ID: 800692
Cookbook: browseurl.jbs
Time: 18:16:43
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report http://technology@improvedcf.com 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Signatures 3
Sigma Signatures 3
Snort Signatures 4
Joe Sandbox Signatures 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
World Map of Contacted IPs 10
Public IPs 11
Private 11
General Information 11
Warnings 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASNs 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
Static File Info 13
Network Behavior 13
Network Port Distribution 13
TCP Packets 13
DNS Queries 15
DNS Answers 15
HTTP Request Dependency Graph 16
Statistics 16
Behavior 16
System Behavior 16
Analysis Process: chrome.exePID: 4472, Parent PID: 2352 16
General 16
File Activities 17
Registry Activities 17
Analysis Process: chrome.exePID: 5128, Parent PID: 4472 17
General 17
File Activities 17
Analysis Process: chrome.exePID: 504, Parent PID: 2352 17
General 17
Registry Activities 18
Disassembly 18

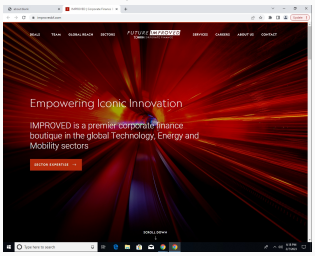
Windows Analysis Report

http://technology@improvedcf.com

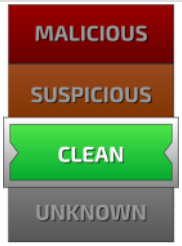
Overview

General Information

Sample URL:	http://technology@improvedcf.com
Analysis ID:	800692
Infos:	



Detection

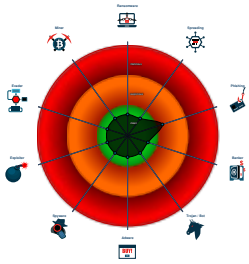


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

URL contains potential PII (phishing…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 4472 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 5128 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1764 --field-trial-handle=1640,i,15160840306292891837,5695472335583488514,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 504 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "http://technology@improvedcf.com MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

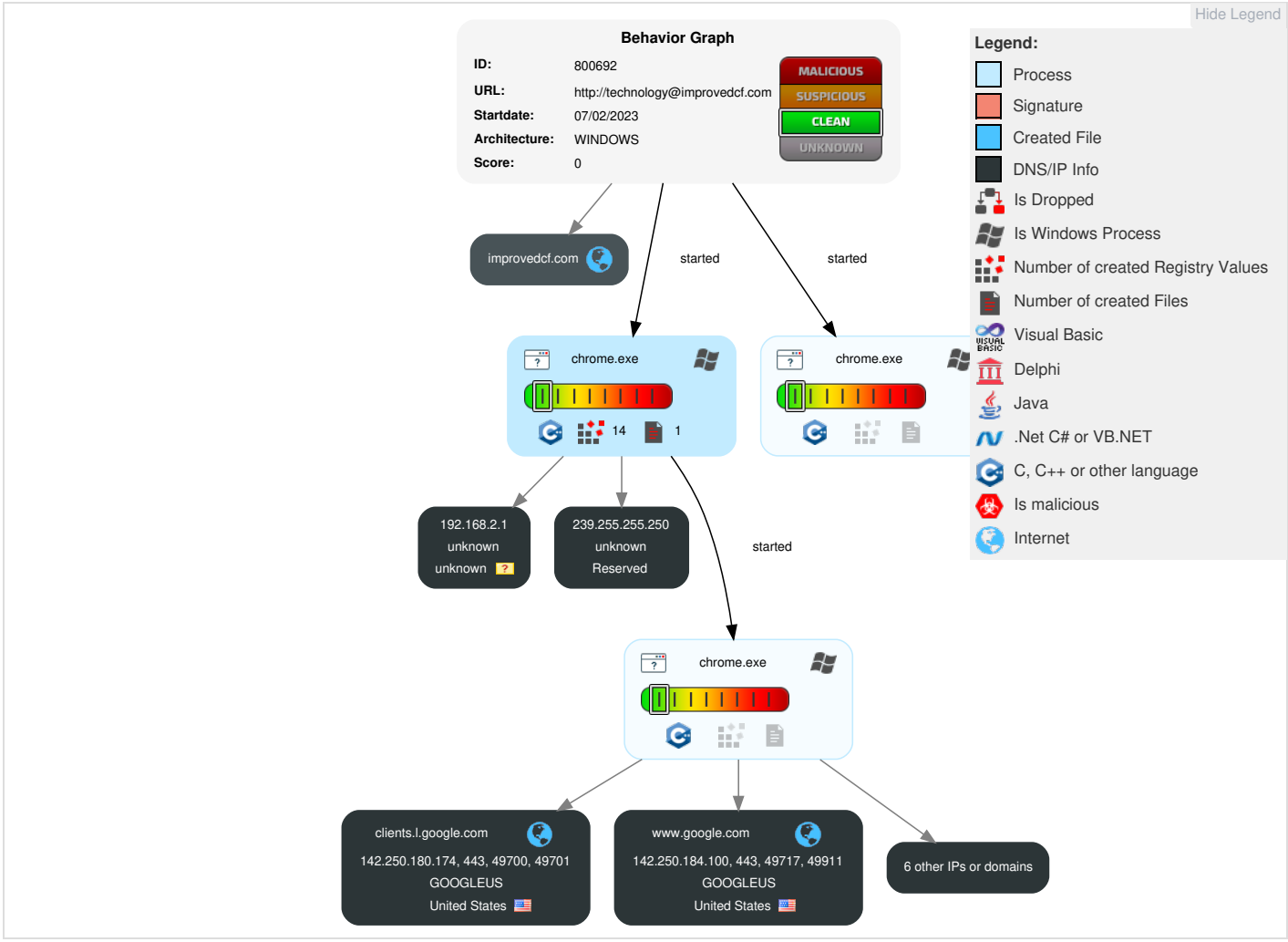
Joe Sandbox Signatures

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

Mitre Att&ck Matrix

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

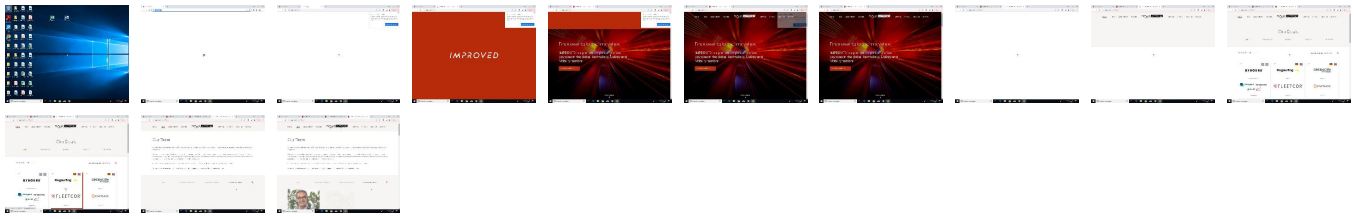
Behavior Graph

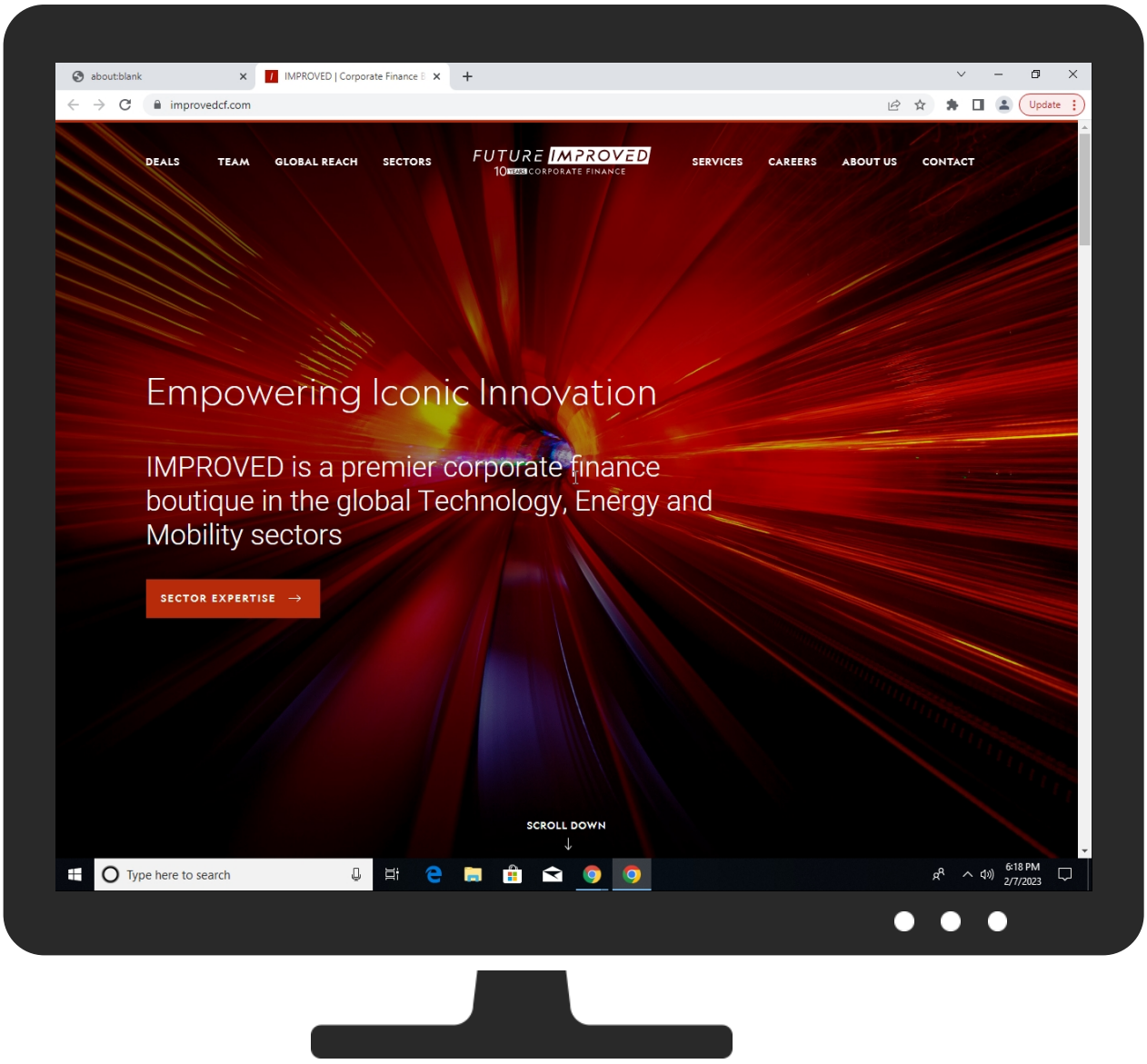


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://technology@improvedcf.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://improvedcf.com/wp-content/uploads/2022/10/Mark-Bradt.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2022/08/BorgWarner.png	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2022/05/Logo_SET_HD_SET_Ventures-1536x269.png	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://improvedcf.com/wp-content/uploads/2022/03/Mobility-Mixx.png	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/11/Gali-Naveh-Stern-1.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2022/03/Cannim.png	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/11/Carl-Peter-Forster.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2022/05/Korys.png	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/12/Thomas-Smal-cropped.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/12/Improved-Map.svg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/themes/improved/_/js/infinite-scroll.pkgd.min.js	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/11/Paul-Zonderland-1.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/themes/improved/_/images/flags/flag-fr.svg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2022/09/Derk-Diepeveen.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/11/Hans-Gieskes-1.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/themes/improved/_/images/flags/flag-fi.svg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/11/Bas-Hendriks-min-min-min.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/themes/improved/_/images/flags/flag-pt.svg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2023/01/Jeroen-Tas.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/11/Walter-van-Damme-1.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/themes/improved/_/js/magnific-popup.min.js	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/11/Robert-Wilhelm-1.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/themes/improved/_/css/screen.min.css?ver=1674228985	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/11/Nicolas-Magnus-min-min-min.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2022/07/cropped-Prachi_edit.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2023/01/SHIFT-logo-dark.svg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/11/img-placeholder-1.svg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2022/02/Slingshot-2.png	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/11/Plugit.png	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2023/01/invest-nl.png	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/11/Gregor-Matthies-1.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2022/09/Walter-van-Kuijen-1.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2022/09/Jai-Malhotra.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2022/09/Enphase.png	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/11/Marcel-Zegger-1.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/themes/improved/_/images/flags/flag-ca.svg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/11/Energy-scaled.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2023/01/87068_FUTURE-IMPROVED_DV_H_04_Cropped.png	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/11/Dominique-Houde-min-min-min.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/themes/improved/_/fonts/GeographLight.woff2	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/themes/improved/_/images/flags/flag-us.svg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/11/Arjen-van-Blokland-1.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/11/Sandrine-Vergnory-Mion-1.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-includes/css/dist/block-library/style.min.css?ver=6.1.1	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2023/02/BYBORRE-2.png	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2022/05/vp-capital.svg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/11/Luuk-Hulzebos-min-min-min.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/11/Vincent-Verellen-min-min-min.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2022/02/Ponooc-3-1.png	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/themes/improved/_/js/jarallax.min.js	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2022/02/Omar-Hatamleh-min.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2022/05/Trunkrs.png	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/11/Jelle-Walsteijn-min-min-min.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2022/07/Plugsurfing-4-1536x313.png	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2022/07/FleetCor.png	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2022/02/Check-1536x781.png	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2022/02/Antin-1536x401.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2022/02/Check.png	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2022/06/Daniel-Lyons-1.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2022/07/FleetCor-1536x165.png	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/11/Hero-Image-med-uncropped.jpeg	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://improvedcf.com/wp-content/uploads/2022/02/Antin.jpg	0%	Avira URL Cloud	safe	
http://improvedcf.com/	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2022/03/Mitsubsihi-HC-Capital.png	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/11/Sherief-Rahim-min-min-min.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/10/linkedin.svg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/themes/improved/_/images/search.svg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2023/01/improved-logo-white.svg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/11/Manus-Weber-min-min-min.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/11/Kevin-Lechner-min-min-min.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/11/DIF.png	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2022/03/Lex-Hartman.jpeg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/themes/improved/style.css?ver=1674228985	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-includes/js/wp-emoji-release.min.js?ver=6.1.1	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/11/Technology-scaled.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/11/Mel-Kroon-1.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/11/Red-background-Motif.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2022/03/Medisun.png	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/themes/improved/_/images/flags/flag-be.svg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/themes/improved/_/js/functions.js?ver=1674228985	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2022/09/GCN-Logo-colour-2.png	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/themes/improved/_/fonts/GeographMedium.woff2	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/themes/improved/_/images/flags/flag-nl.svg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2023/01/Logo-AKEF.png	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/11/Hein-van-der-Zeeuw-1.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/10/Frank-Verbeek-min-min-min.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/11/Jelle-Vastert-1.jpg	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2022/03/Cannim-1536x397.png	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-includes/js/jquery/jquery.min.js?ver=3.6.1	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2022/05/Logo_SET_HD_SET_Ventures.png	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-includes/css/classic-themes.min.css?ver=1	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2022/08/BorgWarner-1536x205.png	0%	Avira URL Cloud	safe	
http://https://improvedcf.com/wp-content/uploads/2021/11/Mobility-scaled.jpg	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	216.58.209.45	true	false		high
www.google.com	142.250.184.100	true	false		high
clients.l.google.com	142.250.180.174	true	false		high
improvedcf.com	34.107.69.108	true	false		unknown
use.typekit.net	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
p.typekit.net	unknown	unknown	false		high

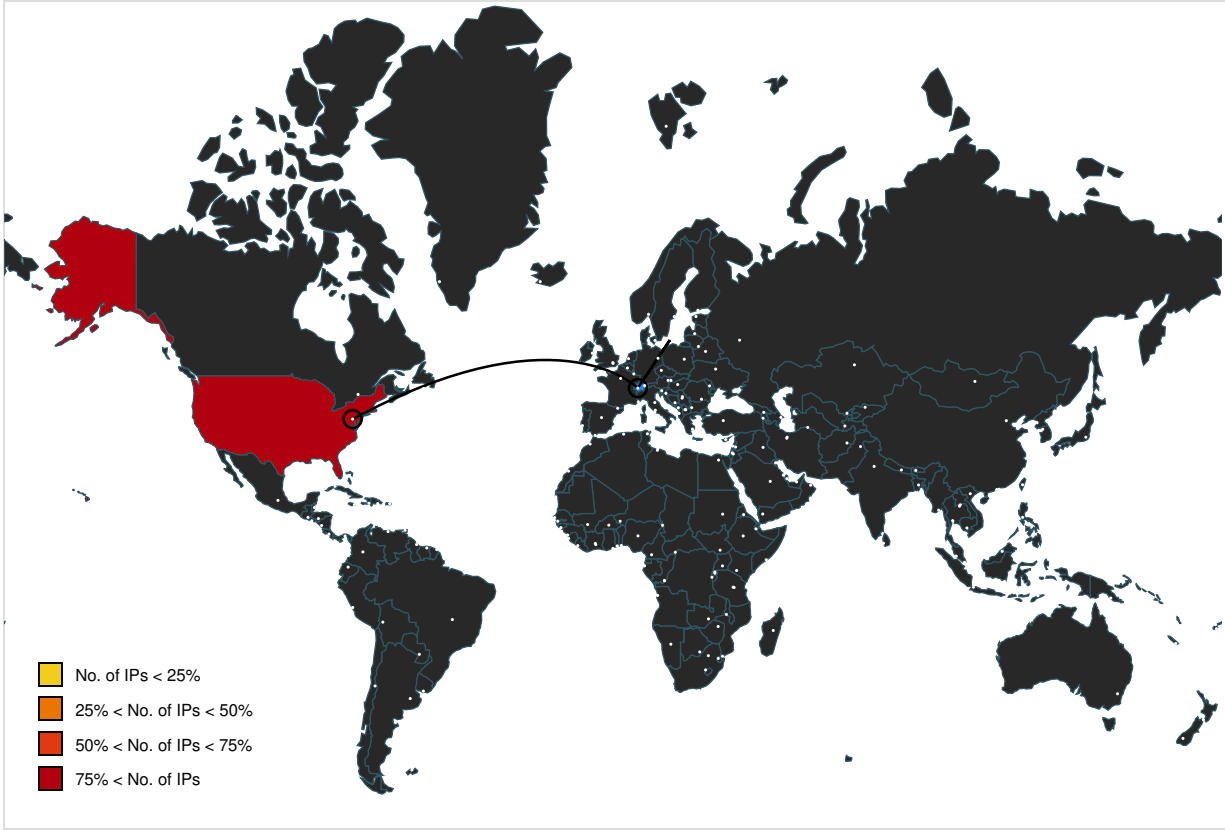
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://improvedcf.com/wp-content/uploads/2022/08/BorgWarner.png	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2022/10/Mark-Bradt.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/11/Gali-Naveh-Stern-1.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2022/05/Logo_SET_HD_SET_Ventures-1536x269.png	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2022/03/Mobility-Mixx.png	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2022/03/Cannim.png	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/11/Carl-Peter-Forster.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2022/05/Korys.png	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://https://improvedcf.com/wp-content/uploads/2021/12/Improved-Map.svg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/12/Thomas-Smal-cropped.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/11/Paul-Zonderland-1.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/11/Hans-Gieskes-1.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/themes/improved/_/images/flags/flag-fr.svg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/themes/improved/_/js/infinite-scroll.pkgd.min.js	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2022/09/Derk-Diepeveen.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/deals/	false		unknown
http://https://improvedcf.com/wp-content/themes/improved/_/images/flags/flag-fi.svg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/11/Bas-Hendriks-min-min-min.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2023/01/Jeroen-Tas.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/themes/improved/_/images/flags/flag-pt.svg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/themes/improved/_/js/magnific-popup.min.js	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/11/Walter-van-Damme-1.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/11/Robert-Wilhelm-1.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/11/Nicolas-Magnus-min-min-min.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/themes/improved/_/css/screen.min.css?ver=1674228985	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2022/07/cropped-Prachi_edit.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/11/img-placeholder-1.svg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2023/01/SHIFT-logo-dark.svg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2022/02/Slingshot-2.png	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/11/Plugit.png	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2023/01/invest-nl.png	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/11/Gregor-Matthies-1.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2022/09/Walter-van-Kuijen-1.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2022/09/Jai-Malhotra.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2022/09/Enphase.png	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/11/Marcel-Zegger-1.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/themes/improved/_/images/flags/flag-ca.svg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2023/01/87068_FUTURE-IMPROVED_DV_H_04_Cropped.png	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/	false		unknown
http://https://improvedcf.com/wp-content/uploads/2021/11/Energy-scaled.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/11/Dominique-Houde-min-min-min.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/themes/improved/_/fonts/GeographLight.woff2	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/11/Sandrine-Vergnory-Mion-1.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/themes/improved/_/images/flags/flag-us.svg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-includes/css/dist/block-library/style.min.css?ver=6.1.1	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/11/Arjen-van-Blokland-1.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/11/Luuk-Hulzebos-min-min-min.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2022/05/vp-capital.svg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2023/02/BYBORRE-2.png	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/11/Vincent-Verellen-min-min-min.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/themes/improved/_/js/jarallax.min.js	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-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://improvedcf.com/deals/	false		unknown
http://https://improvedcf.com/wp-content/uploads/2022/02/Omar-Hatamleh-min.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2022/02/Ponooc-3-1.png	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2022/05/Trunkrs.png	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2022/07/FleetCor.png	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2022/02/Check.png	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/11/Jelle-Walsteijn-min-min-min.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2022/02/Check-1536x781.png	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2022/02/Antin-1536x401.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2022/07/Plugsurfing-4-1536x313.png	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2022/07/FleetCor-1536x165.png	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/11/Hero-Image-med-uncropped.jpeg	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://https://improvedcf.com/wp-content/uploads/2022/06/Daniel-Lyons-1.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/10/linkedin.svg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/11/Sherief-Rahim-min-min-min.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2022/03/Mitsubsihi-HC-Capital.png	false	• Avira URL Cloud: safe	unknown
http://improvedcf.com/	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2022/02/Antin.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/11/Manus-Weber-min-min-min.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/themes/improved/_/images/search.svg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2023/01/improved-logo-white.svg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/11/DIF.png	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/11/Kevin-Lechner-min-min-min.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2022/03/Lex-Hartman.jpeg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/themes/improved/style.css?ver=1674228985	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-includes/js/wp-emoji-release.min.js?ver=6.1.1	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/11/Technology-scaled.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/11/Red-background-Motif.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/11/Mel-Kroon-1.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/themes/improved/_/images/flags/flag-be.svg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/themes/improved/_/js/functions.js?ver=1674228985	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2022/03/Medisun.png	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2022/09/GCN-Logo-colour-2.png	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/11/Hein-van-der-Zeeuw-1.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/themes/improved/_/fonts/GeographMedium.woff2	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2023/01/Logo-AKEF.png	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/themes/improved/_/images/flags/flag-nl.svg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/11/Jelle-Vastert-1.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-includes/js/jquery/jquery.min.js?ver=3.6.1	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/	false		unknown
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://improvedcf.com/wp-content/uploads/2022/05/Logo_SET_HD_SET_Ventures.png	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/10/Frank-Verbeek-min-min-min.jpg	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2022/03/Cannim-1536x397.png	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/team/	false		unknown
http://https://improvedcf.com/wp-includes/css/classic-themes.min.css?ver=1	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2022/08/BorgWarner-1536x205.png	false	• Avira URL Cloud: safe	unknown
http://https://improvedcf.com/wp-content/uploads/2021/11/Mobility-scaled.jpg	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.209.45	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
34.107.69.108	improvedcf.com	United States		15169	GOOGLEUS	false
142.250.184.100	www.google.com	United States		15169	GOOGLEUS	false
142.250.180.174	clients.l.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800692
Start date and time:	2023-02-07 18:16:43 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://technology@improvedcf.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:	12
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@28/0@12/7
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://improvedcf.com/deals/ • Browse: https://improvedcf.com/team/

Warnings

- Exclude process from analysis (whitelisted): SgrmBroker.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.184.99, 34.104.35.123, 173.222.108.232, 173.222.108.216, 80.67.82.195, 173.222.108.192, 142.250.180.168, 142.250.184.110, 216.58.209.42, 142.250.184.74, 142.250.184.106, 142.250.180.138, 142.250.180.170, 142.251.209.10, 142.251.209.42, 142.250.180.163
- Excluded domains from analysis (whitelisted): fs.microsoft.com, edgedl.me.gvt1.com, use-stls.adobe.com.edgesuite.net, content-autofill.googleapis.com, www.googletagmanager.com, update.googleapis.com, clientservices.googleapis.com, a1988.dscg1.akamai.net, a1874.dscg1.akamai.net, p.typekit.net-stls-v3.edgesuite.net, www.google-analytics.com
- 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 NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

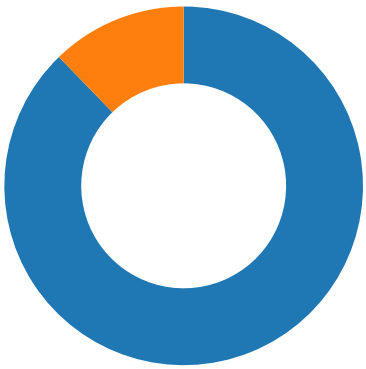
No created / dropped files found

Static File Info

No static file info

Network Behavior

Network Port Distribution



Total Packets: 49

- 80 (HTTP)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:17:50.091136932 CET	49699	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:17:50.091221094 CET	443	49699	216.58.209.45	192.168.2.3
Feb 7, 2023 18:17:50.091415882 CET	49699	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:17:50.091685057 CET	49700	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:17:50.091713905 CET	443	49700	142.250.180.174	192.168.2.3
Feb 7, 2023 18:17:50.091840029 CET	49700	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:17:50.102715969 CET	49701	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:17:50.102773905 CET	443	49701	142.250.180.174	192.168.2.3
Feb 7, 2023 18:17:50.102874041 CET	49701	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:17:50.142429113 CET	49703	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:17:50.142468929 CET	443	49703	216.58.209.45	192.168.2.3
Feb 7, 2023 18:17:50.142539024 CET	49703	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:17:50.144051075 CET	49699	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:17:50.144118071 CET	443	49699	216.58.209.45	192.168.2.3
Feb 7, 2023 18:17:50.144181967 CET	49700	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:17:50.144208908 CET	443	49700	142.250.180.174	192.168.2.3
Feb 7, 2023 18:17:50.144370079 CET	49701	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:17:50.144385099 CET	443	49701	142.250.180.174	192.168.2.3
Feb 7, 2023 18:17:50.145118952 CET	49703	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:17:50.145128965 CET	443	49703	216.58.209.45	192.168.2.3
Feb 7, 2023 18:17:50.243340969 CET	443	49700	142.250.180.174	192.168.2.3
Feb 7, 2023 18:17:50.268640041 CET	443	49701	142.250.180.174	192.168.2.3
Feb 7, 2023 18:17:50.268836975 CET	49700	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:17:50.268919945 CET	443	49700	142.250.180.174	192.168.2.3
Feb 7, 2023 18:17:50.269098043 CET	49701	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:17:50.269130945 CET	443	49701	142.250.180.174	192.168.2.3
Feb 7, 2023 18:17:50.269906998 CET	443	49701	142.250.180.174	192.168.2.3
Feb 7, 2023 18:17:50.270014048 CET	49701	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:17:50.271049023 CET	443	49700	142.250.180.174	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:17:50.271183968 CET	49700	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:17:50.274410009 CET	443	49701	142.250.180.174	192.168.2.3
Feb 7, 2023 18:17:50.274487019 CET	443	49700	142.250.180.174	192.168.2.3
Feb 7, 2023 18:17:50.274507046 CET	49701	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:17:50.274549961 CET	49700	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:17:50.370038033 CET	443	49703	216.58.209.45	192.168.2.3
Feb 7, 2023 18:17:50.370038033 CET	443	49699	216.58.209.45	192.168.2.3
Feb 7, 2023 18:17:50.391984940 CET	49700	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:17:50.397450924 CET	49703	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:17:50.397485971 CET	443	49703	216.58.209.45	192.168.2.3
Feb 7, 2023 18:17:50.397608042 CET	49699	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:17:50.397651911 CET	443	49699	216.58.209.45	192.168.2.3
Feb 7, 2023 18:17:50.399305105 CET	443	49703	216.58.209.45	192.168.2.3
Feb 7, 2023 18:17:50.399388075 CET	49703	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:17:50.399650097 CET	443	49699	216.58.209.45	192.168.2.3
Feb 7, 2023 18:17:50.399729013 CET	49699	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:17:50.700386047 CET	49704	80	192.168.2.3	34.107.69.108
Feb 7, 2023 18:17:50.700886011 CET	49701	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:17:50.700922012 CET	443	49701	142.250.180.174	192.168.2.3
Feb 7, 2023 18:17:50.701329947 CET	443	49701	142.250.180.174	192.168.2.3
Feb 7, 2023 18:17:50.701385021 CET	49700	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:17:50.701432943 CET	443	49700	142.250.180.174	192.168.2.3
Feb 7, 2023 18:17:50.701831102 CET	49703	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:17:50.701842070 CET	443	49703	216.58.209.45	192.168.2.3
Feb 7, 2023 18:17:50.701853991 CET	443	49700	142.250.180.174	192.168.2.3
Feb 7, 2023 18:17:50.702137947 CET	443	49703	216.58.209.45	192.168.2.3
Feb 7, 2023 18:17:50.710766077 CET	49699	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:17:50.710819960 CET	443	49699	216.58.209.45	192.168.2.3
Feb 7, 2023 18:17:50.711227894 CET	443	49699	216.58.209.45	192.168.2.3
Feb 7, 2023 18:17:50.711393118 CET	49701	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:17:50.711421013 CET	443	49701	142.250.180.174	192.168.2.3
Feb 7, 2023 18:17:50.718301058 CET	49705	80	192.168.2.3	34.107.69.108
Feb 7, 2023 18:17:50.718861103 CET	49703	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:17:50.718882084 CET	443	49703	216.58.209.45	192.168.2.3
Feb 7, 2023 18:17:50.720494032 CET	80	49704	34.107.69.108	192.168.2.3
Feb 7, 2023 18:17:50.720597029 CET	49704	80	192.168.2.3	34.107.69.108
Feb 7, 2023 18:17:50.731812000 CET	49704	80	192.168.2.3	34.107.69.108
Feb 7, 2023 18:17:50.738904953 CET	80	49705	34.107.69.108	192.168.2.3
Feb 7, 2023 18:17:50.739101887 CET	49705	80	192.168.2.3	34.107.69.108
Feb 7, 2023 18:17:50.752194881 CET	80	49704	34.107.69.108	192.168.2.3
Feb 7, 2023 18:17:50.752856016 CET	80	49704	34.107.69.108	192.168.2.3
Feb 7, 2023 18:17:50.755409002 CET	443	49701	142.250.180.174	192.168.2.3
Feb 7, 2023 18:17:50.755522966 CET	49701	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:17:50.755552053 CET	443	49701	142.250.180.174	192.168.2.3
Feb 7, 2023 18:17:50.755701065 CET	443	49701	142.250.180.174	192.168.2.3
Feb 7, 2023 18:17:50.755748987 CET	49701	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:17:50.764834881 CET	49701	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:17:50.764863014 CET	443	49701	142.250.180.174	192.168.2.3
Feb 7, 2023 18:17:50.765029907 CET	49703	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:17:50.765140057 CET	49699	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:17:50.765196085 CET	443	49699	216.58.209.45	192.168.2.3
Feb 7, 2023 18:17:50.826520920 CET	443	49703	216.58.209.45	192.168.2.3
Feb 7, 2023 18:17:50.826720953 CET	49703	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:17:50.826762915 CET	443	49703	216.58.209.45	192.168.2.3
Feb 7, 2023 18:17:50.826873064 CET	443	49703	216.58.209.45	192.168.2.3
Feb 7, 2023 18:17:50.826958895 CET	49703	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:17:50.844279051 CET	49703	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:17:50.844300985 CET	443	49703	216.58.209.45	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:17:50.864598989 CET	49706	443	192.168.2.3	34.107.69.108
Feb 7, 2023 18:17:50.864641905 CET	443	49706	34.107.69.108	192.168.2.3
Feb 7, 2023 18:17:50.864727020 CET	49706	443	192.168.2.3	34.107.69.108
Feb 7, 2023 18:17:50.865072966 CET	49704	80	192.168.2.3	34.107.69.108
Feb 7, 2023 18:17:50.865073919 CET	49699	443	192.168.2.3	216.58.209.45
Feb 7, 2023 18:17:50.865135908 CET	49706	443	192.168.2.3	34.107.69.108
Feb 7, 2023 18:17:50.865154028 CET	443	49706	34.107.69.108	192.168.2.3
Feb 7, 2023 18:17:50.895308971 CET	49700	443	192.168.2.3	142.250.180.174
Feb 7, 2023 18:17:50.895361900 CET	443	49700	142.250.180.174	192.168.2.3
Feb 7, 2023 18:17:50.944530010 CET	443	49706	34.107.69.108	192.168.2.3
Feb 7, 2023 18:17:50.957880974 CET	49706	443	192.168.2.3	34.107.69.108
Feb 7, 2023 18:17:50.957931042 CET	443	49706	34.107.69.108	192.168.2.3
Feb 7, 2023 18:17:50.959868908 CET	443	49706	34.107.69.108	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 7, 2023 18:17:49.627994061 CET	192.168.2.3	8.8.8.8	0xe6ca	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:17:49.630248070 CET	192.168.2.3	8.8.8.8	0x6987	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:17:49.632345915 CET	192.168.2.3	8.8.8.8	0x9618	Standard query (0)	improvedcf.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:17:50.683849096 CET	192.168.2.3	8.8.8.8	0x9618	Standard query (0)	improvedcf.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:17:51.507448912 CET	192.168.2.3	8.8.8.8	0xa79d	Standard query (0)	use.typekit.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:17:51.632987022 CET	192.168.2.3	8.8.8.8	0x1169	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:17:51.772389889 CET	192.168.2.3	8.8.8.8	0x5efb	Standard query (0)	p.typekit.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:18:06.619847059 CET	192.168.2.3	8.8.8.8	0x40c6	Standard query (0)	improvedcf.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:18:51.716852903 CET	192.168.2.3	8.8.8.8	0x9ba3	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:18:54.736855984 CET	192.168.2.3	8.8.8.8	0x9d52	Standard query (0)	p.typekit.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:18:54.738099098 CET	192.168.2.3	8.8.8.8	0xe106	Standard query (0)	use.typekit.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:18:54.738548040 CET	192.168.2.3	8.8.8.8	0x1d27	Standard query (0)	improvedcf.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
Feb 7, 2023 18:17:49.656100035 CET	8.8.8.8	192.168.2.3	0xe6ca	No error (0)	accounts.google.com		216.58.209.45	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:17:49.658803940 CET	8.8.8.8	192.168.2.3	0x6987	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:17:49.658803940 CET	8.8.8.8	192.168.2.3	0x6987	No error (0)	clients.l.google.com		142.250.180.174	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:17:50.660697937 CET	8.8.8.8	192.168.2.3	0x9618	No error (0)	improvedcf.com		34.107.69.108	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:17:50.702200890 CET	8.8.8.8	192.168.2.3	0x9618	No error (0)	improvedcf.com		34.107.69.108	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:17:51.538850069 CET	8.8.8.8	192.168.2.3	0xa79d	No error (0)	use.typekit.net	use-stls.adobe.com.edgesuite.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:17:51.651257992 CET	8.8.8.8	192.168.2.3	0x1169	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false

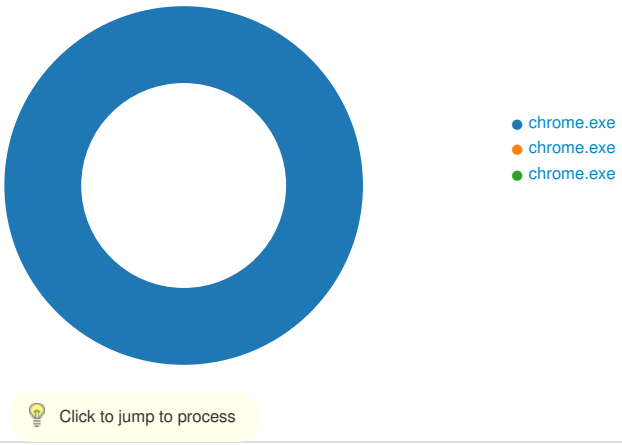
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 18:17:51.792376995 CET	8.8.8.8	192.168.2.3	0x5efb	No error (0)	p.typekit.net	p.typekit.net-stls-v3.edgesuite.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:18:06.648766994 CET	8.8.8.8	192.168.2.3	0x40c6	No error (0)	improvedcf.com		34.107.69.108	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:18:51.743068933 CET	8.8.8.8	192.168.2.3	0x9ba3	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:18:54.757519960 CET	8.8.8.8	192.168.2.3	0x1d27	No error (0)	improvedcf.com		34.107.69.108	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:18:54.757555962 CET	8.8.8.8	192.168.2.3	0x9d52	No error (0)	p.typekit.net	p.typekit.net-stls-v3.edgesuite.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:18:54.760617971 CET	8.8.8.8	192.168.2.3	0xe106	No error (0)	use.typekit.net	use-stls.adobe.com.edgesuite.net		CNAME (Canonical name)	IN (0x0001)	false

HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- improvedcf.com
- https:

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 4472, Parent PID: 2352

General

Target ID:	0
Start time:	18:17:44
Start date:	07/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank
Imagebase:	0x7ff614650000
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: **5128**, Parent PID: **4472**

General

Target ID:	1
Start time:	18:17:46
Start date:	07/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1764 --field-trial-handle=1640,i,15160840306292891837,5695472335583488514,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff614650000
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: **504**, Parent PID: **2352**

General

Target ID:	2

Start time:	18:17:46
Start date:	07/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "http://technology@improvedcf.com
Imagebase:	0x7ff614650000
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