ID: 831167
Cookbook: browseurl.jbs
Time: 07:31:23
Date: 21/03/2023
Version: 37.0.0 Beryl

Table of Contents

Directory Created	12
Permission Modified	12

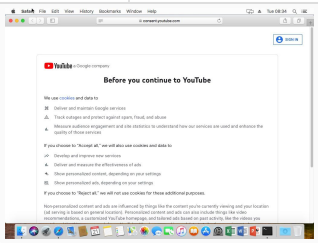
macOS Analysis Report

https://www.youtube.com/channel/UCAuerig2N-RZWJT8x75V9yw

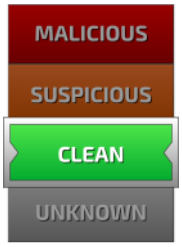
Overview

General Information

Sample URL:	http://https://www.youtube.com/channel/UCAuerig2N-RZWJT8x75V9yw
Analysis ID:	831167
Infos:	



Detection

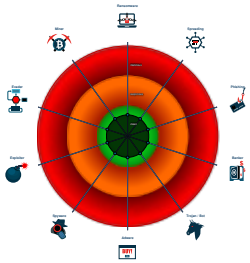


Score:	1
Range:	0 - 100
Whitelisted:	false

Signatures

- Writes 64-bit Mach-O files to disk
- Reads launchservices plist files

Classification



General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	831167
Start date and time:	2023-03-21 07:31:23 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://www.youtube.com/channel/UCAuerig2N-RZWJT8x75V9yw
Analysis system description:	Virtual Machine, High Sierra (Office 2016 16.16, Java 11.0.2+9, Adobe Reader 2019.010.20099)
Analysis Mode:	default
Detection:	CLEAN
Classification:	clean1.mac@0/10@4/0

Warnings

Process Tree

- **System is macvm-highsierra**
- mono-sgen32 New Fork (PID: 878, Parent: 812)
  - open (MD5: 40ed6d8f35c9f20484b97582d296398f) Arguments:
- xpcproxy New Fork (PID: 879, Parent: 1)
  - Safari (MD5: 8e18be737fe87f19fe7a97b4821e2005) Arguments: /Applications/Safari.app/Contents/MacOS/Safari
- **cleanup**

Yara Signatures

No yara matches

Snort Signatures

No Snort rule has matched

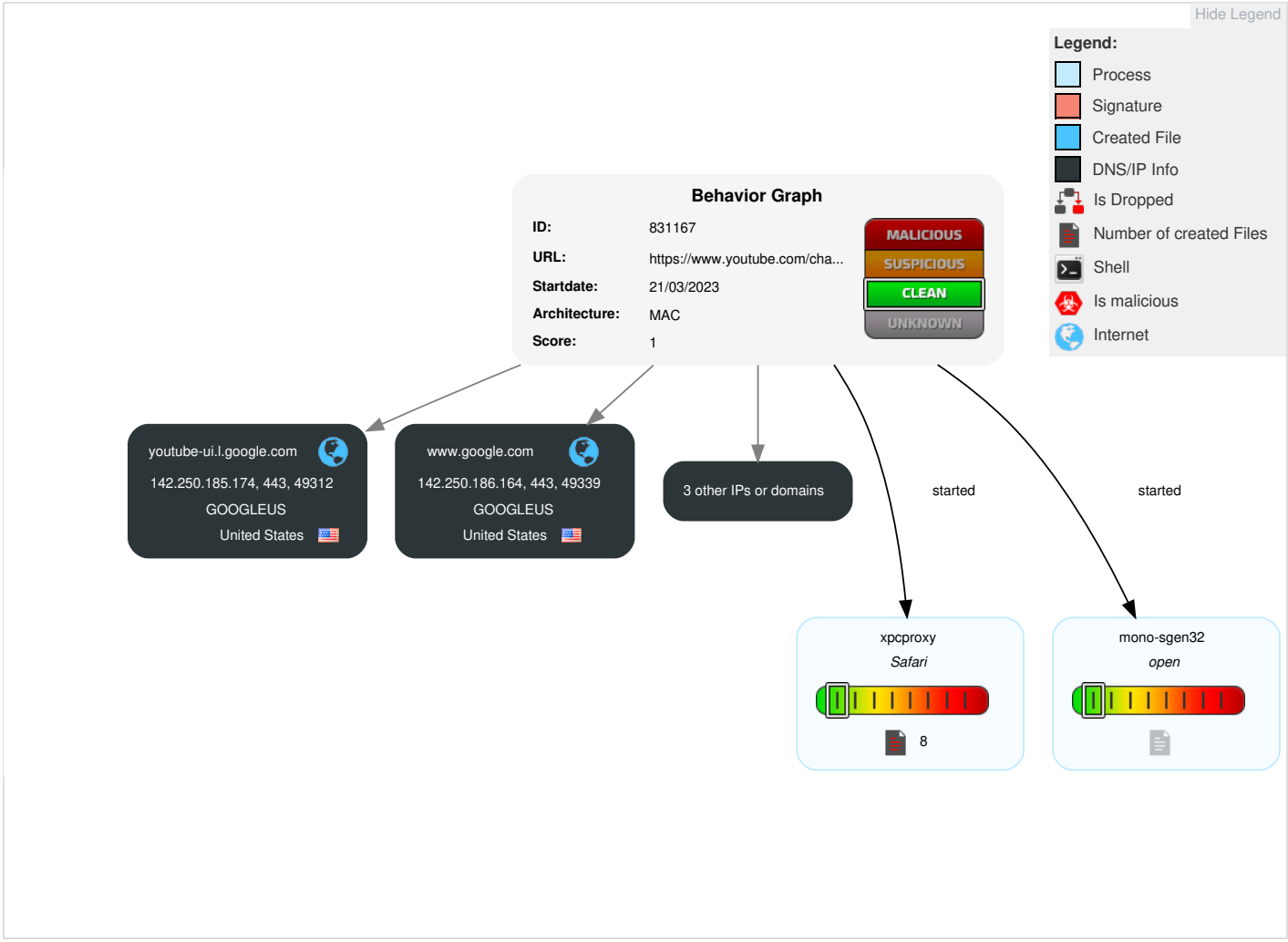
Joe Sandbox Signatures

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	1 Plist Modification	1 Plist Modification	Direct Volume Access	OS Credential Dumping	1 1 System Information 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	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

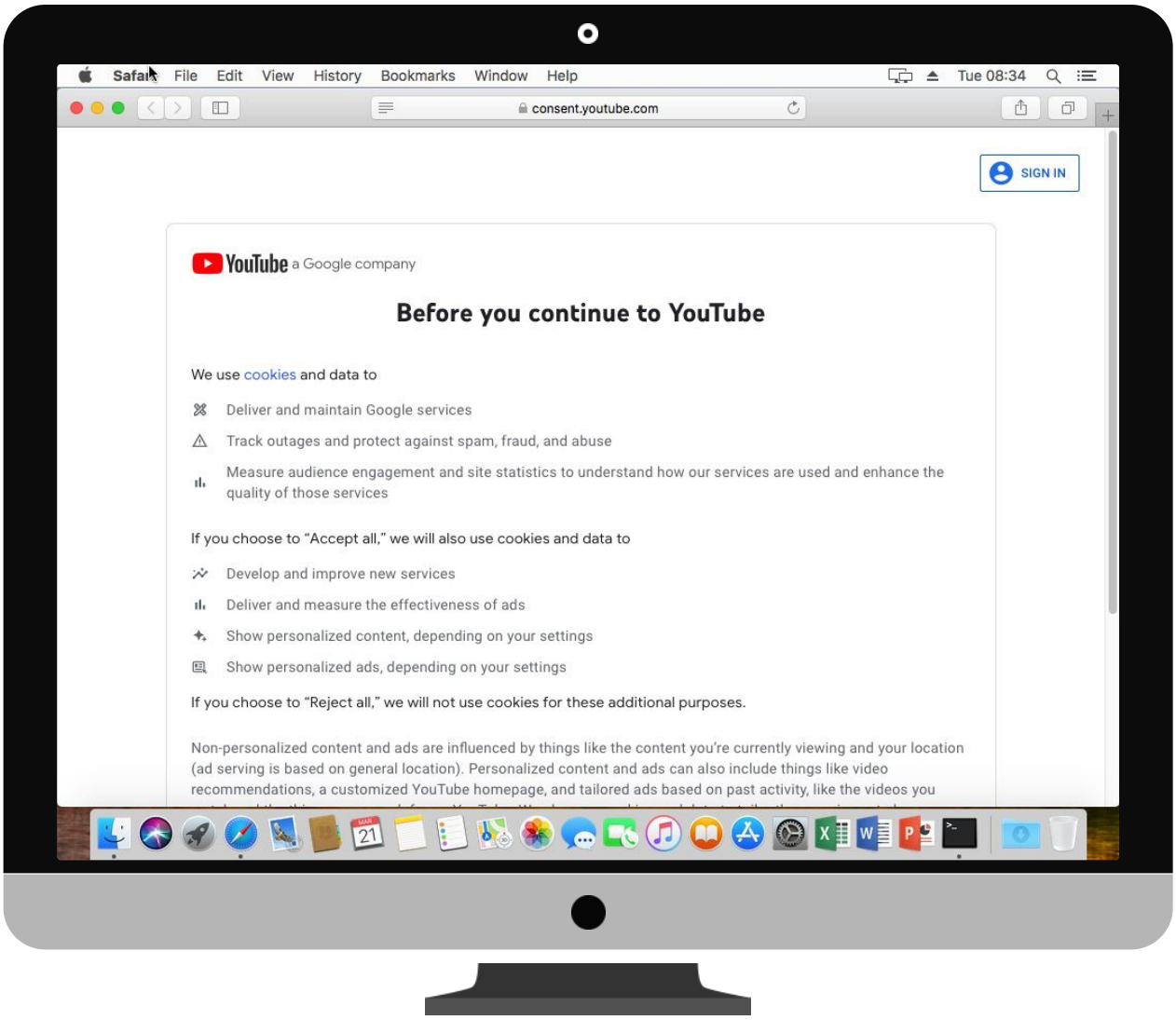
Behavior Graph



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://https://www.youtube.com/channel/UCAuerig2N-RZWJT8x75V9yw	0%	Avira URL Cloud	safe	
http://https://www.youtube.com/channel/UCAuerig2N-RZWJT8x75V9yw	0%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

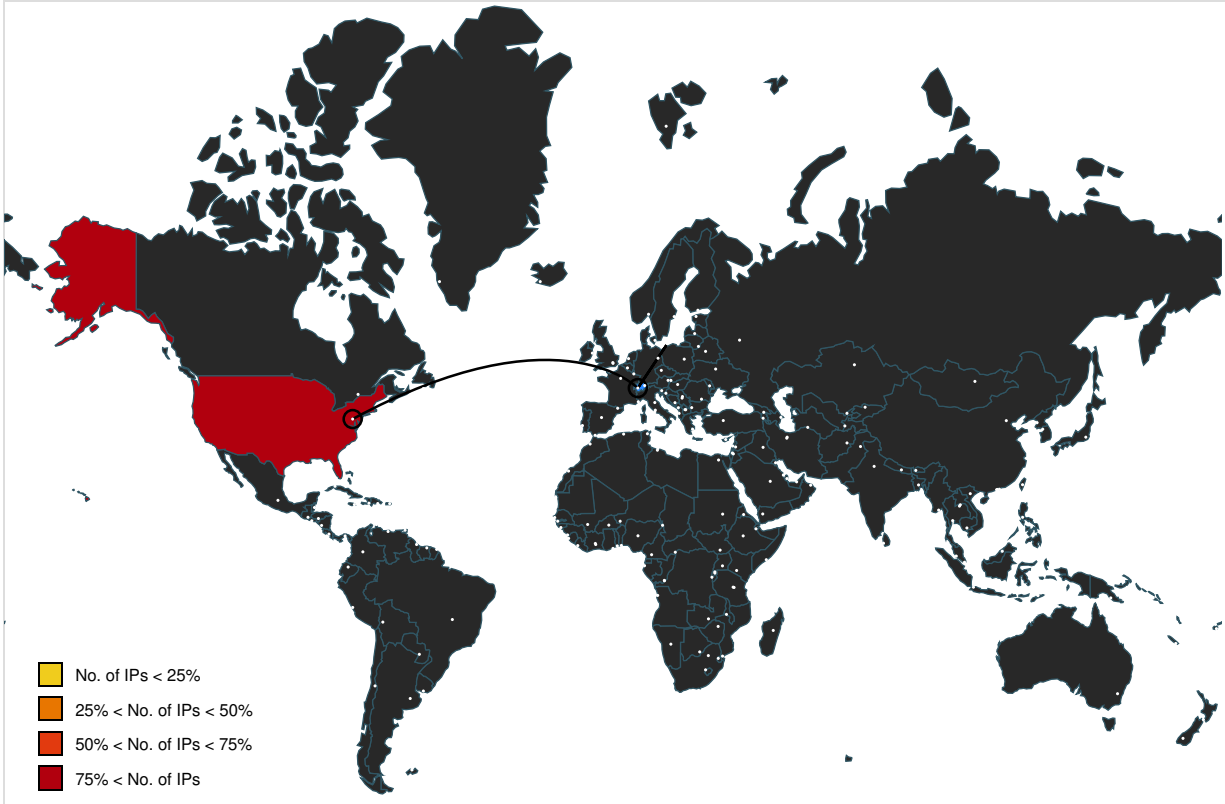
Name	IP	Active	Malicious	Antivirus Detection	Reputation
youtube-ui.l.google.com	142.250.185.174	true	false		high
play.google.com	172.217.16.142	true	false		high
gateway.fe.apple-dns.net	17.248.248.15	true	false		unknown
consent.youtube.com	172.217.16.206	true	false		high
www.google.com	142.250.186.164	true	false		high
www.youtube.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.youtube.com/channel/UCAuerig2N-RZWJT8x75V9yw	false		high
http://https://play.google.com/log?format=json&hasfast=true	false		high
http://https://consent.youtube.com/_/ConsentUi/browserinfo?f.sid=6542961051346440918&bl=boq_identityfrontenduiserver_20230314.06_p1&hl=en&gl=GB&_reqid=30759&rt=j	false		high
http://https://play.google.com/log?format=json&hasfast=true&authuser=0	false		high
http://https://consent.youtube.com/m?continue=https%3A%2F%2Fwww.youtube.com%2Fchannel%2FUCAuerig2N-RZWJT8x75V9yw%3Fcbrd%3D1&gl=GB&m=0&pc=yt&cm=2&hl=en&src=1	false		high
http://https://www.google.com/favicon.ico	false		high
http://https://consent.youtube.com/_/ConsentUi/browserinfo?f.sid=6542961051346440918&bl=boq_identityfrontenduiserver_20230314.06_p1&hl=en&gl=GB&_reqid=130759&rt=j	false		high

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.185.174	youtube-ui.l.google.com	United States		15169	GOOGLEUS	false
172.217.16.206	consent.youtube.com	United States		15169	GOOGLEUS	false
142.250.186.164	www.google.com	United States		15169	GOOGLEUS	false
172.217.16.142	play.google.com	United States		15169	GOOGLEUS	false

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/Users/berri/Library/Safari/.dat.nosync036f.TyISu0

/Users/berri/Library/Safari/Favicon Cache/favicons/.dat.nosync036f.pdcdlR

/Users/berri/Library/WebKit/com.apple.Safari/WebsiteData/ResourceLoadStatistics/full_browsing_session_resourceLog.plist

/dev/null

/private/var/folders/ql/8wfqxrtx52n95h35b6cz4nyw0000gn/0/SafariFamily/Safari/.dat.nosync036f.Pk6yS5

/private/var/folders/ql/8wfqxrtx52n95h35b6cz4nyw0000gn/C/mds/mdsDirectory.db_

/private/var/folders/ql/8wfqxrtx52n95h35b6cz4nyw0000gn/C/mds/mdsObject.db_

/private/var/tmp/NSCreateObjectFileImageFromMemory-GLnGst

/private/var/tmp/NSCreateObjectFileImageFromMemory-TphzPP

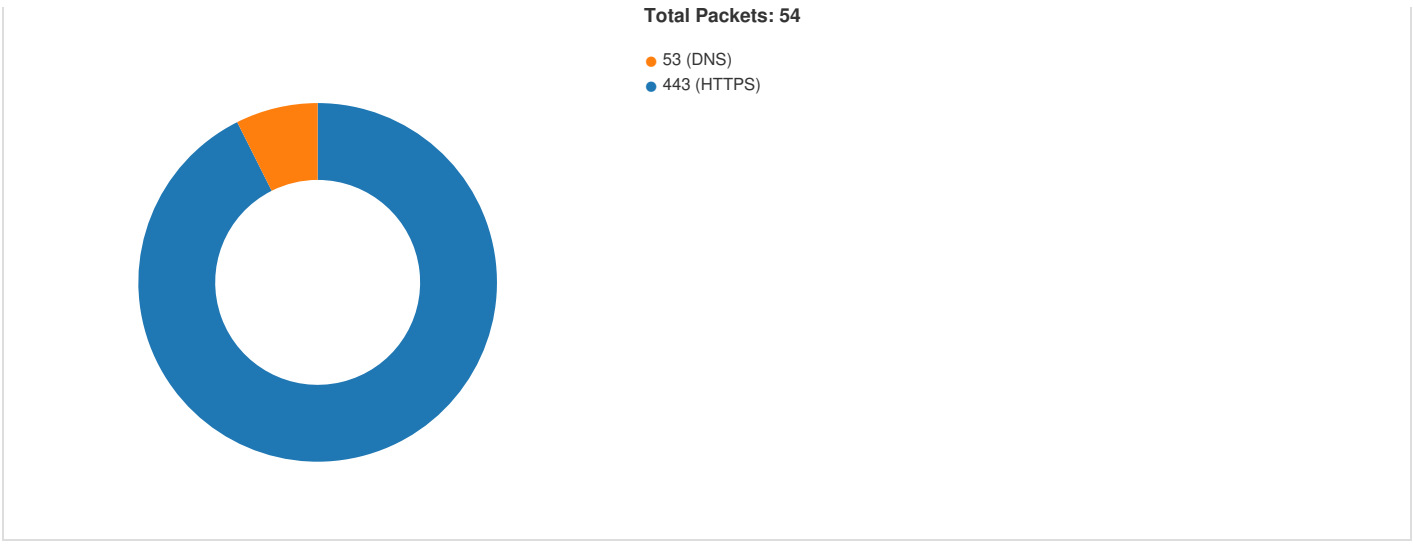
/private/var/tmp/NSCreateObjectFileImageFromMemory-cKdWhB

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 21, 2023 07:32:35.167781115 CET	192.168.11.11	1.1.1.1	0x1dd0	Standard query (0)	www.youtube.com	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:32:35.384959936 CET	192.168.11.11	1.1.1.1	0xf18c	Standard query (0)	consent.youtube.com	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:32:36.907757998 CET	192.168.11.11	1.1.1.1	0x76c1	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:32:37.051582098 CET	192.168.11.11	1.1.1.1	0xe855	Standard query (0)	play.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
Mar 21, 2023 07:32:33.042762041 CET	1.1.1.1	192.168.11.11	0x74a4	No error (0)	gateway.fe.apple-dns.net		17.248.248.15	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:32:33.042762041 CET	1.1.1.1	192.168.11.11	0x74a4	No error (0)	gateway.fe.apple-dns.net		17.248.145.233	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:32:33.042762041 CET	1.1.1.1	192.168.11.11	0x74a4	No error (0)	gateway.fe.apple-dns.net		17.248.145.82	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:32:33.042762041 CET	1.1.1.1	192.168.11.11	0x74a4	No error (0)	gateway.fe.apple-dns.net		17.248.145.83	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:32:33.042762041 CET	1.1.1.1	192.168.11.11	0x74a4	No error (0)	gateway.fe.apple-dns.net		17.248.145.102	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:32:33.042762041 CET	1.1.1.1	192.168.11.11	0x74a4	No error (0)	gateway.fe.apple-dns.net		17.248.145.208	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:32:33.042762041 CET	1.1.1.1	192.168.11.11	0x74a4	No error (0)	gateway.fe.apple-dns.net		17.248.248.17	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:32:33.042762041 CET	1.1.1.1	192.168.11.11	0x74a4	No error (0)	gateway.fe.apple-dns.net		17.248.182.204	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:32:35.177141905 CET	1.1.1.1	192.168.11.11	0x1dd0	No error (0)	www.youtube.com	youtube-ui.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 21, 2023 07:32:35.177141905 CET	1.1.1.1	192.168.11.11	0x1dd0	No error (0)	youtube-ui.l.google.com		142.250.185.174	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:32:35.177141905 CET	1.1.1.1	192.168.11.11	0x1dd0	No error (0)	youtube-ui.l.google.com		216.58.212.174	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 21, 2023 07:32:35.177141905 CET	1.1.1.1	192.168.11.11	0x1dd0	No error (0)	youtube-ui.l.google.com		142.250.185.110	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:32:35.177141905 CET	1.1.1.1	192.168.11.11	0x1dd0	No error (0)	youtube-ui.l.google.com		172.217.18.14	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:32:35.177141905 CET	1.1.1.1	192.168.11.11	0x1dd0	No error (0)	youtube-ui.l.google.com		142.250.186.110	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:32:35.177141905 CET	1.1.1.1	192.168.11.11	0x1dd0	No error (0)	youtube-ui.l.google.com		142.250.186.78	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:32:35.177141905 CET	1.1.1.1	192.168.11.11	0x1dd0	No error (0)	youtube-ui.l.google.com		142.250.185.78	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:32:35.177141905 CET	1.1.1.1	192.168.11.11	0x1dd0	No error (0)	youtube-ui.l.google.com		172.217.23.110	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:32:35.177141905 CET	1.1.1.1	192.168.11.11	0x1dd0	No error (0)	youtube-ui.l.google.com		142.250.181.238	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:32:35.177141905 CET	1.1.1.1	192.168.11.11	0x1dd0	No error (0)	youtube-ui.l.google.com		142.250.184.238	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:32:35.177141905 CET	1.1.1.1	192.168.11.11	0x1dd0	No error (0)	youtube-ui.l.google.com		142.250.185.206	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:32:35.177141905 CET	1.1.1.1	192.168.11.11	0x1dd0	No error (0)	youtube-ui.l.google.com		172.217.16.206	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:32:35.177141905 CET	1.1.1.1	192.168.11.11	0x1dd0	No error (0)	youtube-ui.l.google.com		142.250.186.174	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:32:35.177141905 CET	1.1.1.1	192.168.11.11	0x1dd0	No error (0)	youtube-ui.l.google.com		142.250.185.142	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:32:35.177141905 CET	1.1.1.1	192.168.11.11	0x1dd0	No error (0)	youtube-ui.l.google.com		142.250.184.206	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:32:35.177141905 CET	1.1.1.1	192.168.11.11	0x1dd0	No error (0)	youtube-ui.l.google.com		172.217.16.142	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:32:35.394527912 CET	1.1.1.1	192.168.11.11	0xf18c	No error (0)	consent.youtube.com		172.217.16.206	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:32:36.917454958 CET	1.1.1.1	192.168.11.11	0x76c1	No error (0)	www.google.com		142.250.186.164	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:32:37.060633898 CET	1.1.1.1	192.168.11.11	0xe855	No error (0)	play.google.com		172.217.16.142	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.youtube.com
- consent.youtube.com
- https:
  - www.google.com
  - play.google.com

System Behavior

Analysis Process: mono-sgen32 PID: **878**, Parent PID: **812**

General	
Start time:	07:32:29
Start date:	21/03/2023
Path:	/Library/Frameworks/Mono.framework/Versions/4.4.2/bin/mono-sgen32
Arguments:	n/a
File size:	3722408 bytes
MD5 hash:	8910349f44a940d8d79318367855b236

Analysis Process: open PID: **878**, Parent PID: **812**

General	
Start time:	07:32:29
Start date:	21/03/2023
Path:	/usr/bin/open
Arguments:	
File size:	105952 bytes
MD5 hash:	40ed6d8f35c9f20484b97582d296398f

File Activities

- **File Read**
- **Directory Enumerated**

Analysis Process: xpcproxy PID: **879**, Parent PID: **1**

General	
Start time:	07:32:29
Start date:	21/03/2023
Path:	/usr/libexec/xpcproxy
Arguments:	n/a
File size:	43488 bytes
MD5 hash:	d1bb9a4899f0af921e8188218b20d744

File Activities

- **File Read**
- **Directory Created**

Analysis Process: Safari PID: **879**, Parent PID: **1**

General	
Start time:	07:32:29
Start date:	21/03/2023
Path:	/Applications/Safari.app/Contents/MacOS/Safari
Arguments:	/Applications/Safari.app/Contents/MacOS/Safari
File size:	20896 bytes
MD5 hash:	8e18be737fe87f19fe7a97b4821e2005

File Activities

- **File Created**
- **File Deleted**
- **File Read**
- **File Written**
- **File Moved**
- **Directory Enumerated**
- **Directory Attributes Enumerated Bulk**
- **Directory Created**
- **Permission Modified**