ID: 791307
Sample Name: VM Tue, January 24, 2023 #18654.html
Cookbook: default.jbs
Time: 10:20:14
Date: 25/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

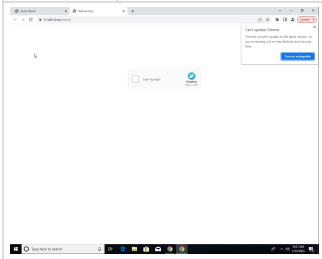
Windows Analysis Report

VM Tue, January 24, 2023 #18654.html

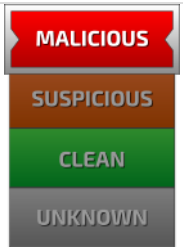
Overview

General Information

Sample Name:	VM Tue, January 24, 2023 #18654.html
Analysis ID:	791307
MD5:	80cc2287a8d923..
SHA1:	fdeb4f5abafd0d9..
SHA256:	e3c04a3f5e27cc...
Infos:	



Detection



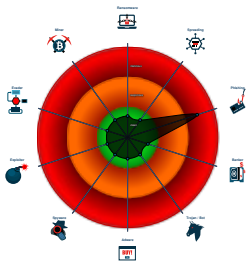
Captcha Phish, HTMLPhisher

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish44
- Yara detected Captcha Phish
- Antivirus detection for URL or domain
- IP address seen in connection with ...

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 6052 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 5208 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=1956 --field-trial-handle=1724,i,2672952510848693389,14012057706382809610,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 4392 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "C:\Users\user\Desktop\VM Tue, January 24, 2023 #18654.html MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
VM Tue, January 24, 2023 #18654.html	JoeSecurity_HtmlPhish_44	Yara detected HtmlPhish_44	Joe Security	

HTML

Source	Rule	Description	Author	Strings
99254.0.pages.csv	JoeSecurity_CaptchaPhish_1	Yara detected Captcha Phish	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Phishing

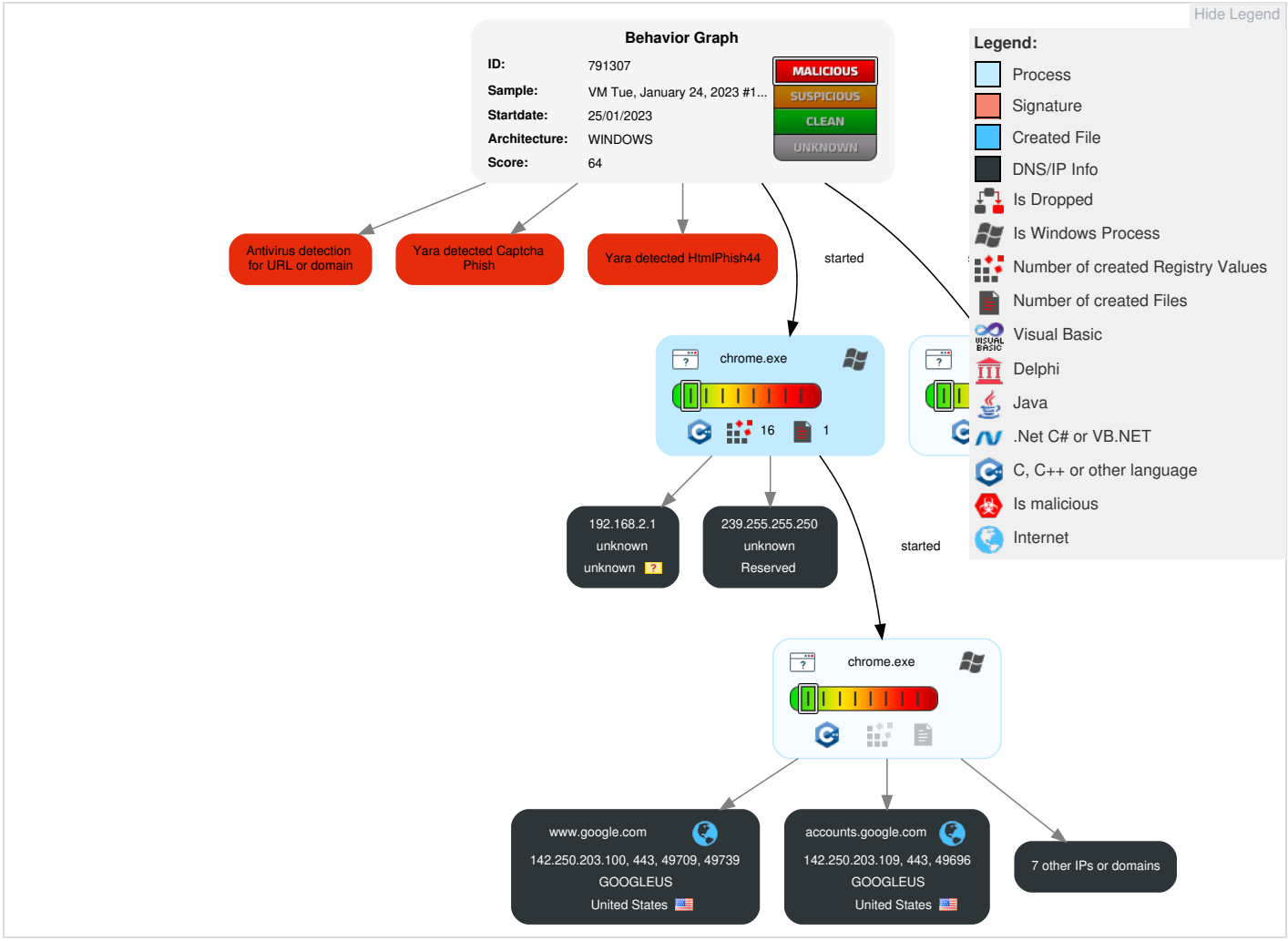
Yara detected HtmlPhish44

Yara detected Captcha Phish

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	2 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	4 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	5 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	3 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

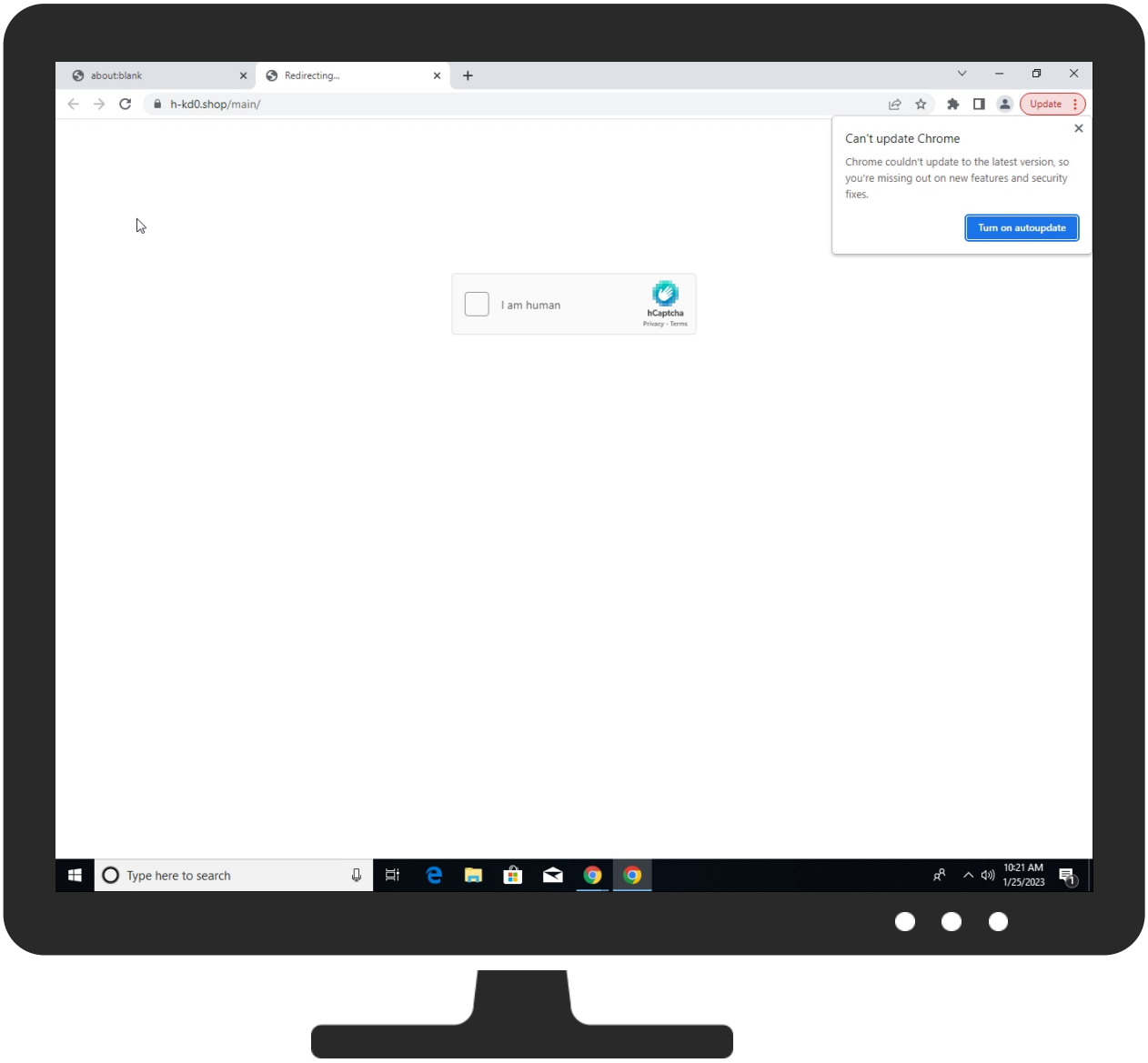
Behavior Graph



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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
hcaptcha.com	0%	Virustotal		Browse
h-kd0.shop	4%	Virustotal		Browse
www.hcaptcha.com	0%	Virustotal		Browse
newassets.hcaptcha.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://h-kd0.shop/main/	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	
http://https://www.hcaptcha.com/1/api.js	0%	URL Reputation	safe	
http://https://h-kd0.shop/favicon.ico	100%	Avira URL Cloud	phishing	
http://https://newassets.hcaptcha.com/i/9b22d05/e	0%	Avira URL Cloud	safe	
http://https://newassets.hcaptcha.com/captcha/v1/48ebaaf/static/hcaptcha.html	0%	Avira URL Cloud	safe	
http://https://newassets.hcaptcha.com/c/9b22d05/hsw.js	0%	Avira URL Cloud	safe	
http://https://hcaptcha.com/checksiteconfig?v=48ebaaf&host=h-kd0.shop&sitekey=f8954f89-2ff5-49a0-afdd-3656b68b442c&sc=1&swa=1	0%	Avira URL Cloud	safe	
http://https://newassets.hcaptcha.com/captcha/v1/48ebaaf/hcaptcha.js	0%	Avira URL Cloud	safe	
http://https://h-kd0.shop/?e=YXNyeUBraW1iby5jby51aw==	100%	Avira URL Cloud	phishing	

Domains and IPs

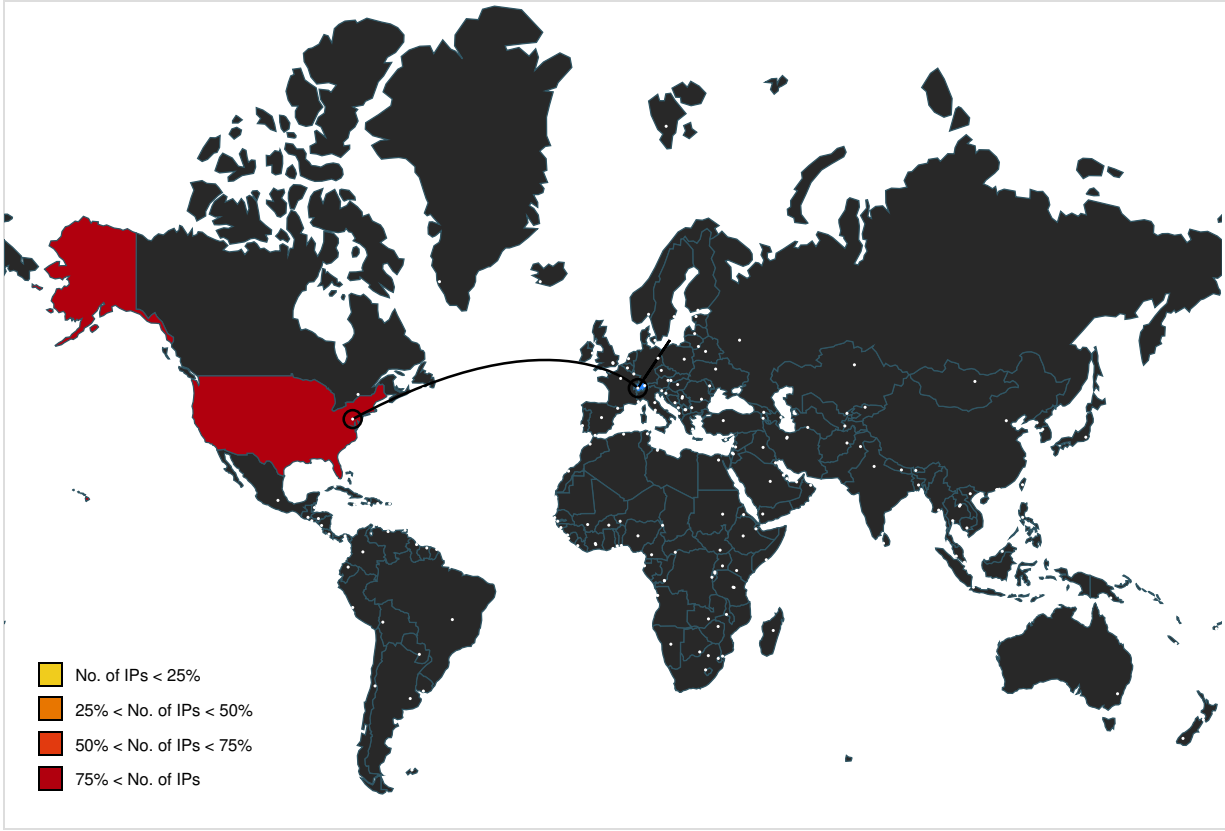
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
hcaptcha.com	104.16.169.131	true	false	• 0%, Virustotal, Browse	unknown
h-kd0.shop	192.111.146.184	true	false	• 4%, Virustotal, Browse	unknown
accounts.google.com	142.250.203.109	true	false		high
www.google.com	142.250.203.100	true	false		high
clients.l.google.com	216.58.215.238	true	false		high
www.hcaptcha.com	104.16.169.131	true	false	• 0%, Virustotal, Browse	unknown
newassets.hcaptcha.com	104.16.169.131	true	false	• 0%, Virustotal, Browse	unknown
clients2.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://h-kd0.shop/main/	true	• SlashNext: Credential Stealing type: Phishing & Social Engineering	unknown
http://https://newassets.hcaptcha.com/captcha/v1/48ebaaf/static/hcaptcha.html	false	• Avira URL Cloud: safe	unknown
http://https://newassets.hcaptcha.com/captcha/v1/48ebaaf/static/hcaptcha.html#frame=challenge&id=0mrxeuynfqs&host=h-kd0.shop&sentry=true&reportapi=https%3A%2F%2Faccounts.hcaptcha.com&recaptchacompat=true&custom=false&hl=en&tplinks=on&sitekey=f8954f89-2ff5-49a0-afdd-3656b68b442c&theme=light&origin=https%3A%2F%2Fh-kd0.shop	false		unknown
http://https://www.hcaptcha.com/1/api.js	false	• URL Reputation: safe	unknown
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://h-kd0.shop/main/	true	• SlashNext: Credential Stealing type: Phishing & Social Engineering	unknown
http://https://h-kd0.shop/favicon.ico	false	• Avira URL Cloud: phishing	unknown
http://https://newassets.hcaptcha.com/i/9b22d05/e	false	• Avira URL Cloud: safe	unknown
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=104.0.5112.81&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://hcaptcha.com/checksiteconfig?v=48ebaaf&host=h-kd0.shop&sitekey=f8954f89-2ff5-49a0-afdd-3656b68b442c&sc=1&swa=1	false	• Avira URL Cloud: safe	unknown
http://https://newassets.hcaptcha.com/c/9b22d05/hsw.js	false	• Avira URL Cloud: safe	unknown
http://https://newassets.hcaptcha.com/captcha/v1/48ebaaf/static/hcaptcha.html#frame=checkbox&id=0mrxeuynfqs&host=h-kd0.shop&sentry=true&reportapi=https%3A%2F%2Faccounts.hcaptcha.com&recaptchacompat=true&custom=false&hl=en&tplinks=on&sitekey=f8954f89-2ff5-49a0-afdd-3656b68b442c&theme=light&origin=https%3A%2F%2Fh-kd0.shop	false		unknown
http://https://h-kd0.shop/?e=YXNyeUBraW1iby5jby51aw==	false	• Avira URL Cloud: phishing	unknown
http://https://newassets.hcaptcha.com/captcha/v1/48ebaaf/hcaptcha.js	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.16.169.131	hcaptcha.com	United States		13335	CLOUDFLARENETUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
216.58.215.238	clients.l.google.com	United States		15169	GOOGLEUS	false
192.111.146.184	h-kd0.shop	United States		31863	DACEN-2US	false
142.250.203.100	www.google.com	United States		15169	GOOGLEUS	false
142.250.203.109	accounts.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	791307
Start date and time:	2023-01-25 10:20:14 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	VM Tue, January 24, 2023 #18654.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:	18
Number of new started drivers analysed:	1
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.phis.winHTML@31/0@8/8
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 • Browse: https://www.hcaptcha.com/what-is-hcaptcha-about?ref=h-kd0.shop&utm_campaign=f8954f89-2ff5-49a0-afdd-3656b68b442c&utm_medium=checkbox

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, qwavedrv.sys, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.203.99, 34.104.35.123, 216.58.215.234, 172.217.168.10, 172.217.168.42, 172.217.168.74, 142.250.203.106
- Excluded domains from analysis (whitelisted): fs.microsoft.com, edgedl.me.gvt1.com, content-autofill.googleapis.com, update.googleapis.com, ctldl.windowsupdate.com, clientservices.googleapis.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

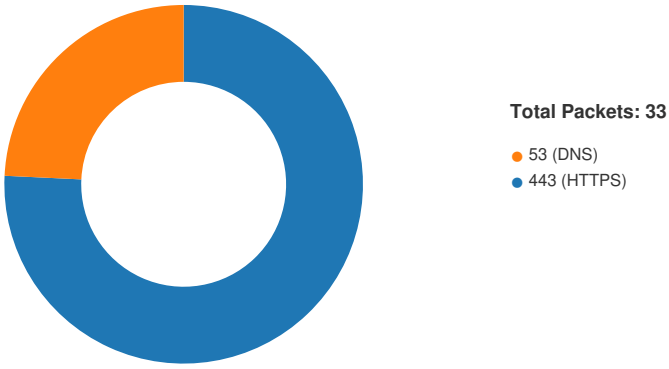
File type:	HTML document, ASCII text, with very long lines (4002), with no line terminators
Entropy (8bit):	3.4266196238262228
TrID:	
File name:	VM Tue, January 24, 2023 #18654.html
File size:	4002
MD5:	80cc2287a8d92303bbb07808b1d7ac08
SHA1:	fdeb4f5abafd0d978ebe0b8b1a8a1026d6282922
SHA256:	e3c04a3f5e27cc3d6630ac9c7e8d8b5c8fe0be2514d7676b538de9c18e45aaa4
SHA512:	c76b561c8859e454f9814390b49610247945025f2cb6dbbec56ecc5e3d273dae959c753071b6283bdb7c6197684a562ff73ec4a53fa4d1a58ab7738257b76e8a
SSDEEP:	96:SadmnL1B9dp6Ml94QtwqS11D8fEsUSnfUV:SadOt/6MIN2qG1D8fEsUSfUV
TLSH:	2181593C6210D88F6D736E3FFCB45E54D018AF97EDC96B84041A44E63BE01AA76042EB
File Content Preview:	<script language="javascript">document.write(unescape('%3C%21%44%4F%43%54%59%50%45%20%68%74%6D%6C%3E%0D%0A%3C%68%74%6D%6C%20%6C%61%6E%67%3D%22%65%6E%22%3E%0D%0A%3C%68%65%61%64%3E%0D%0A%20%20%20%20%3C%6D%65%74%61%20%63%68%61%72%73%65%74%3D%22%55%54%46%2D

File Icon

Icon Hash:	78d0a8cccc88c460

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2023 10:21:09.933392048 CET	49695	443	192.168.2.3	216.58.215.238
Jan 25, 2023 10:21:09.933448076 CET	443	49695	216.58.215.238	192.168.2.3
Jan 25, 2023 10:21:09.933542967 CET	49695	443	192.168.2.3	216.58.215.238
Jan 25, 2023 10:21:09.933958054 CET	49696	443	192.168.2.3	142.250.203.109
Jan 25, 2023 10:21:09.934019089 CET	443	49696	142.250.203.109	192.168.2.3
Jan 25, 2023 10:21:09.934158087 CET	49696	443	192.168.2.3	142.250.203.109
Jan 25, 2023 10:21:09.935447931 CET	49695	443	192.168.2.3	216.58.215.238
Jan 25, 2023 10:21:09.935471058 CET	443	49695	216.58.215.238	192.168.2.3
Jan 25, 2023 10:21:09.935682058 CET	49696	443	192.168.2.3	142.250.203.109
Jan 25, 2023 10:21:09.935715914 CET	443	49696	142.250.203.109	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2023 10:21:09.994476080 CET	443	49695	216.58.215.238	192.168.2.3
Jan 25, 2023 10:21:09.995348930 CET	49695	443	192.168.2.3	216.58.215.238
Jan 25, 2023 10:21:09.995419979 CET	443	49695	216.58.215.238	192.168.2.3
Jan 25, 2023 10:21:09.995959997 CET	443	49695	216.58.215.238	192.168.2.3
Jan 25, 2023 10:21:09.996073008 CET	49695	443	192.168.2.3	216.58.215.238
Jan 25, 2023 10:21:09.996789932 CET	443	49695	216.58.215.238	192.168.2.3
Jan 25, 2023 10:21:09.996866941 CET	49695	443	192.168.2.3	216.58.215.238
Jan 25, 2023 10:21:10.037544966 CET	443	49696	142.250.203.109	192.168.2.3
Jan 25, 2023 10:21:10.038136005 CET	49696	443	192.168.2.3	142.250.203.109
Jan 25, 2023 10:21:10.038177967 CET	443	49696	142.250.203.109	192.168.2.3
Jan 25, 2023 10:21:10.039885044 CET	443	49696	142.250.203.109	192.168.2.3
Jan 25, 2023 10:21:10.040011883 CET	49696	443	192.168.2.3	142.250.203.109
Jan 25, 2023 10:21:10.702723980 CET	49695	443	192.168.2.3	216.58.215.238
Jan 25, 2023 10:21:10.702788115 CET	443	49695	216.58.215.238	192.168.2.3
Jan 25, 2023 10:21:10.703005075 CET	443	49695	216.58.215.238	192.168.2.3
Jan 25, 2023 10:21:10.703443050 CET	49695	443	192.168.2.3	216.58.215.238
Jan 25, 2023 10:21:10.703507900 CET	443	49695	216.58.215.238	192.168.2.3
Jan 25, 2023 10:21:10.704070091 CET	49696	443	192.168.2.3	142.250.203.109
Jan 25, 2023 10:21:10.704102039 CET	443	49696	142.250.203.109	192.168.2.3
Jan 25, 2023 10:21:10.704377890 CET	49696	443	192.168.2.3	142.250.203.109
Jan 25, 2023 10:21:10.704386950 CET	443	49696	142.250.203.109	192.168.2.3
Jan 25, 2023 10:21:10.704441071 CET	443	49696	142.250.203.109	192.168.2.3
Jan 25, 2023 10:21:10.743932009 CET	49696	443	192.168.2.3	142.250.203.109
Jan 25, 2023 10:21:10.743984938 CET	443	49696	142.250.203.109	192.168.2.3
Jan 25, 2023 10:21:10.744127035 CET	49695	443	192.168.2.3	216.58.215.238
Jan 25, 2023 10:21:10.760406971 CET	443	49695	216.58.215.238	192.168.2.3
Jan 25, 2023 10:21:10.760742903 CET	443	49695	216.58.215.238	192.168.2.3
Jan 25, 2023 10:21:10.760898113 CET	49695	443	192.168.2.3	216.58.215.238
Jan 25, 2023 10:21:10.783873081 CET	443	49696	142.250.203.109	192.168.2.3
Jan 25, 2023 10:21:10.783965111 CET	49696	443	192.168.2.3	142.250.203.109
Jan 25, 2023 10:21:10.784017086 CET	443	49696	142.250.203.109	192.168.2.3
Jan 25, 2023 10:21:10.784287930 CET	443	49696	142.250.203.109	192.168.2.3
Jan 25, 2023 10:21:10.784360886 CET	49696	443	192.168.2.3	142.250.203.109
Jan 25, 2023 10:21:10.881444931 CET	49696	443	192.168.2.3	142.250.203.109
Jan 25, 2023 10:21:10.881515980 CET	443	49696	142.250.203.109	192.168.2.3
Jan 25, 2023 10:21:10.882282019 CET	49695	443	192.168.2.3	216.58.215.238
Jan 25, 2023 10:21:10.882330894 CET	443	49695	216.58.215.238	192.168.2.3
Jan 25, 2023 10:21:11.256012917 CET	49698	443	192.168.2.3	192.111.146.184
Jan 25, 2023 10:21:11.256067038 CET	443	49698	192.111.146.184	192.168.2.3
Jan 25, 2023 10:21:11.256232023 CET	49698	443	192.168.2.3	192.111.146.184
Jan 25, 2023 10:21:11.256967068 CET	49698	443	192.168.2.3	192.111.146.184
Jan 25, 2023 10:21:11.257005930 CET	443	49698	192.111.146.184	192.168.2.3
Jan 25, 2023 10:21:11.257355928 CET	49699	443	192.168.2.3	192.111.146.184
Jan 25, 2023 10:21:11.257421017 CET	443	49699	192.111.146.184	192.168.2.3
Jan 25, 2023 10:21:11.257494926 CET	49699	443	192.168.2.3	192.111.146.184
Jan 25, 2023 10:21:11.257812977 CET	49699	443	192.168.2.3	192.111.146.184
Jan 25, 2023 10:21:11.257847071 CET	443	49699	192.111.146.184	192.168.2.3
Jan 25, 2023 10:21:11.743828058 CET	443	49699	192.111.146.184	192.168.2.3
Jan 25, 2023 10:21:11.766611099 CET	443	49698	192.111.146.184	192.168.2.3
Jan 25, 2023 10:21:11.778563976 CET	49698	443	192.168.2.3	192.111.146.184
Jan 25, 2023 10:21:11.778633118 CET	443	49698	192.111.146.184	192.168.2.3
Jan 25, 2023 10:21:11.778795958 CET	49699	443	192.168.2.3	192.111.146.184
Jan 25, 2023 10:21:11.778848886 CET	443	49699	192.111.146.184	192.168.2.3
Jan 25, 2023 10:21:11.781620026 CET	443	49698	192.111.146.184	192.168.2.3
Jan 25, 2023 10:21:11.781708002 CET	49698	443	192.168.2.3	192.111.146.184
Jan 25, 2023 10:21:11.782171965 CET	443	49699	192.111.146.184	192.168.2.3
Jan 25, 2023 10:21:11.782252073 CET	49699	443	192.168.2.3	192.111.146.184
Jan 25, 2023 10:21:11.937261105 CET	49698	443	192.168.2.3	192.111.146.184
Jan 25, 2023 10:21:11.937304974 CET	443	49698	192.111.146.184	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2023 10:21:11.937423944 CET	49699	443	192.168.2.3	192.111.146.184
Jan 25, 2023 10:21:11.937464952 CET	443	49699	192.111.146.184	192.168.2.3
Jan 25, 2023 10:21:11.937791109 CET	443	49698	192.111.146.184	192.168.2.3
Jan 25, 2023 10:21:11.937815905 CET	443	49699	192.111.146.184	192.168.2.3
Jan 25, 2023 10:21:11.938647032 CET	49698	443	192.168.2.3	192.111.146.184
Jan 25, 2023 10:21:11.938676119 CET	443	49698	192.111.146.184	192.168.2.3
Jan 25, 2023 10:21:12.012048006 CET	49699	443	192.168.2.3	192.111.146.184
Jan 25, 2023 10:21:12.012090921 CET	443	49699	192.111.146.184	192.168.2.3
Jan 25, 2023 10:21:12.015979052 CET	49698	443	192.168.2.3	192.111.146.184
Jan 25, 2023 10:21:12.113486052 CET	49699	443	192.168.2.3	192.111.146.184
Jan 25, 2023 10:21:12.220944881 CET	443	49698	192.111.146.184	192.168.2.3
Jan 25, 2023 10:21:12.221200943 CET	443	49698	192.111.146.184	192.168.2.3
Jan 25, 2023 10:21:12.221401930 CET	49698	443	192.168.2.3	192.111.146.184
Jan 25, 2023 10:21:12.228759050 CET	49698	443	192.168.2.3	192.111.146.184
Jan 25, 2023 10:21:12.228807926 CET	443	49698	192.111.146.184	192.168.2.3
Jan 25, 2023 10:21:12.237673998 CET	49699	443	192.168.2.3	192.111.146.184
Jan 25, 2023 10:21:12.237729073 CET	443	49699	192.111.146.184	192.168.2.3
Jan 25, 2023 10:21:12.374614000 CET	443	49699	192.111.146.184	192.168.2.3
Jan 25, 2023 10:21:12.374670029 CET	443	49699	192.111.146.184	192.168.2.3
Jan 25, 2023 10:21:12.374710083 CET	443	49699	192.111.146.184	192.168.2.3
Jan 25, 2023 10:21:12.374835014 CET	49699	443	192.168.2.3	192.111.146.184
Jan 25, 2023 10:21:12.374835014 CET	49699	443	192.168.2.3	192.111.146.184
Jan 25, 2023 10:21:12.374854088 CET	443	49699	192.111.146.184	192.168.2.3
Jan 25, 2023 10:21:12.374907017 CET	49699	443	192.168.2.3	192.111.146.184
Jan 25, 2023 10:21:12.584649086 CET	49699	443	192.168.2.3	192.111.146.184
Jan 25, 2023 10:21:12.584701061 CET	443	49699	192.111.146.184	192.168.2.3
Jan 25, 2023 10:21:12.679800987 CET	49701	443	192.168.2.3	104.16.169.131
Jan 25, 2023 10:21:12.679925919 CET	443	49701	104.16.169.131	192.168.2.3
Jan 25, 2023 10:21:12.680052996 CET	49701	443	192.168.2.3	104.16.169.131
Jan 25, 2023 10:21:12.680505991 CET	49701	443	192.168.2.3	104.16.169.131
Jan 25, 2023 10:21:12.680532932 CET	443	49701	104.16.169.131	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2023 10:21:09.904345989 CET	58921	53	192.168.2.3	8.8.8.8
Jan 25, 2023 10:21:09.905561924 CET	62704	53	192.168.2.3	8.8.8.8
Jan 25, 2023 10:21:09.925120115 CET	53	62704	8.8.8.8	192.168.2.3
Jan 25, 2023 10:21:09.930423975 CET	53	58921	8.8.8.8	192.168.2.3
Jan 25, 2023 10:21:10.750754118 CET	57990	53	192.168.2.3	8.8.8.8
Jan 25, 2023 10:21:10.769975901 CET	53	57990	8.8.8.8	192.168.2.3
Jan 25, 2023 10:21:12.648492098 CET	60625	53	192.168.2.3	8.8.8.8
Jan 25, 2023 10:21:12.668647051 CET	53	60625	8.8.8.8	192.168.2.3
Jan 25, 2023 10:21:13.161659002 CET	49302	53	192.168.2.3	8.8.8.8
Jan 25, 2023 10:21:13.180979967 CET	53	49302	8.8.8.8	192.168.2.3
Jan 25, 2023 10:21:14.067257881 CET	60582	53	192.168.2.3	8.8.8.8
Jan 25, 2023 10:21:14.085923910 CET	53	60582	8.8.8.8	192.168.2.3
Jan 25, 2023 10:21:14.289933920 CET	57134	53	192.168.2.3	8.8.8.8
Jan 25, 2023 10:21:14.309168100 CET	53	57134	8.8.8.8	192.168.2.3
Jan 25, 2023 10:22:14.123693943 CET	65017	53	192.168.2.3	8.8.8.8
Jan 25, 2023 10:22:14.151098967 CET	53	65017	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jan 25, 2023 10:21:09.904345989 CET	192.168.2.3	8.8.8.8	0xa722	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Jan 25, 2023 10:21:09.905561924 CET	192.168.2.3	8.8.8.8	0xc890	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jan 25, 2023 10:21:10.750754118 CET	192.168.2.3	8.8.8.8	0xb5b6	Standard query (0)	h-kd0.shop	A (IP address)	IN (0x0001)	false
Jan 25, 2023 10:21:12.648492098 CET	192.168.2.3	8.8.8.8	0x447e	Standard query (0)	www.hcaptcha.com	A (IP address)	IN (0x0001)	false
Jan 25, 2023 10:21:13.161659002 CET	192.168.2.3	8.8.8.8	0x3987	Standard query (0)	newassets.hcaptcha.com	A (IP address)	IN (0x0001)	false
Jan 25, 2023 10:21:14.067257881 CET	192.168.2.3	8.8.8.8	0x97de	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Jan 25, 2023 10:21:14.289933920 CET	192.168.2.3	8.8.8.8	0x2831	Standard query (0)	hcaptcha.com	A (IP address)	IN (0x0001)	false
Jan 25, 2023 10:22:14.123693943 CET	192.168.2.3	8.8.8.8	0x5323	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

DNS Answers

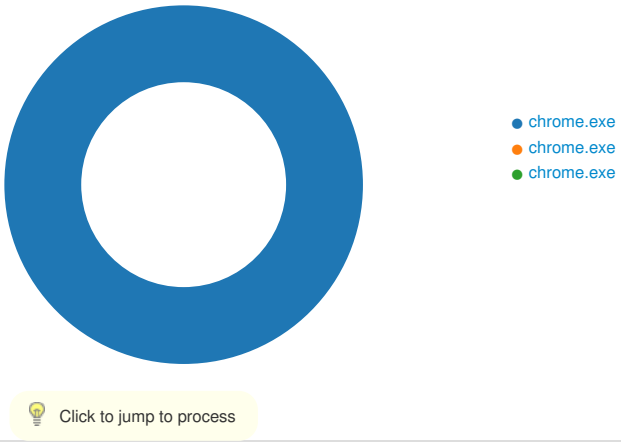
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 25, 2023 10:21:09.925120115 CET	8.8.8.8	192.168.2.3	0xc890	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Jan 25, 2023 10:21:09.925120115 CET	8.8.8.8	192.168.2.3	0xc890	No error (0)	clients.l.google.com		216.58.215.238	A (IP address)	IN (0x0001)	false
Jan 25, 2023 10:21:09.930423975 CET	8.8.8.8	192.168.2.3	0xa722	No error (0)	accounts.google.com		142.250.203.109	A (IP address)	IN (0x0001)	false
Jan 25, 2023 10:21:10.769975901 CET	8.8.8.8	192.168.2.3	0xb5b6	No error (0)	h-kd0.shop		192.111.146.184	A (IP address)	IN (0x0001)	false
Jan 25, 2023 10:21:12.668647051 CET	8.8.8.8	192.168.2.3	0x447e	No error (0)	www.hcaptcha.com		104.16.169.131	A (IP address)	IN (0x0001)	false
Jan 25, 2023 10:21:12.668647051 CET	8.8.8.8	192.168.2.3	0x447e	No error (0)	www.hcaptcha.com		104.16.168.131	A (IP address)	IN (0x0001)	false
Jan 25, 2023 10:21:13.180979967 CET	8.8.8.8	192.168.2.3	0x3987	No error (0)	newassets.hcaptcha.com		104.16.169.131	A (IP address)	IN (0x0001)	false
Jan 25, 2023 10:21:13.180979967 CET	8.8.8.8	192.168.2.3	0x3987	No error (0)	newassets.hcaptcha.com		104.16.168.131	A (IP address)	IN (0x0001)	false
Jan 25, 2023 10:21:14.085923910 CET	8.8.8.8	192.168.2.3	0x97de	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Jan 25, 2023 10:21:14.309168100 CET	8.8.8.8	192.168.2.3	0x2831	No error (0)	hcaptcha.com		104.16.169.131	A (IP address)	IN (0x0001)	false
Jan 25, 2023 10:21:14.309168100 CET	8.8.8.8	192.168.2.3	0x2831	No error (0)	hcaptcha.com		104.16.168.131	A (IP address)	IN (0x0001)	false
Jan 25, 2023 10:22:14.151098967 CET	8.8.8.8	192.168.2.3	0x5323	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- h-kd0.shop
- https:
  - www.hcaptcha.com
  - newassets.hcaptcha.com
  - hcaptcha.com

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 6052, Parent PID: 1764

General

Target ID:	0
Start time:	10:21:07
Start date:	25/01/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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: 5208, Parent PID: 6052

General

Target ID:	1

Start time:	10:21:08
Start date:	25/01/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1956 --field-trial-handle=1724,i,2672952510848693389,14012057706382809610,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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

Analysis Process: chrome.exe PID: **4392**, Parent PID: **1764**

General

Target ID:	2
Start time:	10:21:09
Start date:	25/01/2023
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\VM Tue, January 24, 2023 #18654.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:	high

Registry Activities

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

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

Disassembly

No disassembly