ID: 764047
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 11:06:24
Date: 09/12/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

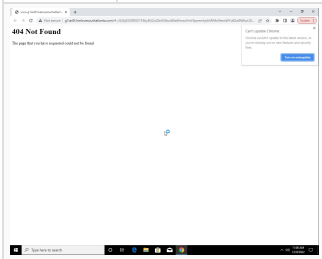
Windows Analysis Report

http://www.g1iar8f.livelovesouthatlanta.com/#.=02bj5SZ0RXZ1F3byBUZul2btVGbu4WatFmauVmY6p...

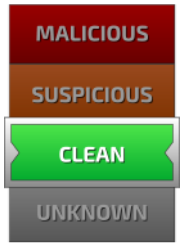
Overview

General Information

Sample URL:	www.g1iar8f.livelovesouthatlanta.com/#.=02bj5SZ0RXZ1F3byBUZul2btVGbu4WatFma...BUZul2btVGbu4WatFmauVmY6pnemhjchlWMn9ievsWYu8Sai9WbuUGbpJ2btxWYi9Gbn5SZt9Ga
Analysis ID:	764047
Infos:	



Detection

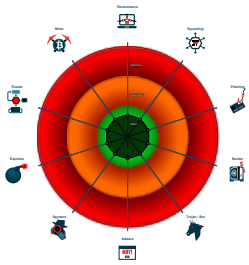


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64_ra
- chrome.exe (PID: 5496 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument http://www.g1iar8f.livelovesouthatlanta.com/#.=02bj5SZ0RXZ1F3byBUZul2btVGbu4WatFmauVmY6pnemhjchlWMn9ievsWYu8Sai9WbuUGbpJ2btxWYi9Gbn5SZt9Ga MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 3552 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=2036 --field-trial-handle=1764,i,13192198239046418531,5295402104946012676,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- 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

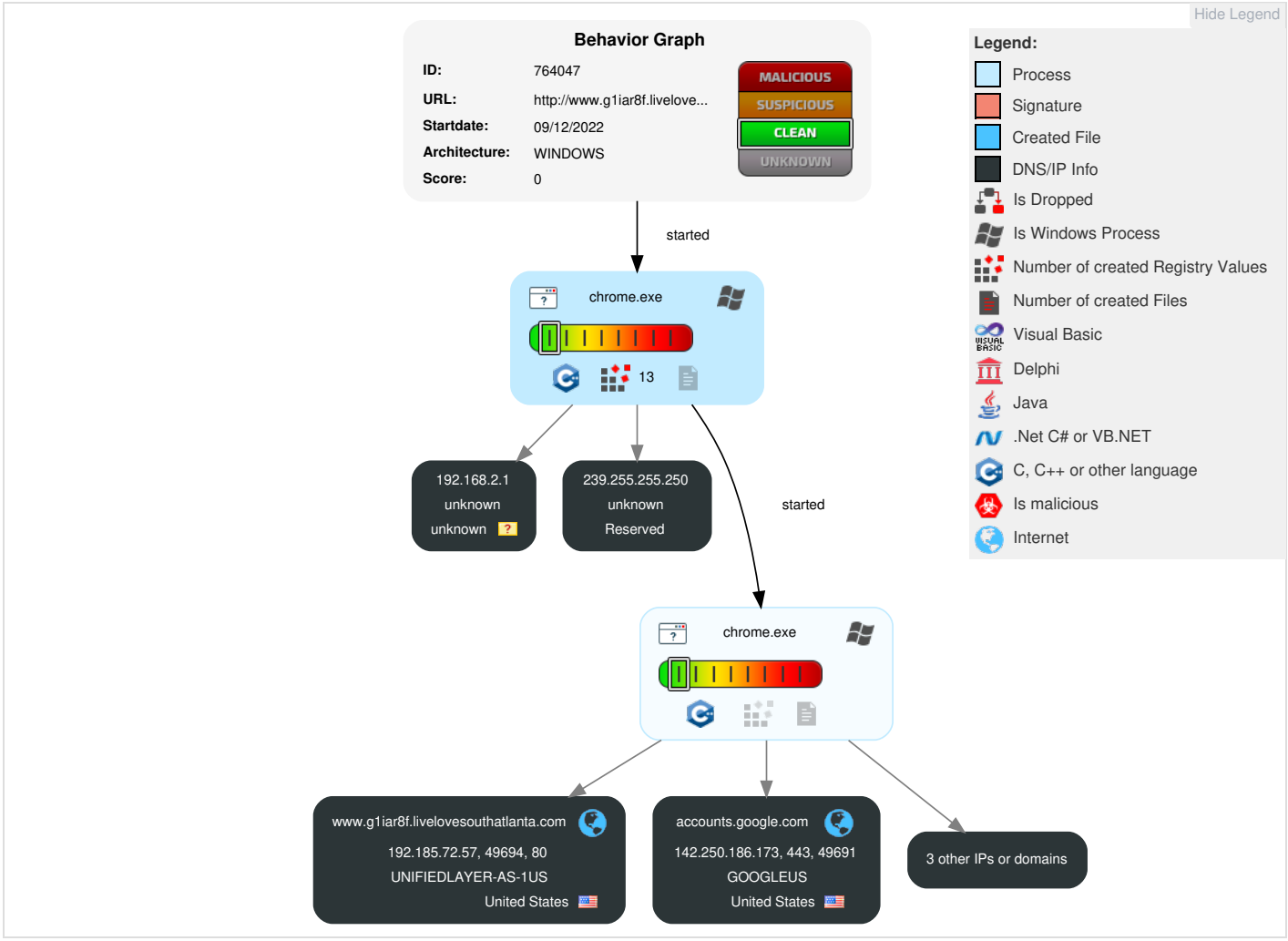
Joe Sandbox Signatures

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	1 Process Injection	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	Rootkit	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

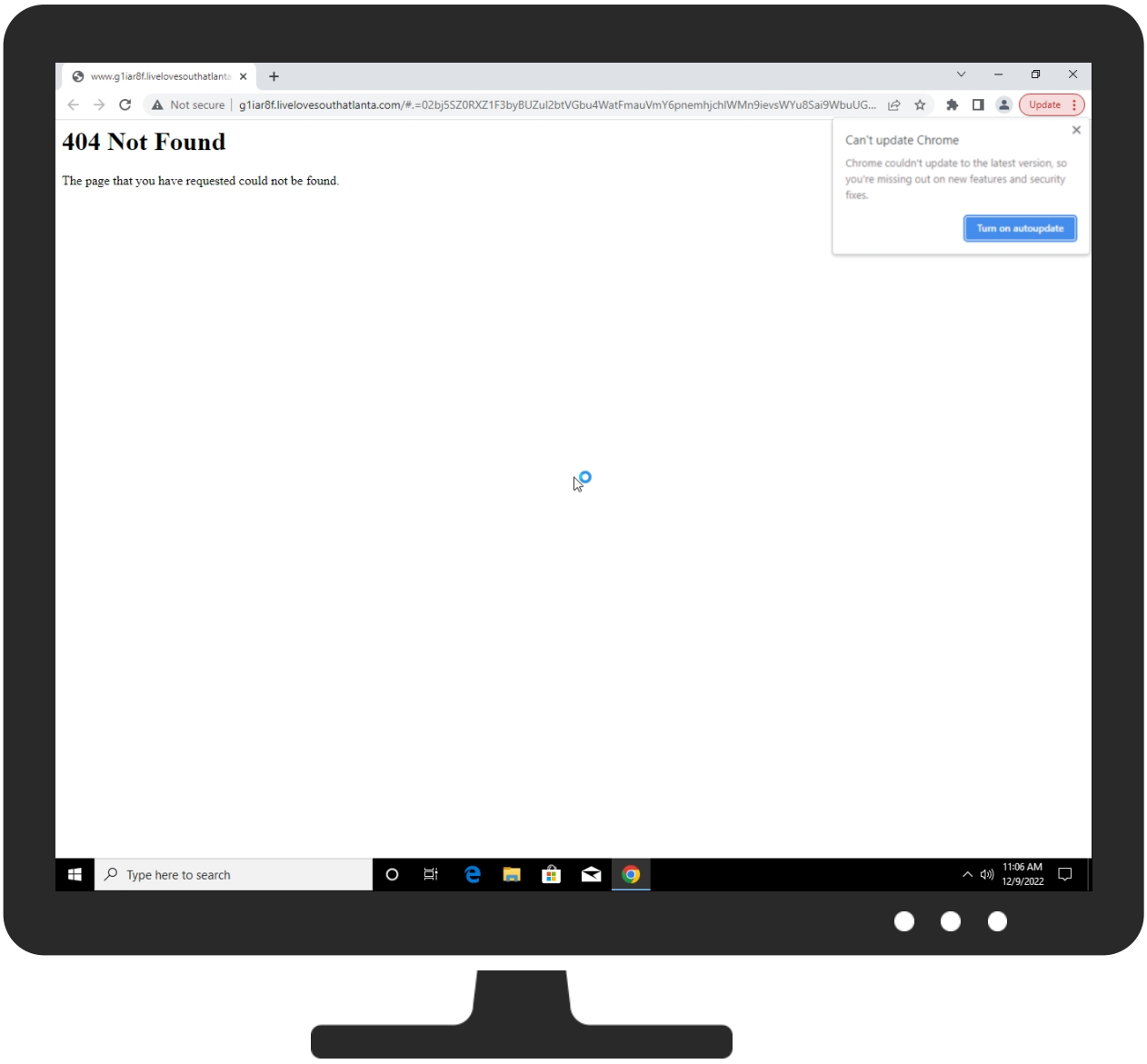
Behavior Graph



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://www.g1iar8f.livelovesouthatlanta.com/#.=02bj5SZ0RXZ1F3byBUZul2btVGbu4WatFmauVmY6pnemhjchIWMn9ievsWYu8Sai9WbuUGbpJ2btxWYi9Gbn5SZt9Ga	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://www.g1iar8f.livelovesouthatlanta.com/	0%	Avira URL Cloud	safe	
http://www.g1iar8f.livelovesouthatlanta.com/favicon.ico	0%	Avira URL Cloud	safe	

Domains and IPs

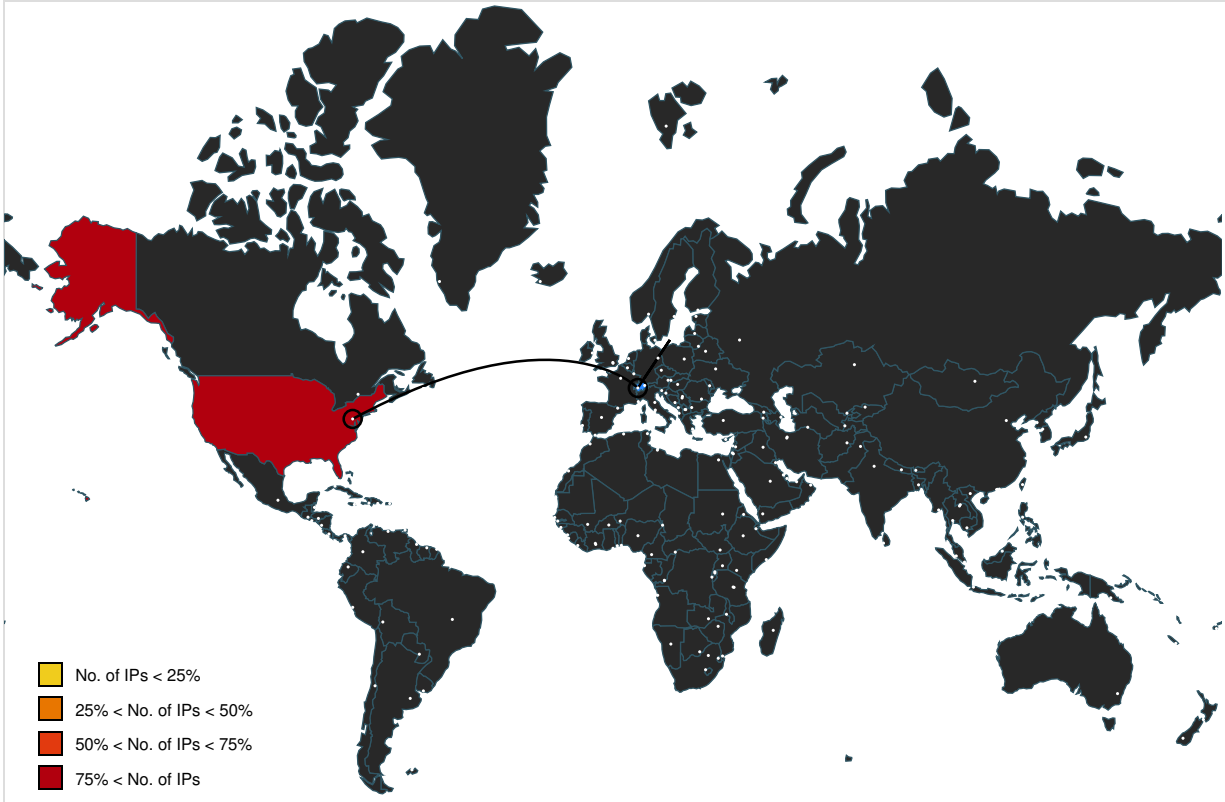
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.250.186.173	true	false		high
www.g1iar8f.livelovesouthatlanta.com	192.185.72.57	true	false		unknown
clients.l.google.com	172.217.18.14	true	false		high
clients2.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.g1iar8f.livelovesouthatlanta.com/	false	• Avira URL Cloud: safe	unknown
http://www.g1iar8f.livelovesouthatlanta.com/#.=02bj5SZ0RXZ1F3byBUZul2btVGbu4WatFmauVmY6pnemhjchlWMn9ievsWYu8Sai9WbuUGbpJ2btxWYi9Gbn5SZt9Ga	false		unknown
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=104.0.5112.102&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
http://www.g1iar8f.livelovesouthatlanta.com/favicon.ico	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.72.57	www.g1iar8f.livelovesouthatlanta.com	United States		46606	UNIFIEDLAYER-AS-1US	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.186.173	accounts.google.com	United States		15169	GOOGLEUS	false
172.217.18.14	clients.l.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:	764047
Start date and time:	2022-12-09 11:06:24 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Sample URL:	http://www.g1iar8f.livelovesouthatlanta.com/#.=02bj5SZ0RXZ1F3byBUZul2btVGbu4WatFmauVmY6pnemhjchlWMn9ievsWYu8Sai9WbuUGbpJ2btxWYi9Gbn5SZt9Ga
Analysis system description:	Windows 10 64 bit version 1909 (MS Office 2019, IE 11, Chrome 104, Firefox 88, Adobe Reader DC 21, Java 8 u291, 7-Zip)
Number of analysed new started processes analysed:	10
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@21/0@4/6
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): SgrmBroker.exe, usocoreworker.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 142.250.185.67, 34.104.35.123
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, edgedl.me.gvt1.com, login.live.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

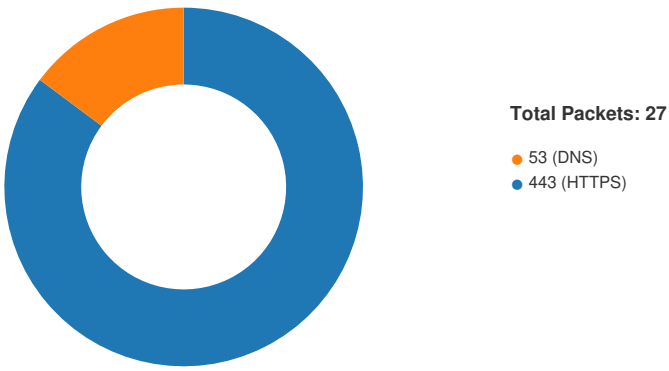
No created / dropped files found

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 11:06:53.412899971 CET	49691	443	192.168.2.3	142.250.186.173
Dec 9, 2022 11:06:53.412976027 CET	443	49691	142.250.186.173	192.168.2.3
Dec 9, 2022 11:06:53.413065910 CET	49691	443	192.168.2.3	142.250.186.173
Dec 9, 2022 11:06:53.413753033 CET	49691	443	192.168.2.3	142.250.186.173
Dec 9, 2022 11:06:53.413789034 CET	443	49691	142.250.186.173	192.168.2.3
Dec 9, 2022 11:06:53.421082973 CET	49693	443	192.168.2.3	172.217.18.14

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 11:06:53.421123028 CET	443	49693	172.217.18.14	192.168.2.3
Dec 9, 2022 11:06:53.421212912 CET	49693	443	192.168.2.3	172.217.18.14
Dec 9, 2022 11:06:53.421477079 CET	49693	443	192.168.2.3	172.217.18.14
Dec 9, 2022 11:06:53.421490908 CET	443	49693	172.217.18.14	192.168.2.3
Dec 9, 2022 11:06:53.498603106 CET	443	49693	172.217.18.14	192.168.2.3
Dec 9, 2022 11:06:53.505534887 CET	443	49691	142.250.186.173	192.168.2.3
Dec 9, 2022 11:06:53.539304018 CET	49693	443	192.168.2.3	172.217.18.14
Dec 9, 2022 11:06:53.540966988 CET	49693	443	192.168.2.3	172.217.18.14
Dec 9, 2022 11:06:53.540981054 CET	443	49693	172.217.18.14	192.168.2.3
Dec 9, 2022 11:06:53.542150021 CET	49691	443	192.168.2.3	142.250.186.173
Dec 9, 2022 11:06:53.542208910 CET	443	49691	142.250.186.173	192.168.2.3
Dec 9, 2022 11:06:53.542548895 CET	443	49693	172.217.18.14	192.168.2.3
Dec 9, 2022 11:06:53.542665958 CET	49693	443	192.168.2.3	172.217.18.14
Dec 9, 2022 11:06:53.543346882 CET	49694	80	192.168.2.3	192.185.72.57
Dec 9, 2022 11:06:53.545958042 CET	443	49693	172.217.18.14	192.168.2.3
Dec 9, 2022 11:06:53.546044111 CET	49693	443	192.168.2.3	172.217.18.14
Dec 9, 2022 11:06:53.546097040 CET	443	49691	142.250.186.173	192.168.2.3
Dec 9, 2022 11:06:53.546185970 CET	49691	443	192.168.2.3	142.250.186.173
Dec 9, 2022 11:06:53.662862062 CET	80	49694	192.185.72.57	192.168.2.3
Dec 9, 2022 11:06:53.663049936 CET	49694	80	192.168.2.3	192.185.72.57
Dec 9, 2022 11:06:53.663376093 CET	49694	80	192.168.2.3	192.185.72.57
Dec 9, 2022 11:06:53.782907009 CET	80	49694	192.185.72.57	192.168.2.3
Dec 9, 2022 11:06:53.868274927 CET	80	49694	192.185.72.57	192.168.2.3
Dec 9, 2022 11:06:53.869252920 CET	49693	443	192.168.2.3	172.217.18.14
Dec 9, 2022 11:06:53.869282961 CET	443	49693	172.217.18.14	192.168.2.3
Dec 9, 2022 11:06:53.869401932 CET	49693	443	192.168.2.3	172.217.18.14
Dec 9, 2022 11:06:53.869410038 CET	443	49693	172.217.18.14	192.168.2.3
Dec 9, 2022 11:06:53.869519949 CET	443	49693	172.217.18.14	192.168.2.3
Dec 9, 2022 11:06:53.872556925 CET	49691	443	192.168.2.3	142.250.186.173
Dec 9, 2022 11:06:53.872627020 CET	443	49691	142.250.186.173	192.168.2.3
Dec 9, 2022 11:06:53.872661114 CET	49691	443	192.168.2.3	142.250.186.173
Dec 9, 2022 11:06:53.872675896 CET	443	49691	142.250.186.173	192.168.2.3
Dec 9, 2022 11:06:53.872961998 CET	443	49691	142.250.186.173	192.168.2.3
Dec 9, 2022 11:06:53.899290085 CET	443	49693	172.217.18.14	192.168.2.3
Dec 9, 2022 11:06:53.899382114 CET	49693	443	192.168.2.3	172.217.18.14
Dec 9, 2022 11:06:53.899405003 CET	443	49693	172.217.18.14	192.168.2.3
Dec 9, 2022 11:06:53.899554014 CET	443	49693	172.217.18.14	192.168.2.3
Dec 9, 2022 11:06:53.899614096 CET	49693	443	192.168.2.3	172.217.18.14
Dec 9, 2022 11:06:53.906086922 CET	49693	443	192.168.2.3	172.217.18.14
Dec 9, 2022 11:06:53.906110048 CET	443	49693	172.217.18.14	192.168.2.3
Dec 9, 2022 11:06:53.909457922 CET	49694	80	192.168.2.3	192.185.72.57
Dec 9, 2022 11:06:53.912466049 CET	49691	443	192.168.2.3	142.250.186.173
Dec 9, 2022 11:06:53.912518978 CET	443	49691	142.250.186.173	192.168.2.3
Dec 9, 2022 11:06:53.921487093 CET	443	49691	142.250.186.173	192.168.2.3
Dec 9, 2022 11:06:53.921619892 CET	49691	443	192.168.2.3	142.250.186.173
Dec 9, 2022 11:06:53.921650887 CET	443	49691	142.250.186.173	192.168.2.3
Dec 9, 2022 11:06:53.921935081 CET	443	49691	142.250.186.173	192.168.2.3
Dec 9, 2022 11:06:53.922022104 CET	49691	443	192.168.2.3	142.250.186.173
Dec 9, 2022 11:06:53.943238020 CET	49691	443	192.168.2.3	142.250.186.173
Dec 9, 2022 11:06:53.943298101 CET	443	49691	142.250.186.173	192.168.2.3
Dec 9, 2022 11:06:54.448055983 CET	49694	80	192.168.2.3	192.185.72.57
Dec 9, 2022 11:06:54.567329884 CET	80	49694	192.185.72.57	192.168.2.3
Dec 9, 2022 11:06:54.580435038 CET	80	49694	192.185.72.57	192.168.2.3
Dec 9, 2022 11:06:54.706752062 CET	49694	80	192.168.2.3	192.185.72.57
Dec 9, 2022 11:06:59.581233978 CET	80	49694	192.185.72.57	192.168.2.3
Dec 9, 2022 11:06:59.581343889 CET	49694	80	192.168.2.3	192.185.72.57
Dec 9, 2022 11:07:00.763979912 CET	49694	80	192.168.2.3	192.185.72.57
Dec 9, 2022 11:07:00.883883953 CET	80	49694	192.185.72.57	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 11:06:53.300400972 CET	53954	53	192.168.2.3	1.1.1.1
Dec 9, 2022 11:06:53.302572966 CET	56286	53	192.168.2.3	1.1.1.1
Dec 9, 2022 11:06:53.304286003 CET	52420	53	192.168.2.3	1.1.1.1
Dec 9, 2022 11:06:53.319915056 CET	53	53954	1.1.1.1	192.168.2.3
Dec 9, 2022 11:06:53.322498083 CET	53	52420	1.1.1.1	192.168.2.3
Dec 9, 2022 11:06:53.529401064 CET	53	56286	1.1.1.1	192.168.2.3
Dec 9, 2022 11:06:54.446341991 CET	50150	53	192.168.2.3	1.1.1.1
Dec 9, 2022 11:06:54.673108101 CET	53	50150	1.1.1.1	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Dec 9, 2022 11:06:53.300400972 CET	192.168.2.3	1.1.1.1	0x49de	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Dec 9, 2022 11:06:53.302572966 CET	192.168.2.3	1.1.1.1	0x876	Standard query (0)	www.g1iar8f.livelovesouthatlanta.com	A (IP address)	IN (0x0001)	false
Dec 9, 2022 11:06:53.304286003 CET	192.168.2.3	1.1.1.1	0x9ec5	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Dec 9, 2022 11:06:54.446341991 CET	192.168.2.3	1.1.1.1	0x6e45	Standard query (0)	www.g1iar8f.livelovesouthatlanta.com	A (IP address)	IN (0x0001)	false

DNS Answers

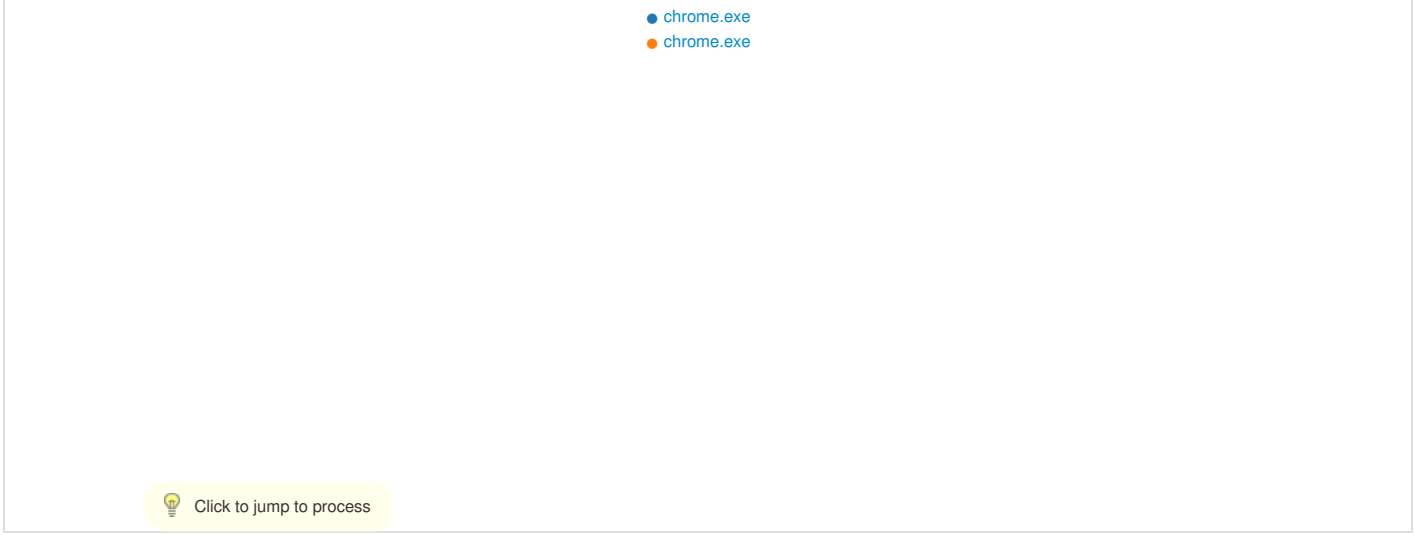
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Dec 9, 2022 11:06:53.319915056 CET	1.1.1.1	192.168.2.3	0x49de	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Dec 9, 2022 11:06:53.319915056 CET	1.1.1.1	192.168.2.3	0x49de	No error (0)	clients.l.google.com		172.217.18.14	A (IP address)	IN (0x0001)	false
Dec 9, 2022 11:06:53.322498083 CET	1.1.1.1	192.168.2.3	0x9ec5	No error (0)	accounts.google.com		142.250.186.173	A (IP address)	IN (0x0001)	false
Dec 9, 2022 11:06:53.529401064 CET	1.1.1.1	192.168.2.3	0x876	No error (0)	www.g1iar8f.livelovesouthatlanta.com		192.185.72.57	A (IP address)	IN (0x0001)	false
Dec 9, 2022 11:06:54.673108101 CET	1.1.1.1	192.168.2.3	0x6e45	No error (0)	www.g1iar8f.livelovesouthatlanta.com		192.185.72.57	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- www.g1iar8f.livelovesouthatlanta.com

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 5496, Parent PID: 5548

General

Target ID:	0
Start time:	11:06:50
Start date:	09/12/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument http://www.g1iar8f.livelovesouthatlanta.com/#.=02bj5SZ0RXZ1F3byBUZul2btVGbu4WatFmauVmY6pnemhjchlWMn9ievsWYu8Sai9WbuUGbpJ2btxWYi9Gbn5SZt9Ga
Imagebase:	0x7ff6566b0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
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

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: chrome.exe PID: 3552, Parent PID: 5496

General	
Target ID:	1
Start time:	11:06:51
Start date:	09/12/2022
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=2036 --field-trial-handle=1764,i,13192198239046418531,5295402104946012676,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6566b0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
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

Disassembly

No disassembly