ID: 753415
Cookbook: browseurl.jbs
Time: 19:37:28
Date: 24/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Copyright Joe Security LLC 2022

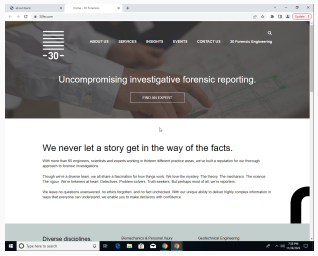
Windows Analysis Report

http://www.30fe.com/

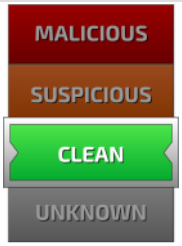
Overview

General Information

Sample URL:	http://www.30fe.com/
Analysis ID:	753415
Infos:	



Detection

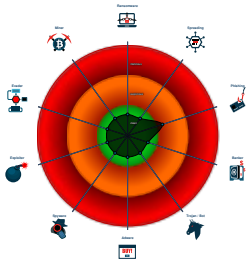


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

No HTML title found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 3584 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 1400 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=1968 --field-trial-handle=1764,i,17311812855738133621,17887974914451854333,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 5204 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "http://www.30fe.com/ MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Copyright Joe Security LLC 2022

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

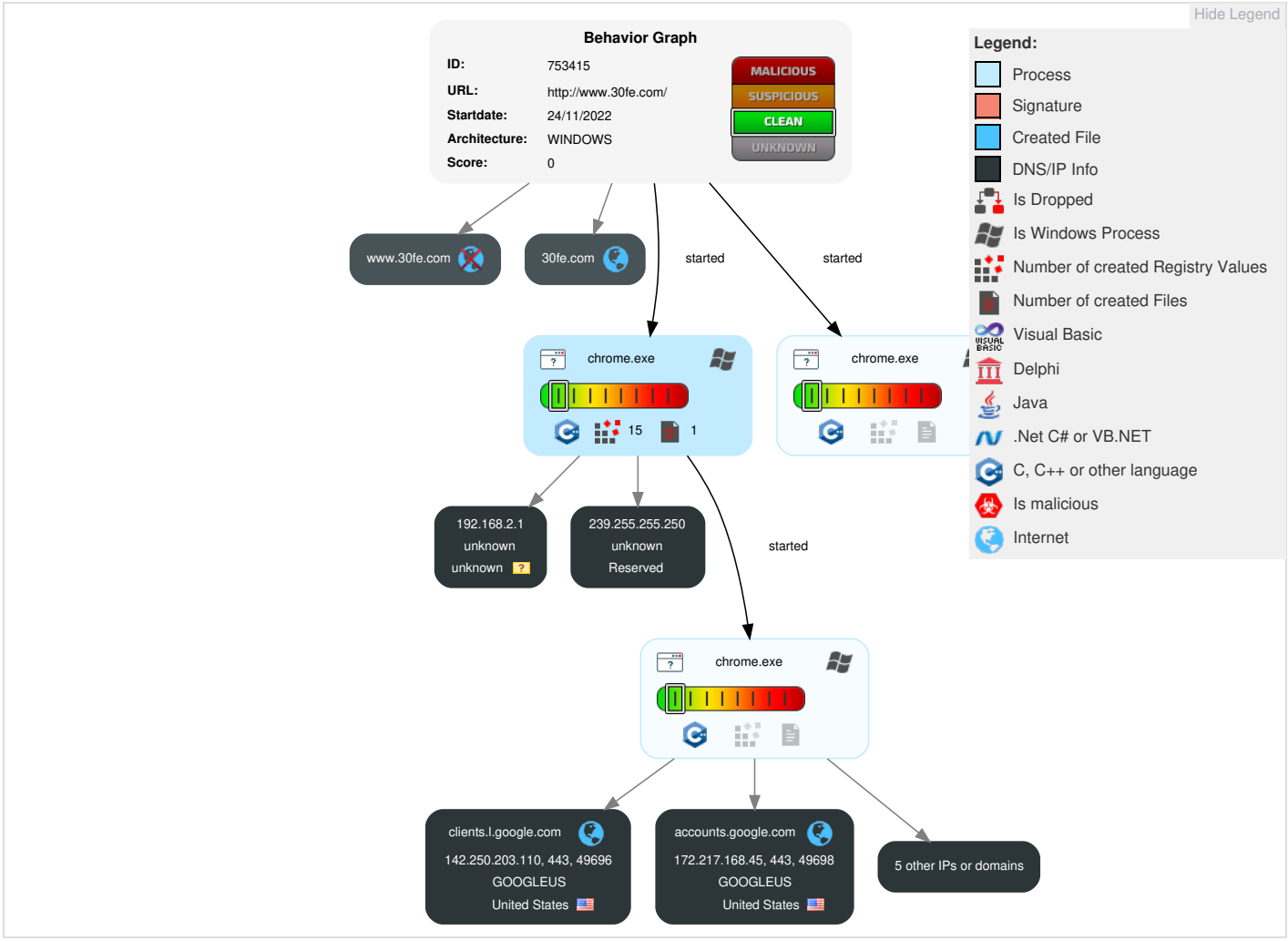
There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	2 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	4 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

Behavior Graph

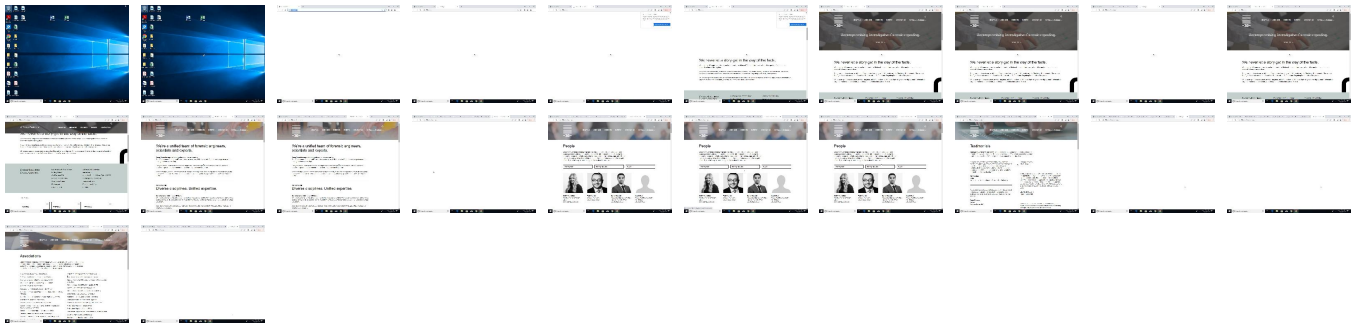
Copyright Joe Security LLC 2022

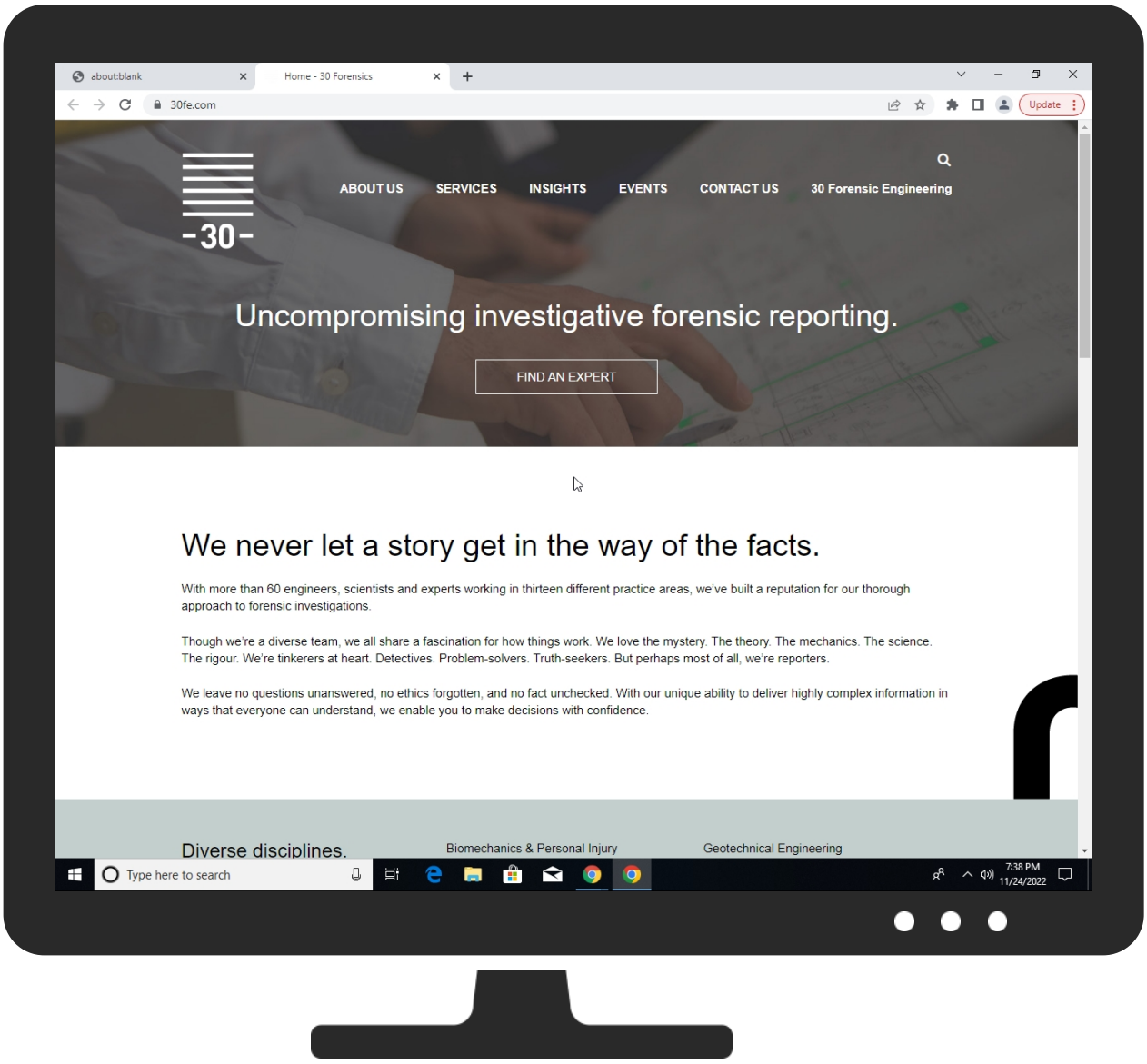


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://www.30fe.com/	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://www.30fe.com/wp-content/uploads/elementor/css/post-4870.css	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/20220117-Antone-Dabeet_5204111-360x360.png	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/DSCF0248-Edit-copy-2-360x360.png	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
http://https://www.30fe.com/wp-content/themes/30forensics/assets/images/30logo_CropE.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/30fe_homepage_May2017.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/DSCF9169-Edit-360x360.png	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/Matt-Hartog-Final-web-3-2-360x360.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/Sparling_Rob-360x360.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/DSCF7763-Crop-center-360x360.png	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/DSCF9541-copy-3-360x360.png	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/DSCF0796_AI-360x360.png	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/DSCF7991_edit2-360x360.png	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/themes/30forensics/assets/css/slick-theme.css	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/30fe-f-360x360.png	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/themes/30forensics/assets/images/30logo_cropC.png	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/DSCF1339-Edit4-crop-2-360x360.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/30fe-f-150x150.png	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/Sinclair-Brittany-Final-DSCF5431-Edit-highres-360x360.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/plugins/elementor/assets/css/frontend-legacy.min.css	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/Chris-Ciasnocha-FinalDSCF5912-Edit-highres-e1505313763214-360x360.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/themes/30forensics/assets/js/30f.main.js	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/FUJI0990-22-360x360.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/Fabbroni_Mark-360x360.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/themes/30forensics/assets/images/30logo_cropA.png	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/DSCF2814-360x360.png	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/plugins/gp-premium/general/icons/icons.min.css	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/plugins/formidable/css/formidableforms.css	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/2017/03/subscribe-bg.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/DSCF6937_ps-360x360.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/plugins/elementor/assets/lib/font-awesome/fonts/fontawesome-webfont.woff2?v=4.7.0	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/2017/04/30Logo_White_RGB.png	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/themes/generatepress/assets/css/unsemantic-grid.min.css	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/DSCF6328-360x360.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/plugins/gp-premium/menu-plus/functions/css/sticky.min.css	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/DSCF6593-360x360.png	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/DSCF3966-2_AI-360x360.png	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/Rhode_John-360x360.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/DSCF9905-copy-crop-size.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/Saleh_Emily-360x360.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/plugins/elementor/assets/lib/font-awesome/css/v4-shims.min.css	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/plugins/elementor/assets/lib/font-awesome/css/font-awesome.min.css	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/iStock-520410819_Testimonials_1920x200.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/themes/30forensics/assets/js/slick.min.js	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/plugins/enable-jquery-migrate-helper/js/jquery/jquery-1.12.4-wp.js	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/Muir_Brad-360x360.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/plugins/elementor/assets/lib/font-awesome/js/v4-shims.min.js	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/Paquette_Mark-360x360.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/themes/30forensics/assets/css/magnific-popup.css	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/plugins/gp-premium/menu-plus/functions/js/sticky.min.js	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/plugins/gp-premium/menu-plus/functions/css/menu-logo.min.css	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/CivilStructural-Failure.png	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/Jamie_Final_Web-Main-360x360.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/Robalino_Pablo-360x360.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/FUJI2327-editse-360x360.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/FUJI3217-copy-3-360x360.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/FUJI1444-360x360.png	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/themes/30forensics/assets/images/social/twitter.png	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/themes/30forensics/style.css	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/plugins/gp-premium/sections/functions/js/parallax.min.js	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://www.30fe.com/wp-content/plugins/gp-premium/menu-plus/functions/js/offside.min.js	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/DSCF6999-360x360.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/DSCF5151-cc-crop-360x360.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/themes/30forensics/assets/images/30logo_cropB.png	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/DSCF6501crop-360x360.png	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-includes/css/dist/block-library/style.min.css	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/DSCF5137-360x360.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/themes/generatepress/assets/css/mobile.min.css	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/themes/30forensics/assets/css/slick.css	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/themes/30forensics/assets/js/jquery.magnific-popup.min.js	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/Fire-Electrical.png	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/DSCF7468-copy-360x360.png	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/DSCF3067-Recovered-copy-4-360x360.png	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/Aquino_Paul-360x360.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/DSCF9289-copy-360x360.png	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/plugins/gp-premium/sections/functions/css/style.min.css	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/themes/30forensics/assets/images/social/linkedin.png	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/FUJI2992-copy-2-360x360.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/jfabmedia-15-edit-360x360.png	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/elementor/css/global.css	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/Jim_Rob3-360x352.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/General_April25.png	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/Parkinson_Rob-360x360.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-includes/css/classic-themes.min.css	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/DSCF4467-Edit-360x360.png	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/Toughlouian_Jennifer-360x360.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/themes/30forensics/assets/js/list.min.js	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/plugins/elementor/assets/lib/font-awesome/css/all.min.css	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/DSCF7323-edit-360x360.png	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/FUJI1354-edit2-crop-360x360.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/iStock-530188857_AboutUs_1920x200.jpg	0%	Avira URL Cloud	safe	
http://https://www.30fe.com/wp-content/uploads/Fisher_Derek-360x360.jpg	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	172.217.168.45	true	false		high
30fe.com	35.206.111.91	true	false		unknown
www.google.com	172.217.168.68	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
clients2.google.com	unknown	unknown	false		high
www.30fe.com	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.30fe.com/news/	false		unknown
http://https://www.30fe.com/wp-content/themes/30forensics/assets/images/30logo_CropE.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/DSCF0248-Edit-copy-2-360x360.png	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/testimonials/	false		unknown
http://https://www.30fe.com/wp-content/uploads/elementor/css/post-4870.css	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/DSCF9169-Edit-360x360.png	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/about-us/	false		unknown
http://https://www.30fe.com/wp-content/uploads/20220117-Antone-Dabeet_5204111-360x360.png	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/30fe_homepage_May2017.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/Matt-Hartog-Final-web-3-2-360x360.jpg	false	• Avira URL Cloud: safe	unknown

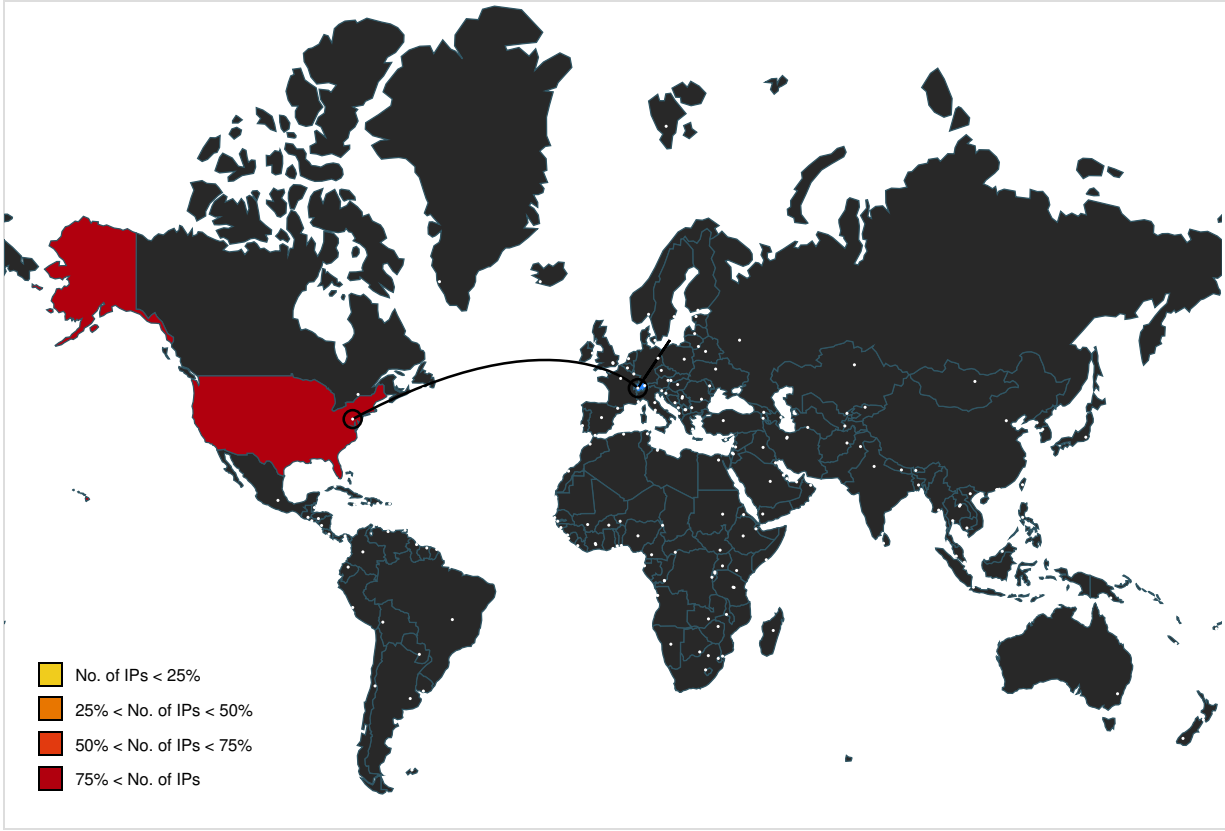
Copyright Joe Security LLC 2022

Name	Malicious	Antivirus Detection	Reputation
http://https://www.30fe.com/wp-content/uploads/Sparling_Rob-360x360.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/DSCF9541-copy-3-360x360.png	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/DSCF7763-Crop-center-360x360.png	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/DSCF7991_edit2-360x360.png	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/DSCF0796_AI-360x360.png	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/themes/30forensics/assets/css/slick-theme.css	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/themes/30forensics/assets/images/30logo_cropC.png	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/30fe-f-360x360.png	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/DSCF1339-Edit4-crop-2-360x360.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/plugins/elementor/assets/css/frontend-legacy.min.css	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/Chris-Ciasnocha-FinalDSCF5912-Edit-highres-e1505313763214-360x360.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/Sinclair-Brittany-Final-DSCF5431-Edit-highres-360x360.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/30fe-f-150x150.png	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/themes/30forensics/assets/js/30f.main.js	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/Fabbroni_Mark-360x360.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/FUJI0990-22-360x360.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/DSCF2814-360x360.png	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/themes/30forensics/assets/images/30logo_cropA.png	false	• Avira URL Cloud: safe	unknown
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=104.0.5112.81&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.30fe.com/wp-content/plugins/formidable/css/formidableforms.css	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/plugins/gp-premium/general/icons/icons.min.css	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/plugins/elementor/assets/lib/font-awesome/fonts/fontawesome-webfont.woff2?v=4.7.0	false	• Avira URL Cloud: safe	unknown
http://www.30fe.com/	false		unknown
http://https://www.30fe.com/wp-content/uploads/2017/03/subscribe-bg.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/2017/04/30Logo_White_RGB.png	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/DSCF6937_ps-360x360.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/DSCF6328-360x360.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/themes/generatepress/assets/css/unsemantic-grid.min.css	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/plugins/gp-premium/menu-plus/functions/css/sticky.min.css	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/DSCF6593-360x360.png	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/people/	false		unknown
http://https://www.30fe.com/wp-content/uploads/DSCF3966-2_AI-360x360.png	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/Saleh_Emily-360x360.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/DSCF9905-copy-crop-size.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/plugins/elementor/assets/lib/font-awesome/css/v4-shims.min.css	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/Rhode_John-360x360.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/plugins/elementor/assets/lib/font-awesome/css/font-awesome.min.css	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/plugins/elementor/assets/lib/font-awesome/js/v4-shims.min.js	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/#content	false		unknown
http://https://www.30fe.com/wp-content/uploads/Muir_Brad-360x360.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/themes/30forensics/assets/js/slick.min.js	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/Paquette_Mark-360x360.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/iStock-520410819_Testimonials_1920x200.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/plugins/enable-jquery-migrate-helper/js/jquery/jquery-1.12.4-wp.js	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/plugins/gp-premium/menu-plus/functions/js/sticky.min.js	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/plugins/gp-premium/menu-plus/functions/css/menu-logo.min.css	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/themes/30forensics/assets/css/magnific-popup.css	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/CivilStructural-Failure.png	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/Jamie_Final_Web-Main-360x360.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/FUJI2327-editse-360x360.jpg	false	• Avira URL Cloud: safe	unknown

Copyright Joe Security LLC 2022

Name	Malicious	Antivirus Detection	Reputation
http://https://www.30fe.com/wp-content/uploads/Robalino_Pablo-360x360.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/about-us/	false		unknown
http://https://www.30fe.com/wp-content/uploads/FUJI3217-copy-3-360x360.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/plugins/gp-premium/menu-plus/functions/js/offside.min.js	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/themes/30forensics/assets/images/social/twitter.png	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/plugins/gp-premium/sections/functions/js/parallax.min.js	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/FUJI1444-360x360.png	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/themes/30forensics/style.css	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/themes/30forensics/assets/images/30logo_cropB.png	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/DSCF6999-360x360.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/themes/generatepress/assets/css/mobile.min.css	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/DSCF5151-cc-crop-360x360.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/DSCF5137-360x360.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/DSCF6501crop-360x360.png	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-includes/css/dist/block-library/style.min.css	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/themes/30forensics/assets/css/slick.css	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/Fire-Electrical.png	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/themes/30forensics/assets/js/jquery.magnific-popup.min.js	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/Aquino_Paul-360x360.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/DSCF7468-copy-360x360.png	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/DSCF3067-Recovered-copy-4-360x360.png	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/DSCF9289-copy-360x360.png	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/plugins/gp-premium/sections/functions/css/style.min.css	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/FUJI2992-copy-2-360x360.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/themes/30forensics/assets/images/social/linkedin.png	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/Jim_Rob3-360x352.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/jfabmedia-15-edit-360x360.png	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/elementor/css/global.css	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/General_April25.png	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/Parkinson_Rob-360x360.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-includes/css/classic-themes.min.css	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/DSCF7323-edit-360x360.png	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/DSCF4467-Edit-360x360.png	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/Toughlouian_Jennifer-360x360.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/themes/30forensics/assets/js/list.min.js	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/plugins/elementor/assets/lib/font-awesome/css/all.min.css	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/associations/	false		unknown
http://https://www.30fe.com/wp-content/uploads/FUJI1354-edit2-crop-360x360.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/iStock-530188857_AboutUs_1920x200.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.30fe.com/wp-content/uploads/Fisher_Derek-360x360.jpg	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
172.217.168.68	www.google.com	United States		15169	GOOGLEUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
35.206.111.91	30fe.com	United States		19527	GOOGLE-2US	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	753415
Start date and time:	2022-11-24 19:37:28 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://www.30fe.com/
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	5
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Copyright Joe Security LLC 2022

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@32/0@10/7
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://www.30fe.com/#content • Browse: https://www.30fe.com/about-us/ • Browse: https://www.30fe.com/people/ • Browse: https://www.30fe.com/testimonials/ • Browse: https://www.30fe.com/associations/ • Browse: https://www.30fe.com/news/

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 172.217.168.67, 34.104.35.123, 142.250.203.104, 142.250.203.106, 216.239.36.178, 216.239.32.178, 216.239.38.178, 216.239.34.178, 172.217.168.42, 172.217.168.74, 216.58.215.234, 172.217.168.10
- Excluded domains from analysis (whitelisted): fonts.googleapis.com, edgedl.me.gvt1.com, content-autofill.googleapis.com, www.googletagmanager.com, fonts.gstatic.com, www-alv.google-analytics.com, update.googleapis.com, clientservices.googleapis.com, www.google-analytics.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtWriteVirtualMemory calls found.
- VT rate limit hit for: http://www.30fe.com/

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

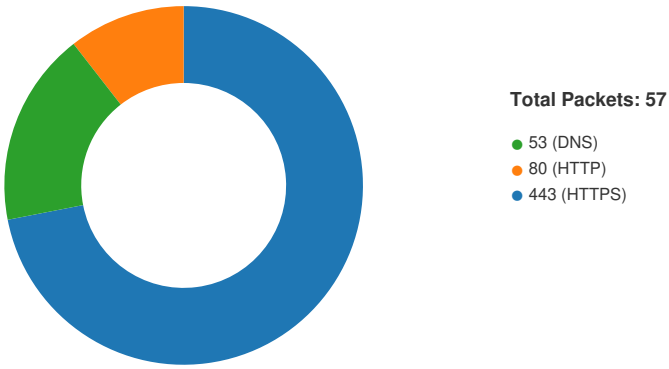
No created / dropped files found

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 19:38:19.633610964 CET	49696	443	192.168.2.4	142.250.203.110
Nov 24, 2022 19:38:19.633697033 CET	443	49696	142.250.203.110	192.168.2.4
Nov 24, 2022 19:38:19.633852005 CET	49696	443	192.168.2.4	142.250.203.110
Nov 24, 2022 19:38:19.634294987 CET	49696	443	192.168.2.4	142.250.203.110
Nov 24, 2022 19:38:19.634334087 CET	443	49696	142.250.203.110	192.168.2.4
Nov 24, 2022 19:38:19.706437111 CET	443	49696	142.250.203.110	192.168.2.4
Nov 24, 2022 19:38:19.707771063 CET	49696	443	192.168.2.4	142.250.203.110
Nov 24, 2022 19:38:19.707813025 CET	443	49696	142.250.203.110	192.168.2.4
Nov 24, 2022 19:38:19.708355904 CET	443	49696	142.250.203.110	192.168.2.4
Nov 24, 2022 19:38:19.708458900 CET	49696	443	192.168.2.4	142.250.203.110
Nov 24, 2022 19:38:19.709671021 CET	443	49696	142.250.203.110	192.168.2.4
Nov 24, 2022 19:38:19.709758043 CET	49696	443	192.168.2.4	142.250.203.110
Nov 24, 2022 19:38:20.028103113 CET	49698	443	192.168.2.4	172.217.168.45
Nov 24, 2022 19:38:20.028173923 CET	443	49698	172.217.168.45	192.168.2.4
Nov 24, 2022 19:38:20.028237104 CET	49698	443	192.168.2.4	172.217.168.45
Nov 24, 2022 19:38:20.028487921 CET	49698	443	192.168.2.4	172.217.168.45
Nov 24, 2022 19:38:20.028507948 CET	443	49698	172.217.168.45	192.168.2.4
Nov 24, 2022 19:38:20.097610950 CET	443	49698	172.217.168.45	192.168.2.4
Nov 24, 2022 19:38:20.098849058 CET	49698	443	192.168.2.4	172.217.168.45
Nov 24, 2022 19:38:20.098908901 CET	443	49698	172.217.168.45	192.168.2.4
Nov 24, 2022 19:38:20.102221012 CET	443	49698	172.217.168.45	192.168.2.4
Nov 24, 2022 19:38:20.102391958 CET	49698	443	192.168.2.4	172.217.168.45
Nov 24, 2022 19:38:20.518843889 CET	49696	443	192.168.2.4	142.250.203.110
Nov 24, 2022 19:38:20.518908978 CET	443	49696	142.250.203.110	192.168.2.4

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 19:38:20.518975973 CET	49696	443	192.168.2.4	142.250.203.110
Nov 24, 2022 19:38:20.518987894 CET	443	49696	142.250.203.110	192.168.2.4
Nov 24, 2022 19:38:20.519059896 CET	443	49696	142.250.203.110	192.168.2.4
Nov 24, 2022 19:38:20.554886103 CET	443	49696	142.250.203.110	192.168.2.4
Nov 24, 2022 19:38:20.554960012 CET	49696	443	192.168.2.4	142.250.203.110
Nov 24, 2022 19:38:20.555005074 CET	443	49696	142.250.203.110	192.168.2.4
Nov 24, 2022 19:38:20.555027008 CET	443	49696	142.250.203.110	192.168.2.4
Nov 24, 2022 19:38:20.555075884 CET	49696	443	192.168.2.4	142.250.203.110
Nov 24, 2022 19:38:20.718365908 CET	49696	443	192.168.2.4	142.250.203.110
Nov 24, 2022 19:38:20.718461037 CET	443	49696	142.250.203.110	192.168.2.4
Nov 24, 2022 19:38:20.719270945 CET	49698	443	192.168.2.4	172.217.168.45
Nov 24, 2022 19:38:20.719331980 CET	443	49698	172.217.168.45	192.168.2.4
Nov 24, 2022 19:38:20.719795942 CET	443	49698	172.217.168.45	192.168.2.4
Nov 24, 2022 19:38:20.723251104 CET	49698	443	192.168.2.4	172.217.168.45
Nov 24, 2022 19:38:20.723309040 CET	443	49698	172.217.168.45	192.168.2.4
Nov 24, 2022 19:38:20.778060913 CET	443	49698	172.217.168.45	192.168.2.4
Nov 24, 2022 19:38:20.778232098 CET	49698	443	192.168.2.4	172.217.168.45
Nov 24, 2022 19:38:20.778292894 CET	443	49698	172.217.168.45	192.168.2.4
Nov 24, 2022 19:38:20.778323889 CET	443	49698	172.217.168.45	192.168.2.4
Nov 24, 2022 19:38:20.778383970 CET	49698	443	192.168.2.4	172.217.168.45
Nov 24, 2022 19:38:20.803164005 CET	49698	443	192.168.2.4	172.217.168.45
Nov 24, 2022 19:38:20.803241968 CET	443	49698	172.217.168.45	192.168.2.4
Nov 24, 2022 19:38:21.474885941 CET	49699	80	192.168.2.4	35.206.111.91
Nov 24, 2022 19:38:21.475090027 CET	49700	80	192.168.2.4	35.206.111.91
Nov 24, 2022 19:38:21.615019083 CET	80	49699	35.206.111.91	192.168.2.4
Nov 24, 2022 19:38:21.615098953 CET	80	49700	35.206.111.91	192.168.2.4
Nov 24, 2022 19:38:21.615225077 CET	49699	80	192.168.2.4	35.206.111.91
Nov 24, 2022 19:38:21.615983963 CET	49700	80	192.168.2.4	35.206.111.91
Nov 24, 2022 19:38:21.768460035 CET	49700	80	192.168.2.4	35.206.111.91
Nov 24, 2022 19:38:21.908463955 CET	80	49700	35.206.111.91	192.168.2.4
Nov 24, 2022 19:38:21.909229994 CET	80	49700	35.206.111.91	192.168.2.4
Nov 24, 2022 19:38:22.027700901 CET	49700	80	192.168.2.4	35.206.111.91
Nov 24, 2022 19:38:22.104413986 CET	49702	443	192.168.2.4	35.206.111.91
Nov 24, 2022 19:38:22.104512930 CET	443	49702	35.206.111.91	192.168.2.4
Nov 24, 2022 19:38:22.104648113 CET	49702	443	192.168.2.4	35.206.111.91
Nov 24, 2022 19:38:22.105031967 CET	49702	443	192.168.2.4	35.206.111.91
Nov 24, 2022 19:38:22.105073929 CET	443	49702	35.206.111.91	192.168.2.4
Nov 24, 2022 19:38:22.565840960 CET	443	49702	35.206.111.91	192.168.2.4
Nov 24, 2022 19:38:22.574919939 CET	49702	443	192.168.2.4	35.206.111.91
Nov 24, 2022 19:38:22.574985981 CET	443	49702	35.206.111.91	192.168.2.4
Nov 24, 2022 19:38:22.576386929 CET	443	49702	35.206.111.91	192.168.2.4
Nov 24, 2022 19:38:22.576472044 CET	49702	443	192.168.2.4	35.206.111.91
Nov 24, 2022 19:38:22.578507900 CET	49702	443	192.168.2.4	35.206.111.91
Nov 24, 2022 19:38:22.578533888 CET	443	49702	35.206.111.91	192.168.2.4
Nov 24, 2022 19:38:22.578722954 CET	49702	443	192.168.2.4	35.206.111.91
Nov 24, 2022 19:38:22.578732967 CET	443	49702	35.206.111.91	192.168.2.4
Nov 24, 2022 19:38:22.578761101 CET	443	49702	35.206.111.91	192.168.2.4
Nov 24, 2022 19:38:22.625760078 CET	49702	443	192.168.2.4	35.206.111.91
Nov 24, 2022 19:38:22.625792980 CET	443	49702	35.206.111.91	192.168.2.4
Nov 24, 2022 19:38:22.725744009 CET	49702	443	192.168.2.4	35.206.111.91
Nov 24, 2022 19:38:23.216794968 CET	49703	443	192.168.2.4	172.217.168.68
Nov 24, 2022 19:38:23.216881037 CET	443	49703	172.217.168.68	192.168.2.4
Nov 24, 2022 19:38:23.216948032 CET	49703	443	192.168.2.4	172.217.168.68
Nov 24, 2022 19:38:23.217236996 CET	49703	443	192.168.2.4	172.217.168.68
Nov 24, 2022 19:38:23.217273951 CET	443	49703	172.217.168.68	192.168.2.4
Nov 24, 2022 19:38:23.283060074 CET	443	49703	172.217.168.68	192.168.2.4
Nov 24, 2022 19:38:23.283538103 CET	49703	443	192.168.2.4	172.217.168.68
Nov 24, 2022 19:38:23.283617020 CET	443	49703	172.217.168.68	192.168.2.4
Nov 24, 2022 19:38:23.284943104 CET	443	49703	172.217.168.68	192.168.2.4

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 19:38:23.285037994 CET	49703	443	192.168.2.4	172.217.168.68
Nov 24, 2022 19:38:23.287318945 CET	49703	443	192.168.2.4	172.217.168.68
Nov 24, 2022 19:38:23.287342072 CET	443	49703	172.217.168.68	192.168.2.4
Nov 24, 2022 19:38:23.287513018 CET	443	49703	172.217.168.68	192.168.2.4
Nov 24, 2022 19:38:23.417438030 CET	443	49702	35.206.111.91	192.168.2.4
Nov 24, 2022 19:38:23.417512894 CET	443	49702	35.206.111.91	192.168.2.4
Nov 24, 2022 19:38:23.417536974 CET	443	49702	35.206.111.91	192.168.2.4
Nov 24, 2022 19:38:23.417593002 CET	443	49702	35.206.111.91	192.168.2.4
Nov 24, 2022 19:38:23.417610884 CET	49702	443	192.168.2.4	35.206.111.91
Nov 24, 2022 19:38:23.417617083 CET	443	49702	35.206.111.91	192.168.2.4
Nov 24, 2022 19:38:23.417639017 CET	443	49702	35.206.111.91	192.168.2.4
Nov 24, 2022 19:38:23.417649984 CET	49702	443	192.168.2.4	35.206.111.91
Nov 24, 2022 19:38:23.417701960 CET	49702	443	192.168.2.4	35.206.111.91
Nov 24, 2022 19:38:23.417706966 CET	443	49702	35.206.111.91	192.168.2.4
Nov 24, 2022 19:38:23.417735100 CET	49702	443	192.168.2.4	35.206.111.91
Nov 24, 2022 19:38:23.417804956 CET	49702	443	192.168.2.4	35.206.111.91
Nov 24, 2022 19:38:23.417828083 CET	443	49702	35.206.111.91	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 19:38:19.241061926 CET	59683	53	192.168.2.4	8.8.8.8
Nov 24, 2022 19:38:19.269078016 CET	53	59683	8.8.8.8	192.168.2.4
Nov 24, 2022 19:38:19.327512026 CET	58565	53	192.168.2.4	8.8.8.8
Nov 24, 2022 19:38:19.353121042 CET	53	58565	8.8.8.8	192.168.2.4
Nov 24, 2022 19:38:20.819869995 CET	56807	53	192.168.2.4	8.8.8.8
Nov 24, 2022 19:38:20.837531090 CET	53	56807	8.8.8.8	192.168.2.4
Nov 24, 2022 19:38:21.998358011 CET	61124	53	192.168.2.4	8.8.8.8
Nov 24, 2022 19:38:22.017689943 CET	53	61124	8.8.8.8	192.168.2.4
Nov 24, 2022 19:38:23.157866955 CET	55570	53	192.168.2.4	8.8.8.8
Nov 24, 2022 19:38:23.175462008 CET	53	55570	8.8.8.8	192.168.2.4
Nov 24, 2022 19:38:23.196583986 CET	64906	53	192.168.2.4	8.8.8.8
Nov 24, 2022 19:38:23.215626955 CET	53	64906	8.8.8.8	192.168.2.4
Nov 24, 2022 19:38:38.774898052 CET	52825	53	192.168.2.4	8.8.8.8
Nov 24, 2022 19:38:38.796338081 CET	53	52825	8.8.8.8	192.168.2.4
Nov 24, 2022 19:39:23.253051996 CET	61709	53	192.168.2.4	8.8.8.8
Nov 24, 2022 19:39:23.270663023 CET	53	61709	8.8.8.8	192.168.2.4
Nov 24, 2022 19:39:23.338109016 CET	59182	53	192.168.2.4	8.8.8.8
Nov 24, 2022 19:39:23.357542038 CET	53	59182	8.8.8.8	192.168.2.4
Nov 24, 2022 19:39:24.033183098 CET	61657	53	192.168.2.4	8.8.8.8
Nov 24, 2022 19:39:24.059345007 CET	53	61657	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 24, 2022 19:38:19.241061926 CET	192.168.2.4	8.8.8.8	0xea8e	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:38:19.327512026 CET	192.168.2.4	8.8.8.8	0xe11a	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:38:20.819869995 CET	192.168.2.4	8.8.8.8	0xb7cd	Standard query (0)	www.30fe.com	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:38:21.998358011 CET	192.168.2.4	8.8.8.8	0xc826	Standard query (0)	www.30fe.com	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:38:23.157866955 CET	192.168.2.4	8.8.8.8	0x6d60	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:38:23.196583986 CET	192.168.2.4	8.8.8.8	0xe1de	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:38:38.774898052 CET	192.168.2.4	8.8.8.8	0x3f03	Standard query (0)	www.30fe.com	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:39:23.253051996 CET	192.168.2.4	8.8.8.8	0x7a2	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

Copyright Joe Security LLC 2022

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 24, 2022 19:39:23.338109016 CET	192.168.2.4	8.8.8.8	0x759f	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:39:24.033183098 CET	192.168.2.4	8.8.8.8	0x2039	Standard query (0)	www.30fe.com	A (IP address)	IN (0x0001)	false

DNS Answers

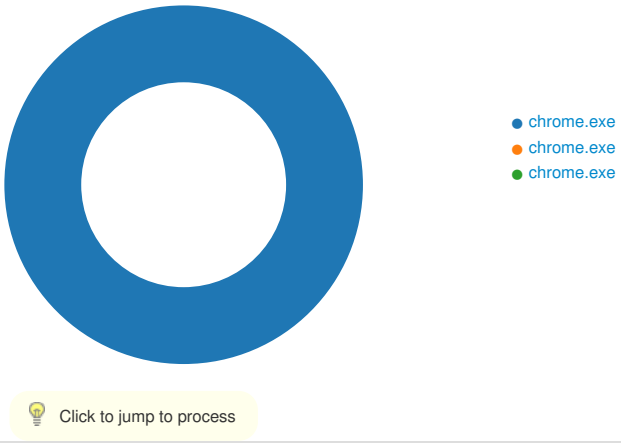
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 24, 2022 19:38:19.269078016 CET	8.8.8.8	192.168.2.4	0xea8e	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 24, 2022 19:38:19.269078016 CET	8.8.8.8	192.168.2.4	0xea8e	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:38:19.353121042 CET	8.8.8.8	192.168.2.4	0xe11a	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:38:20.837531090 CET	8.8.8.8	192.168.2.4	0xb7cd	No error (0)	www.30fe.com	30fe.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 24, 2022 19:38:20.837531090 CET	8.8.8.8	192.168.2.4	0xb7cd	No error (0)	30fe.com		35.206.111.91	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:38:22.017689943 CET	8.8.8.8	192.168.2.4	0xc826	No error (0)	www.30fe.com	30fe.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 24, 2022 19:38:22.017689943 CET	8.8.8.8	192.168.2.4	0xc826	No error (0)	30fe.com		35.206.111.91	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:38:23.175462008 CET	8.8.8.8	192.168.2.4	0x6d60	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:38:23.215626955 CET	8.8.8.8	192.168.2.4	0xe1de	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:38:38.796338081 CET	8.8.8.8	192.168.2.4	0x3f03	No error (0)	www.30fe.com	30fe.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 24, 2022 19:38:38.796338081 CET	8.8.8.8	192.168.2.4	0x3f03	No error (0)	30fe.com		35.206.111.91	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:39:23.270663023 CET	8.8.8.8	192.168.2.4	0x7a2	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:39:23.357542038 CET	8.8.8.8	192.168.2.4	0x759f	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:39:24.059345007 CET	8.8.8.8	192.168.2.4	0x2039	No error (0)	www.30fe.com	30fe.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 24, 2022 19:39:24.059345007 CET	8.8.8.8	192.168.2.4	0x2039	No error (0)	30fe.com		35.206.111.91	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- www.30fe.com
- https:

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 3584, Parent PID: 4744

General

Target ID:	0
Start time:	19:38:16
Start date:	24/11/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank
Imagebase:	0x7ff683680000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: chrome.exe PID: 1400, Parent PID: 3584

General

Target ID:	1
Start time:	19:38:17

Start date:	24/11/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-GB --service-sandbox-type=none --mojo-platform-channel-handle=1968 --field-trial-handle=1764,i,17311812855738133621,17887974914451854333,131072 --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: **5204**, Parent PID: **4744**

General

Target ID:	2
Start time:	19:38:18
Start date:	24/11/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "http://www.30fe.com/
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