


**ID:** 1443490
**Cookbook:** browseurl.jbs
**Time:** 21:31:11
**Date:** 17/05/2024
**Version:** 40.0.0 Tourmaline

# Table of Contents

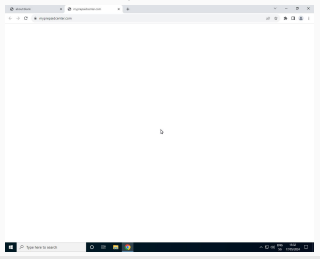
# Windows Analysis Report

## https://www.myprepaidcenter.com

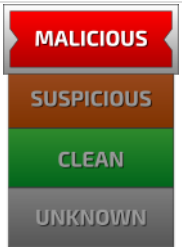
## Overview

### General Information

| | |
|---|---|
| Sample URL: | http://https://www.myprepaidcenter.com |
| Analysis ID: | 1443490 |
| Infos: | |



### Detection

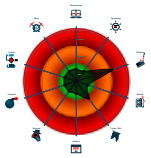



| | |
|---|---|
| Score: | 48 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- AI detected suspicious sample via s…
- HTML page contains obfuscate onlo…
- Creates files inside the system direc…
- Deletes files inside the Windows fol…
- Detected non-DNS traffic on DNS po…

### Classification



## Process Tree

- **System is w10x64**
- chrome.exe (PID: 6112 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank" MD5: 45DE480806D1B5D462A7DDE4DCEFC4E4)
  - chrome.exe (PID: 1360 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=2040 --field-trial-handle=1964,i,9150512431500774702,5457701197967585519,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction /prefetch:8 MD5: 45DE480806D1B5D462A7DDE4DCEFC4E4)
  - chrome.exe (PID: 6436 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=audio.mojom.AudioService --lang=en-US --service-sandbox-type=audio --mojo-platform-channel-handle=5588 --field-trial-handle=1964,i,9150512431500774702,5457701197967585519,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction /prefetch:8 MD5: 45DE480806D1B5D462A7DDE4DCEFC4E4)
  - chrome.exe (PID: 6416 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=video_capture.mojom.VideoCaptureService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=3444 --field-trial-handle=1964,i,9150512431500774702,5457701197967585519,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction /prefetch:8 MD5: 45DE480806D1B5D462A7DDE4DCEFC4E4)
- chrome.exe (PID: 6396 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" "https://www.myprepaidcenter.com" MD5: 45DE480806D1B5D462A7DDE4DCEFC4E4)
- **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

### AV Detection

AI detected suspicious sample via syscall and static analysis

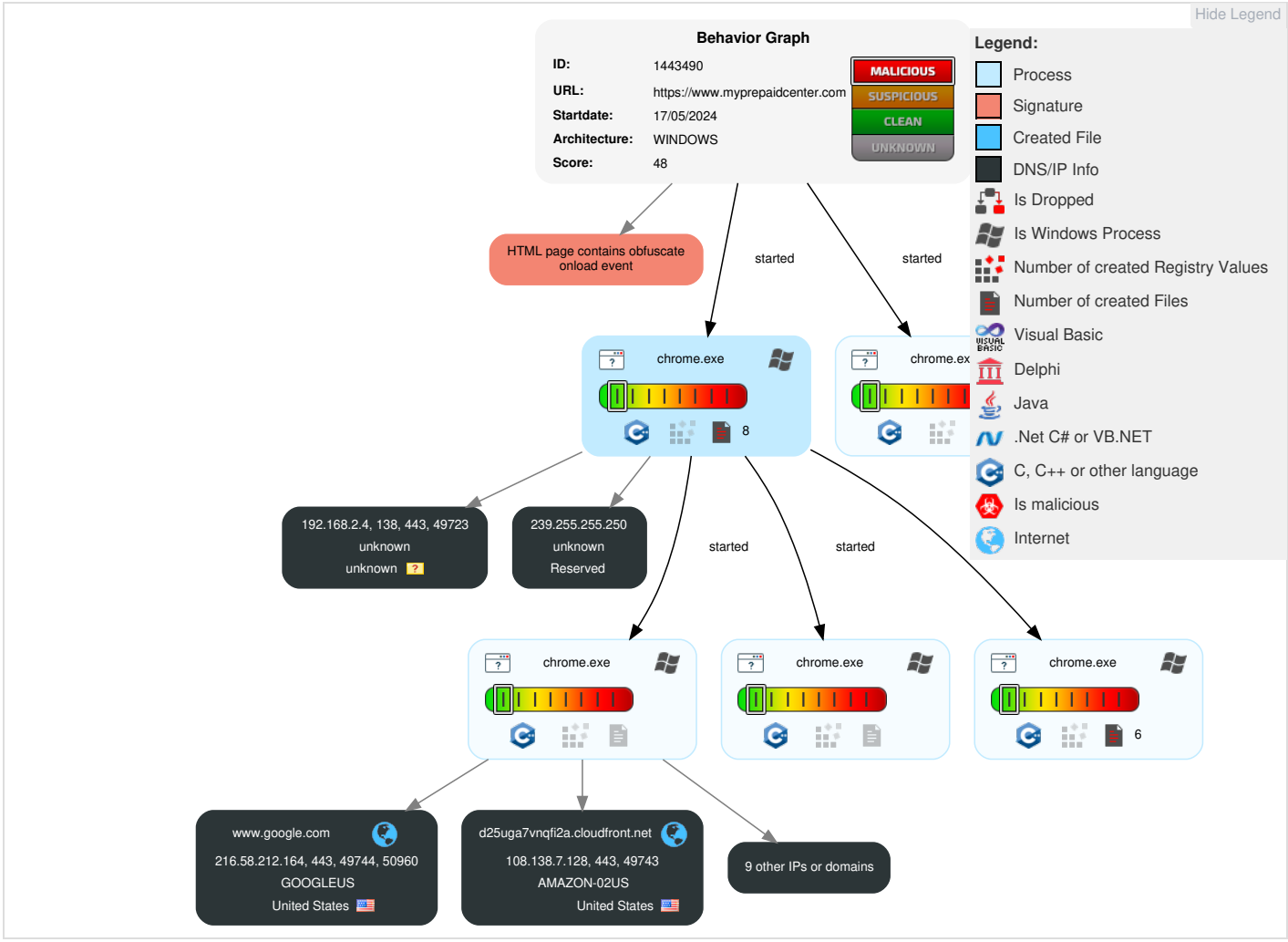
### Phishing

HTML page contains obfuscate onload event

## Mitre Att&ck Matrix

| Reconnai... | Resource Developm... | Initial Access | Execution | Persisten... | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Gather Victim Identity Information | Acquire Infrastructure | Valid Accounts | Windows Management Instrumentation | Path Interception | 1 Process Injection | 1 Masquerading | OS Credential Dumping | System Service Discovery | Remote Services | Data from Local System | 1 Encrypted Channel | Exfiltration Over Other Network Medium | Abuse Accessibility Features |
| Credentials | Domains | 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 | 3 Non-Application Layer Protocol | Exfiltration Over Bluetooth | Network Denial of Service |
| Email Addresses | DNS Server | Domain Accounts | At | Logon Script (Windows) | Logon Script (Windows) | 1 File Deletion | Security Account Manager | Query Registry | SMB/Windows Admin Shares | Data from Network Shared Drive | 4 Application Layer Protocol | Automated Exfiltration | Data Encrypted for Impact |
| Employee Names | Virtual Private Server | Local Accounts | Cron | Login Hook | Login Hook | Binary Padding | NTDS | System Network Configuration Discovery | Distributed Component Object Model | Input Capture | 1 Ingress Tool Transfer | Traffic Duplication | Data Destruction |

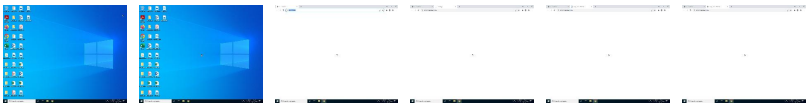
## Behavior Graph

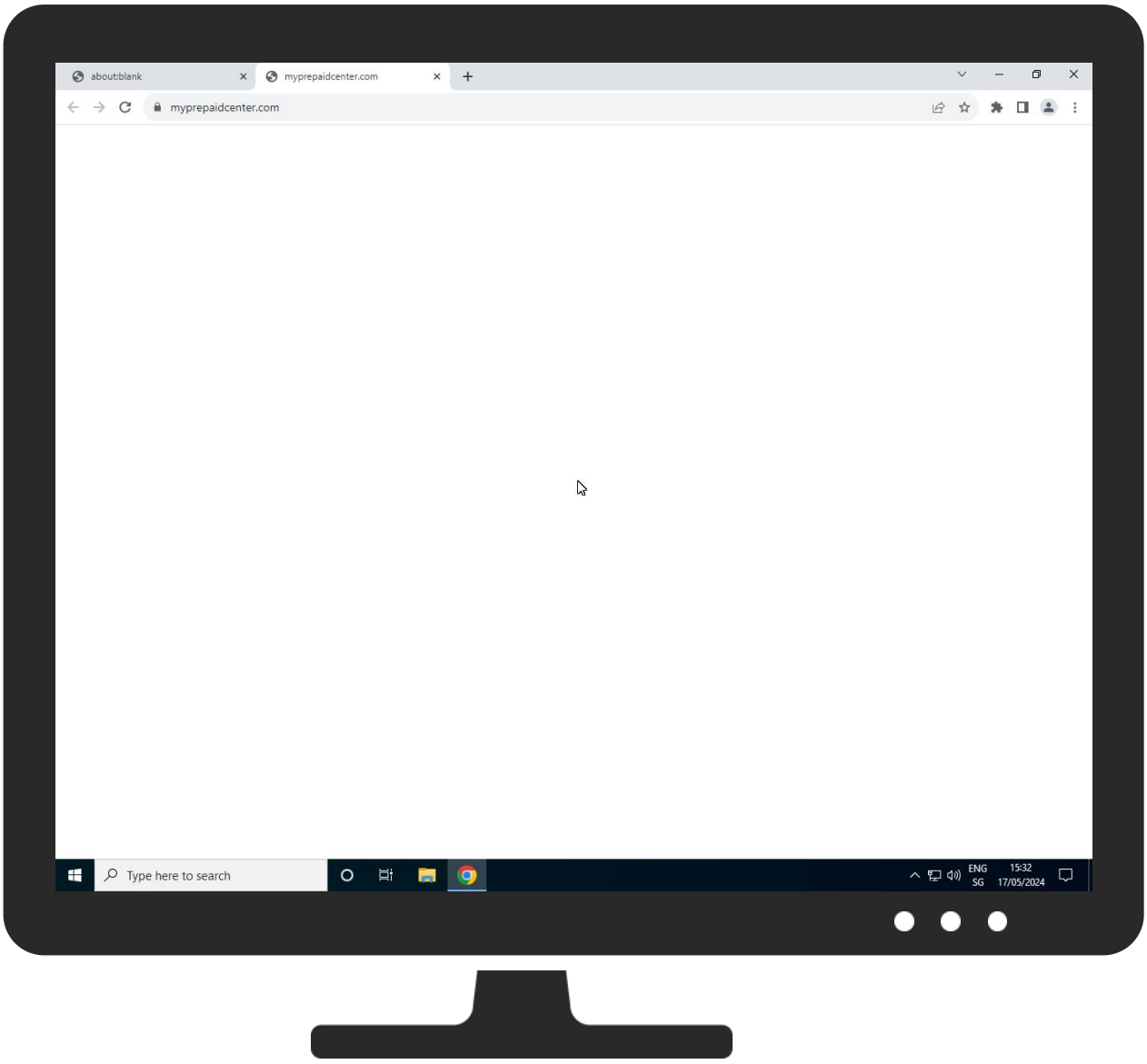



## Screenshots

### Thumbnails

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






## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://https://www.myprepaidcenter.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://fontawesome.com | 0% | URL Reputation | safe | |
| http://https://fontawesome.com/license/free | 0% | URL Reputation | safe | |
| http://https://reshim.org | 0% | Avira URL Cloud | safe | |

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://https://gliadomain.com | 0% | Avira URL Cloud | safe | |
| http://https://nourishingpursuits.com | 0% | Avira URL Cloud | safe | |
| http://https://mercadolivre.com | 0% | Avira URL Cloud | safe | |
| http://https://www.myprepaidcenter.com/vendor-es2015.0f83a55a77a277fa1347.js | 0% | Avira URL Cloud | safe | |
| http://https://poalim.xyz | 0% | Avira URL Cloud | safe | |
| http://https://mercadoshops.com.co | 0% | Avira URL Cloud | safe | |
| http://https://unotv.com | 0% | Avira URL Cloud | safe | |
| http://https://medonet.pl | 0% | Avira URL Cloud | safe | |
| http://https://wieistmeineip.de | 0% | Avira URL Cloud | safe | |
| http://https://mercadoshops.com.br | 0% | Avira URL Cloud | safe | |
| http://https://joyreactor.cc | 0% | Avira URL Cloud | safe | |
| http://https://bolasport.com | 0% | Avira URL Cloud | safe | |
| http://https://datadome.co | 0% | Avira URL Cloud | safe | |
| http://https://supereva.it | 0% | Avira URL Cloud | safe | |
| http://https://songstats.com | 0% | Avira URL Cloud | safe | |
| http://https://zdrowietvn.pl | 0% | Avira URL Cloud | safe | |
| http://https://elfinancierocr.com | 0% | Avira URL Cloud | safe | |
| http://https://rws1nvtvt.com | 0% | Avira URL Cloud | safe | |
| http://https://baomoi.com | 0% | Avira URL Cloud | safe | |
| http://https://ht.blackhawknetwork.com/assets/bXlwcmVwYWlkY2VudGVyLmNvbSxteXByZXBhaWRjZW50cmUuY29tLmF1LGJwc | 0% | Avira URL Cloud | safe | |
| http://https://js.datadome.co/tags.js | 0% | Avira URL Cloud | safe | |
| http://https://hearty.app | 0% | Avira URL Cloud | safe | |
| http://https://heartymail.com | 0% | Avira URL Cloud | safe | |
| http://https://radio2.be | 0% | Avira URL Cloud | safe | |
| http://https://mercadoshops.com | 0% | Avira URL Cloud | safe | |
| http://https://desimartini.com | 0% | Avira URL Cloud | safe | |
| http://https://finn.no | 0% | Avira URL Cloud | safe | |
| http://https://hearty.gift | 0% | Avira URL Cloud | safe | |
| http://https://hc1.com | 0% | Avira URL Cloud | safe | |
| http://https://kompas.tv | 0% | Avira URL Cloud | safe | |
| http://https://songshare.com | 0% | Avira URL Cloud | safe | |
| http://https://mercadopago.com.mx | 0% | Avira URL Cloud | safe | |
| http://https://mystudentdashboard.com | 0% | Avira URL Cloud | safe | |
| http://https://talkdeskqaid.com | 0% | Avira URL Cloud | safe | |
| http://https://mercadopago.com.pe | 0% | Avira URL Cloud | safe | |
| http://https://github.com/tkrotoff/jquery-simplecolorpicker | 0% | Avira URL Cloud | safe | |
| http://https://cardsayings.net | 0% | Avira URL Cloud | safe | |
| http://https://mightytext.net | 0% | Avira URL Cloud | safe | |
| http://https://pudelek.pl | 0% | Avira URL Cloud | safe | |
| http://https://joyreactor.com | 0% | Avira URL Cloud | safe | |
| http://https://eworkbookcloud.com | 0% | Avira URL Cloud | safe | |
| http://https://wildixin.com | 0% | Avira URL Cloud | safe | |
| http://https://mercadopago.cl | 0% | Avira URL Cloud | safe | |
| http://https://nacion.com | 0% | Avira URL Cloud | safe | |
| http://https://cookreactor.com | 0% | Avira URL Cloud | safe | |
| http://https://chennien.com | 0% | Avira URL Cloud | safe | |
| http://https://bonvivir.com | 0% | Avira URL Cloud | safe | |
| http://https://talkdeskstgid.com | 0% | Avira URL Cloud | safe | |
| http://https://carcostadvisor.be | 0% | Avira URL Cloud | safe | |
| http://https://salemovetravel.com | 0% | Avira URL Cloud | safe | |
| http://https://wpext.pl | 0% | Avira URL Cloud | safe | |
| http://https://welt.de | 0% | Avira URL Cloud | safe | |
| http://https://poalim.site | 0% | Avira URL Cloud | safe | |
| http://https://blackrockadvisorelite.it | 0% | Avira URL Cloud | safe | |
| http://https://cafemedia.com | 0% | Avira URL Cloud | safe | |
| http://https://landyrev.com | 0% | Avira URL Cloud | safe | |
| http://https://mercadoshops.com.ar | 0% | Avira URL Cloud | safe | |
| http://https://elpais.uy | 0% | Avira URL Cloud | safe | |

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://https://commentcamarche.com | 0% | Avira URL Cloud | safe | |
| http://https://tucarro.com.ve | 0% | Avira URL Cloud | safe | |
| http://https://eleconomista.net | 0% | Avira URL Cloud | safe | |
| http://https://rws3nvtvt.com | 0% | Avira URL Cloud | safe | |
| http://https://clmbtech.com | 0% | Avira URL Cloud | safe | |
| http://https://mercadolivre.com.br | 0% | Avira URL Cloud | safe | |
| http://https://standardsandpraiserepurpose.com | 0% | Avira URL Cloud | safe | |
| http://https://salemovefinancial.com | 0% | Avira URL Cloud | safe | |
| http://https://mercadopago.com.br | 0% | Avira URL Cloud | safe | |
| http://https://commentcamarche.net | 0% | Avira URL Cloud | safe | |
| http://https://www.myprepaidcenter.com/scripts.593eeb7a748a9c2bc8d1.js | 0% | Avira URL Cloud | safe | |
| http://https://hj.rs | 0% | Avira URL Cloud | safe | |
| http://https://mighty-app.appspot.com | 0% | Avira URL Cloud | safe | |
| http://https://etfacademy.it | 0% | Avira URL Cloud | safe | |
| http://https://hearty.me | 0% | Avira URL Cloud | safe | |
| http://https://mercadolibre.com.gt | 0% | Avira URL Cloud | safe | |
| http://https://mercadolibre.co.cr | 0% | Avira URL Cloud | safe | |
| http://https://idbs-staging.com | 0% | Avira URL Cloud | safe | |
| http://https://timesinternet.in | 0% | Avira URL Cloud | safe | |
| http://https://blackrock.com | 0% | Avira URL Cloud | safe | |
| http://https://idbs-eworkbook.com | 0% | Avira URL Cloud | safe | |
| http://https://hjck.com | 0% | Avira URL Cloud | safe | |
| http://https://prisjakt.no | 0% | Avira URL Cloud | safe | |
| http://https://vrt.be | 0% | Avira URL Cloud | safe | |
| http://https://kompas.com | 0% | Avira URL Cloud | safe | |
| http://https://idbs-dev.com | 0% | Avira URL Cloud | safe | |
| http://https://linternaute.com | 0% | Avira URL Cloud | safe | |
| http://https://wingify.com | 0% | Avira URL Cloud | safe | |
| http://https://player.pl | 0% | Avira URL Cloud | safe | |
| http://https://mercadolibre.com.hn | 0% | Avira URL Cloud | safe | |
| http://https://mercadolibre.cl | 0% | Avira URL Cloud | safe | |
| http://https://mercadopago.com.ar | 0% | Avira URL Cloud | safe | |
| http://https://www.myprepaidcenter.com/styles.24de6c171e32458ed4d1.css | 0% | Avira URL Cloud | safe | |
| http://https://landyrev.ru | 0% | Avira URL Cloud | safe | |
| http://https://tucarro.com.co | 0% | Avira URL Cloud | safe | |
| http://https://een.be | 0% | Avira URL Cloud | safe | |
| http://https://clarosports.com | 0% | Avira URL Cloud | safe | |
| http://https://punjabijagran.com | 0% | Avira URL Cloud | safe | |
| http://https://nien.com | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| bg.microsoft.map.fastly.net | 199.232.210.172 | true | false | | unknown |
| d-52ccktk4i3.execute-api.us-east-2.amazonaws.com | 3.130.102.116 | true | false | | unknown |
| d25uga7vnqfi2a.cloudfront.net | 108.138.7.128 | true | false | | unknown |
| www.google.com | 216.58.212.164 | true | false | | unknown |
| www.myprepaidcenter.com | 18.239.69.89 | true | false | | unknown |
| js.datadome.co | 18.238.243.98 | true | false | | unknown |
| fp2e7a.wpc.phicdn.net | 192.229.221.95 | true | false | | unknown |
| api-alb-eu-central-1.datadome.co | 18.194.25.151 | true | false | | unknown |
| ht.blackhawknetwork.com | unknown | unknown | false | | unknown |
| content.blackhawknetwork.com | unknown | unknown | false | | unknown |
| api-js.datadome.co | unknown | unknown | false | | unknown |

## Contacted URLs

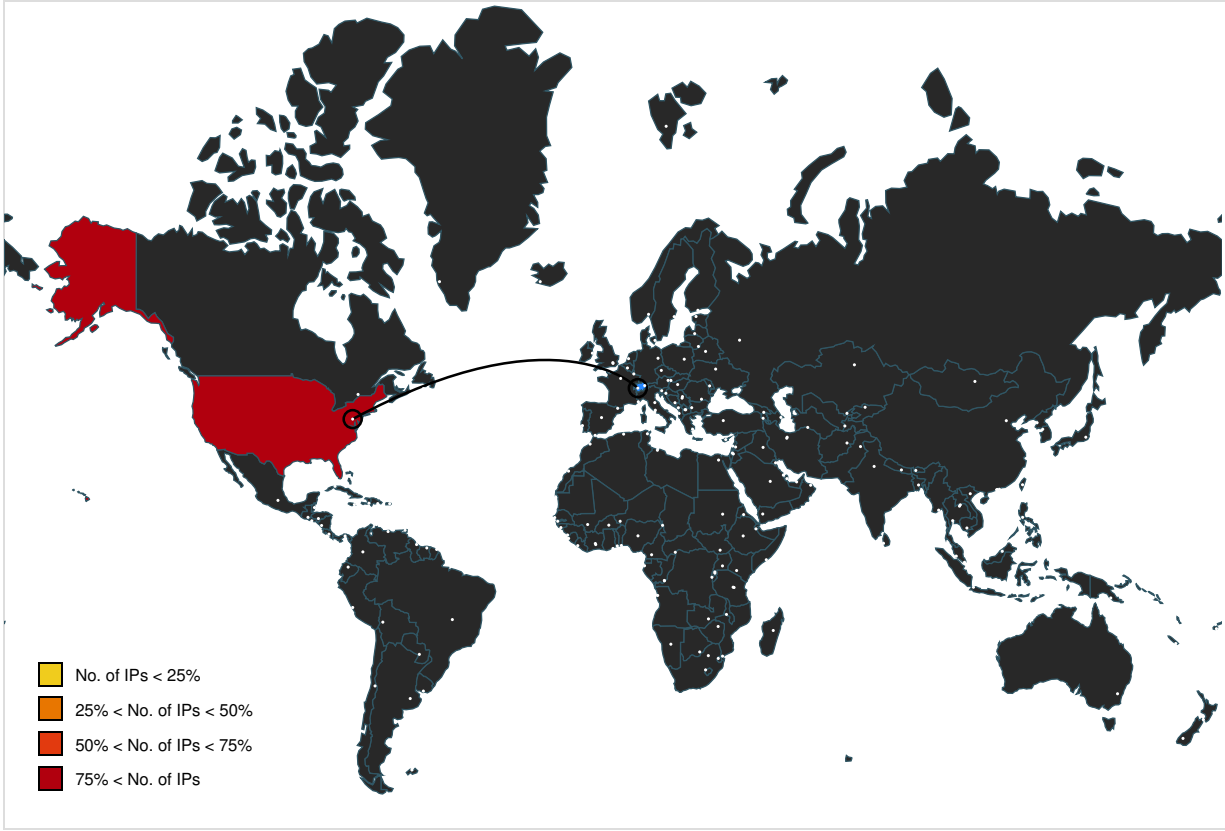
| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://https://www.myprepaidcenter.com/vendor-es2015.0f83a55a77a277fa1347.js | false | • Avira URL Cloud: safe | unknown |
| http://https://js.datadome.co/tags.js | false | • Avira URL Cloud: safe | unknown |
| http://https://www.myprepaidcenter.com/scripts.593eeb7a748a9c2bc8d1.js | false | • Avira URL Cloud: safe | unknown |
| http://https://www.myprepaidcenter.com/styles.24de6c171e32458ed4d1.css | false | • Avira URL Cloud: safe | unknown |

## URLs from Memory and Binaries

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://wieistmeineip.de | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://mercadoshops.com.co | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://gliadomain.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://poalim.xyz | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://mercadolivre.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://reshim.org | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://nourishingpursuits.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://medonet.pl | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://unotv.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://mercadoshops.com.br | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://joyreactor.cc | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://zdrowietvn.pl | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://fontawesome.com | chromecache_125.2.dr | false | • URL Reputation: safe | unknown |
| http://https://songstats.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://baomoi.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://supereva.it | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://datadome.co | chromecache_127.2.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://elfinancierocr.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://bolasport.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://rws1nvtvt.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://ht.blackhawknetwork.com/assets/bXlwcmVwYWlkY2VudGVyLmNvbSxteXByZXBhaWRjZW50cmUuY29tLmF1LGJwc | chromecache_126.2.dr, chromecache_117.2.dr, chromecache_118.2.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://desimartini.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://hearty.app | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://hearty.gift | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://mercadoshops.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://heartymail.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://radio2.be | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://finn.no | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://hc1.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://kompas.tv | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://mystudentdashboard.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://songshare.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://mercadopago.com.mx | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://talkdeskqaid.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://mercadopago.com.pe | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://github.com/tkrotoff/jquery-simplecolorpicker | chromecache_125.2.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://cardsayings.net | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://mightytext.net | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://pudelek.pl | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://joyreactor.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://cookreactor.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://wildixin.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://eworkbookcloud.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://nacion.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://chennien.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://mercadopago.cl | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://talkdeskstgid.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://bonvivir.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://carcostadvisor.be | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://salemovetravel.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://wpext.pl | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://welt.de | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://poalim.site | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://blackrockadvisorelite.it | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://cafemedia.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://mercadoshops.com.ar | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://elpais.uy | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://landyrev.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://commentcamarche.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://tucarro.com.ve | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://rws3nvtvt.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://eleconomista.net | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://mercadolivre.com.br | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://clmbtech.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://standardsandpraiserepurpose.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://salemovefinancial.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://mercadopago.com.br | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://commentcamarche.net | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://etfacademy.it | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://mighty-app.appspot.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://fontawesome.com/license/free | chromecache_125.2.dr | false | • URL Reputation: safe | unknown |
| http://https://hj.rs | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://hearty.me | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://mercadolibre.com.gt | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://timesinternet.in | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://idbs-staging.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://blackrock.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://idbs-eworkbook.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://mercadolibre.co.cr | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://hjck.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://vrt.be | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://prisjakt.no | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://kompas.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://idbs-dev.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://wingify.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://mercadolibre.cl | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://player.pl | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://mercadopago.com.ar | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://mercadolibre.com.hn | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://linternaute.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://tucarro.com.co | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://landyrev.ru | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://clarosports.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://een.be | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://nien.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://punjabijagran.com | sets.json.0.dr | false | • Avira URL Cloud: safe | unknown |

## World Map of Contacted IPs




**Public IPs**

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 216.58.212.164 | www.google.com | United States | | 15169 | GOOGLEUS | false |
| 18.239.69.89 | www.myprepaidcenter.com | United States | | 16509 | AMAZON-02US | false |
| 108.156.2.79 | unknown | United States | | 16509 | AMAZON-02US | false |
| 3.130.102.116 | d-52ccktk4i3.execute-api.us-east-2.amazonaws.com | United States | | 16509 | AMAZON-02US | false |
| 18.194.25.151 | api-alb-eu-central-1.datadome.co | United States | | 16509 | AMAZON-02US | false |
| 18.238.243.98 | js.datadome.co | United States | | 16509 | AMAZON-02US | false |
| 239.255.255.250 | unknown | Reserved | | unknown | unknown | false |
| 108.138.7.128 | d25uga7vnqfi2a.cloudfront.net | United States | | 16509 | AMAZON-02US | false |

**Private**

| IP |
|---|
| 192.168.2.4 |

## General Information

| | |
|---|---|
| Joe Sandbox version: | 40.0.0 Tourmaline |
| Analysis ID: | 1443490 |
| Start date and time: | 2024-05-17 21:31:11 +02:00 |
| Joe Sandbox product: | CloudBasic |
| Overall analysis duration: | 0h 3m 18s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Cookbook file name: | browseurl.jbs |
| Sample URL: | http://https://www.myprepaidcenter.com |
| Analysis system description: | Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01 |
| Number of analysed new started processes analysed: | 9 |

| | |
|---|---|
| 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<br>• EGA enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal48.phis.win@26/30@16/9 |
| EGA Information: | Failed |
| HCA Information: | • Successful, ratio: 100%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |

### Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SIHClient.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.185.163, 142.250.184.206, 64.233.167.84, 34.104.35.123, 142.250.185.227, 40.68.123.157, 199.232.210.172, 192.229.221.95, 20.3.187.198, 13.85.23.206, 142.250.184.195
- Excluded domains from analysis (whitelisted): fs.microsoft.com, accounts.google.com, fonts.gstatic.com, slscr.update.microsoft.com, ctldl.windowsupdate.com.delivery.microsoft.com, clientservices.googleapis.com, ctldl.windowsupdate.com, fe3cr.delivery.mp.microsoft.com, fe3.delivery.mp.microsoft.com, clients2.google.com, edgedl.me.gvt1.com, ocsp.digicert.com, ocsp.edge.digicert.com, glb.cws.prod.dcat.dsp.trafficmanager.net, sls.update.microsoft.com, update.googleapis.com, clients.l.google.com, wu-b-net.trafficmanager.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- HTTPS proxy raw data packets have been limited to 10 per session. Please view the PCAPs for the complete data.
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtSetInformationFile calls found.
- VT rate limit hit for: https://www.myprepaidcenter.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

**C:\Windows\SystemTemp\chrome_PuffinComponentUnpacker_BeginUnzipping6112_1630002529\LICENSE**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 1558 |
| Entropy (8bit): | 5.11458514637545 |
| Encrypted: | false |
| SSDEEP: | 48:OBOCrYJ4rYJVwUCLHDy43HV713XEyMmZ3teTHn:LCrYJ4rYJVwUCHZ3Z13XtdUTH |
| MD5: | EE002CB9E51BB8DFA89640A406A1090A |
| SHA1: | 49EE3AD535947D8821FFDEB67FFC9BC37D1EBBB2 |
| SHA-256: | 3DBD2C90050B652D63656481C3E5871C52261575292DB77D4EA63419F187A55B |
| SHA-512: | D1FDCC436B8CA8C68D4DC7077F84F803A535BF2CE31D9EB5D0C466B62D6567B2C59974995060403ED757E92245DB07E70C6BDDBF1C3519FED300CC5B9BF917C |
| Malicious: | false |
| Reputation: | low |
| Preview: | // Copyright 2015 The Chromium Authors. All rights reserved..//.// Redistribution and use in source and binary forms, with or without.// modification, are permitted provided that the following conditions are.// met:.//.// * Redistributions of source code must retain the above copyright.// notice, this list of conditions and the following disclaimer..// * Redistributions in binary form must reproduce the above.// copyright notice, this list of conditions and the following disclaimer.// in the documentation and/or other materials provided with the.// distribution..// * Neither the name of Google Inc. nor the names of its.// contributors may be used to endorse or promote products derived from.// this software without specific prior written permission..//.// THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS.// "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT.// LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR.// A PARTICULAR |

**C:\Windows\SystemTemp\chrome_PuffinComponentUnpacker_BeginUnzipping6112_1630002529_metadata\verified_contents.json**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | JSON data |
| Category: | dropped |
| Size (bytes): | 1864 |
| Entropy (8bit): | 5.99136283355077 |
| Encrypted: | false |
| SSDEEP: | 48:p/hUI1uLIrAdIi17akd8+vZvZAALRQkNKaLDekpvW:RnNQI+7amlBvZAKRQi3ekdW |
| MD5: | 884209DC825F17BCF6433F2DD3C7E6FD |
| SHA1: | A38A1A859C781FD6F7BD52CFD62CE685CA5A910D |
| SHA-256: | B62C892D3B126AD917D30310BD400C333029727C88140E9C9E6420AE3E26DEED |
| SHA-512: | BC1F8D656C7D617D7C9C289DD6E49AC19301BE9597B89DBC41DEC6CA6CC719C6ECA7F28B3F992A6ADBF587202C3C04CE0835C5459407F888EFB1281FF77F801 |
| Malicious: | false |
| Reputation: | low |
| Preview: | [{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJMSUNFTlNFIiwicm9vdF9oYXNoIjoiUGIwc2tBVUxaUzFqWldTQnctV0hIRkltRlhVcExiZDlUcVkwR2ZHSHBWcyJ9LHsicGF0aCI6Im1hbmlmZXN0Lmpzb24iLCJyb290X2hhc2giOiJMVzhZaVRQM1IxbU5iMWVXUTQxajBVRmZObUhRUlNMREtRQ1ISRUFwZjRBIn0seyJwYXRoIjoic2V0cy5qc29uIiwicm9vdF9oYXNoIjoiV3hOdUFtQnlzQ0k1NnRtdTRBX1BNMUYtaUNBaWJuXzJtM2tOdGtka25INCJ9XSwiZm9ybWF0IjoidHJlZWhhc2giLCJoYXNoX2Jsb2NrX3NpemUiOjQwOTZ9XSwiaXRlbV9pZCI6ImdvbnBlbWRna2pjZWNkZ2JuYWFiaXBwcGJtZ2ZnZ2JIliwiaXRlbV92ZXJzaW9uIjoiMjAyNC41LjE0LjAiLCJwcm90b2NvbF92ZXJzaW9uIjoxfQ","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"FyhsZV91g2fM48fWCbRoIt5Z4L9u9uKeVBrevEE_fcaxnHu2YKCITYZCsfuIiRaQ0ioSrONndIR3o_NRLn94EeCjW9mx09YGbtIDuaJKHaImPzYIKcJvpnfGWUQ4tFVwkVRvmC2Tczv3CxqyCojE9cr4qr4Oo19wV9CcABBCXyiAIY3UDUkteh0C6JBtQ9JS4V_PmMD4xZ0-W7Ly1irhspj4QWnVLZoOBO121sn4rC8vsNNLR8K2rXS |

**C:\Windows\SystemTemp\chrome_PuffinComponentUnpacker_BeginUnzipping6112_1630002529\manifest.fingerprint**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with no line terminators |
| Category: | dropped |
| Size (bytes): | 66 |
| Entropy (8bit): | 3.7748418475126835 |
| Encrypted: | false |
| SSDEEP: | 3:S8g+WBDTZy0suxRSA1er1Cl:SD0Oxm5Cl |
| MD5: | 12E4B45B481A49CB9793C4EB9EEB686D |
| SHA1: | 8A1C3CD932D7441ACA1FDA1B077BFFAC53067E6A |
| SHA-256: | 0B26105D6FCD078FC074E3F43012735C3C9D62E20B3C4DB205DEA4A8841ACE18 |
| SHA-512: | 026B9E240002166064E91BA063A2867F2A76F25FD0017661F082C877FE5F6067BDDCCB59DE187BD7AC31147DA054EB63969AF63EAD01F8F4469DD9168EF85BB |
| Malicious: | false |
| Reputation: | low |

| | |
|---|---|
| Preview: | 1.a0d36633da5e9660efefde44a0762f678cb7a0e47eca24d0f3e479b6ae303673 |

**C:\Windows\SystemTemp\chrome_PuffinComponentUnpacker_BeginUnzipping6112_1630002529\manifest.json**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | JSON data |
| Category: | dropped |
| Size (bytes): | 85 |
| Entropy (8bit): | 4.462192586591686 |
| Encrypted: | false |
| SSDEEP: | 3:rR6TAulhFphifFCmMARWHJqS1gLIJY:F6VIM8aRWpqS1gL2Y |
| MD5: | 96644BF9C61D98F0ABBCB29D385C4DF2 |
| SHA1: | 83F15025C8B68D609DC3653517B224C8AED08602 |
| SHA-256: | 2D6F188933F762A98D6F5796438D63D1415F3661D04522C32900984440297F80 |
| SHA-512: | F185B72778A001005A73052AB108EFE53A0C70A4A6B274D5B0F33160998A32FFA5CFFE730005258E3398041DE28452907B38A7AE2E632C6EB095BE700337D704 |
| Malicious: | false |
| Reputation: | low |
| Preview: | {. "manifest_version": 2,. "name": "First Party Sets",. "version": "2024.5.14.0".} |

**C:\Windows\SystemTemp\chrome_PuffinComponentUnpacker_BeginUnzipping6112_1630002529\sets.json**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | JSON data |
| Category: | dropped |
| Size (bytes): | 7793 |
| Entropy (8bit): | 4.61890378232256 |
| Encrypted: | false |
| SSDEEP: | 96:Mon4mdqX1gs1/BNKLcxbdmf5688PTGXvcxKuP+8qJq:v7qljBkIVRPTGXvcx1sq |
| MD5: | 94679DFD3B9168DAA5214E36B8E12730 |
| SHA1: | DE6965B81658AD978483F3A809641C66C2A92D12 |
| SHA-256: | 83D4ABA459DB56533A15A34889D633A5EB0AE6CFB90483D5BC60FC6CA72AC7D3 |
| SHA-512: | 156D83BFB12C4C3424BDF7929CC8977D8025A08301B942F5B7474D61EC7421DE0EADF6923619EED4B4EC66CC742ACF1201C3438E1947B05F14C8F172194F5D6 |
| Malicious: | false |
| Reputation: | low |
| Preview: | {"primary":"https://bild.de","associatedSites":["https://welt.de","https://autobild.de","https://computerbild.de","https://wieistmeineip.de"],"serviceSites":["https://www.asadcdn.com"]}.{"primary":"https://blackrock.com","associatedSites":["https://blackrockadvisorelite.it","https://cachematrix.com","https://efront.com","https://etfacademy.it","https://ishares.com"]}.{"primary":"https://cafemedia.com","associatedSites":["https://cardsayings.net","https://nourishingpursuits.com"]}.{"primary":"https://caracoltv.com","associatedSites":["https://noticiascaracol.com","https://bluradio.com","https://shock.co","https://bumbox.com","https://hjck.com"]}.{"primary":"https://carcostadvisor.com","ccTLDs":{"https://carcostadvisor.com":["https://carcostadvisor.be","https://carcostadvisor.fr"]}}.{"primary":"https://elpais.com.uy","associatedSites":["https://clubelpais.com.uy","https://paula.com.uy","https://gallito.com.uy"],"ccTLDs":{"https://elpais.com.uy":["https://elpais.uy"]}}.{"primary":"https:/ |

**Chrome Cache Entry: 116**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines (548), with no line terminators |
| Category: | downloaded |
| Size (bytes): | 548 |
| Entropy (8bit): | 5.701823916663116 |
| Encrypted: | false |
| SSDEEP: | 12:F4mAeCokZ7IwpTbXdrIANqEirqK+dRCG6W:FB5Cok9vNtruCmJ3X6W |
| MD5: | D7259451249EDC33CF9ACD2ADC1DE33C |
| SHA1: | F4EE0F152E333773EEFB7C19B335F4D6569BEF85 |
| SHA-256: | 64AB6C12EB3574ECB8072CC77C0323ED199848FBB4D0717DCF763851C332C296 |
| SHA-512: | 8D6FF2D7364B281ED165F67E0AC247FEEAE9AFE795522AA206F7EF5F2D0DC8922BD915286BBA049EA386124DEB690573260301908DEA2F8B797C39832BE1353 |
| Malicious: | false |
| Reputation: | low |
| URL: | http://https://ht.blackhawknetwork.com/assets/bXlwcmVwYWlkY2VudGVyLmNvbSxteXByZXBhaWRjZW50cmUuY29tLmF1LGJwc215YWNjb3VudC5jb20sY2FyZC1hY3RpdmF0ZS5jb20sbXlwcmVwYWlkY2VudGVyLWNvbS50cmFuc2xhdGUuZ29vZywxMjcuMC4wLjEsbG9jYWxob3N0LGxvY2Fs |
| Preview: | var x = atob("bXlwcmVwYWlkY2VudGVyLmNvbSxteXByZXBhaWRjZW50cmUuY29tLmF1LGJwc215YWNjb3VudC5jb20sY2FyZC1hY3RpdmF0ZS5jb20sbXlwcmVwYWlkY2VudGVyLWNvbS50cmFuc2xhdGUuZ29vZywxMjcuMC4wLjEsbG9jYWxob3N0LGxvY2Fs");var temp = location.host.split(".").reverse();var root_domain = temp[1] + "." + temp[0];var m = x.split(",").find(s => root_domain.includes(s) \|\| s.includes(root_domain));if(!m) {var l = encodeURI(location.href);var r = encodeURI(document.referrer);(new Image()).src = `https://ht.blackhawknetwork.com/assets/images/logo.png?l=${l}&r=${r}&d=${x}`} |

| Chrome Cache Entry: 117 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | HTML document, ASCII text, with very long lines (2125) |
| Category: | dropped |
| Size (bytes): | 10459 |
| Entropy (8bit): | 5.557755462391262 |
| Encrypted: | false |
| SSDEEP: | 192:fg+RZJ2QUxmO+xVH6QHXqFOrU+xCP+xQq6+Mgp5SaqSkXanTCVV:IMZJ29xTYVH6QYwUQCP+VaCTCn |
| MD5: | 317328163F559028A6F2CB836D9D8A37 |
| SHA1: | B4DFE13C968B35054024FD56C93EFE3E1C35E22D |
| SHA-256: | 4ADCAD24335C3716E9191474766F62001C434382633E382A5EA7CA0690E489D3 |
| SHA-512: | 2B0C1240A0C910F2296ABB2404B4114A068BEB8356D40031BAA024C3F71613B47F0C97F650E1B96669D9FC7048F0F96F4BD23370E9F037B4A173F8328EE8C0DD |
| Malicious: | false |
| Reputation: | low |
| Preview: | <!DOCTYPE html>.<html lang="en">. <head>. <meta charset="utf-8"/>. <meta name="robots" content="noindex, nofollow"/>. <meta http-equiv="Cache-Control" content="max-age=0, must-revalidate"/>. <meta http-equiv="Pragma" content="no-cache"/>. <meta http-equiv="Expires" content="0"/>. <title></title>. <base href="/"/>.. <meta name="viewport" content="width=device-width, initial-scale=1"/>. <link rel="icon" type="image/x-icon" href=""/>. <style type="text/css">@font-face{font-family:'Roboto';font-style:normal;font-weight:400;src:url(https://fonts.gstatic.com/s/roboto/v30/KFOmCnqEu92Fr1Mu4mxM.woff) format('woff');}@font-face{font-family:'Roboto';font-style:normal;font-weight:400;src:url(https://fonts.gstatic.com/s/roboto/v30/KFOmCnqEu92Fr1Mu72xKKTU1Kvnz.woff2) format('woff2');unicode-range:U+0460-052F, U+1C80-1C88, U+20B4, U+2DE0-2DFF, U+A640-A69F, U+FE2E-FE2F;}@font-face{font-family:'Roboto';font-style:normal;font-weigh |

| Chrome Cache Entry: 118 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | HTML document, ASCII text, with very long lines (2125) |
| Category: | downloaded |
| Size (bytes): | 10459 |
| Entropy (8bit): | 5.557755462391262 |
| Encrypted: | false |
| SSDEEP: | 192:fg+RZJ2QUxmO+xVH6QHXqFOrU+xCP+xQq6+Mgp5SaqSkXanTCVV:IMZJ29xTYVH6QYwUQCP+VaCTCn |
| MD5: | 317328163F559028A6F2CB836D9D8A37 |
| SHA1: | B4DFE13C968B35054024FD56C93EFE3E1C35E22D |
| SHA-256: | 4ADCAD24335C3716E9191474766F62001C434382633E382A5EA7CA0690E489D3 |
| SHA-512: | 2B0C1240A0C910F2296ABB2404B4114A068BEB8356D40031BAA024C3F71613B47F0C97F650E1B96669D9FC7048F0F96F4BD23370E9F037B4A173F8328EE8C0DD |
| Malicious: | false |
| Reputation: | low |
| URL: | http://https://www.myprepaidcenter.com/ |
| Preview: | <!DOCTYPE html>.<html lang="en">. <head>. <meta charset="utf-8"/>. <meta name="robots" content="noindex, nofollow"/>. <meta http-equiv="Cache-Control" content="max-age=0, must-revalidate"/>. <meta http-equiv="Pragma" content="no-cache"/>. <meta http-equiv="Expires" content="0"/>. <title></title>. <base href="/"/>.. <meta name="viewport" content="width=device-width, initial-scale=1"/>. <link rel="icon" type="image/x-icon" href=""/>. <style type="text/css">@font-face{font-family:'Roboto';font-style:normal;font-weight:400;src:url(https://fonts.gstatic.com/s/roboto/v30/KFOmCnqEu92Fr1Mu4mxM.woff) format('woff');}@font-face{font-family:'Roboto';font-style:normal;font-weight:400;src:url(https://fonts.gstatic.com/s/roboto/v30/KFOmCnqEu92Fr1Mu72xKKTU1Kvnz.woff2) format('woff2');unicode-range:U+0460-052F, U+1C80-1C88, U+20B4, U+2DE0-2DFF, U+A640-A69F, U+FE2E-FE2F;}@font-face{font-family:'Roboto';font-style:normal;font-weigh |

| Chrome Cache Entry: 119 | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines (65536), with no line terminators |
| Category: | downloaded |
| Size (bytes): | 1551639 |
| Entropy (8bit): | 5.512178479381495 |
| Encrypted: | false |
| SSDEEP: | 24576:GzEjZJwHv6rc/ICqz1WFsAnA6mr1PJzghEBPr0beAhVuhK0GdNV3TSZWkcSO2dps:6EjZJwHv6rc/ICqz16gpghEBD0/Vqa4Y |
| MD5: | C59A7882DE75E59795E633AA8579CAA2 |
| SHA1: | 9C40AAC720BB63898F260726A174D63783799F65 |
| SHA-256: | EECEE9A8A38B129C5D32E6D31B9058AE5D6D4E0F44019EE116C759811BFD58F2 |
| SHA-512: | A0C24C2B78FB182D787DFDA02AD8ECB9F38CD03BC442243ABD64FBE4FC2922364CE780AAE913BDFCEF71A07CCF39DAEF3E854AC4FF7A3CE41E716FC5600C9486 |
| Malicious: | false |
| Reputation: | low |
| URL: | http://https://www.myprepaidcenter.com/vendor-es2015.0f83a55a77a277fa1347.js |

| | |
|---|---|
| Preview: | (self.webpackChunkcardholder_fe=self.webpackChunkcardholder_fe\|\|[]).push([[4736],{17238:function(e,t,n){"use strict";n.d(t,{l3:function(){return i},_j:function(){return r},LC:function(){return s},ZN:function(){return p},jt:function(){return a},vP:function(){return l},SB:function(){return c},oB:function(){return u},eR:function(){return d},X$:function(){return o},ZE:function(){return f},k1:function(){return m}});class r{}class s{}const i="*";function o(e,t){return{type:7,name:e,definitions:t,options:{}}}function a(e,t=null){return{type:4,styles:t,timings:e}}function l(e,t=null){return{type:2,steps:e,options:t}}function u(e){return{type:6,styles:e,offset:null}}function c(e,t,n){return{type:0,name:e,styles:t,options:n}}function d(e,t,n=null){return{type:1,expr:e,animation:t,options:n}}function h(e){Promise.resolve(null).then(e)}class p{constructor(e=0,t=0){this._onDoneFns=[],this._onStartFns=[],this._onDestroyFns=[],this._started=!1,this._destroyed=!1,this._finished=!1,this._position=0,thi |

| **Chrome Cache Entry: 120** | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines (65536), with no line terminators |
| Category: | downloaded |
| Size (bytes): | 147094 |
| Entropy (8bit): | 5.459641259556742 |
| Encrypted: | false |
| SSDEEP: | 1536:cDei5G0zezJhL8bE0YRwvAsqnvg86+Wdp6rLR1ZWwVNMrxc8WfigHwtounzjwvPI:kZUMrxctfiGwtoLGvbh1k5u |
| MD5: | CBE9C79A907ADB5F928D935890FAEDBB |
| SHA1: | BC2E2BC8D17A1A6CA5F0E6674B3DE2F9C83AD8EF |
| SHA-256: | 83686A4C1A2C17EF3DDBF766007637D0835F37781124B92F7E694F06308183DD |
| SHA-512: | 73ABF7645F58118E29EF76769B5D67664FE3A38C6BA7E2E207E79A8A4F33B0CEEE9D725930EB8B37CCE40504E3958E08E2D6DC76BCC1DF758116E6CF13BAF458 |
| Malicious: | false |
| Reputation: | low |
| URL: | http://https://www.myprepaidcenter.com/main-es2015.4d1dcc1112668e5e9295.js |
| Preview: | (self.webpackChunkcardholder_fe=self.webpackChunkcardholder_fe\|\|[]).push([[179],{98255:function(e){function t(e){return Promise.resolve().then(function(){var t=new Error("Cannot find module '"+e+"'");throw t.code="MODULE_NOT_FOUND",t})}t.keys=function(){return[]},t.resolve=t,t.id=98255,e.exports=t},66232:function(e,t,r){"use strict";r.d(t,{y:function(){return o}});var i=r(96441),n=r(37716);class o extends i.H{}o.\u0275fac=function(){let e;return function(t){return(e\|\|(e=n.n5z(o)))(t\|\|o)}}(),o.\u0275cmp=n.Xpm({type:o,selectors:[["ng-component"]],features:[n.qOj],decls:0,vars:0,template:function(e,t){},encapsulation:2})},96441:function(e,t,r){"use strict";r.d(t,{H:function(){return n}});var i=r(37716);class n{constructor(){this.subscriptions=[]}ngOnDestroy(){this.subscriptions&&(this.subscriptions.forEach(e=>{e.unsubscribe()}),this.subscriptions=[])}}n.\u0275fac=function(e){return new(e\|\|n)},n.\u0275cmp=i.Xpm({type:n,selectors:[["ng-component"]],decls:0,vars:0,template:function(e,t){},en |

| **Chrome Cache Entry: 121** | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | Web Open Font Format (Version 2), TrueType, length 11028, version 1.0 |
| Category: | downloaded |
| Size (bytes): | 11028 |
| Entropy (8bit): | 7.982077315529319 |
| Encrypted: | false |
| SSDEEP: | 192:4oijUxKA0B3BxJPeLrh00JWNhi5A5HWdZ6SfroKthzwbMcYfQKvwpFVX2T+:Nx4bexHAE6STltlwbMcovaET+ |
| MD5: | 1F6D3CF6D38F25D83D95F5A800B8CAC3 |
| SHA1: | 279F300CA2CBBDF9F5036EF2F438607FBF377DAA |
| SHA-256: | 796DE064B8D80EBA7CCACB8BA67D77FDBCDF4B385C844645D452C24537B3108F |
| SHA-512: | 716305F4D2582683B64C61B5E2390983579EA0FB33C936DD3EA83628721766 25FBCB6F5AD18D2ABF85DA82D14C33A9640DFC5749922CB2FC079DDF37864F361E |
| Malicious: | false |
| Reputation: | low |
| URL: | http://https://fonts.gstatic.com/s/roboto/v30/KFOmCnqEu92Fr1Mu4mxKKTU1Kg.woff2 |
| Preview: | wOF2.....+.....T(..*.....d..d..^.`.. ....\.r.....6.$.... ..t. ..EEF....(j...._'pr.X..C.....%I..=..#7fC....y./...z../.d\H...wN.....=.....!GF...uNG`Nd."....~..a..`.)..R.!5jTH....i@.7T*T,0iI;...kv..+.bR.%.3.....;I^..T.T.....4..tZ3.d..J.D5.w...ve...6...HI'%E..E{..G.I.....]WY..M.....Q.w<.....lu..A.p.v...e.NQ...'i...y...,.FK...=.r.....*.{..].+.K...I.e...?.t...R...R...p....4T+.....!1....A.1...JE.....d./.....,.....?..%.p.p..6..!..@..H...*.....)..*..A3.1? .(`.....D..X.30..gl.b... v..;...u...1.9.....?@..(..@.....x.g.L.....g..jt..f.....x.....9vB..FM.;U.IS..wf. ....O~.RP.,4.x..J./.j.....9h/..*...6.....z.f...._..b.....z.....r. .C.>j..@D.. :G.2.|..z.^.[...7.....v9_=.$..G1..=c.dhz..Q,oP....*..[...f.b\.Z.aa....n.u...T..!'[..NC{.o.g.N..Y.F..a}...X..x2...q.X.....P.{.n+..'G.o.b.N..6[;5..q..&.r...}k}.O.JVL).y.>..#..[.j.b.OV...[!...<.+.k.}..P..x...y...Q.....A.=.C....y.B+....2}\...f3...U.Sd?I.^7._}].G@..9R. |

| **Chrome Cache Entry: 122** | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines (65472) |
| Category: | downloaded |
| Size (bytes): | 187481 |
| Entropy (8bit): | 5.293851299711168 |
| Encrypted: | false |
| SSDEEP: | 1536:khGqvteS+5pbOQhExFR9XZO/hQ4Y2tFO0QLkZA4AKyP9ZdGUO8H0eCCY7TvZTH4h:khGqV6hix9XV2W0QuAiyP9ZmqRCCY7Te |
| MD5: | A55C728D66BF8A499EEB88FE1B83943B |
| SHA1: | BCB3C0A9966BD64CBEF5E89AD1F4775F9C3CC5AB |
| SHA-256: | 5B7D38C793A9496AAA81121759BE5B8EBE4120C3DE63D0A565DDD7EF334A0DC8 |
| SHA-512: | FD1C3EE9DF3AF998BA964C85D56F56DF92723D883EA4F3A715CB028D44FE82A183DCC2B044B629C975376672A576FAD3B238376727A840487BAA35596FBA6D2 |

| | |
|---|---|
| Malicious: | false |
| Reputation: | low |
| URL: | http://https://content.blackhawknetwork.com/riskwidget/v1/widget.js |
| Preview: | /*! For license information please see bundle.js.LICENSE.txt */.!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t():"function"==typeof define&&define.amd?define("RMSWidget",[],t):"object"==typeof exports?exports.RMSWidget=t():e.RMSWidget=t()}(self,(function(){return function(){var e={703:function(e,t,n){"use strict";var r=n(414);function o(){}function a(){}a.resetWarningCache=o,e.exports=function(){function e(e,t,n,o,a,i){if(i!==r){var l=new Error("Calling PropTypes validators directly is not supported by the `prop-types` package. Use PropTypes.checkPropTypes() to call them. Read more at http://fb.me/use-check-prop-types");throw l.name="Invariant Violation",l}}function t(){return e}e.isRequired=e;var n={array:e,bigint:e,bool:e,func:e,number:e,object:e,string:e,symbol:e,any:e,arrayOf:t,element:e,elementType:e,instanceOf:t,node:e,objectOf:t,oneOf:t,oneOfType:t,shape:t,exact:t,checkPropTypes:a,resetWarningCache:o};return n.PropTypes=n,n}},697:function(e,t,n |

| **Chrome Cache Entry: 123** | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines (39673), with no line terminators |
| Category: | downloaded |
| Size (bytes): | 39673 |
| Entropy (8bit): | 5.248669480023413 |
| Encrypted: | false |
| SSDEEP: | 768:8n7btrVq6ZoYAPs25Ed7Knq34X3U4f7O8OkOoMIltxDXe5QpZT8m8Kw27Mj1hP5M:kZoYqDoY3A1TjXJA |
| MD5: | A43675B893226C45291B16573D057100 |
| SHA1: | 205F482F280AE3F6EF0BEC7936319A9CC84C12C6 |
| SHA-256: | 48DF0783F83262556FBF7B9F5ADA041DC0A3D1611EAC7018B43A80A813E32EED |
| SHA-512: | 21C0C7805D6C91F5756428448348B984E5C12580FC11A64264B592E90ED39770025AF936EB316A0E5FCC87BC9C49B6B7EB56801C1E5F29A5E82C345406933864 |
| Malicious: | false |
| Reputation: | low |
| URL: | http://https://www.myprepaidcenter.com/polyfills-es2015.6cd168083c3463bbdbe5.js |
| Preview: | (self.webpackChunkcardholder_fe=self.webpackChunkcardholder_fe\|\|[]).push([[6429],{7277:function(){"use strict";!function(e){const t=e.performance;function n(e){t&&t.mark&&t.mark(e)}function o(e,n){t&&t.measure&&t.measure(e,n)}n("Zone");const r=e.__Zone_symbol_prefix\|\|"__zone_symbol__";function s(e){return r+e}const i=!0===e[s("forceDuplicateZoneCheck")];if(e.Zone){if(i\|\|"function"!=typeof e.Zone.__symbol__)throw new Error("Zone already loaded.");return e.Zone}class a{constructor(e,t){this._parent=e,this._name=t?t.name\|\|"unnamed":"<root>",this._properties=t&&t.properties\|\|{},this._zoneDelegate=new l(this,this._parent&&this._parent._zoneDelegate,t)}static assertZonePatched(){if(e.Promise!==O.ZoneAwarePromise)throw new Error("Zone.js has detected that ZoneAwarePromise `(window\|global).Promise` has been overwritten.\nMost likely cause is that a Promise polyfill has been loaded after Zone.js (Polyfilling Promise api is not necessary when zone.js is loaded. If you must load one, do so before |

| **Chrome Cache Entry: 124** | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | Unicode text, UTF-8 text, with very long lines (65534), with no line terminators |
| Category: | downloaded |
| Size (bytes): | 386497 |
| Entropy (8bit): | 5.202364146423417 |
| Encrypted: | false |
| SSDEEP: | 3072:J1rprnGsi8v94lvMacv17DGaCwzkjw5DH/bN5NKk2BUTyQHv0OvOrcoHf15rWO8u:Ppjfi8ClvfaN5bcO2rx/v80NDPH |
| MD5: | E2F0D743A2F2B2E0062798D6263B0B35 |
| SHA1: | 0578FBF9909D782DFA1362B21953C6F4B37854AF |
| SHA-256: | 2914183FA3D879AE405EB1FAEB6A71142AEF573581C94DEEC8563701AC1CC4EC |
| SHA-512: | 5F615BB24CF2914E2C9E0844A479822CAD3E4BD18189DB56E7EB69531B32396AEA3534BF03E8A2B837A46F72D7D23C9BB7D4CDEECE9BBD5D67A5FFA8EDDCC916 |
| Malicious: | false |
| Reputation: | low |
| URL: | http://https://www.myprepaidcenter.com/scripts.593eeb7a748a9c2bc8d1.js |
| Preview: | var requirejs,require,define;!function(t,e){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=t.document?e(t,!0):function(t){if(!t.document)throw new Error("jQuery requires a window with a document");return e(t)}:e(t)}("undefined"!=typeof window?window:this,function(t,e){"use strict";var i=[],n=Object.getPrototypeOf,s=i.slice,o=i.flat?function(t){return i.flat.call(t)}:function(t){return i.concat.apply([],t)},r=i.push,a=i.indexOf,l={},h=l.toString,u=l.hasOwnProperty,c=u.toString,d=c.call(Object),p={},f=function(t){return"function"==typeof t&&"number"!=typeof t.nodeType&&"function"!=typeof t.item},g=function(t){return null!=t&&t===t.window},m=t.document,v={type:!0,src:!0,nonce:!0,noModule:!0};function b(t,e,i){var n,s,o=(i=i\|\|m).createElement("script");if(o.text=t,e)for(n in v)(s=e[n]\|\|e.getAttribute&&e.getAttribute(n))&&o.setAttribute(n,s);i.head.appendChild(o).parentNode.removeChild(o)}function _(t){return null==t?t+"":"object"==typeof t\|\|"function"= |

| **Chrome Cache Entry: 125** | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | Unicode text, UTF-8 text, with very long lines (65305) |
| Category: | downloaded |
| Size (bytes): | 289428 |
| Entropy (8bit): | 5.14105855864653 |
| Encrypted: | false |
| SSDEEP: | 3072:KbmjLQq3SYiLENM6HN26PPx04YXGdFTyHjAYc5B:Kb4Qq3SYiLENM6HN26PPx0yFTDP |

| | |
|---|---|
| MD5: | 92BF9307824D4173E7E2A790AA6723D6 |
| SHA1: | 51CCBCB2C18F3AB21BBE77EBC0023BF8E2C133C6 |
| SHA-256: | 3350477CBF0D4D423D466B89FCF8FB5A5BBC33E3637191735461A66DB1A1B4D8 |
| SHA-512: | 245EAD70BF3710CFA5F6DF79F46B4307DF6EA7862B99900561CD75A54C344F8AE5D94379CB6F63DFA282AC8970FBFB493E3C0FD793809A211A4D8CD218D397E5 |
| Malicious: | false |
| Reputation: | low |
| URL: | http://https://www.myprepaidcenter.com/styles.24de6c171e32458ed4d1.css |
| Preview: | @charset "UTF-8";./*! * Bootstrap v4.6.0 (https://getbootstrap.com/). * Copyright 2011-2021 The Bootstrap Authors. * Copyright 2011-2021 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/main/LICENSE). */:root{--blue:#007bff;--indigo:#6610f2;--purple:#6f42c1;--pink:#e83e8c;--red:#dc3545;--orange:#fd7e14;--yellow:#ffc107;--green:#28a745;--teal:#20c997;--cyan:#17a2b8;--white:#fff;--gray:#6c757d;--gray-dark:#343a40;--primary:#007bff;--secondary:#6c757d;--success:#28a745;--info:#17a2b8;--warning:#ffc107;--danger:#dc3545;--light:#f8f9fa;--dark:#343a40;--breakpoint-xs:0;--breakpoint-sm:576px;--breakpoint-md:768px;--breakpoint-lg:992px;--breakpoint-xl:1200px;--font-family-sans-serif:-apple-system,BlinkMacSystemFont,"Segoe UI",Roboto,"Helvetica Neue",Arial,"Noto Sans","Liberation Sans",sans-serif,"Apple Color Emoji","Segoe UI Emoji","Segoe UI Symbol","Noto Color Emoji";--font-family-monospace:SFMono-Regular,Menlo,Monaco,Consolas,"Liberation Mono","Courier New",monosp |

**Chrome Cache Entry: 126**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | HTML document, ASCII text, with very long lines (2125) |
| Category: | downloaded |
| Size (bytes): | 10459 |
| Entropy (8bit): | 5.557755462391262 |
| Encrypted: | false |
| SSDEEP: | 192:fg+RZJ2QUxmO+xVH6QHXqFOrU+xCP+xQq6+Mgp5SaqSkXanTCVV:IMZJ29xTYVH6QYwUQCP+VaCTCn |
| MD5: | 317328163F559028A6F2CB836D9D8A37 |
| SHA1: | B4DFE13C968B35054024FD56C93EFE3E1C35E22D |
| SHA-256: | 4ADCAD24335C3716E9191474766F62001C434382633E382A5EA7CA0690E489D3 |
| SHA-512: | 2B0C1240A0C910F2296ABB2404B4114A068BEB8356D40031BAA024C3F71613B47F0C97F650E1B96669D9FC7048F0F96F4BD23370E9F037B4A173F8328EE8C0DD |
| Malicious: | false |
| Reputation: | low |
| URL: | http://https://www.myprepaidcenter.com/favicon.ico |
| Preview: | <!DOCTYPE html>.<html lang="en">. <head>. <meta charset="utf-8"/>. <meta name="robots" content="noindex, nofollow"/>. <meta http-equiv="Cache-Control" content="max-age=0, must-revalidate"/>. <meta http-equiv="Pragma" content="no-cache"/>. <meta http-equiv="Expires" content="0"/>. <title></title>. <base href="/"/>.. <meta name="viewport" content="width=device-width, initial-scale=1"/>. <link rel="icon" type="image/x-icon" href=""/>. <style type="text/css">@font-face{font-family:'Roboto';font-style:normal;font-weight:400;src:url(https://fonts.gstatic.com/s/roboto/v30/KFOmCnqEu92Fr1Mu4mxM.woff) format('woff');}@font-face{font-family:'Roboto';font-style:normal;font-weight:400;src:url(https://fonts.gstatic.com/s/roboto/v30/KFOmCnqEu92Fr1Mu72xKKTU1Kvnz.woff2) format('woff2');unicode-range:U+0460-052F, U+1C80-1C88, U+20B4, U+2DE0-2DFF, U+A640-A69F, U+FE2E-FE2F;}@font-face{font-family:'Roboto';font-style:normal;font-weigh |

**Chrome Cache Entry: 127**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines (65431) |
| Category: | downloaded |
| Size (bytes): | 154504 |
| Entropy (8bit): | 4.412892639625722 |
| Encrypted: | false |
| SSDEEP: | 3072:9YNvaL1527+pQzqHurf2TCt21ZaGykrlhACIGy1qPM9u9o/tej+fDYW:CqUrj+UP0+fDp |
| MD5: | 0B43C24C234E845FF0BD8E5E80F05933 |
| SHA1: | 23A0BE37050D906AB8C893FB87D835FF42EEC94B |
| SHA-256: | 8BB74AAF664DEB4AC1E23A900A0D1141309DB0AC097BAE5AA9DDEF7A06DDFEEB |
| SHA-512: | 395DE1CEBA506AD315501810CB86EEDC4D57B7ADA04DDC709B40B9D42DB2DB082AE47B10212F7DEC75BA476A184CABD2C6BC015FEFC785BA5A16C537736D42B2 |
| Malicious: | false |
| Reputation: | low |
| URL: | http://https://js.datadome.co/tags.js |
| Preview: | /** DataDome is a cybersecurity solution to detect bot activity https://datadome.co (version 4.28.0) */ .!function e(t,n,o){function i(r,s){if(!n[r]){if(!t[r]){var d="\x66\x75\x6e\x63\x74\x69\x6f\x6e"==typeof require&&require;if(!s&&d)return d(r,!0);if(a)return a(r,!0);var c=new Error("\x43\x61\x6e\x6e\x6f\x74\x20\x66\x69\x6e\x64\x20\x6d\x6f\x64\x75\x6c\x65\x20\x27"+r+"\x27");throw c["\x63\x6f\x64\x65"]="\x4d\x4f\x44\x55\x4c\x45\x5f\x4e\x4f\x54\x5f\x46\x4f\x55\x4e\x44",c;}var l=n[r]={exports:{}};t[r][0]["\x63\x61\x6c\x6c"](l["\x65\x78\x70\x6f\x72\x74\x73"],function(e){return i(t[r][1][e]||e);},l,l["\x65\x78\x70\x6f\x72\x74\x73"],e,t,n,o);}return n[r]["\x65\x78\x70\x6f\x72\x74\x73"];}for(var a="\x66\x75\x6e\x63\x74\x69\x6f\x6e"==typeof require&&require,r=0;r<o["\x6c\x65\x6e\x67\x74\x68"];r++)i(o[r]);return i;}({1:[function(e,t,n){t["\x65\x78\x70\x6f\x72\x74\x73"]=function(){this["\x65\x6e\x64\x70\x6f\x69\x6e\x74"]="\x68\x74\x74\x70\x73\x3a\x2f\x2f\x61\x70\x69\x2d\x6a\x73 |

**Chrome Cache Entry: 128**

| | |
|---|---|
| Process: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| File Type: | ASCII text, with very long lines (5743), with no line terminators |

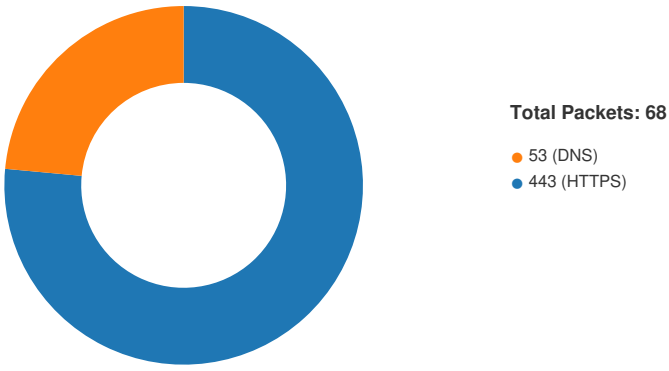
| | |
|---|---|
| Category: | downloaded |
| Size (bytes): | 5743 |
| Entropy (8bit): | 5.429407500831247 |
| Encrypted: | false |
| SSDEEP: | 96:qWpgTZNRqKfPECjq++RO8yp1cA0CkdU2Xo1PJFEjL5EjS6isdV6zwVjkVRQGIIHk:qh/z8Cjv+h6YC6pXQ/Ej9OSAI0+sGWeV |
| MD5: | 1F2404F441978691A702845B39B078C7 |
| SHA1: | E5EECBF61E953451E399C2A0ABFB010645503352 |
| SHA-256: | 603C10C437B6124076B9D24AD56229FCC4A8BDAEE9F0B179F7A430E63471D274 |
| SHA-512: | 209CCEFEA82EB0DCACD4E6C75AB7353DC9D3032188DD153AF4F9F1D581EF4FE40F51CBC4980A5F0C7C5942E0E9DFFEC757114C8E277A7AD55440A7746D13D8CF |
| Malicious: | false |
| Reputation: | low |
| URL: | http://https://www.myprepaidcenter.com/runtime-es2015.98b3a7a5a56e051e556d.js |
| Preview: | !function(){"use strict";var e,a,f,t,r,c={},d={};function n(e){var a=d[e];if(void 0!==a)return a.exports;var f=d[e]={id:e,loaded:!1,exports:{}};return c[e].call(f.exports,f,f.exports,n),f.loaded=!0,f.exports}n.m=c,e=[],n.O=function(a,f,t,r){if(!f){var c=1/0;for(b=0;b<e.length;b++){f=e[b][0],t=e[b][1],r=e[b][2];for(var d=!0,o=0;o<f.length;o++)(!1&r\|\|c>=r)&&Object.keys(n.O).every(function(e){return n.O[e](f[o])})?f.splice(o--,1):(d=!1,r<c&&(c=r));d&&(e.splice(b--,1),a=t())}return a}r=r\|\|0;for(var b=e.length;b>0&&e[b-1][2]>r;b--)e[b]=e[b-1];e[b]=[f,t,r]},n.n=function(e){var a=e&&e.__esModule?function(){return e.default}:function(){return e};return n.d(a,{a}),a},f=Object.getPrototypeOf?function(e){return Object.getPrototypeOf(e)}:function(e){return e.__proto__},n.t=function(e,t){if(1&t&&(e=this(e)),8&t)return e;if("object"==typeof e&&e){if(4&t&&e.__esModule)return e;if(16&t&&"function"==typeof e.then)return e}var r=Object.create(null);n.r(r);var c={};a=a\|\|[null,f({}),f([]),f(f)];for(var d= |

## Static File Info

No static file info

## Network Behavior

### Network Port Distribution




### TCP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| May 17, 2024 21:31:53.851289034 CEST | 49678 | 443 | 192.168.2.4 | 104.46.162.224 |
| May 17, 2024 21:31:55.132481098 CEST | 49675 | 443 | 192.168.2.4 | 173.222.162.32 |
| May 17, 2024 21:32:03.541914940 CEST | 49735 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:03.541943073 CEST | 443 | 49735 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:03.542016983 CEST | 49735 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:03.542172909 CEST | 49736 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:03.542229891 CEST | 443 | 49736 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:03.542282104 CEST | 49736 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:03.542367935 CEST | 49735 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:03.542376995 CEST | 443 | 49735 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:03.542551994 CEST | 49736 | 443 | 192.168.2.4 | 18.239.69.89 |

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| May 17, 2024 21:32:03.542571068 CEST | 443 | 49736 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:04.742388010 CEST | 49675 | 443 | 192.168.2.4 | 173.222.162.32 |
| May 17, 2024 21:32:04.769222975 CEST | 443 | 49736 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:04.769769907 CEST | 49736 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:04.769838095 CEST | 443 | 49736 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:04.770221949 CEST | 443 | 49736 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:04.770308018 CEST | 49736 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:04.770828009 CEST | 443 | 49736 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:04.770879984 CEST | 49736 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:04.771806002 CEST | 49736 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:04.771876097 CEST | 443 | 49736 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:04.771986961 CEST | 49736 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:04.772017002 CEST | 443 | 49736 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:04.799236059 CEST | 443 | 49735 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:04.815406084 CEST | 49736 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:04.820935011 CEST | 49735 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:04.820957899 CEST | 443 | 49735 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:04.822197914 CEST | 443 | 49735 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:04.822307110 CEST | 49735 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:04.824717999 CEST | 443 | 49735 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:04.824784040 CEST | 49735 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:04.825429916 CEST | 49735 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:04.825627089 CEST | 443 | 49735 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:04.878338099 CEST | 49735 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:04.878350973 CEST | 443 | 49735 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:04.924808979 CEST | 49735 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:05.252232075 CEST | 443 | 49736 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:05.252245903 CEST | 443 | 49736 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:05.252506971 CEST | 49736 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:05.262480021 CEST | 443 | 49736 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:05.262487888 CEST | 443 | 49736 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:05.262526989 CEST | 443 | 49736 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:05.262556076 CEST | 443 | 49736 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:05.262586117 CEST | 49736 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:05.262619019 CEST | 49736 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:05.263614893 CEST | 49736 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:05.263655901 CEST | 443 | 49736 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:05.295640945 CEST | 49735 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:05.296314001 CEST | 49739 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:05.296364069 CEST | 443 | 49739 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:05.296439886 CEST | 49739 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:05.296760082 CEST | 49739 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:05.296780109 CEST | 443 | 49739 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:05.298306942 CEST | 49740 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:05.298388958 CEST | 443 | 49740 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:05.298485041 CEST | 49740 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:05.298836946 CEST | 49741 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:05.298862934 CEST | 443 | 49741 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:05.298912048 CEST | 49741 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:05.299056053 CEST | 49740 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:05.299093962 CEST | 443 | 49740 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:05.299231052 CEST | 49741 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:05.299245119 CEST | 443 | 49741 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:05.299793005 CEST | 49742 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:05.299892902 CEST | 443 | 49742 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:05.299958944 CEST | 49742 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:05.300143957 CEST | 49742 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:05.300180912 CEST | 443 | 49742 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:05.327822924 CEST | 49743 | 443 | 192.168.2.4 | 108.138.7.128 |

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| May 17, 2024 21:32:05.327852011 CEST | 443 | 49743 | 108.138.7.128 | 192.168.2.4 |
| May 17, 2024 21:32:05.327899933 CEST | 49743 | 443 | 192.168.2.4 | 108.138.7.128 |
| May 17, 2024 21:32:05.328238964 CEST | 49743 | 443 | 192.168.2.4 | 108.138.7.128 |
| May 17, 2024 21:32:05.328249931 CEST | 443 | 49743 | 108.138.7.128 | 192.168.2.4 |
| May 17, 2024 21:32:05.336149931 CEST | 443 | 49735 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:05.897403002 CEST | 49744 | 443 | 192.168.2.4 | 216.58.212.164 |
| May 17, 2024 21:32:05.897445917 CEST | 443 | 49744 | 216.58.212.164 | 192.168.2.4 |
| May 17, 2024 21:32:05.897505045 CEST | 49744 | 443 | 192.168.2.4 | 216.58.212.164 |
| May 17, 2024 21:32:05.901067972 CEST | 49744 | 443 | 192.168.2.4 | 216.58.212.164 |
| May 17, 2024 21:32:05.901082993 CEST | 443 | 49744 | 216.58.212.164 | 192.168.2.4 |
| May 17, 2024 21:32:06.304680109 CEST | 443 | 49735 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:06.304717064 CEST | 443 | 49735 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:06.304764032 CEST | 49735 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:06.304802895 CEST | 443 | 49735 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:06.304827929 CEST | 49735 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:06.360089064 CEST | 49735 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:06.459242105 CEST | 443 | 49735 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:06.459280968 CEST | 443 | 49735 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:06.459321022 CEST | 49735 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:06.459321022 CEST | 443 | 49735 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:06.459350109 CEST | 443 | 49735 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:06.459371090 CEST | 443 | 49735 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:06.459376097 CEST | 49735 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:06.459389925 CEST | 443 | 49735 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:06.459398985 CEST | 49735 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:06.459418058 CEST | 49735 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:06.459422112 CEST | 443 | 49735 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:06.459461927 CEST | 49735 | 443 | 192.168.2.4 | 18.239.69.89 |
| May 17, 2024 21:32:06.459887981 CEST | 443 | 49735 | 18.239.69.89 | 192.168.2.4 |
| May 17, 2024 21:32:06.468601942 CEST | 443 | 49735 | 18.239.69.89 | 192.168.2.4 |

## UDP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| May 17, 2024 21:32:02.125562906 CEST | 53 | 50260 | 1.1.1.1 | 192.168.2.4 |
| May 17, 2024 21:32:02.125683069 CEST | 53 | 58408 | 1.1.1.1 | 192.168.2.4 |
| May 17, 2024 21:32:03.506100893 CEST | 50768 | 53 | 192.168.2.4 | 1.1.1.1 |
| May 17, 2024 21:32:03.506396055 CEST | 57267 | 53 | 192.168.2.4 | 1.1.1.1 |
| May 17, 2024 21:32:03.533307076 CEST | 53 | 50768 | 1.1.1.1 | 192.168.2.4 |
| May 17, 2024 21:32:03.551220894 CEST | 53 | 57267 | 1.1.1.1 | 192.168.2.4 |
| May 17, 2024 21:32:03.851054907 CEST | 53 | 59922 | 1.1.1.1 | 192.168.2.4 |
| May 17, 2024 21:32:05.292037964 CEST | 50432 | 53 | 192.168.2.4 | 1.1.1.1 |
| May 17, 2024 21:32:05.292392015 CEST | 64682 | 53 | 192.168.2.4 | 1.1.1.1 |
| May 17, 2024 21:32:05.326862097 CEST | 53 | 64682 | 1.1.1.1 | 192.168.2.4 |
| May 17, 2024 21:32:05.326900959 CEST | 53 | 50432 | 1.1.1.1 | 192.168.2.4 |
| May 17, 2024 21:32:05.877698898 CEST | 52404 | 53 | 192.168.2.4 | 1.1.1.1 |
| May 17, 2024 21:32:05.878173113 CEST | 64897 | 53 | 192.168.2.4 | 1.1.1.1 |
| May 17, 2024 21:32:05.888298988 CEST | 53 | 52404 | 1.1.1.1 | 192.168.2.4 |
| May 17, 2024 21:32:05.895596027 CEST | 53 | 64897 | 1.1.1.1 | 192.168.2.4 |
| May 17, 2024 21:32:07.497210979 CEST | 60200 | 53 | 192.168.2.4 | 1.1.1.1 |
| May 17, 2024 21:32:07.497757912 CEST | 62367 | 53 | 192.168.2.4 | 1.1.1.1 |
| May 17, 2024 21:32:07.508819103 CEST | 53 | 60200 | 1.1.1.1 | 192.168.2.4 |
| May 17, 2024 21:32:07.510881901 CEST | 53 | 62367 | 1.1.1.1 | 192.168.2.4 |
| May 17, 2024 21:32:07.513282061 CEST | 53 | 64705 | 1.1.1.1 | 192.168.2.4 |
| May 17, 2024 21:32:10.088447094 CEST | 52927 | 53 | 192.168.2.4 | 1.1.1.1 |
| May 17, 2024 21:32:10.088963032 CEST | 64250 | 53 | 192.168.2.4 | 1.1.1.1 |
| May 17, 2024 21:32:10.099180937 CEST | 61662 | 53 | 192.168.2.4 | 1.1.1.1 |
| May 17, 2024 21:32:10.099359035 CEST | 58401 | 53 | 192.168.2.4 | 1.1.1.1 |
| May 17, 2024 21:32:10.112391949 CEST | 53 | 61662 | 1.1.1.1 | 192.168.2.4 |

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| May 17, 2024 21:32:10.112437963 CEST | 53 | 58401 | 1.1.1.1 | 192.168.2.4 |
| May 17, 2024 21:32:10.117132902 CEST | 53 | 64250 | 1.1.1.1 | 192.168.2.4 |
| May 17, 2024 21:32:10.121895075 CEST | 53 | 52927 | 1.1.1.1 | 192.168.2.4 |
| May 17, 2024 21:32:11.788775921 CEST | 57956 | 53 | 192.168.2.4 | 1.1.1.1 |
| May 17, 2024 21:32:11.788937092 CEST | 50086 | 53 | 192.168.2.4 | 1.1.1.1 |
| May 17, 2024 21:32:11.881185055 CEST | 53 | 50086 | 1.1.1.1 | 192.168.2.4 |
| May 17, 2024 21:32:11.881225109 CEST | 53 | 57956 | 1.1.1.1 | 192.168.2.4 |
| May 17, 2024 21:32:12.435211897 CEST | 51181 | 53 | 192.168.2.4 | 1.1.1.1 |
| May 17, 2024 21:32:12.435619116 CEST | 54324 | 53 | 192.168.2.4 | 1.1.1.1 |
| May 17, 2024 21:32:12.469152927 CEST | 53 | 51181 | 1.1.1.1 | 192.168.2.4 |
| May 17, 2024 21:32:12.473875999 CEST | 53 | 54324 | 1.1.1.1 | 192.168.2.4 |
| May 17, 2024 21:32:20.879254103 CEST | 53 | 57598 | 1.1.1.1 | 192.168.2.4 |
| May 17, 2024 21:32:24.375849009 CEST | 138 | 138 | 192.168.2.4 | 192.168.2.255 |
| May 17, 2024 21:32:39.554311991 CEST | 53 | 59864 | 1.1.1.1 | 192.168.2.4 |
| May 17, 2024 21:33:01.531156063 CEST | 53 | 60528 | 1.1.1.1 | 192.168.2.4 |
| May 17, 2024 21:33:02.265307903 CEST | 53 | 52933 | 1.1.1.1 | 192.168.2.4 |
| May 17, 2024 21:33:04.531286955 CEST | 53 | 65187 | 1.1.1.1 | 192.168.2.4 |

## ICMP Packets

| Timestamp | Source IP | Dest IP | Checksum | Code | Type |
|---|---|---|---|---|---|
| May 17, 2024 21:32:03.551314116 CEST | 192.168.2.4 | 1.1.1.1 | c241 | (Port unreachable) | Destination Unreachable |

## DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class | DNS over HTTPS |
|---|---|---|---|---|---|---|---|---|
| May 17, 2024 21:32:03.506100893 CEST | 192.168.2.4 | 1.1.1.1 | 0x53da | Standard query (0) | www.myprepaidcenter.com | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:03.506396055 CEST | 192.168.2.4 | 1.1.1.1 | 0xa798 | Standard query (0) | www.myprepaidcenter.com | 65 | IN (0x0001) | false |
| May 17, 2024 21:32:05.292037964 CEST | 192.168.2.4 | 1.1.1.1 | 0x57b | Standard query (0) | content.blackhawknetwork.com | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:05.292392015 CEST | 192.168.2.4 | 1.1.1.1 | 0x4e43 | Standard query (0) | content.blackhawknetwork.com | 65 | IN (0x0001) | false |
| May 17, 2024 21:32:05.877698898 CEST | 192.168.2.4 | 1.1.1.1 | 0xe9de | Standard query (0) | www.google.com | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:05.878173113 CEST | 192.168.2.4 | 1.1.1.1 | 0x852d | Standard query (0) | www.google.com | 65 | IN (0x0001) | false |
| May 17, 2024 21:32:07.497210979 CEST | 192.168.2.4 | 1.1.1.1 | 0xeff | Standard query (0) | js.datadome.co | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:07.497757912 CEST | 192.168.2.4 | 1.1.1.1 | 0x5677 | Standard query (0) | js.datadome.co | 65 | IN (0x0001) | false |
| May 17, 2024 21:32:10.088447094 CEST | 192.168.2.4 | 1.1.1.1 | 0x938f | Standard query (0) | ht.blackhawknetwork.com | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:10.088963032 CEST | 192.168.2.4 | 1.1.1.1 | 0x37e6 | Standard query (0) | ht.blackhawknetwork.com | 65 | IN (0x0001) | false |
| May 17, 2024 21:32:10.099180937 CEST | 192.168.2.4 | 1.1.1.1 | 0x176d | Standard query (0) | api-js.datadome.co | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:10.099359035 CEST | 192.168.2.4 | 1.1.1.1 | 0x60de | Standard query (0) | api-js.datadome.co | 65 | IN (0x0001) | false |
| May 17, 2024 21:32:11.788775921 CEST | 192.168.2.4 | 1.1.1.1 | 0xe3a4 | Standard query (0) | api-js.datadome.co | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:11.788937092 CEST | 192.168.2.4 | 1.1.1.1 | 0xaf4 | Standard query (0) | api-js.datadome.co | 65 | IN (0x0001) | false |
| May 17, 2024 21:32:12.435211897 CEST | 192.168.2.4 | 1.1.1.1 | 0xfc0f | Standard query (0) | www.myprepaidcenter.com | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:12.435619116 CEST | 192.168.2.4 | 1.1.1.1 | 0xc537 | Standard query (0) | www.myprepaidcenter.com | 65 | IN (0x0001) | false |

## DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class | DNS over HTTPS |
|---|---|---|---|---|---|---|---|---|---|---|
| May 17, 2024 21:32:03.533307076 CEST | 1.1.1.1 | 192.168.2.4 | 0x53da | No error (0) | www.myprepaidcenter.com | | 18.239.69.89 | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:03.533307076 CEST | 1.1.1.1 | 192.168.2.4 | 0x53da | No error (0) | www.myprepaidcenter.com | | 18.239.69.66 | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:03.533307076 CEST | 1.1.1.1 | 192.168.2.4 | 0x53da | No error (0) | www.myprepaidcenter.com | | 18.239.69.79 | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:03.533307076 CEST | 1.1.1.1 | 192.168.2.4 | 0x53da | No error (0) | www.myprepaidcenter.com | | 18.239.69.40 | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:05.326862097 CEST | 1.1.1.1 | 192.168.2.4 | 0x4e43 | No error (0) | content.blackhawknetwork.com | d25uga7vnqfi2a.cloudfront.net | | CNAME (Canonical name) | IN (0x0001) | false |
| May 17, 2024 21:32:05.326900959 CEST | 1.1.1.1 | 192.168.2.4 | 0x57b | No error (0) | content.blackhawknetwork.com | d25uga7vnqfi2a.cloudfront.net | | CNAME (Canonical name) | IN (0x0001) | false |
| May 17, 2024 21:32:05.326900959 CEST | 1.1.1.1 | 192.168.2.4 | 0x57b | No error (0) | d25uga7vnqfi2a.cloudfront.net | | 108.138.7.128 | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:05.326900959 CEST | 1.1.1.1 | 192.168.2.4 | 0x57b | No error (0) | d25uga7vnqfi2a.cloudfront.net | | 108.138.7.13 | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:05.326900959 CEST | 1.1.1.1 | 192.168.2.4 | 0x57b | No error (0) | d25uga7vnqfi2a.cloudfront.net | | 108.138.7.69 | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:05.326900959 CEST | 1.1.1.1 | 192.168.2.4 | 0x57b | No error (0) | d25uga7vnqfi2a.cloudfront.net | | 108.138.7.70 | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:05.888298988 CEST | 1.1.1.1 | 192.168.2.4 | 0xe9de | No error (0) | www.google.com | | 216.58.212.164 | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:05.895596027 CEST | 1.1.1.1 | 192.168.2.4 | 0x852d | No error (0) | www.google.com | | | 65 | IN (0x0001) | false |
| May 17, 2024 21:32:07.508819103 CEST | 1.1.1.1 | 192.168.2.4 | 0xeff | No error (0) | js.datadome.co | | 18.238.243.98 | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:07.508819103 CEST | 1.1.1.1 | 192.168.2.4 | 0xeff | No error (0) | js.datadome.co | | 18.238.243.106 | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:07.508819103 CEST | 1.1.1.1 | 192.168.2.4 | 0xeff | No error (0) | js.datadome.co | | 18.238.243.46 | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:07.508819103 CEST | 1.1.1.1 | 192.168.2.4 | 0xeff | No error (0) | js.datadome.co | | 18.238.243.100 | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:10.112391949 CEST | 1.1.1.1 | 192.168.2.4 | 0x176d | No error (0) | api-js.datadome.co | geoprox-js-sdk.datadome.co | | CNAME (Canonical name) | IN (0x0001) | false |
| May 17, 2024 21:32:10.112391949 CEST | 1.1.1.1 | 192.168.2.4 | 0x176d | No error (0) | geoprox-js-sdk.datadome.co | api-alb-eu-central-1.datadome.co | | CNAME (Canonical name) | IN (0x0001) | false |
| May 17, 2024 21:32:10.112391949 CEST | 1.1.1.1 | 192.168.2.4 | 0x176d | No error (0) | api-alb-eu-central-1.datadome.co | | 18.194.25.151 | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:10.112391949 CEST | 1.1.1.1 | 192.168.2.4 | 0x176d | No error (0) | api-alb-eu-central-1.datadome.co | | 35.156.2.81 | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:10.112391949 CEST | 1.1.1.1 | 192.168.2.4 | 0x176d | No error (0) | api-alb-eu-central-1.datadome.co | | 52.58.60.52 | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:10.112437963 CEST | 1.1.1.1 | 192.168.2.4 | 0x60de | No error (0) | api-js.datadome.co | geoprox-js-sdk.datadome.co | | CNAME (Canonical name) | IN (0x0001) | false |
| May 17, 2024 21:32:10.112437963 CEST | 1.1.1.1 | 192.168.2.4 | 0x60de | No error (0) | geoprox-js-sdk.datadome.co | api-alb-eu-central-1.datadome.co | | CNAME (Canonical name) | IN (0x0001) | false |
| May 17, 2024 21:32:10.117132902 CEST | 1.1.1.1 | 192.168.2.4 | 0x37e6 | No error (0) | ht.blackhawknetwork.com | d-52ccktk4i3.execute-api.us-east-2.amazonaws.com | | CNAME (Canonical name) | IN (0x0001) | false |

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class | DNS over HTTPS |
|---|---|---|---|---|---|---|---|---|---|---|
| May 17, 2024 21:32:10.121895075 CEST | 1.1.1.1 | 192.168.2.4 | 0x938f | No error (0) | ht.blackhawknetwork.com | d-52ccktk4i3.execute-api.us-east-2.amazonaws.com | | CNAME (Canonical name) | IN (0x0001) | false |
| May 17, 2024 21:32:10.121895075 CEST | 1.1.1.1 | 192.168.2.4 | 0x938f | No error (0) | d-52ccktk4i3.execute-api.us-east-2.amazonaws.com | | 3.130.102.116 | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:10.121895075 CEST | 1.1.1.1 | 192.168.2.4 | 0x938f | No error (0) | d-52ccktk4i3.execute-api.us-east-2.amazonaws.com | | 3.14.229.201 | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:10.121895075 CEST | 1.1.1.1 | 192.168.2.4 | 0x938f | No error (0) | d-52ccktk4i3.execute-api.us-east-2.amazonaws.com | | 3.12.62.51 | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:11.881185055 CEST | 1.1.1.1 | 192.168.2.4 | 0xaf4 | No error (0) | api-js.datadome.co | geoprox-js-sdk.datadome.co | | CNAME (Canonical name) | IN (0x0001) | false |
| May 17, 2024 21:32:11.881185055 CEST | 1.1.1.1 | 192.168.2.4 | 0xaf4 | No error (0) | geoprox-js-sdk.datadome.co | api-alb-eu-central-1.datadome.co | | CNAME (Canonical name) | IN (0x0001) | false |
| May 17, 2024 21:32:11.881225109 CEST | 1.1.1.1 | 192.168.2.4 | 0xe3a4 | No error (0) | api-js.datadome.co | geoprox-js-sdk.datadome.co | | CNAME (Canonical name) | IN (0x0001) | false |
| May 17, 2024 21:32:11.881225109 CEST | 1.1.1.1 | 192.168.2.4 | 0xe3a4 | No error (0) | geoprox-js-sdk.datadome.co | api-alb-eu-central-1.datadome.co | | CNAME (Canonical name) | IN (0x0001) | false |
| May 17, 2024 21:32:11.881225109 CEST | 1.1.1.1 | 192.168.2.4 | 0xe3a4 | No error (0) | api-alb-eu-central-1.datadome.co | | 18.194.25.151 | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:11.881225109 CEST | 1.1.1.1 | 192.168.2.4 | 0xe3a4 | No error (0) | api-alb-eu-central-1.datadome.co | | 52.58.60.52 | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:11.881225109 CEST | 1.1.1.1 | 192.168.2.4 | 0xe3a4 | No error (0) | api-alb-eu-central-1.datadome.co | | 35.156.2.81 | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:12.469152927 CEST | 1.1.1.1 | 192.168.2.4 | 0xfc0f | No error (0) | www.myprepaidcenter.com | | 108.156.2.79 | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:12.469152927 CEST | 1.1.1.1 | 192.168.2.4 | 0xfc0f | No error (0) | www.myprepaidcenter.com | | 108.156.2.56 | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:12.469152927 CEST | 1.1.1.1 | 192.168.2.4 | 0xfc0f | No error (0) | www.myprepaidcenter.com | | 108.156.2.113 | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:12.469152927 CEST | 1.1.1.1 | 192.168.2.4 | 0xfc0f | No error (0) | www.myprepaidcenter.com | | 108.156.2.20 | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:19.565953970 CEST | 1.1.1.1 | 192.168.2.4 | 0xbd08 | No error (0) | bg.microsoft.map.fastly.net | | 199.232.210.172 | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:19.565953970 CEST | 1.1.1.1 | 192.168.2.4 | 0xbd08 | No error (0) | bg.microsoft.map.fastly.net | | 199.232.214.172 | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:20.410931110 CEST | 1.1.1.1 | 192.168.2.4 | 0x267 | No error (0) | fp2e7a.wpc.2be4.phicdn.net | fp2e7a.wpc.phicdn.net | | CNAME (Canonical name) | IN (0x0001) | false |
| May 17, 2024 21:32:20.410931110 CEST | 1.1.1.1 | 192.168.2.4 | 0x267 | No error (0) | fp2e7a.wpc.phicdn.net | | 192.229.221.95 | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:33.969444036 CEST | 1.1.1.1 | 192.168.2.4 | 0x523f | No error (0) | fp2e7a.wpc.2be4.phicdn.net | fp2e7a.wpc.phicdn.net | | CNAME (Canonical name) | IN (0x0001) | false |
| May 17, 2024 21:32:33.969444036 CEST | 1.1.1.1 | 192.168.2.4 | 0x523f | No error (0) | fp2e7a.wpc.phicdn.net | | 192.229.221.95 | A (IP address) | IN (0x0001) | false |
| May 17, 2024 21:32:54.624892950 CEST | 1.1.1.1 | 192.168.2.4 | 0xc5b2 | No error (0) | fp2e7a.wpc.2be4.phicdn.net | fp2e7a.wpc.phicdn.net | | CNAME (Canonical name) | IN (0x0001) | false |

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class | DNS over HTTPS |
|---|---|---|---|---|---|---|---|---|---|---|
| May 17, 2024 21:32:54.624892950 CEST | 1.1.1.1 | 192.168.2.4 | 0xc5b2 | No error (0) | fp2e7a.wpc.phicdn.net | | 192.229.221.95 | A (IP address) | IN (0x0001) | false |

### HTTP Request Dependency Graph

- www.myprepaidcenter.com
- https:
  - content.blackhawknetwork.com
  - js.datadome.co
  - ht.blackhawknetwork.com
  - api-js.datadome.co
- fs.microsoft.com

## Statistics

### Behavior

Click to jump to process

## System Behavior

All data are 0.

## Disassembly

**No disassembly**