ID: 756336
Sample Name: RemitAdvise.htm
Cookbook:
defaultwindowshtmlcookbook.jbs
Time: 02:01:15
Date: 30/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

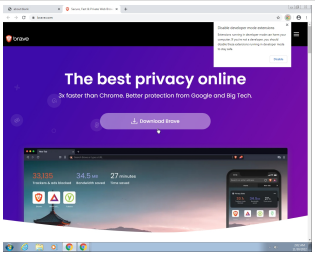
Windows Analysis Report

RemitAdvise.htm

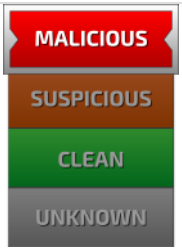
Overview

General Information

Sample Name:	RemitAdvise.htm
Analysis ID:	756336
MD5:	c362c76446daf0…
SHA1:	7e026d5740662c..
SHA256:	e313c6a9462722..
Infos:	



Detection



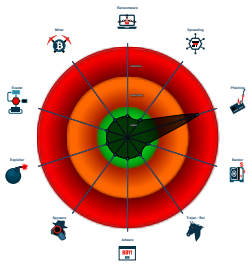
HTMLPhisher

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish44
- Yara detected obfuscated html page
- HTML document with suspicious na…
- JA3 SSL client fingerprint seen in co…
- Yara signature match
- IP address seen in connection with …

Classification



Process Tree

- **System is w7x64**
- chrome.exe (PID: 3000 cmdline: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 6ACAE527E744C80997B25EF2A0485D5E)
  - chrome.exe (PID: 832 cmdline: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=952,1834247139616653473 9,13915805133651195408,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1452 /prefetch:8 MD5: 6ACAE527E744C80997B25EF2A0485D5E)
- chrome.exe (PID: 804 cmdline: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" "C:\Users\user\Desktop\RemitAdvise.htm MD5: 6ACAE527E744C80997B25EF2A0485D5E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
RemitAdvise.htm	SUSP_obfuscated_JS_obfuscatorio	Detects JS obfuscation done by the js obfuscator (often malicious)	@imp0rtp3	• 0x157f:$c8: while(!![]) • 0x159d:$d1: parseInt(_0x18051d(0x99))/0x1*(parseInt(_0x18051d(0x9d))/0x2)+-parseInt(_0x18051d(0xa7))/0x3*(parseInt(_0x18051d(0x9c))/0x4)+-parseInt(_0x18051d(0xa1))/0x5+-parseInt(_0x18051d(0xa3))/0x6*(• 0x15bc:$d1: parseInt(_0x18051d(0x9d))/0x2)+-parseInt(_0x18051d(0xa7))/0x3*(parseInt(_0x18051d(0x9c))/0x4)+-parseInt(_0x18051d(0xa1))/0x5+-parseInt(_0x18051d(0xa3))/0x6*(parseInt(_0x18051d(0x9a))/0x7)+ • 0x15dc:$d1: parseInt(_0x18051d(0xa7))/0x3*(parseInt(_0x18051d(0x9c))/0x4)+-parseInt(_0x18051d(0xa1))/0x5+-parseInt(_0x18051d(0xa3))/0x6*(parseInt(_0x18051d(0x9a))/0x7)+parseInt(_0x18051d(0xa0))/0x8*(- • 0x15fb:$d1: parseInt(_0x18051d(0x9c))/0x4)+-parseInt(_0x18051d(0xa1))/0x5+-parseInt(_0x18051d(0xa3))/0x6*(parseInt(_0x18051d(0x9a))/0x7)+parseInt(_0x18051d(0xa0))/0x8*(-parseInt(_0x18051d(0x9b))/0x9)+- • 0x161b:$d1: parseInt(_0x18051d(0xa1))/0x5+-parseInt(_0x18051d(0xa3))/0x6*(parseInt(_0x18051d(0x9a))/0x7)+parseInt(_0x18051d(0xa0))/0x8*(-parseInt(_0x18051d(0x9b))/0x9)+-parseInt(_0x18051d(0x9f))/0xa*(- • 0x163a:$d1: parseInt(_0x18051d(0xa3))/0x6*(parseInt(_0x18051d(0x9a))/0x7)+parseInt(_0x18051d(0xa0))/0x8*(-parseInt(_0x18051d(0x9b))/0x9)+-parseInt(_0x18051d(0x9f))/0xa*(-parseInt(_0x18051d(0xa4))/0xb)+- • 0x1659:$d1: parseInt(_0x18051d(0x9a))/0x7)+parseInt(_0x18051d(0xa0))/0x8*(-parseInt(_0x18051d(0x9b))/0x9)+-parseInt(_0x18051d(0x9f))/0xa*(-parseInt(_0x18051d(0xa4))/0xb)+-parseInt(_0x18051d(0xa6))/0xc*(-
RemitAdvise.htm	JoeSecurity_Obshtml	Yara detected obfuscated html page	Joe Security	
RemitAdvise.htm	JoeSecurity_HtmlPhish_44	Yara detected HtmlPhish_44	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Phishing

Yara detected HtmlPhish44

Yara detected obfuscated html page

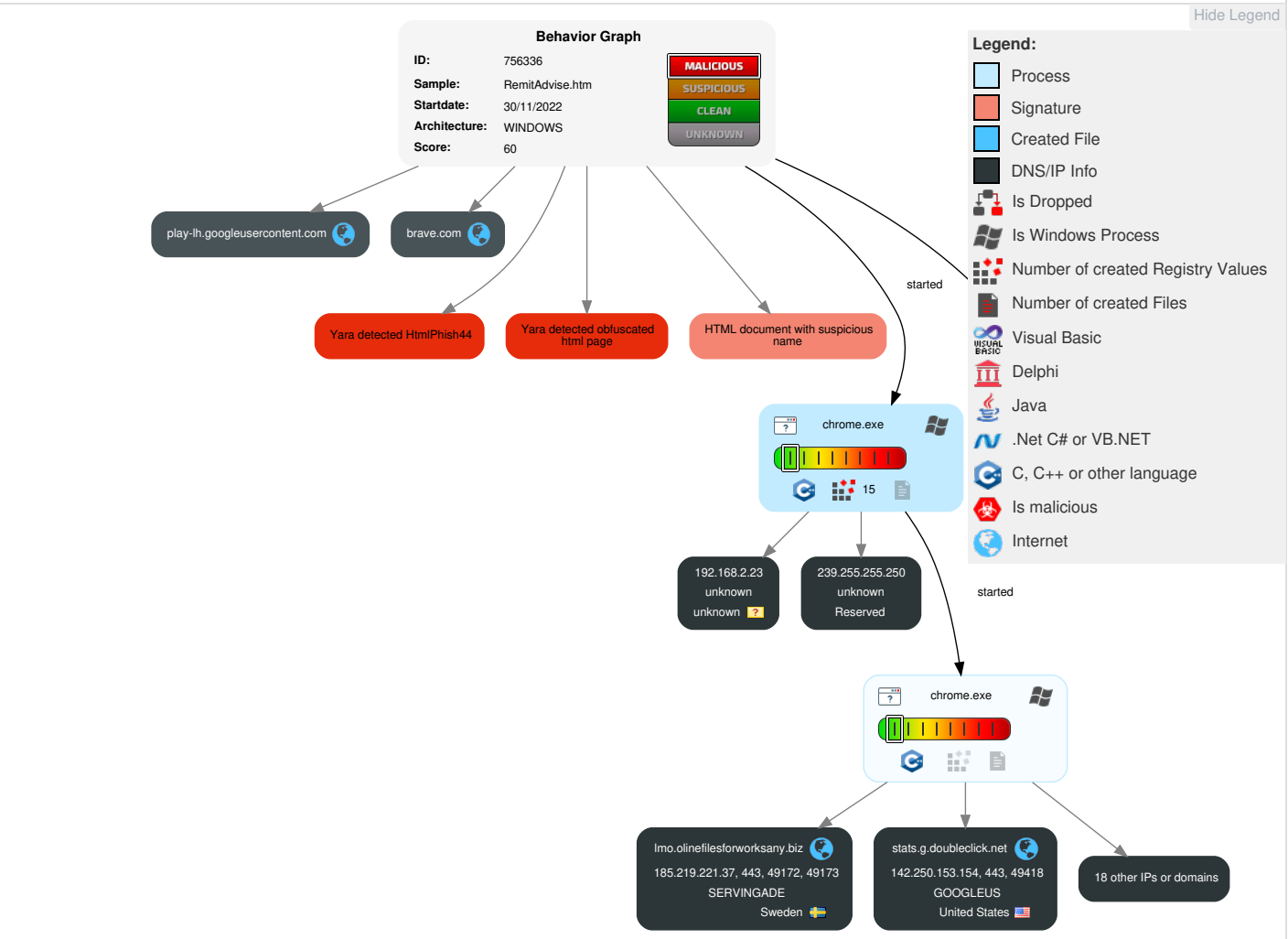
System Summary

HTML document with suspicious name

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	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

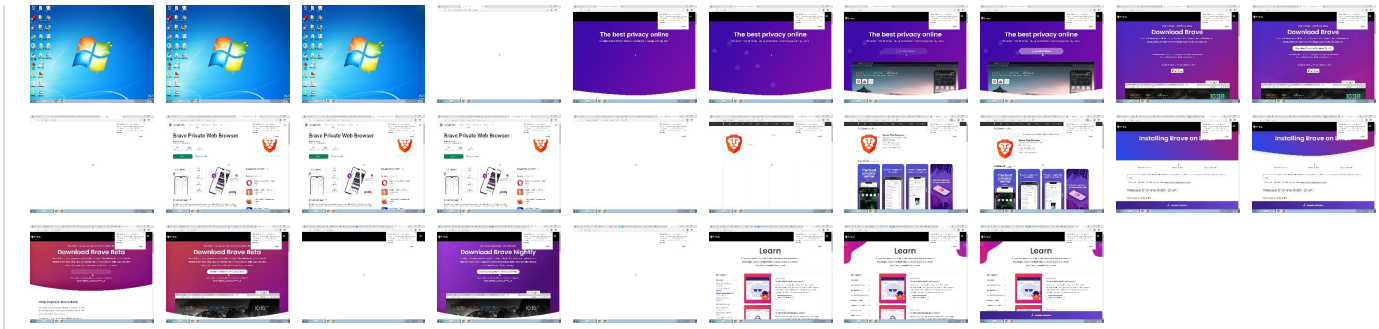
Behavior Graph

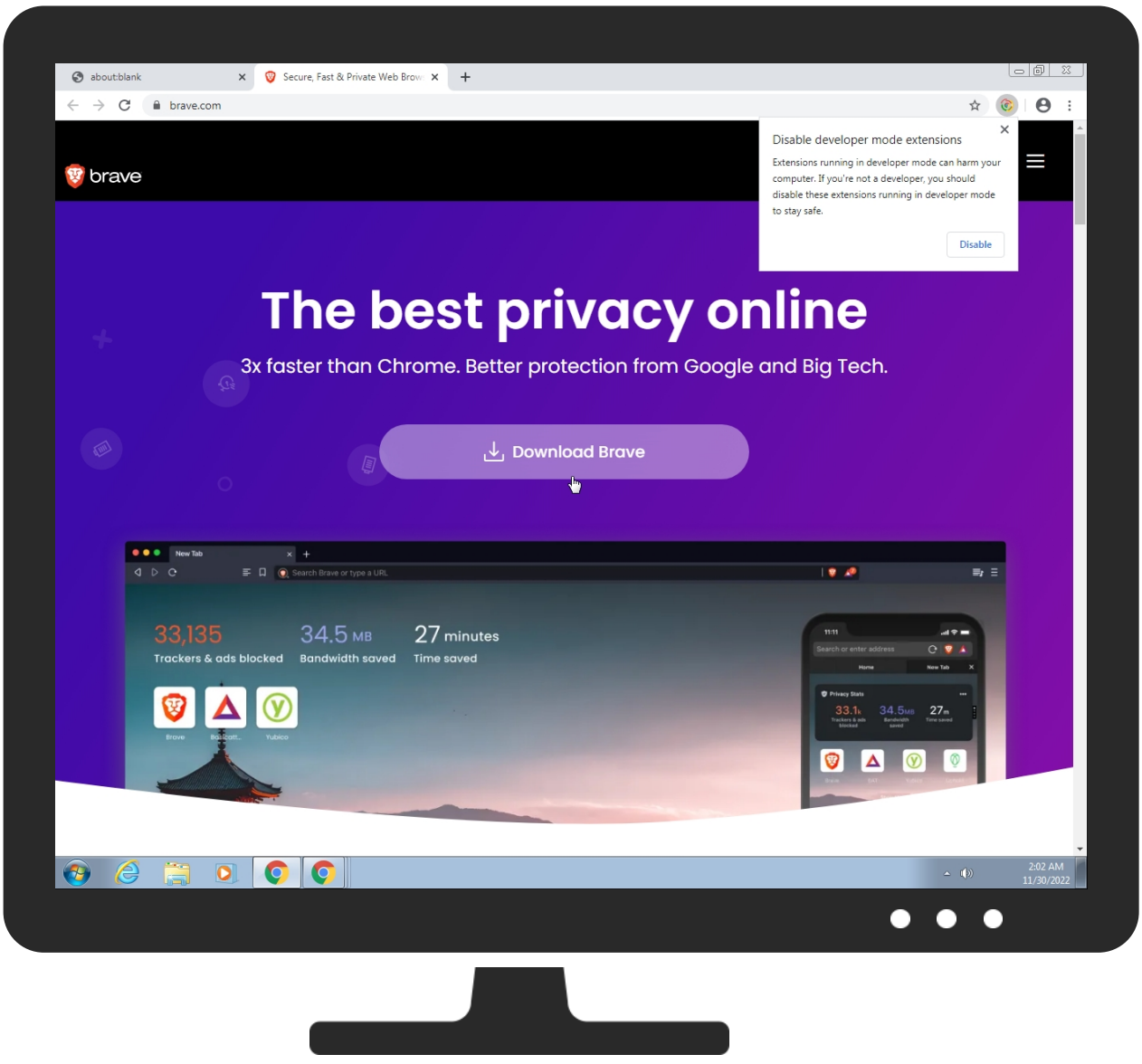


Screenshots

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
RemitAdvise.htm	0%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://lmo.olinefilesforworksany.biz/?username=lexa_hobenshield@transmountain.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
lmo.olinefilesforworksany.biz	185.219.221.37	true	false		unknown
accounts.google.com	172.217.168.77	true	false		high
play.google.com	172.217.168.78	true	false		high
brave.com	13.32.27.109	true	false		high
www.google.fr	172.217.168.3	true	false		high
play-lh.googleusercontent.com	142.250.203.118	true	false		high
d2cbcq2c2d2d1v.cloudfront.net	108.156.60.111	true	false		high
www.google.com	172.217.168.68	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
stats.g.doubleclick.net	142.250.153.154	true	false		high
is2-ssl.mzstatic.com	unknown	unknown	false		high
analytics.brave.com	unknown	unknown	false		high
is4-ssl.mzstatic.com	unknown	unknown	false		high
is3-ssl.mzstatic.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
is1-ssl.mzstatic.com	unknown	unknown	false		high
is5-ssl.mzstatic.com	unknown	unknown	false		high

Contacted URLs

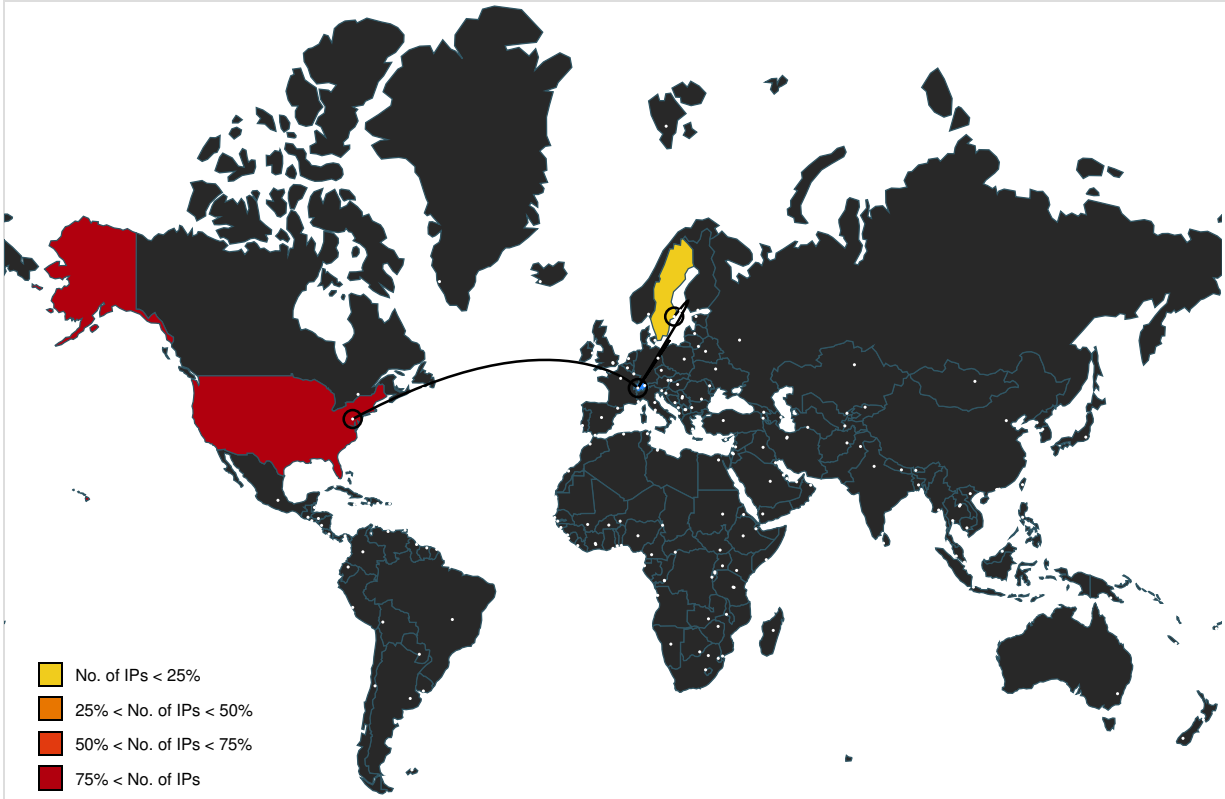
Name	Malicious	Antivirus Detection	Reputation
http://https://play.google.com/play/log?format=json&authuser=	false		high
http://https://brave.com/static-assets/images/brave-logo-no-shadow.png	false		high
http://https://brave.com/static-assets/images/optimized/november-wallet-partners/images/featured.webp	false		high
http://https://brave.com/download-beta/	false		high
http://https://stats.g.doubleclick.net/j/collect?t=dc&aip=1&_r=3&v=1&_v=j98&tid=UA-19995903-1&cid=368165947.1669802569&jid=1800514385&gjid=525004988&_gid=1726787713.1669802569&_u=YEBAAEAAAAAAACgDI~&z=1295807090	false		high
http://https://brave.com/static-assets/images/icon-download.svg	false		high
http://https://brave.com/js/persistent-cta.js	false		high
http://https://brave.com/static-assets/images/contribute.svg	false		high
http://https://brave.com/static-assets/images/edge-logo.svg	false		high
http://https://brave.com/static-assets/images/optimized/learn/images/fastest-browser@1x.webp	false		high
http://https://brave.com/static-assets/images/safari-logo.svg	false		high
http://https://play-lh.googleusercontent.com/WKlNHhjh9npwwp0m-3Jc4O2yRLg0xFaF0HO2fX9piYhHg_r_rNkFB60MSWsfuOYsPGUt=w526-h296-rw	false		high
http://https://brave.com/js/category-accordion.js	false		high
http://https://brave.com/static-assets/images/optimized/learn/images/secure-browser@1x.webp	false		high
http://https://brave.com/download/	false		high
http://https://play-lh.googleusercontent.com/sTPusxi30AHxiRHEFK9i5BCK-Y8BJ6Y_NCQNq6l9U6BuDv8kNRdIfsHzvmIA1XULDb3c=s64-rw	false		high
http://https://brave.com/js/3-delay-animations.js	false		high
http://https://brave.com/static-assets/icons/close-icon.svg	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://brave.com/static-assets/images/coding-background-texture.jpg	false		high
http://https://play-lh.googleusercontent.com/12USW7aflgz466ifDehKTnMoAep_VHxDmKJ6jEBoDZWCSefOC-ThRX14Mqe0r8KF9XCzrpMqJts=s20-rw	false		high
http://https://brave.com/static-assets/icons/chevron-right-icon.svg	false		high
http://https://analytics.brave.com/piwik.php?action_name=Installing%20Brave%20on%20Linux%20%7C%20Brave%20Browser&idsite=2&rec=1&r=091593&h=2&m=3&s=2&url=https%3A%2F%2Fbrave.com%2Flinux%2F&_id=&_idn=1&send_image=1&_refts=0&pdf=0&qt=0&realp=0&wma=0&fla=0&java=0&ag=0&cookie=1&res=1280x1024&pv_id=oUzxKL&pf_net=0&pf_srv=69&pf_tfr=19&pf_dm1=550&uadata=%7B%7D	false		high
http://https://brave.com/download-nightly/	false		high
http://https://brave.com/static-assets/fonts/Poppins/Poppins-Medium.ttf	false		high
http://https://brave.com/static-assets/images/optimized/browser-1280x339.webp	false		high
http://https://brave.com/static-assets/fonts/Poppins/Poppins-Regular.ttf	false		high
http://https://brave.com/static-assets/images/category-thumbnail-web3-browsers.svg	false		high
http://https://brave.com/js/interstitial.js	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=84.0.4147.135&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelpbcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc	false		high
http://https://play-lh.googleusercontent.com/Yxa9AnKKAnMGFov2uBQ5dWfovUpIKtZs2tLgJUbh6AzEv3owH8lBSux975PEuaB8aIc=w526-h296-rw	false		high
http://https://brave.com/static-assets/images/optimized/home-illustration-01.webp	false		high
http://https://lmo.olinefilesforworksany.biz/?username=lexa_hobenshield@transmountain.com	false	• Avira URL Cloud: safe	unknown
http://https://brave.com/static-assets/images/interstitial-download-qr.png	false		high
http://https://analytics.brave.com/piwik.php?action_name=Download%20Brave%20%7C%20Brave%20Browser&idsite=2&rec=1&r=684466&h=2&m=2&s=38&url=https%3A%2F%2Fbrave.com%2Fdownload%2F&_id=&_idn=1&send_image=1&_refts=0&pdf=0&qt=0&realp=0&wma=0&fla=0&java=0&ag=0&cookie=1&res=1280x1024&pv_id=zTY2M9&pf_net=216&pf_srv=24&pf_tfr=42&pf_dm1=764&uadata=%7B%7D	false		high
http://https://brave.com/static-assets/js/announcement-banner.js	false		high
http://https://analytics.brave.com/piwik.php?action_name=Download%20Brave%20Beta%20%7C%20Brave%20Browser&idsite=2&rec=1&r=216260&h=2&m=3&s=9&url=https%3A%2F%2Fbrave.com%2Fdownload-beta%2F&_id=&_idn=1&send_image=1&_refts=0&pdf=0&qt=0&realp=0&wma=0&fla=0&java=0&ag=0&cookie=1&res=1280x1024&pv_id=FQELc9&pf_net=115&pf_srv=97&pf_tfr=66&pf_dm1=582&uadata=%7B%7D	false		high
http://https://brave.com/static-assets/images/app-store-badge.png	false		high
http://https://brave.com/ios/	false		high
http://https://play-lh.googleusercontent.com/rWoDevKXfJpuqVmCKiwMxfWWFzci7Ts7eXCNqc3UnVJTYgyEJ9RjkZAugxl3c95LhA=w526-h296-rw	false		high
http://https://brave.com/js/perfundo.js	false		high
http://https://brave.com/static-assets/images/site-nav-download-qr.png	false		high
http://https://brave.com/static-assets/images/optimized/home-illustration-02.webp	false		high
http://https://play-lh.googleusercontent.com/a/ALm5wu3zwDUeZE2KhibfbXvAXtliOp5VhxyOJNGZv5JL=s32-rw-mo	false		high
http://https://brave.com/static-assets/images/border_white.svg	false		high
http://https://brave.com/js/accordion-alt.js	false		high
http://https://brave.com/static-assets/images/optimized/security-illustration.webp	false		high
http://https://brave.com/js/dev.js	false		high
http://https://brave.com/js/referral.js	false		high
http://https://brave.com/js/is-browser.min.js	false		high
http://https://brave.com/static-assets/vendors/lodash.throttle.min.js	false		high
http://https://brave.com/static-assets/images/optimized/privacy-browser-video-cover.jpg	false		high
http://https://brave.com/static-assets/images/playstore.png	false		high
http://https://brave.com/js/navigation.js	false		high
http://https://play.google.com/log?format=json&hasfast=true	false		high
http://https://brave.com/js/detect-platform.js	false		high
http://https://brave.com/static-assets/images/optimized/desktop-hero-screenshot@1x.webp	false		high
http://https://brave.com/android/	false		high
http://https://brave.com/static-assets/images/logo-verizon.svg	false		high
http://https://brave.com/	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://play-lh.googleusercontent.com/Ea12V8BesGX1BqYZT8UEC6r7zfn_Njdx-IkljrMvi_NGcnThCQ__CpbApLwJYmLLB6Y=w526-h296-rw	false		high
http://https://play.google.com/_/PlayStoreUi/browserinfo?f.sid=2554518561800276 73&bl=boq_playuiserver_20221121.06_p1&hl=en-US&authuser&soc-app=121&soc-platform=1&soc-device=1&_reqid=7370&rt=j	false		high
http://https://brave.com/static-assets/images/mobile.svg	false		high
http://https://brave.com/static-assets/images/optimized/bat-nft/images/featured.webp	false		high
http://https://brave.com/static-assets/images/optimized/mobile-plank-download-qr.png	false		high
http://https://analytics.brave.com/piwik.php?action_name=Download%20Brave%20Nightly%20%7C%20Brave%20Browser&idsite=2&rec=1&r=912209&h=2&m=3&s=15&url=https%3A%2F%2Fbrave.com%2Fdownload-nightly%2F&_id=&_idn=1&send_image=1&_refts=0&pdf=0&qt=0&realp=0&wma=0&fla=0&java=0&ag=0&cookie=1&res=1280x1024&pv_id=Z4kXcM&pf_net=185&pf_srv=696&pf_tfr=289&pf_dm1=776&uadata=%7B%7D	false		high
http://https://brave.com/static-assets/images/optimized/learn/images/ad-blocker@1x.webp	false		high
http://https://brave.com/static-assets/images/optimized/import-settings.svg	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=84.0.4147.135&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelpbcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://www.google.com/recaptcha/api2/anchor?ar=1&k=6LcA2tEZAAAAAJj7FTYTF9cZ4NL3ShgBCBfkWov0&co=aHR0cHM6Ly9wbGF5Lmdvb2dsZS5jb206NDQz&hl=en&v=Km9gKuG06He-isPsP6saG8cn&size=invisible&cb=vdlaomx45go3	false		high
http://https://www.google.com/ads/ga-audiences?t=sr&aip=1&_r=4&slf_rd=1&v=1&_v=j98&tid=UA-19995903-1&cid=368165947.1669802569&jid=1800514385&_u=YEBAAEAAAAAAACgDI~&z=1982277960	false		high
http://https://play-lh.googleusercontent.com/PcRA92AlF3NafNYMb2BVFSIohyJVEgEKusVuDZj0nGKV-oQujZANLR4-enR46SqUmg=s64-rw	false		high
http://https://brave.com/linux/	false		high
http://https://play.google.com/store/apps/details?id=com.brave.browser	false		high
http://https://brave.com/static-assets/images/optimized/browser-bw-1212x.webp	false		high
http://https://brave.com/static-assets/images/optimized/speed-past-chrome-cover.png	false		high
http://https://brave.com/learn/	false		high
http://https://analytics.brave.com/piwik.php?action_name=Secure%2C%20Fast%20%26%20Private%20Web%20Browser%20with%20Adblocker%20%7C%20Brave%20Browser&idsite=2&rec=1&r=114220&h=2&m=2&s=22&url=https%3A%2F%2Fbrave.com%2F&_id=&_idn=1&send_image=1&_refts=0&pdf=0&qt=0&realp=0&wma=0&fla=0&java=0&ag=0&cookie=1&res=1280x1024&pv_id=wgQGqp&pf_net=252&pf_srv=26&pf_tfr=93&pf_dm1=1875&uadata=%7B%7D	false		high
http://https://brave.com/static-assets/fonts/Poppins/Poppins-Bold.ttf	false		high
http://https://brave.com/static-assets/images/separator_curve.svg	false		high
http://https://brave.com/static-assets/css/main.min.css	false		high
http://https://play-lh.googleusercontent.com/rh_JsaDPC_ArUMPdZFSEgCM6N-EbS0urR6k9VETap0CAQROivBPjJ6K5g99bXwHXUd1m=w526-h296-rw	false		high
http://https://brave.com/static-assets/images/abstract-shape-light-gradient-06-right.svg	false		high
http://https://brave.com/static-assets/images/logo-etoro.svg	false		high
http://https://brave.com/static-assets/images/shapes-dingbats-left.svg	false		high
http://https://play-lh.googleusercontent.com/maODa6yJ4GcLMwJ0oqbOOa2zUfy8hZPeTclRoH__2B1Ch5yV7L2hRa-Gk7PeIu_utgMr=w526-h296-rw	false		high
http://https://brave.com/static-assets/images/brave-logo.svg	false		high
http://https://www.google.com/tools/feedback/chat_load.js	false		high
http://https://brave.com/static-assets/images/brave-favicon.png	false		high
http://https://brave.com/static-assets/images/filler.png	false		high
http://https://play-lh.googleusercontent.com/6eOk4kfniz8QOP_OhKMuw4ILpK-6TlQGIVdD3unMG0zZBgdaJnMxZKyJqSRQsZe-WmvN=w526-h296-rw	false		high
http://https://brave.com/static-assets/images/optimized/safer-signing/images/featured.webp	false		high
http://https://analytics.brave.com/piwik.php?action_name=Learn%20%7C%20Brave%20Browser&idsite=2&rec=1&r=927765&h=2&m=3&s=20&url=https%3A%2F%2Fbrave.com%2Flearn%2F&_id=&_idn=1&send_image=1&_refts=0&pdf=0&qt=0&realp=0&wma=0&fla=0&java=0&ag=0&cookie=1&res=1280x1024&pv_id=vq91pY&pf_net=277&pf_srv=688&pf_tfr=284&pf_dm1=772&uadata=%7B%7D	false		high
http://https://play-lh.googleusercontent.com/vvjvZn0l16nn8j1KfCAbHlBn7wm6la_55pfxGOW9Wg0ut6C51wKVb3DWJTqSJc-eCnA=s64-rw	false		high
http://https://brave.com/download-beta/	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://play-lh.googleusercontent.com/isI4Bh1A1UnjBfqD33BKhFJKLCc1S43Uy0H0PZ176pxvYU_QAI1XDEhtzpwklqVTgA4=s64-rw	false		high
http://https://brave.com/static-assets/images/browser-embellishments.svg	false		high
http://https://brave.com/js/1-ie-compat.js	false		high
http://https://brave.com/static-assets/images/logo-dentsu.svg	false		high
http://https://play-lh.googleusercontent.com/diXzCee0FKktbzQrA7Bnzw1HjjISjhWLGpqBB7hTp6R_Yqgr1jQaLuhFA0V3eTTI8qg=w526-h296-rw	false		high
http://https://brave.com/static-assets/images/optimized/home-illustration-04.webp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.203.118	play-lh.googleusercontent.com	United States		15169	GOOGLEUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
185.219.221.37	lmo.olinefilesforworksany.biz	Sweden		39378	SERVINGADE	false
172.217.168.68	www.google.com	United States		15169	GOOGLEUS	false
172.217.168.3	www.google.fr	United States		15169	GOOGLEUS	false
13.32.27.109	brave.com	United States		7018	ATT-INTERNET4US	false
13.32.27.82	unknown	United States		7018	ATT-INTERNET4US	false
172.217.168.78	play.google.com	United States		15169	GOOGLEUS	false
142.250.153.154	stats.g.doubleclick.net	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
172.217.168.77	accounts.google.com	United States		15169	GOOGLEUS	false
108.156.60.111	d2cbcq2c2d2d1v.cloudfront.net	United States		16509	AMAZON-02US	false

Private

IP
192.168.2.23
192.168.2.255
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756336
Start date and time:	2022-11-30 02:01:15 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RemitAdvise.htm
Cookbook file name:	defaultwindowshtmlcookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	5
Number of new started drivers analysed:	2
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:	MAL
Classification:	mal60.phis.winHTM@50/0@18/15
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .htm • Browse: https://brave.com/download/ • Browse: https://brave.com/android/ • Browse: https://brave.com/ios/ • Browse: https://brave.com/linux/ • Browse: https://brave.com/download-beta/ • Browse: https://brave.com/download-nightly/ • Browse: https://brave.com/learn/

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, vga.dll
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 172.217.168.67, 34.104.35.123, 172.217.168.42, 142.250.203.106, 172.217.168.35, 142.250.203.99, 172.217.168.46, 23.201.255.245, 23.54.112.17, 23.211.5.73, 23.211.6.156, 2.19.65.180, 23.211.5.115, 95.100.53.185, 172.217.168.10
- Excluded domains from analysis (whitelisted): www.apple.com.edgekey.net.globalredir.akadns.net, xp.itunes-apple.com.akadns.net, ssl.gstatic.com, js-cdn.music.apple.com, linkmaker.itunes.apple.com.edgekey.net, geo.itunes.apple.com, clientservices.googleapis.com, api-edge.apps.apple.com.edgekey.net, amp-api.apps.apple.com.edgekey.net, www.apple.com, api-edge.apps-lb.itunes-apple.com.akadns.net, e17437.dsct.akamaiedge.net, xp.apple.com, itunes.apple.com.edgekey.net, e3925.dscx.akamaiedge.net, update.googleapis.com, xp.apple.com.edgekey.net, www.gstatic.com, js-cdn-music-lb.itunes-apple.com.akadns.net, amp-api.apps-lb.itunes-apple.com.akadns.net, www.google-analytics.com, e8143.dscb.akamaiedge.net, content-autofill.googleapis.com, fonts.gstatic.com, e673.dsce9.akamaiedge.net, amp-api.apps.apple.com, e4541.dsce9.akamaiedge.net, authorize.music.apple.com.edgekey.net, e6858.dscx.akamaiedge.net, api-edge.apps.apple.com, apps.apple.com, itunes-cdn.itunes-apple.com.akadns.net, e673.dscx.akamaiedge.net, edgedl.me.gvt1.c
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing network information.
- Report size getting too big, too many NtSetInformationFile calls found.
- 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

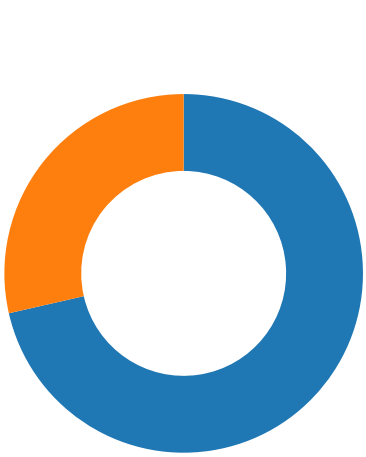
General

File type:	HTML document, ASCII text, with very long lines (6161), with CRLF line terminators
Entropy (8bit):	3.818974399863528
TrID:	• HyperText Markup Language (28028/1) 100.00%
File name:	RemitAdvise.htm
File size:	6163
MD5:	c362c76446daf05abf9c15bfdc302f8e
SHA1:	7e026d5740662c82d66aeebc50c60a0845b0c6cf
SHA256:	e313c6a9462722e28a6703945b639ab5104ae189645c33a0eb6d724558159bb2
SHA512:	0aa58b64c4739ac716ca90298c2a929879b9aa7b64c39bfcd4be71135fe1574680329805ea2b3d17a92e6d3720bde22590acc9558b9f610b35a443f0994407e2
SSDEEP:	48:FjSBHejEcTrxhI2wAHXyVyL2lyhqKu/qMoLjqlA+03kxkWqiaKTSyFyfbDy01QOB:JSZeYcTd3eJy5eaGHJXLpiQ78JnDVBGL
TLSH:	9BD112C4EB9CE5071B8D4D8AA9D79DDB5074C466D4C56383D2E8FC8C28E991ECB9CCA0
File Content Preview:	<script language=javascript>var _0x563af2=_0x5bb0;function _0x5bb0(_0x4895f1,_0x56e935){var _0x424a06=_0x424a();return _0x5bb0=function(_0x5bb033,_0x38e947){_0x5bb033=_0x5bb033-0x99;var _0x1084ca=_0x424a06[_0x5bb033];return _0x1084ca;},_0x5bb0(_0x4895f1,_

Network Behavior

Network Port Distribution

Total Packets: 63



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 02:02:09.870985985 CET	49172	443	192.168.2.22	185.219.221.37
Nov 30, 2022 02:02:09.871062994 CET	443	49172	185.219.221.37	192.168.2.22
Nov 30, 2022 02:02:09.871128082 CET	49172	443	192.168.2.22	185.219.221.37
Nov 30, 2022 02:02:09.872013092 CET	49173	443	192.168.2.22	185.219.221.37
Nov 30, 2022 02:02:09.872066975 CET	443	49173	185.219.221.37	192.168.2.22
Nov 30, 2022 02:02:09.872123003 CET	49173	443	192.168.2.22	185.219.221.37
Nov 30, 2022 02:02:09.873418093 CET	49172	443	192.168.2.22	185.219.221.37
Nov 30, 2022 02:02:09.873449087 CET	443	49172	185.219.221.37	192.168.2.22
Nov 30, 2022 02:02:09.873773098 CET	49173	443	192.168.2.22	185.219.221.37
Nov 30, 2022 02:02:09.873796940 CET	443	49173	185.219.221.37	192.168.2.22
Nov 30, 2022 02:02:09.881747007 CET	49175	443	192.168.2.22	142.250.203.110
Nov 30, 2022 02:02:09.881793976 CET	443	49175	142.250.203.110	192.168.2.22
Nov 30, 2022 02:02:09.881892920 CET	49175	443	192.168.2.22	142.250.203.110
Nov 30, 2022 02:02:09.882128000 CET	49175	443	192.168.2.22	142.250.203.110
Nov 30, 2022 02:02:09.882152081 CET	443	49175	142.250.203.110	192.168.2.22
Nov 30, 2022 02:02:09.883446932 CET	49176	443	192.168.2.22	172.217.168.77
Nov 30, 2022 02:02:09.883491039 CET	443	49176	172.217.168.77	192.168.2.22
Nov 30, 2022 02:02:09.883555889 CET	49176	443	192.168.2.22	172.217.168.77
Nov 30, 2022 02:02:09.883795023 CET	49176	443	192.168.2.22	172.217.168.77
Nov 30, 2022 02:02:09.883824110 CET	443	49176	172.217.168.77	192.168.2.22
Nov 30, 2022 02:02:09.928596020 CET	443	49173	185.219.221.37	192.168.2.22
Nov 30, 2022 02:02:09.932131052 CET	443	49172	185.219.221.37	192.168.2.22
Nov 30, 2022 02:02:09.936626911 CET	49173	443	192.168.2.22	185.219.221.37
Nov 30, 2022 02:02:09.936660051 CET	443	49173	185.219.221.37	192.168.2.22
Nov 30, 2022 02:02:09.937175035 CET	49172	443	192.168.2.22	185.219.221.37
Nov 30, 2022 02:02:09.937211037 CET	443	49172	185.219.221.37	192.168.2.22
Nov 30, 2022 02:02:09.938929081 CET	443	49172	185.219.221.37	192.168.2.22
Nov 30, 2022 02:02:09.939006090 CET	49172	443	192.168.2.22	185.219.221.37
Nov 30, 2022 02:02:09.940270901 CET	443	49173	185.219.221.37	192.168.2.22
Nov 30, 2022 02:02:09.940342903 CET	49173	443	192.168.2.22	185.219.221.37
Nov 30, 2022 02:02:09.959259033 CET	443	49176	172.217.168.77	192.168.2.22
Nov 30, 2022 02:02:09.960578918 CET	49176	443	192.168.2.22	172.217.168.77
Nov 30, 2022 02:02:09.960633039 CET	443	49176	172.217.168.77	192.168.2.22
Nov 30, 2022 02:02:09.961920977 CET	443	49176	172.217.168.77	192.168.2.22
Nov 30, 2022 02:02:09.962014914 CET	49176	443	192.168.2.22	172.217.168.77
Nov 30, 2022 02:02:09.967482090 CET	443	49175	142.250.203.110	192.168.2.22
Nov 30, 2022 02:02:09.967886925 CET	49175	443	192.168.2.22	142.250.203.110
Nov 30, 2022 02:02:09.967920065 CET	443	49175	142.250.203.110	192.168.2.22
Nov 30, 2022 02:02:09.968913078 CET	443	49175	142.250.203.110	192.168.2.22
Nov 30, 2022 02:02:09.968988895 CET	49175	443	192.168.2.22	142.250.203.110
Nov 30, 2022 02:02:09.970366001 CET	443	49175	142.250.203.110	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 02:02:09.970421076 CET	49175	443	192.168.2.22	142.250.203.110
Nov 30, 2022 02:02:10.427983046 CET	49176	443	192.168.2.22	172.217.168.77
Nov 30, 2022 02:02:10.428046942 CET	443	49176	172.217.168.77	192.168.2.22
Nov 30, 2022 02:02:10.428234100 CET	443	49176	172.217.168.77	192.168.2.22
Nov 30, 2022 02:02:10.428610086 CET	49176	443	192.168.2.22	172.217.168.77
Nov 30, 2022 02:02:10.428639889 CET	443	49176	172.217.168.77	192.168.2.22
Nov 30, 2022 02:02:10.444356918 CET	49175	443	192.168.2.22	142.250.203.110
Nov 30, 2022 02:02:10.444441080 CET	443	49175	142.250.203.110	192.168.2.22
Nov 30, 2022 02:02:10.444622993 CET	443	49175	142.250.203.110	192.168.2.22
Nov 30, 2022 02:02:10.444854021 CET	49172	443	192.168.2.22	185.219.221.37
Nov 30, 2022 02:02:10.444895983 CET	443	49172	185.219.221.37	192.168.2.22
Nov 30, 2022 02:02:10.444977999 CET	49173	443	192.168.2.22	185.219.221.37
Nov 30, 2022 02:02:10.445004940 CET	443	49173	185.219.221.37	192.168.2.22
Nov 30, 2022 02:02:10.445101976 CET	49175	443	192.168.2.22	142.250.203.110
Nov 30, 2022 02:02:10.445106030 CET	443	49172	185.219.221.37	192.168.2.22
Nov 30, 2022 02:02:10.445131063 CET	443	49175	142.250.203.110	192.168.2.22
Nov 30, 2022 02:02:10.445297956 CET	443	49173	185.219.221.37	192.168.2.22
Nov 30, 2022 02:02:10.445674896 CET	49172	443	192.168.2.22	185.219.221.37
Nov 30, 2022 02:02:10.445702076 CET	443	49172	185.219.221.37	192.168.2.22
Nov 30, 2022 02:02:10.480714083 CET	443	49175	142.250.203.110	192.168.2.22
Nov 30, 2022 02:02:10.480779886 CET	49175	443	192.168.2.22	142.250.203.110
Nov 30, 2022 02:02:10.480803967 CET	443	49175	142.250.203.110	192.168.2.22
Nov 30, 2022 02:02:10.480887890 CET	443	49175	142.250.203.110	192.168.2.22
Nov 30, 2022 02:02:10.480940104 CET	49175	443	192.168.2.22	142.250.203.110
Nov 30, 2022 02:02:10.482100964 CET	443	49176	172.217.168.77	192.168.2.22
Nov 30, 2022 02:02:10.482162952 CET	49176	443	192.168.2.22	172.217.168.77
Nov 30, 2022 02:02:10.482201099 CET	443	49176	172.217.168.77	192.168.2.22
Nov 30, 2022 02:02:10.482278109 CET	443	49176	172.217.168.77	192.168.2.22
Nov 30, 2022 02:02:10.482325077 CET	49176	443	192.168.2.22	172.217.168.77
Nov 30, 2022 02:02:10.485585928 CET	49175	443	192.168.2.22	142.250.203.110
Nov 30, 2022 02:02:10.485608101 CET	443	49175	142.250.203.110	192.168.2.22
Nov 30, 2022 02:02:10.487008095 CET	49176	443	192.168.2.22	172.217.168.77
Nov 30, 2022 02:02:10.487040997 CET	443	49176	172.217.168.77	192.168.2.22
Nov 30, 2022 02:02:10.511945963 CET	443	49172	185.219.221.37	192.168.2.22
Nov 30, 2022 02:02:10.512043953 CET	49172	443	192.168.2.22	185.219.221.37
Nov 30, 2022 02:02:10.533257008 CET	49172	443	192.168.2.22	185.219.221.37
Nov 30, 2022 02:02:10.533307076 CET	443	49172	185.219.221.37	192.168.2.22
Nov 30, 2022 02:02:10.650918007 CET	443	49173	185.219.221.37	192.168.2.22
Nov 30, 2022 02:02:10.651076078 CET	49173	443	192.168.2.22	185.219.221.37
Nov 30, 2022 02:02:10.696391106 CET	49180	443	192.168.2.22	13.32.27.109
Nov 30, 2022 02:02:10.696479082 CET	443	49180	13.32.27.109	192.168.2.22
Nov 30, 2022 02:02:10.696578979 CET	49180	443	192.168.2.22	13.32.27.109
Nov 30, 2022 02:02:10.697118044 CET	49180	443	192.168.2.22	13.32.27.109
Nov 30, 2022 02:02:10.697158098 CET	443	49180	13.32.27.109	192.168.2.22
Nov 30, 2022 02:02:10.747747898 CET	443	49180	13.32.27.109	192.168.2.22
Nov 30, 2022 02:02:10.764036894 CET	49180	443	192.168.2.22	13.32.27.109
Nov 30, 2022 02:02:10.764071941 CET	443	49180	13.32.27.109	192.168.2.22
Nov 30, 2022 02:02:10.765532970 CET	443	49180	13.32.27.109	192.168.2.22
Nov 30, 2022 02:02:10.765646935 CET	49180	443	192.168.2.22	13.32.27.109
Nov 30, 2022 02:02:10.792428970 CET	49180	443	192.168.2.22	13.32.27.109
Nov 30, 2022 02:02:10.792464018 CET	443	49180	13.32.27.109	192.168.2.22
Nov 30, 2022 02:02:10.792666912 CET	443	49180	13.32.27.109	192.168.2.22
Nov 30, 2022 02:02:10.792855024 CET	49180	443	192.168.2.22	13.32.27.109
Nov 30, 2022 02:02:10.792872906 CET	443	49180	13.32.27.109	192.168.2.22
Nov 30, 2022 02:02:10.817615032 CET	443	49180	13.32.27.109	192.168.2.22
Nov 30, 2022 02:02:10.817646980 CET	443	49180	13.32.27.109	192.168.2.22
Nov 30, 2022 02:02:10.817662954 CET	443	49180	13.32.27.109	192.168.2.22
Nov 30, 2022 02:02:10.817673922 CET	49180	443	192.168.2.22	13.32.27.109
Nov 30, 2022 02:02:10.817701101 CET	443	49180	13.32.27.109	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 02:02:07.701484919 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:02:08.451370001 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:02:09.147629976 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:02:09.202126980 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:02:09.243455887 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:02:09.848303080 CET	54408	53	192.168.2.22	8.8.8.8
Nov 30, 2022 02:02:09.853604078 CET	50108	53	192.168.2.22	8.8.8.8
Nov 30, 2022 02:02:09.854718924 CET	58062	53	192.168.2.22	8.8.8.8
Nov 30, 2022 02:02:09.865802050 CET	53	54408	8.8.8.8	192.168.2.22
Nov 30, 2022 02:02:09.879867077 CET	53	58062	8.8.8.8	192.168.2.22
Nov 30, 2022 02:02:09.882285118 CET	53	50108	8.8.8.8	192.168.2.22
Nov 30, 2022 02:02:09.897150993 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:02:09.993223906 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:02:10.630156040 CET	56703	53	192.168.2.22	8.8.8.8
Nov 30, 2022 02:02:10.647308111 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:02:10.651102066 CET	53	56703	8.8.8.8	192.168.2.22
Nov 30, 2022 02:02:10.743251085 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:02:12.732223034 CET	55244	53	192.168.2.22	8.8.8.8
Nov 30, 2022 02:02:12.756011009 CET	53	55244	8.8.8.8	192.168.2.22
Nov 30, 2022 02:02:13.515991926 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:02:13.517414093 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:02:13.517597914 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:02:14.265815973 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:02:14.266741037 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:02:14.266763926 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:02:15.015898943 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:02:15.016844034 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:02:15.016868114 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:02:16.505009890 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:02:17.254829884 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:02:18.004993916 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:02:18.161231995 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:02:18.162872076 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:02:18.924283028 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:02:18.926609993 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:02:19.674344063 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:02:19.674393892 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:02:26.518843889 CET	52276	53	192.168.2.22	8.8.8.8
Nov 30, 2022 02:02:26.538994074 CET	53	52276	8.8.8.8	192.168.2.22
Nov 30, 2022 02:02:34.887208939 CET	53057	53	192.168.2.22	8.8.8.8
Nov 30, 2022 02:02:34.914674997 CET	53	53057	8.8.8.8	192.168.2.22
Nov 30, 2022 02:02:35.338120937 CET	56509	53	192.168.2.22	8.8.8.8
Nov 30, 2022 02:02:35.365209103 CET	53	56509	8.8.8.8	192.168.2.22
Nov 30, 2022 02:02:38.990597963 CET	51840	53	192.168.2.22	8.8.8.8
Nov 30, 2022 02:02:39.009623051 CET	53	51840	8.8.8.8	192.168.2.22
Nov 30, 2022 02:02:39.920795918 CET	51454	53	192.168.2.22	8.8.8.8
Nov 30, 2022 02:02:39.946594000 CET	53	51454	8.8.8.8	192.168.2.22
Nov 30, 2022 02:02:40.313373089 CET	63972	53	192.168.2.22	8.8.8.8
Nov 30, 2022 02:02:40.353683949 CET	53	63972	8.8.8.8	192.168.2.22
Nov 30, 2022 02:02:41.646581888 CET	138	138	192.168.2.22	192.168.2.255
Nov 30, 2022 02:02:45.108043909 CET	51302	53	192.168.2.22	8.8.8.8
Nov 30, 2022 02:02:45.453130007 CET	54031	53	192.168.2.22	8.8.8.8
Nov 30, 2022 02:02:45.454031944 CET	57939	53	192.168.2.22	8.8.8.8
Nov 30, 2022 02:02:45.804205894 CET	58584	53	192.168.2.22	8.8.8.8
Nov 30, 2022 02:02:45.914413929 CET	64769	53	192.168.2.22	8.8.8.8
Nov 30, 2022 02:02:50.209343910 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:02:50.968570948 CET	137	137	192.168.2.22	192.168.2.255

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 02:02:51.733062029 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:03:02.095618963 CET	62240	53	192.168.2.22	8.8.8.8
Nov 30, 2022 02:03:02.115124941 CET	53	62240	8.8.8.8	192.168.2.22
Nov 30, 2022 02:03:07.880156040 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:03:08.633939028 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:03:09.398438931 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:03:11.152112007 CET	56031	53	192.168.2.22	8.8.8.8
Nov 30, 2022 02:03:11.174747944 CET	53	56031	8.8.8.8	192.168.2.22
Nov 30, 2022 02:04:11.222244024 CET	138	138	192.168.2.22	192.168.2.255
Nov 30, 2022 02:05:13.194169044 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:05:13.949223995 CET	137	137	192.168.2.22	192.168.2.255
Nov 30, 2022 02:05:14.713828087 CET	137	137	192.168.2.22	192.168.2.255

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 30, 2022 02:02:09.848303080 CET	192.168.2.22	8.8.8.8	0xc279	Standard query (0)	lmo.olinef ilesforwor ksany.biz	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:09.853604078 CET	192.168.2.22	8.8.8.8	0x6392	Standard query (0)	accounts.g oogle.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:09.854718924 CET	192.168.2.22	8.8.8.8	0x4cb4	Standard query (0)	clients2.g oogle.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:10.630156040 CET	192.168.2.22	8.8.8.8	0xa3e8	Standard query (0)	brave.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:12.732223034 CET	192.168.2.22	8.8.8.8	0x7faa	Standard query (0)	analytics. brave.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:26.518843889 CET	192.168.2.22	8.8.8.8	0x9d46	Standard query (0)	brave.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:34.887208939 CET	192.168.2.22	8.8.8.8	0xeccb	Standard query (0)	play.google.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:35.338120937 CET	192.168.2.22	8.8.8.8	0x9d90	Standard query (0)	play-lh.go ogleuserco ntent.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:38.990597963 CET	192.168.2.22	8.8.8.8	0x8cb	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:39.920795918 CET	192.168.2.22	8.8.8.8	0x3e35	Standard query (0)	stats.g.do ubleclick.net	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:40.313373089 CET	192.168.2.22	8.8.8.8	0x174f	Standard query (0)	www.google.fr	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:45.108043909 CET	192.168.2.22	8.8.8.8	0x8323	Standard query (0)	is1-ssl.mz static.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:45.453130007 CET	192.168.2.22	8.8.8.8	0x3a3	Standard query (0)	is5-ssl.mz static.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:45.454031944 CET	192.168.2.22	8.8.8.8	0xb6d3	Standard query (0)	is4-ssl.mz static.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:45.804205894 CET	192.168.2.22	8.8.8.8	0xc0fb	Standard query (0)	is3-ssl.mz static.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:45.914413929 CET	192.168.2.22	8.8.8.8	0x27b4	Standard query (0)	is2-ssl.mz static.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:03:02.095618963 CET	192.168.2.22	8.8.8.8	0x97bf	Standard query (0)	play-lh.go ogleuserco ntent.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:03:11.152112007 CET	192.168.2.22	8.8.8.8	0x3512	Standard query (0)	brave.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 30, 2022 02:02:09.865802050 CET	8.8.8.8	192.168.2.22	0xc279	No error (0)	lmo.olinef ilesforwor ksany.biz		185.219.221.3 7	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:09.879867077 CET	8.8.8.8	192.168.2.22	0x4cb4	No error (0)	clients2.g oogle.com	clients.l.google .com		CNAME (Canonical name)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 02:02:09.879867077 CET	8.8.8.8	192.168.2.22	0x4cb4	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:09.882285118 CET	8.8.8.8	192.168.2.22	0x6392	No error (0)	accounts.google.com		172.217.168.77	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:10.651102066 CET	8.8.8.8	192.168.2.22	0xa3e8	No error (0)	brave.com		13.32.27.109	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:10.651102066 CET	8.8.8.8	192.168.2.22	0xa3e8	No error (0)	brave.com		13.32.27.82	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:10.651102066 CET	8.8.8.8	192.168.2.22	0xa3e8	No error (0)	brave.com		13.32.27.67	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:10.651102066 CET	8.8.8.8	192.168.2.22	0xa3e8	No error (0)	brave.com		13.32.27.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:12.756011009 CET	8.8.8.8	192.168.2.22	0x7faa	No error (0)	analytics.brave.com	d2cbcq2c2d2d1v.cloudfront.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 30, 2022 02:02:12.756011009 CET	8.8.8.8	192.168.2.22	0x7faa	No error (0)	d2cbcq2c2d2d1v.cloudfront.net		108.156.60.111	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:12.756011009 CET	8.8.8.8	192.168.2.22	0x7faa	No error (0)	d2cbcq2c2d2d1v.cloudfront.net		108.156.60.34	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:12.756011009 CET	8.8.8.8	192.168.2.22	0x7faa	No error (0)	d2cbcq2c2d2d1v.cloudfront.net		108.156.60.128	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:12.756011009 CET	8.8.8.8	192.168.2.22	0x7faa	No error (0)	d2cbcq2c2d2d1v.cloudfront.net		108.156.60.99	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:26.538994074 CET	8.8.8.8	192.168.2.22	0x9d46	No error (0)	brave.com		13.32.27.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:26.538994074 CET	8.8.8.8	192.168.2.22	0x9d46	No error (0)	brave.com		13.32.27.109	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:26.538994074 CET	8.8.8.8	192.168.2.22	0x9d46	No error (0)	brave.com		13.32.27.82	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:26.538994074 CET	8.8.8.8	192.168.2.22	0x9d46	No error (0)	brave.com		13.32.27.67	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:34.914674997 CET	8.8.8.8	192.168.2.22	0xeccb	No error (0)	play.google.com		172.217.168.78	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:35.365209103 CET	8.8.8.8	192.168.2.22	0x9d90	No error (0)	play-lh.googleusercontent.com		142.250.203.118	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:39.009623051 CET	8.8.8.8	192.168.2.22	0x8cb	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:39.946594000 CET	8.8.8.8	192.168.2.22	0x3e35	No error (0)	stats.g.doubleclick.net		142.250.153.154	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:39.946594000 CET	8.8.8.8	192.168.2.22	0x3e35	No error (0)	stats.g.doubleclick.net		142.250.153.156	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:39.946594000 CET	8.8.8.8	192.168.2.22	0x3e35	No error (0)	stats.g.doubleclick.net		142.250.153.157	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:39.946594000 CET	8.8.8.8	192.168.2.22	0x3e35	No error (0)	stats.g.doubleclick.net		142.250.153.155	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:40.353683949 CET	8.8.8.8	192.168.2.22	0x174f	No error (0)	www.google.fr		172.217.168.3	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:02:45.139105082 CET	8.8.8.8	192.168.2.22	0x8323	No error (0)	is1-ssl.mzstatic.com	is-ssl.mzstatic.com.itunes-apple.com.akadns.net		CNAME (Canonical name)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 02:02:45.482409000 CET	8.8.8.8	192.168.2.22	0x3a3	No error (0)	is5-ssl.mzstatic.com	is-ssl.mzstatic.com.itunes-apple.com.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 30, 2022 02:02:45.485385895 CET	8.8.8.8	192.168.2.22	0xb6d3	No error (0)	is4-ssl.mzstatic.com	is-ssl.mzstatic.com.itunes-apple.com.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 30, 2022 02:02:45.833405018 CET	8.8.8.8	192.168.2.22	0xc0fb	No error (0)	is3-ssl.mzstatic.com	is-ssl.mzstatic.com.itunes-apple.com.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 30, 2022 02:02:45.958981037 CET	8.8.8.8	192.168.2.22	0x27b4	No error (0)	is2-ssl.mzstatic.com	is-ssl.mzstatic.com.itunes-apple.com.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 30, 2022 02:03:02.115124941 CET	8.8.8.8	192.168.2.22	0x97bf	No error (0)	play-lh.googleusercontent.com		142.250.203.118	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:03:11.174747944 CET	8.8.8.8	192.168.2.22	0x3512	No error (0)	brave.com		13.32.27.82	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:03:11.174747944 CET	8.8.8.8	192.168.2.22	0x3512	No error (0)	brave.com		13.32.27.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:03:11.174747944 CET	8.8.8.8	192.168.2.22	0x3512	No error (0)	brave.com		13.32.27.67	A (IP address)	IN (0x0001)	false
Nov 30, 2022 02:03:11.174747944 CET	8.8.8.8	192.168.2.22	0x3512	No error (0)	brave.com		13.32.27.109	A (IP address)	IN (0x0001)	false

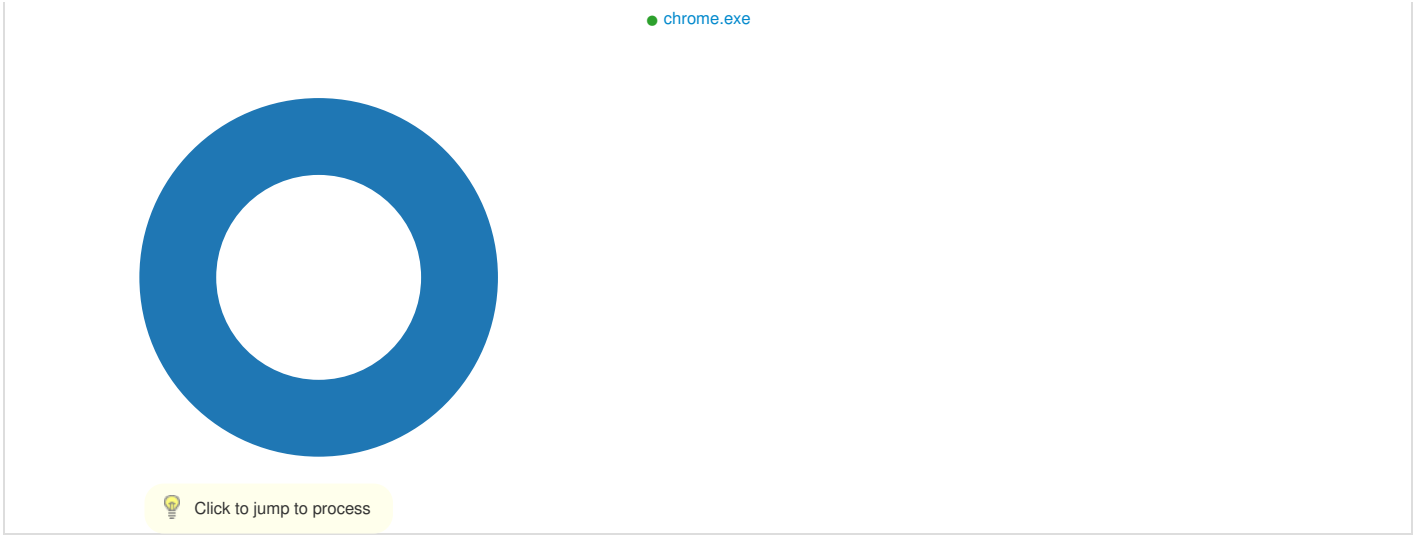
HTTP Request Dependency Graph

- accounts.google.com
- clients2.google.com
- lmo.olinefilesforworksany.biz
- brave.com
- https:
  - analytics.brave.com
  - play-lh.googleusercontent.com
  - play.google.com
  - www.google.com
  - stats.g.doubleclick.net
  - www.google.fr

Statistics

Behavior

chrome.exe
chrome.exe



System Behavior

Analysis Process: chrome.exe PID: 3000, Parent PID: 2600

General

Target ID:	0
Start time:	02:02:12
Start date:	30/11/2022
Path:	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank
Imagebase:	0x13f930000
File size:	1820656 bytes
MD5 hash:	6ACAE527E744C80997B25EF2A0485D5E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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

Analysis Process: chrome.exe PID: 832, Parent PID: 3000

General

Target ID:	1
Start time:	02:02:15
Start date:	30/11/2022
Path:	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false

Commandline:	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=952,1834247139616653473 9,13915805133651195408,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1452 /prefetch:8
Imagebase:	0x13f930000
File size:	1820656 bytes
MD5 hash:	6ACAE527E744C80997B25EF2A0485D5E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **804**, Parent PID: **2600**

General

Target ID:	4
Start time:	02:02:16
Start date:	30/11/2022
Path:	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" "C:\Users\user\Desktop\RemitAdvise.htm
Imagebase:	0x13f930000
File size:	1820656 bytes
MD5 hash:	6ACAE527E744C80997B25EF2A0485D5E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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