google.com		142.251.143.141	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:32:35.525162935 CET	8.8.8.8	192.168.2.4	0x68	No error (0)	google.com		142.251.143.206	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:32:35.536830902 CET	8.8.8.8	192.168.2.4	0xe310	No error (0)	google.com		142.251.143.206	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:32:37.045268059 CET	8.8.8.8	192.168.2.4	0x2fb9	No error (0)	www.google.com		142.251.143.132	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:32:37.237991095 CET	8.8.8.8	192.168.2.4	0x69f2	No error (0)	www.google.com		142.251.143.132	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:33:37.100749969 CET	8.8.8.8	192.168.2.4	0xba9	No error (0)	www.google.com		142.251.143.132	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: **5832**, Parent PID: **3256**

General

Target ID:	0
Start time:	12:32:30
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:	0x7ff683680000
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: **1888**, Parent PID: **5832**

General

Target ID:	1
Start time:	12:32:31
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-GB --service-sandbox-type=none --mojo-platform-channel-handle=1948 --field-trial-handle=1724,i,4462561947179942 75,7506232099030024805,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff683680000
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: **3216**, Parent PID: **3256**

General

Target ID:	2
Start time:	12:32:33
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://tracker.birkenwald.de
Imagebase:	0x7ff683680000
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