ID: 791296
Cookbook: browseurl.jbs
Time: 09:42:25
Date: 25/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report https://listfoo.org/zmg5f 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 9
Public IPs 9
Private 9
General Information 9
Warnings 10
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASNs 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 11
Static File Info 11
Network Behavior 11
Network Port Distribution 11
TCP Packets 11
UDP Packets 13
DNS Queries 13
DNS Answers 14
HTTP Request Dependency Graph 14
Statistics 15
Behavior 15
System Behavior 15
Analysis Process: chrome.exePID: 5112, Parent PID: 3696 15
General 15
File Activities 15
Registry Activities 15
Analysis Process: chrome.exePID: 4136, Parent PID: 5112 15
General 15
File Activities 16
Analysis Process: chrome.exePID: 6288, Parent PID: 3696 16
General 16
Registry Activities 16
Disassembly 16

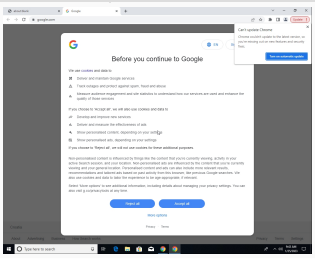
Windows Analysis Report

https://listfoo.org/zmg5f

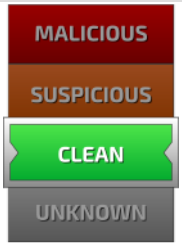
Overview

General Information

Sample URL:	http://https://listfoo.org/zmg5f
Analysis ID:	791296
Infos:	



Detection

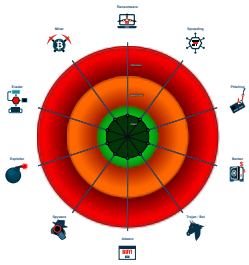


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64
- chrome.exe (PID: 5112 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 4136 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=1972 --field-trial-handle=1772,i,13714808044369432181,11901859910510463980,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 6288 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://listfoo.org/zmg5f 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

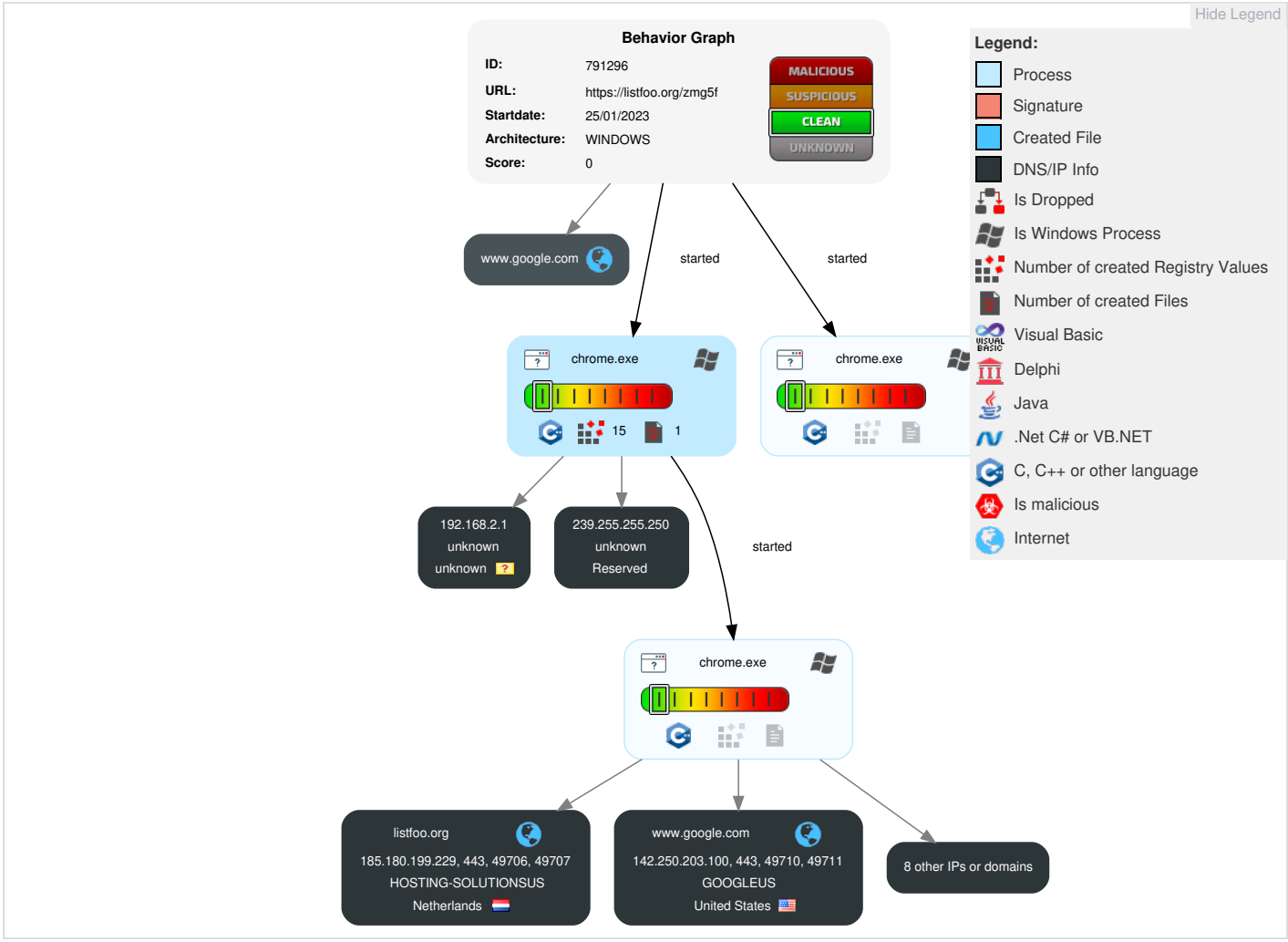
Joe Sandbox Signatures

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

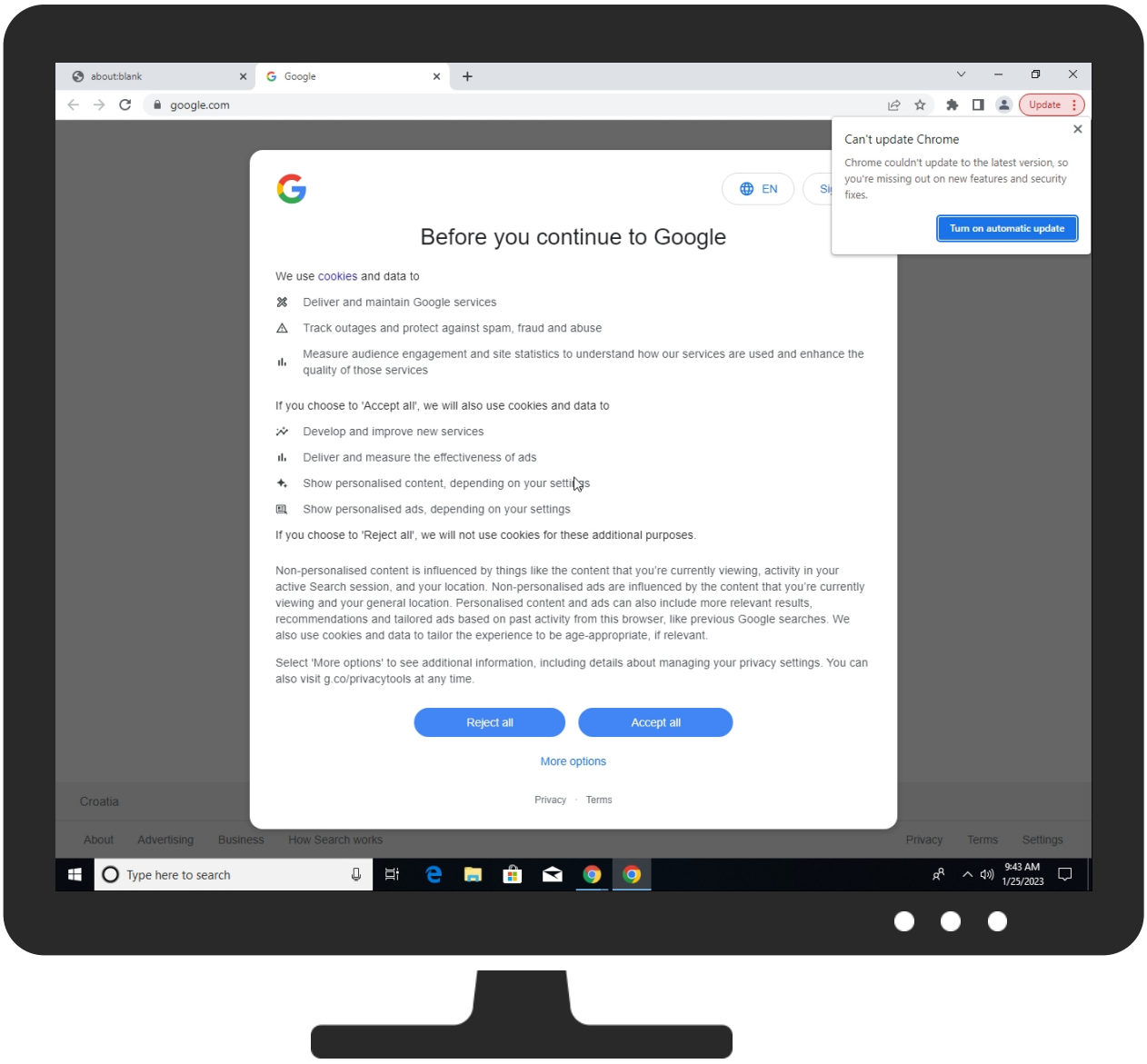
Behavior Graph



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://listfoo.org/zmg5f	0%	Virustotal		Browse
http://https://listfoo.org/zmg5f	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://listfoo.org/favicon.ico	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
google.com	172.217.168.14	true	false		high
consent.google.com	216.58.215.238	true	false		high
accounts.google.com	142.250.203.109	true	false		high
plus.l.google.com	172.217.168.78	true	false		high
listfoo.org	185.180.199.229	true	false		unknown
www.google.com	142.250.203.100	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
clients2.google.com	unknown	unknown	false		high
apis.google.com	unknown	unknown	false		high

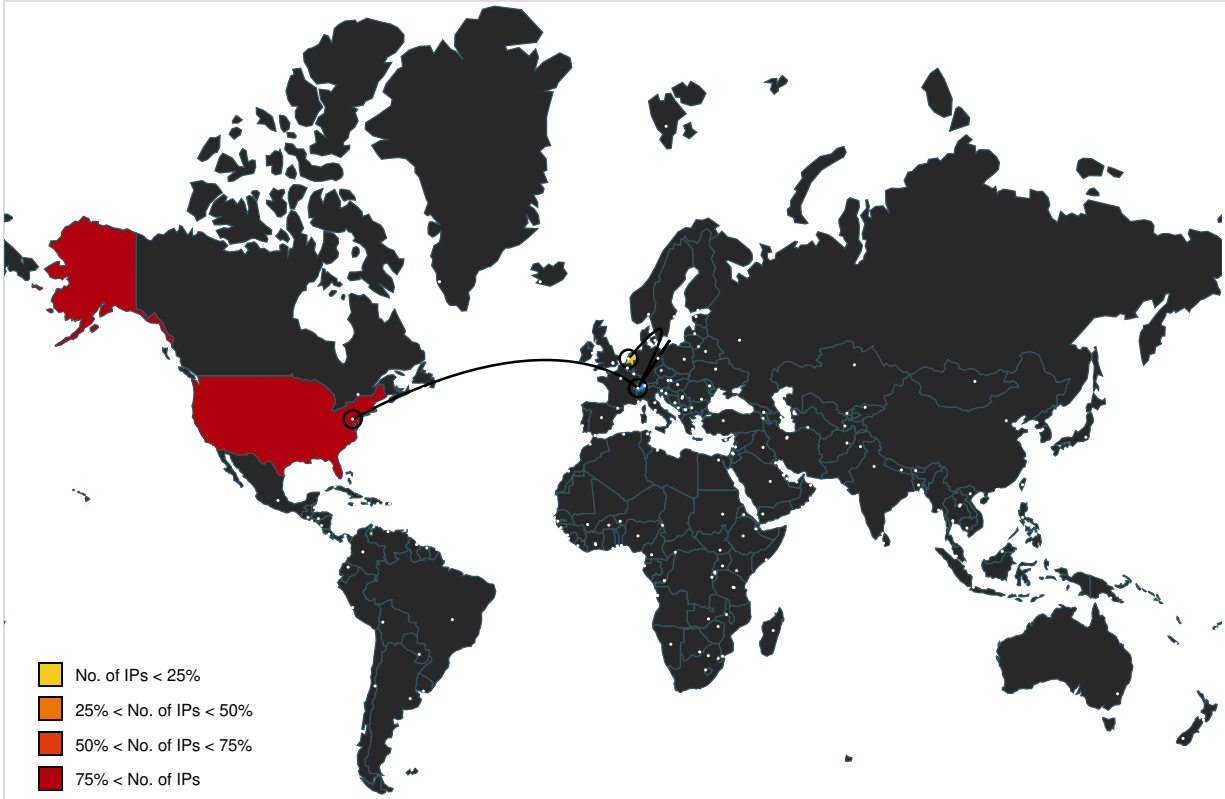
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.google.com/gen_204?atyp=i&ct=bxjs&cad=&b=0&ei=ruvQY6uHDeSP9u8PlpqO-Ak&zx=1674636206145	false		high
http://https://www.google.com/	false		high
http://https://www.google.com/manifest?pwa=webhp	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://www.google.com/gen_204?s=webhp&t=aft&atyp=csi&ei=ruvQY6uHDeSP9u8PlpqO-Ak&rt=wsrt.486,aft.423,afti.423,prt.322&wh=913&imn=3&ima=3&imad=0&imac=0&aftp=913&bl=m-wt	false		high
http://https://www.google.com/client_204?cs=1	false		high
http://https://www.google.com/images/branding/googlelogo/1x/googlelogo_color_272x92dp.png	false		high
http://https://www.google.com/gen_204?atyp=i&ct=bxjs&cad=&b=1&ei=ruvQY6uHDeSP9u8PlpqO-Ak&zx=1674636232161	false		high
http://https://listfoo.org/zmg5f	false		unknown
http://https://www.google.com/gen_204?atyp=csi&ei=ruvQY6uHDeSP9u8PlpqO-Ak&s=webhp&t=all&bl=m-wt&wh=913&imn=3&ima=3&imad=0&imac=0&aftp=913&adh=&ime=3&imex=3&imeh=0&imea=0&imeb=0&imel=0&scp=0&net=dl.1300,ect.4g,rtt.100&mem=ujhs.10,tjhs.11,jhsl.2173,dm.8&sys=hc.4&rt=aft.423,afti.423,prt.322,dcl.327,aftqf.424,ol.904,xjsls.26226,xjses.26870,xjsee.26920,xjs.26921,lcp.356,fcp.193,wsrt.486,cst.75,dnst.32,rqst.232,rspt.116,sslt.75,rqstt.370,unt.257,cstt.295,dit.813&zx=1674636232860	false		high
http://https://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.WEPncdil2Uw.O/m=gapi_iframes,googleapis_client/rt=j/sv=1/d=1/ed=1/rs=AHpOoo-eOecLLtOXEl3I3kIuMsKXRkDMmA/cb=gapi.loaded_0	false		high
http://https://www.google.com/gen_204?atyp=i&ei=ruvQY6uHDeSP9u8PlpqO-Ak&dt19=2&zx=1674636233492	false		high
http://https://www.google.com/xjs/_/js/k=xjs.s.en_GB.zobC7UqdsqU.O/ck=xjs.s.F0fY5Pm-eS0.L.W.O/am=AAEqCFcAOAAAQAAAAAAkIAAAAAAAAgAwBkDwIA0I2BAOEIMBsCwBIAAgiNEPEQAABgADGBYABAAAAED-AAQ8AQCDCQsAAAAAAAAAELAEweAGCQoCQAAAAAAAAACU0uTFASAIAgAAAQ/d=1/exm=cdos,csi,d,dpf,hsm,jsa/ed=1/dg=2/br=1/rs=ACT90oHWjJk68F8W9qa5QTlNuGD_7xu0jA/ee=Pjplud:PoEs9b;QGR0gd:Mlhmy;uY49fb:COQbmf;EVNhjf:pw70Gc;sTsDMc:kHVSUb;g8nkx:U4MzKc;wQlYve:aLUfP;kbAm9d:MkHyGd;F9mqte:UoRcbe;oUlnpc:RagDlc;YV5bee:IvPZ6d;dtl0hd:lLQWFe;yGxLoc:FmAr0c;dIoSBb:ZgGg9b;pXdRYb:JKoKVe;wR5FRb:TtcOte;KpRAue:Tia57b;aZ61od:arTwJ;JXS8fb:Qj0suc;rQSrae:C6D5Fc;qavrXe:zQzcXe;UDrY1c:eps46d;w3bZCb:ZPGaIb;VGRfx:VFqbr;imqimf:jKGL2e;Np8Qkd:Dpx6qc;BjwMce:cXX2Wb;oGtAuc:sOXFj;NPKaK:PVlQOd;EmZ2Bf:zr1jrb;daB6be:lMxGPd;Fmv9Nc:O1Tzwc;hK67qb:QWEO5b;R4IIlb:QWfeKf;BMxAGc:E5bFse;WDGyFe:jcVOxd;wV5Pjc:L8KGxe;xbe2wc:wbTLEd;DpcR3d:zL72xf;tosKvd:ZCqP3;ESrPQc:mNTJvc;NSEoX:lazG7b;G6wU6e:hezEbd;kCQyJ:ueyPK;okUaUd:wltadb;GleZL:J1A7Od;Xeq57c:wZTUNc;eJZqRc:wUwbse;RiX1h:uiAbXc;oSUNyd:fTfGO;SJsSc:H1GVub;SMDL4c:fTfGO;JsbNhc:Xd8iUd;zOsCQe:Ko78Df;KcokUb:KiuZBf;WCEKNd:l46Hvd;LBgRLc:XVMNvd;LsNahb:ucGLNb;UyG7Kb:wQd0G;TxfV6d:YORN0b;qaS3gd:yiLg6e;aAJE9c:WHW6Ef;BgS6mb:fidj5d;UVmjEd:EesRsb;z97YGf:oug9te;CxXAWb:YyRLvc;VN6jIc:ddQyuf;SLtqO:Kh1xYe;VxQ32b:k0XsBb;DULqB:RKfG5c;bcPXSc:gSZLJb;cFTWae:gT8qnd;gaub4:TN6bMe;hjRo6e:F62sG;whEZac:F4AmNb;qddgKe:x4FYXe;eBAeSb:Ck63tb;vfVwPd:OXTqFb;w9w86d:dt4g2b;lkq0A:Z0MWEf;KQzWid:mB4wNe;pNsl2d:j9Yuyc;eHDfl:ofjVkb;Nyt6ic:jn2sGd;SNUn3:x8cHvb;LEikZe:byfTOb,lsjVmc;io8t5d:sgY6Zb;Oj465e:KG2eXe;sP4Vbe:VwDzFe;kMFpHd:OTA3Ae;nAFL3:s39S4;iFQyKf:QIhFr/m=DhPYme,EkevXb,GU4Gab,MpJwZc,NzU6V,UUJqVe,aa,abd,async,epYOx,pHXghd,q0xTif,s39S4,sOXFj,sb_wiz,sf,sonic,spch?xjs=s1	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://www.google.com/xjs/_/js/k=xjs.s.en_GB.zobC7UqdsqU.O/ck=xjs.s.F0fY5Pm-eS0.L.W.O/am=AAEqCFcAOAAAQAAAAAAkIAAAAAAAAgAwBkDwIA0I2BAOEIMBsCwBIAAgiNEPEQAABgADGBYABAAAAED-AAQ8AQCDCQsAAAAAAAAAELAEweAGCQoCQAAAAAAAAACU0uTFASAIAgAAAQ/d=1/exm=CnSW2d,DPreE,DhPYme,EkevXb,GU4Gab,MpJwZc,NzU6V,UUJqVe,WlNQGd,aa,abd,async,cdos,csi,d,dpf,epYOx,fXO0xe,hsm,jsa,kQvlef,nabPbb,pHXghd,q0xTif,s39S4,sOXFj,sb_wiz,sf,sonic,spch/ed=1/dg=2/br=1/rs=ACT90oHWjJk68F8W9qa5QTlNuGD_7xu0jA/ee=Pjplud:PoEs9b;QGR0gd:Mlhmy;uY49fb:COQbmf;EVNhjf:pw70Gc;sTsDMc:kHVSUb;g8nkx:U4MzKc;wQlYve:aLUfP;kbAm9d:MkHyGd;F9mqte:UoRcbe;oUlnpc:RagDlc;YV5bee:IvPZ6d;dtl0hd:lLQWFe;yGxLoc:FmAr0c;dIoSBb:ZgGg9b;pXdRYb:JKoKVe;wR5FRb:TtcOte;KpRAue:Tia57b;aZ61od:arTwJ;JXS8fb:Qj0suc;rQSrae:C6D5Fc;qavrXe:zQzcXe;UDrY1c:eps46d;w3bZCb:ZPGaIb;VGRfx:VFqbr;imqimf:jKGL2e;Np8Qkd:Dpx6qc;BjwMce:cXX2Wb;oGtAuc:sOXFj;NPKaK:PVlQOd;EmZ2Bf:zr1jrb;daB6be:lMxGPd;Fmv9Nc:O1Tzwc;hK67qb:QWEO5b;R4IIIb:QWfeKf;BMxAGc:E5bFse;WDGyFe:jcVOxd;wV5Pjc:L8KGxe;xbe2wc:wbTLEd;DpcR3d:zL72xf;tosKvd:ZCqP3;ESrPQc:mNTJvc;NSEoX:lazG7b;G6wU6e:hezEbd;kCQyJ:ueyPK;okUaUd:wItadb;GleZL:J1A7Od;Xeq57c:wZTUNc;eJZqRc:wUwbse;RiX1h:uiAbXc;oSUNyd:fTfGO;SJsSc:H1GVub;SMDL4c:fTfGO;JsbNhc:Xd8iUd;zOsCQe:Ko78Df;KcokUb:KiuZBf;WCEKNd:I46Hvd;LBgRLc:XVMNvd;LsNahb:ucGLNb;UyG7Kb:wQd0G;TxfV6d:YORN0b;qaS3gd:yiLg6e;aAJE9c:WHW6Ef;BgS6mb:fidj5d;UVmjEd:EesRsb;z97YGf:oug9te;CxXAWb:YyRLvc;VN6jIc:ddQyuf;SLtqO:Kh1xYe;VxQ32b:k0XsBb;DULqB:RKfG5c;bcPXSc:gSZLJb;cFTWae:gT8qnd;gaub4:TN6bMe;hjRo6e:F62sG;whEZac:F4AmNb;qddgKe:x4FYXe;eBAeSb:Ck63tb;vfVwPd:OXTqFb;w9w86d:dt4g2b;lkq0A:Z0MWEf;KQzWid:mB4wNe;pNsl2d:j9Yuyc;eHDfl:ofjVkb;Nyt6ic:jn2sGd;SNUn3:x8cHvb;LEikZe:byfTOb,lsjVmc;io8t5d:sgY6Zb;Oj465e:KG2eXe;sP4Vbe:VwDzFe;kMFpHd:OTA3Ae;nAFL3:s39S4;iFQyKf:QIhFr/m=aLUfP?xjs=s2	false		high
http://https://www.google.com/favicon.ico	false		high
http://https://google.com/	false		high
http://https://www.google.com/images/branding/googlelogo/2x/googlelogo_color_272x92dp.png	false		high
http://https://listfoo.org/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/xjs/_/js/k=xjs.s.en_GB.zobC7UqdsqU.O/ck=xjs.s.F0fY5Pm-eS0.L.W.O/am=AAEqCFcAOAAAQAAAAAAkIAAAAAAAAgAwBkDwIA0I2BAOEIMBsCwBIAAgiNEPEQAABgADGBYABAAAAED-AAQ8AQCDCQsAAAAAAAAAELAEweAGCQoCQAAAAAAAAACU0uTFASAIAgAAAQ/d=1/exm=DhPYme,EkevXb,GU4Gab,MpJwZc,NzU6V,UUJqVe,aa,abd,async,cdos,csi,d,dpf,epYOx,hsm,jsa,pHXghd,q0xTif,s39S4,sOXFj,sb_wiz,sf,sonic,spch/ed=1/dg=2/br=1/rs=ACT90oHWjJk68F8W9qa5QTlNuGD_7xu0jA/ee=Pjplud:PoEs9b;QGR0gd:Mlhmy;uY49fb:COQbmf;EVNhjf:pw70Gc;sTsDMc:kHVSUb;g8nkx:U4MzKc;wQlYve:aLUfP;kbAm9d:MkHyGd;F9mqte:UoRcbe;oUlnpc:RagDlc;YV5bee:IvPZ6d;dtl0hd:lLQWFe;yGxLoc:FmAr0c;dIoSBb:ZgGg9b;pXdRYb:JKoKVe;wR5FRb:TtcOte;KpRAue:Tia57b;aZ61od:arTwJ;JXS8fb:Qj0suc;rQSrae:C6D5Fc;qavrXe:zQzcXe;UDrY1c:eps46d;w3bZCb:ZPGaIb;VGRfx:VFqbr;imqimf:jKGL2e;Np8Qkd:Dpx6qc;BjwMce:cXX2Wb;oGtAuc:sOXFj;NPKaK:PVlQOd;EmZ2Bf:zr1jrb;daB6be:lMxGPd;Fmv9Nc:O1Tzwc;hK67qb:QWEO5b;R4IIIb:QWfeKf;BMxAGc:E5bFse;WDGyFe:jcVOxd;wV5Pjc:L8KGxe;xbe2wc:wbTLEd;DpcR3d:zL72xf;tosKvd:ZCqP3;ESrPQc:mNTJvc;NSEoX:lazG7b;G6wU6e:hezEbd;kCQyJ:ueyPK;okUaUd:wItadb;GleZL:J1A7Od;Xeq57c:wZTUNc;eJZqRc:wUwbse;RiX1h:uiAbXc;oSUNyd:fTfGO;SJsSc:H1GVub;SMDL4c:fTfGO;JsbNhc:Xd8iUd;zOsCQe:Ko78Df;KcokUb:KiuZBf;WCEKNd:I46Hvd;LBgRLc:XVMNvd;LsNahb:ucGLNb;UyG7Kb:wQd0G;TxfV6d:YORN0b;qaS3gd:yiLg6e;aAJE9c:WHW6Ef;BgS6mb:fidj5d;UVmjEd:EesRsb;z97YGf:oug9te;CxXAWb:YyRLvc;VN6jIc:ddQyuf;SLtqO:Kh1xYe;VxQ32b:k0XsBb;DULqB:RKfG5c;bcPXSc:gSZLJb;cFTWae:gT8qnd;gaub4:TN6bMe;hjRo6e:F62sG;whEZac:F4AmNb;qddgKe:x4FYXe;eBAeSb:Ck63tb;vfVwPd:OXTqFb;w9w86d:dt4g2b;lkq0A:Z0MWEf;KQzWid:mB4wNe;pNsl2d:j9Yuyc;eHDfl:ofjVkb;Nyt6ic:jn2sGd;SNUn3:x8cHvb;LEikZe:byfTOb,lsjVmc;io8t5d:sgY6Zb;Oj465e:KG2eXe;sP4Vbe:VwDzFe;kMFpHd:OTA3Ae;nAFL3:s39S4;iFQyKf:QIhFr/m=CnSW2d,DPreE,WlNQGd,fXO0xe,kQvlef,nabPbb?xjs=s2	false		high
http://https://www.google.com/xjs/_/js/md=1/k=xjs.s.en_GB.zobC7UqdsqU.O/am=AAEqCFcAOAAAQAAAAAAkIAAAAAAAAgAwBkDwIA0I2BAOEIMBsCwBIAAgiNEPEQAABgADGBYABAAAAED-AAQ8AQCDCQsAAAAAAAAAELAEweAGCQoCQAAAAAAAAACU0uTFASAIAgAAAQ/rs=ACT90oFLXSotrQJhVFHbtpFxrnCGNSmSlQ	false		high
http://https://www.google.com/gen_204?ei=ruvQY6uHDeSP9u8PlpqO-Ak&ved=0ahUKEwirlsyBquL8AhXkh_0HHRaNA58QiZAHCCA&uact=3	false		high
http://https://consent.google.com/save?continue=https://www.google.com/&gl=HR&m=0&pc=shp&x=5&src=2&hl=en&bl=gws_20230118-0_RC1&uxe=none&set_eom=false&set_aps=true&set_sc=true	false		high
http://https://www.google.com/images/searchbox/desktop_searchbox_sprites318_hr.webp	false		high
http://https://www.google.com/complete/search?q&cp=0&client=gws-wiz&xssi=t&hl=en-HR&authuser=0&psi=ruvQY6uHDeSP9u8PlpqO-Ak.1674636232907&nolsbt=1&dpr=1	false		high
http://https://www.google.com/gen_204?atyp=csi&ei=ruvQY6uHDeSP9u8PlpqO-Ak&s=webhp&st=20420&fid=1&t=fi&zx=1674636232867	false		high
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://www.google.com/client_204?&atyp=i&biw=1280&bih=913&ei=ruvQY6uHDeSP9u8PlpqO-Ak	false		high
http://https://www.google.com/gen_204?ei=ruvQY6uHDeSP9u8PlpqO-Ak&vet=10ahUKEwirlsyBquL8AhXkh_0HHRaNA58QhJAHCBk..s&gl=HR&pc=SEARCH_HOMEPAGE&isMobile=false	false		high
http://https://www.google.com/gen_204?ei=ruvQY6uHDeSP9u8PlpqO-Ak&vet=10ahUKEwirlsyBquL8AhXkh_0HHRaNA58QhJAHCBk..h&va=26014	false		high
http://https://www.google.com/	false		high

Name	Malicious	Antivirus Detection	Reputation
http:// https://www.google.com/xjs/_/js/k=xjs.s.en_GB.zobC7UqdsqU.O/am=AAEqCFcAOAAAQAAAAAAkIAAAAAAAAgAwBkDwIA0I2BAOEIMBsCwBIAAgiNEPEQAABgADGBYABAAAAED-AAQ8AQCDCQsAAAAAAAAAELAEweAGCQoCQAAAAAAAAACU0uTFASAIAgAAAQ/d=1/ed=1/dg=2/br=1/rs=ACT90oFLXSotrQJhVFHbtpFxrnCGNSmSlQ/m=cdos,dpf,hsm,jsa,d,csi	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.215.238	consent.google.com	United States		15169	GOOGLEUS	false
142.250.203.100	www.google.com	United States		15169	GOOGLEUS	false
185.180.199.229	listfoo.org	Netherlands		14576	HOSTING-SOLUTIONSUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
172.217.168.78	plus.l.google.com	United States		15169	GOOGLEUS	false
172.217.168.14	google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.203.109	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:	791296
Start date and time:	2023-01-25 09:42:25 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 2s
Hypervisor based Inspection enabled:	false
Report type:	light

Cookbook file name:	browseurl.jbs
Sample URL:	http://https://listfoo.org/zmg5f
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:	12
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@26/0@11/10
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Browse: https://mail.google.com/mail/&ogbl

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.203.99, 34.104.35.123, 172.217.168.74, 142.250.203.106, 216.58.215.234
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, edgedl.me.gvt1.com, content-autofill.googleapis.com, login.live.com, eudb.ris.api.iris.microsoft.com, fonts.gstatic.com, update.googleapis.com, ctldl.windowsupdate.com, clientservices.googleapis.com, img-prod-cms-rt-microsoft-com.akamaized.net, www.gstatic.com, arc.msn.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

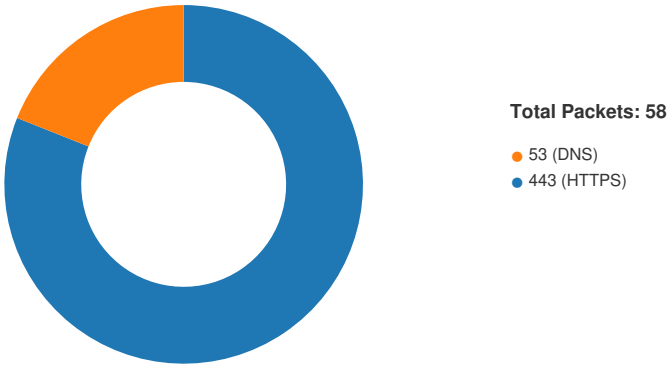
No created / dropped files found

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2023 09:43:23.907602072 CET	49704	443	192.168.2.4	142.250.203.110
Jan 25, 2023 09:43:23.907681942 CET	443	49704	142.250.203.110	192.168.2.4
Jan 25, 2023 09:43:23.907773972 CET	49704	443	192.168.2.4	142.250.203.110
Jan 25, 2023 09:43:23.908062935 CET	49705	443	192.168.2.4	142.250.203.109
Jan 25, 2023 09:43:23.908127069 CET	443	49705	142.250.203.109	192.168.2.4
Jan 25, 2023 09:43:23.908193111 CET	49705	443	192.168.2.4	142.250.203.109
Jan 25, 2023 09:43:23.909796000 CET	49704	443	192.168.2.4	142.250.203.110
Jan 25, 2023 09:43:23.909835100 CET	443	49704	142.250.203.110	192.168.2.4
Jan 25, 2023 09:43:23.911474943 CET	49705	443	192.168.2.4	142.250.203.109
Jan 25, 2023 09:43:23.911506891 CET	443	49705	142.250.203.109	192.168.2.4
Jan 25, 2023 09:43:24.020153046 CET	443	49704	142.250.203.110	192.168.2.4
Jan 25, 2023 09:43:24.024331093 CET	443	49705	142.250.203.109	192.168.2.4
Jan 25, 2023 09:43:24.061716080 CET	49704	443	192.168.2.4	142.250.203.110
Jan 25, 2023 09:43:24.065656900 CET	49705	443	192.168.2.4	142.250.203.109
Jan 25, 2023 09:43:24.183048010 CET	49705	443	192.168.2.4	142.250.203.109
Jan 25, 2023 09:43:24.183094978 CET	443	49705	142.250.203.109	192.168.2.4
Jan 25, 2023 09:43:24.183289051 CET	49704	443	192.168.2.4	142.250.203.110
Jan 25, 2023 09:43:24.183329105 CET	443	49704	142.250.203.110	192.168.2.4
Jan 25, 2023 09:43:24.185353994 CET	443	49704	142.250.203.110	192.168.2.4
Jan 25, 2023 09:43:24.185482979 CET	49704	443	192.168.2.4	142.250.203.110
Jan 25, 2023 09:43:24.186855078 CET	443	49705	142.250.203.109	192.168.2.4
Jan 25, 2023 09:43:24.186943054 CET	49705	443	192.168.2.4	142.250.203.109

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2023 09:43:24.187645912 CET	443	49704	142.250.203.110	192.168.2.4
Jan 25, 2023 09:43:24.187722921 CET	49704	443	192.168.2.4	142.250.203.110
Jan 25, 2023 09:43:25.366568089 CET	49706	443	192.168.2.4	185.180.199.229
Jan 25, 2023 09:43:25.366636038 CET	443	49706	185.180.199.229	192.168.2.4
Jan 25, 2023 09:43:25.366767883 CET	49706	443	192.168.2.4	185.180.199.229
Jan 25, 2023 09:43:25.367397070 CET	49705	443	192.168.2.4	142.250.203.109
Jan 25, 2023 09:43:25.367418051 CET	443	49705	142.250.203.109	192.168.2.4
Jan 25, 2023 09:43:25.367835999 CET	443	49705	142.250.203.109	192.168.2.4
Jan 25, 2023 09:43:25.368930101 CET	49706	443	192.168.2.4	185.180.199.229
Jan 25, 2023 09:43:25.368976116 CET	443	49706	185.180.199.229	192.168.2.4
Jan 25, 2023 09:43:25.369982004 CET	49704	443	192.168.2.4	142.250.203.110
Jan 25, 2023 09:43:25.370057106 CET	443	49704	142.250.203.110	192.168.2.4
Jan 25, 2023 09:43:25.370682955 CET	443	49704	142.250.203.110	192.168.2.4
Jan 25, 2023 09:43:25.371494055 CET	49705	443	192.168.2.4	142.250.203.109
Jan 25, 2023 09:43:25.371515036 CET	443	49705	142.250.203.109	192.168.2.4
Jan 25, 2023 09:43:25.371959925 CET	49704	443	192.168.2.4	142.250.203.110
Jan 25, 2023 09:43:25.371999025 CET	443	49704	142.250.203.110	192.168.2.4
Jan 25, 2023 09:43:25.411290884 CET	443	49704	142.250.203.110	192.168.2.4
Jan 25, 2023 09:43:25.411470890 CET	49704	443	192.168.2.4	142.250.203.110
Jan 25, 2023 09:43:25.411539078 CET	443	49704	142.250.203.110	192.168.2.4
Jan 25, 2023 09:43:25.411586046 CET	443	49704	142.250.203.110	192.168.2.4
Jan 25, 2023 09:43:25.411679029 CET	49704	443	192.168.2.4	142.250.203.110
Jan 25, 2023 09:43:25.445579052 CET	443	49705	142.250.203.109	192.168.2.4
Jan 25, 2023 09:43:25.445696115 CET	49705	443	192.168.2.4	142.250.203.109
Jan 25, 2023 09:43:25.445719957 CET	443	49705	142.250.203.109	192.168.2.4
Jan 25, 2023 09:43:25.445899010 CET	443	49705	142.250.203.109	192.168.2.4
Jan 25, 2023 09:43:25.445983887 CET	49705	443	192.168.2.4	142.250.203.109
Jan 25, 2023 09:43:25.503937960 CET	49705	443	192.168.2.4	142.250.203.109
Jan 25, 2023 09:43:25.503981113 CET	443	49705	142.250.203.109	192.168.2.4
Jan 25, 2023 09:43:25.505192041 CET	49704	443	192.168.2.4	142.250.203.110
Jan 25, 2023 09:43:25.505253077 CET	443	49704	142.250.203.110	192.168.2.4
Jan 25, 2023 09:43:25.594564915 CET	443	49706	185.180.199.229	192.168.2.4
Jan 25, 2023 09:43:25.625833035 CET	49706	443	192.168.2.4	185.180.199.229
Jan 25, 2023 09:43:25.625906944 CET	443	49706	185.180.199.229	192.168.2.4
Jan 25, 2023 09:43:25.628380060 CET	443	49706	185.180.199.229	192.168.2.4
Jan 25, 2023 09:43:25.628463984 CET	49706	443	192.168.2.4	185.180.199.229
Jan 25, 2023 09:43:25.681019068 CET	49706	443	192.168.2.4	185.180.199.229
Jan 25, 2023 09:43:25.681056976 CET	443	49706	185.180.199.229	192.168.2.4
Jan 25, 2023 09:43:25.681278944 CET	443	49706	185.180.199.229	192.168.2.4
Jan 25, 2023 09:43:25.681668997 CET	49706	443	192.168.2.4	185.180.199.229
Jan 25, 2023 09:43:25.681696892 CET	443	49706	185.180.199.229	192.168.2.4
Jan 25, 2023 09:43:25.747380972 CET	443	49706	185.180.199.229	192.168.2.4
Jan 25, 2023 09:43:25.747494936 CET	49706	443	192.168.2.4	185.180.199.229
Jan 25, 2023 09:43:25.752106905 CET	49706	443	192.168.2.4	185.180.199.229
Jan 25, 2023 09:43:25.752141953 CET	443	49706	185.180.199.229	192.168.2.4
Jan 25, 2023 09:43:25.898211956 CET	49707	443	192.168.2.4	185.180.199.229
Jan 25, 2023 09:43:25.898288012 CET	443	49707	185.180.199.229	192.168.2.4
Jan 25, 2023 09:43:25.898396015 CET	49707	443	192.168.2.4	185.180.199.229
Jan 25, 2023 09:43:25.898858070 CET	49707	443	192.168.2.4	185.180.199.229
Jan 25, 2023 09:43:25.898901939 CET	443	49707	185.180.199.229	192.168.2.4
Jan 25, 2023 09:43:25.916371107 CET	49708	443	192.168.2.4	172.217.168.14
Jan 25, 2023 09:43:25.916464090 CET	443	49708	172.217.168.14	192.168.2.4
Jan 25, 2023 09:43:25.916610956 CET	49708	443	192.168.2.4	172.217.168.14
Jan 25, 2023 09:43:25.922799110 CET	49708	443	192.168.2.4	172.217.168.14
Jan 25, 2023 09:43:25.922852993 CET	443	49708	172.217.168.14	192.168.2.4
Jan 25, 2023 09:43:25.985939026 CET	443	49708	172.217.168.14	192.168.2.4
Jan 25, 2023 09:43:25.996577024 CET	49708	443	192.168.2.4	172.217.168.14
Jan 25, 2023 09:43:25.996627092 CET	443	49708	172.217.168.14	192.168.2.4
Jan 25, 2023 09:43:25.997574091 CET	443	49708	172.217.168.14	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2023 09:43:25.997658968 CET	49708	443	192.168.2.4	172.217.168.14
Jan 25, 2023 09:43:25.998918056 CET	443	49708	172.217.168.14	192.168.2.4
Jan 25, 2023 09:43:25.998984098 CET	49708	443	192.168.2.4	172.217.168.14
Jan 25, 2023 09:43:26.000960112 CET	49708	443	192.168.2.4	172.217.168.14
Jan 25, 2023 09:43:26.000996113 CET	443	49708	172.217.168.14	192.168.2.4
Jan 25, 2023 09:43:26.001152992 CET	443	49708	172.217.168.14	192.168.2.4
Jan 25, 2023 09:43:26.001674891 CET	49708	443	192.168.2.4	172.217.168.14
Jan 25, 2023 09:43:26.001723051 CET	443	49708	172.217.168.14	192.168.2.4
Jan 25, 2023 09:43:26.028537035 CET	443	49707	185.180.199.229	192.168.2.4
Jan 25, 2023 09:43:26.030111074 CET	49707	443	192.168.2.4	185.180.199.229
Jan 25, 2023 09:43:26.030160904 CET	443	49707	185.180.199.229	192.168.2.4
Jan 25, 2023 09:43:26.031291008 CET	443	49707	185.180.199.229	192.168.2.4
Jan 25, 2023 09:43:26.031903982 CET	49707	443	192.168.2.4	185.180.199.229
Jan 25, 2023 09:43:26.031945944 CET	443	49707	185.180.199.229	192.168.2.4
Jan 25, 2023 09:43:26.032047033 CET	49707	443	192.168.2.4	185.180.199.229
Jan 25, 2023 09:43:26.032061100 CET	443	49707	185.180.199.229	192.168.2.4
Jan 25, 2023 09:43:26.032116890 CET	443	49707	185.180.199.229	192.168.2.4
Jan 25, 2023 09:43:26.041414022 CET	443	49708	172.217.168.14	192.168.2.4
Jan 25, 2023 09:43:26.041522026 CET	49708	443	192.168.2.4	172.217.168.14

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2023 09:43:23.711551905 CET	64167	53	192.168.2.4	8.8.8.8
Jan 25, 2023 09:43:23.711925983 CET	58565	53	192.168.2.4	8.8.8.8
Jan 25, 2023 09:43:23.737365961 CET	53	64167	8.8.8.8	192.168.2.4
Jan 25, 2023 09:43:23.738249063 CET	53	58565	8.8.8.8	192.168.2.4
Jan 25, 2023 09:43:23.835452080 CET	56807	53	192.168.2.4	8.8.8.8
Jan 25, 2023 09:43:23.882839918 CET	53	56807	8.8.8.8	192.168.2.4
Jan 25, 2023 09:43:25.876192093 CET	61124	53	192.168.2.4	8.8.8.8
Jan 25, 2023 09:43:25.895842075 CET	53	61124	8.8.8.8	192.168.2.4
Jan 25, 2023 09:43:26.088342905 CET	55570	53	192.168.2.4	8.8.8.8
Jan 25, 2023 09:43:26.114576101 CET	53	55570	8.8.8.8	192.168.2.4
Jan 25, 2023 09:43:27.011023045 CET	58729	53	192.168.2.4	8.8.8.8
Jan 25, 2023 09:43:27.038729906 CET	53	58729	8.8.8.8	192.168.2.4
Jan 25, 2023 09:43:27.238797903 CET	64700	53	192.168.2.4	8.8.8.8
Jan 25, 2023 09:43:27.258802891 CET	53	64700	8.8.8.8	192.168.2.4
Jan 25, 2023 09:43:29.870573997 CET	60550	53	192.168.2.4	8.8.8.8
Jan 25, 2023 09:43:29.898292065 CET	53	60550	8.8.8.8	192.168.2.4
Jan 25, 2023 09:43:52.546322107 CET	51419	53	192.168.2.4	8.8.8.8
Jan 25, 2023 09:43:52.573548079 CET	53	51419	8.8.8.8	192.168.2.4
Jan 25, 2023 09:44:27.441205978 CET	65133	53	192.168.2.4	8.8.8.8
Jan 25, 2023 09:44:27.461000919 CET	53	65133	8.8.8.8	192.168.2.4
Jan 25, 2023 09:44:27.500570059 CET	60998	53	192.168.2.4	8.8.8.8
Jan 25, 2023 09:44:27.520157099 CET	53	60998	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
Jan 25, 2023 09:43:23.711551905 CET	192.168.2.4	8.8.8.8	0x88f4	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:43:23.711925983 CET	192.168.2.4	8.8.8.8	0x4787	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:43:23.835452080 CET	192.168.2.4	8.8.8.8	0x51e3	Standard query (0)	listfoo.org	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:43:25.876192093 CET	192.168.2.4	8.8.8.8	0xe9c3	Standard query (0)	google.com	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:43:26.088342905 CET	192.168.2.4	8.8.8.8	0x5681	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:43:27.011023045 CET	192.168.2.4	8.8.8.8	0xcc03	Standard query (0)	apis.google.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jan 25, 2023 09:43:27.238797903 CET	192.168.2.4	8.8.8.8	0xeb89	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:43:29.870573997 CET	192.168.2.4	8.8.8.8	0x931e	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:43:52.546322107 CET	192.168.2.4	8.8.8.8	0x5baa	Standard query (0)	consent.google.com	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:44:27.441205978 CET	192.168.2.4	8.8.8.8	0xa820	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:44:27.500570059 CET	192.168.2.4	8.8.8.8	0x432f	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

DNS Answers

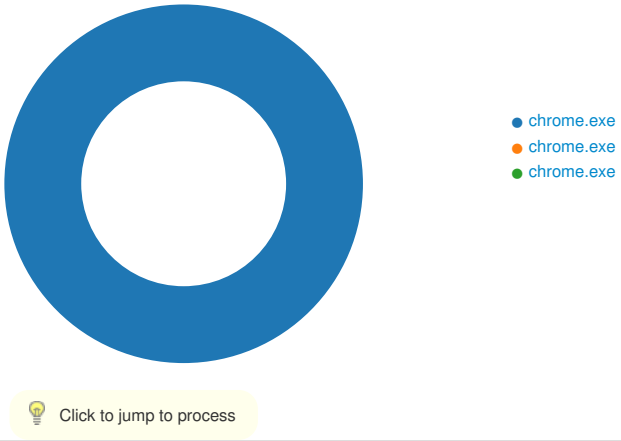
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 25, 2023 09:43:23.737365961 CET	8.8.8.8	192.168.2.4	0x88f4	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Jan 25, 2023 09:43:23.737365961 CET	8.8.8.8	192.168.2.4	0x88f4	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:43:23.738249063 CET	8.8.8.8	192.168.2.4	0x4787	No error (0)	accounts.google.com		142.250.203.109	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:43:23.882839918 CET	8.8.8.8	192.168.2.4	0x51e3	No error (0)	listfoo.org		185.180.199.229	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:43:25.895842075 CET	8.8.8.8	192.168.2.4	0xe9c3	No error (0)	google.com		172.217.168.14	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:43:26.114576101 CET	8.8.8.8	192.168.2.4	0x5681	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:43:27.038729906 CET	8.8.8.8	192.168.2.4	0xcc03	No error (0)	apis.google.com	plus.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Jan 25, 2023 09:43:27.038729906 CET	8.8.8.8	192.168.2.4	0xcc03	No error (0)	plus.l.google.com		172.217.168.78	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:43:27.258802891 CET	8.8.8.8	192.168.2.4	0xeb89	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:43:29.898292065 CET	8.8.8.8	192.168.2.4	0x931e	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:43:52.573548079 CET	8.8.8.8	192.168.2.4	0x5baa	No error (0)	consent.google.com		216.58.215.238	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:44:27.461000919 CET	8.8.8.8	192.168.2.4	0xa820	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:44:27.520157099 CET	8.8.8.8	192.168.2.4	0x432f	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
- listfoo.org
- https:
  - google.com
  - www.google.com
  - apis.google.com
  - consent.google.com

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **5112**, Parent PID: **3696**

General

Target ID:	0
Start time:	09:43:20
Start date:	25/01/2023
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:	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: **4136**, Parent PID: **5112**

General

Target ID:	1
Start time:	09:43:21
Start date:	25/01/2023
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-GB --service-sandbox-type=none --mojo-platform-channel-handle=1972 --field-trial-handle=1772,i,13714808044369432181,11901859910510463980,131072 --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: **6288**, Parent PID: **3696**

General

Target ID:	2
Start time:	09:43:22
Start date:	25/01/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "https://listfoo.org/zmg5f
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