ID: 736954
Cookbook: browseurl.jbs
Time: 12:28:45
Date: 03/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

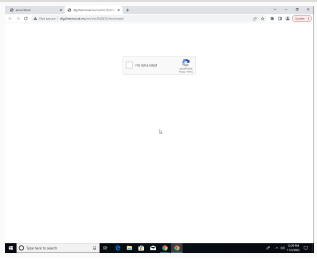
Windows Analysis Report

http://dlg.thermoval.mx/vn/mic (1)/mic/?e=amxnQGRsZy5kaw==

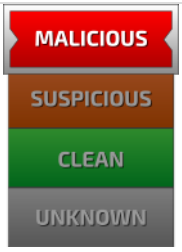
Overview

General Information

Sample URL:	http://dlg.thermoval.mx/vn/mic (1)/mic/?e=amxnQGRsZy5kaw==
Analysis ID:	736954
Infos:	



Detection



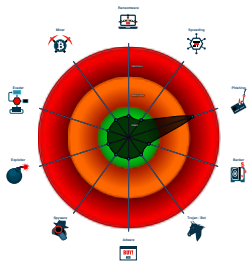
Captcha Phish

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

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected Captcha Phish
- Antivirus detection for URL or domain

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5008 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 5248 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=1660 --field-trial-handle=1632,i,5625803513214026422,4861494269649546728,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 3712 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "http://dlg.thermoval.mx/vn/mic%20(1)/mic/?e=amxnQGRsZy5kaw== MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

HTML

Source	Rule	Description	Author	Strings
30138.0.pages.csv	JoeSecurity_CaptchaPhish_1	Yara detected Captcha Phish	Joe Security	
71540.2.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 / Scanner detection for submitted sample

Antivirus detection for URL or domain

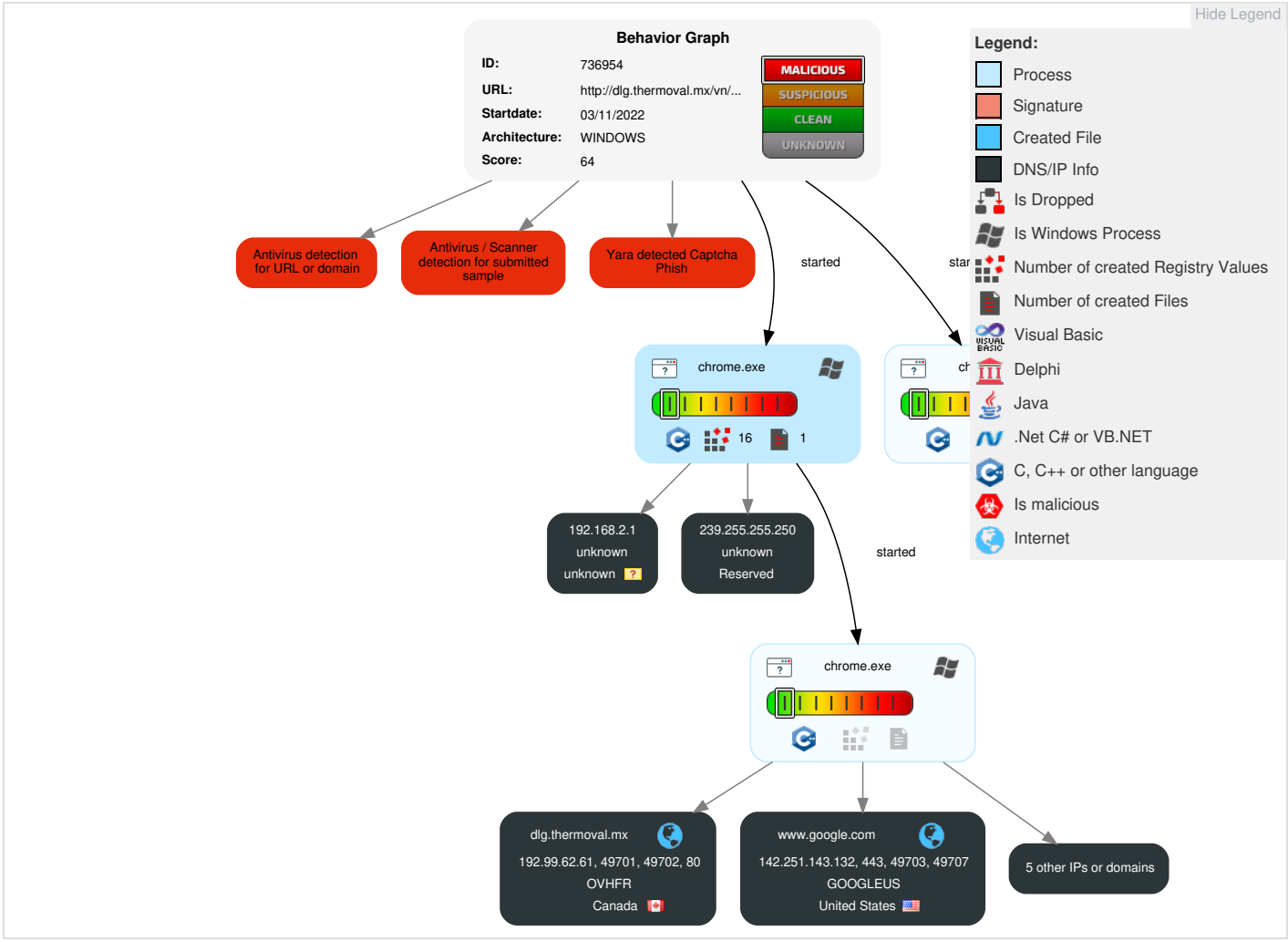
Phishing

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

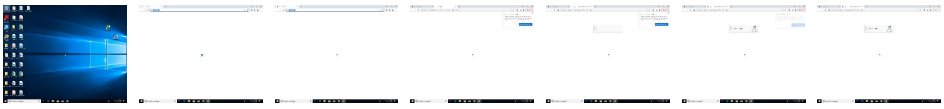
Behavior Graph

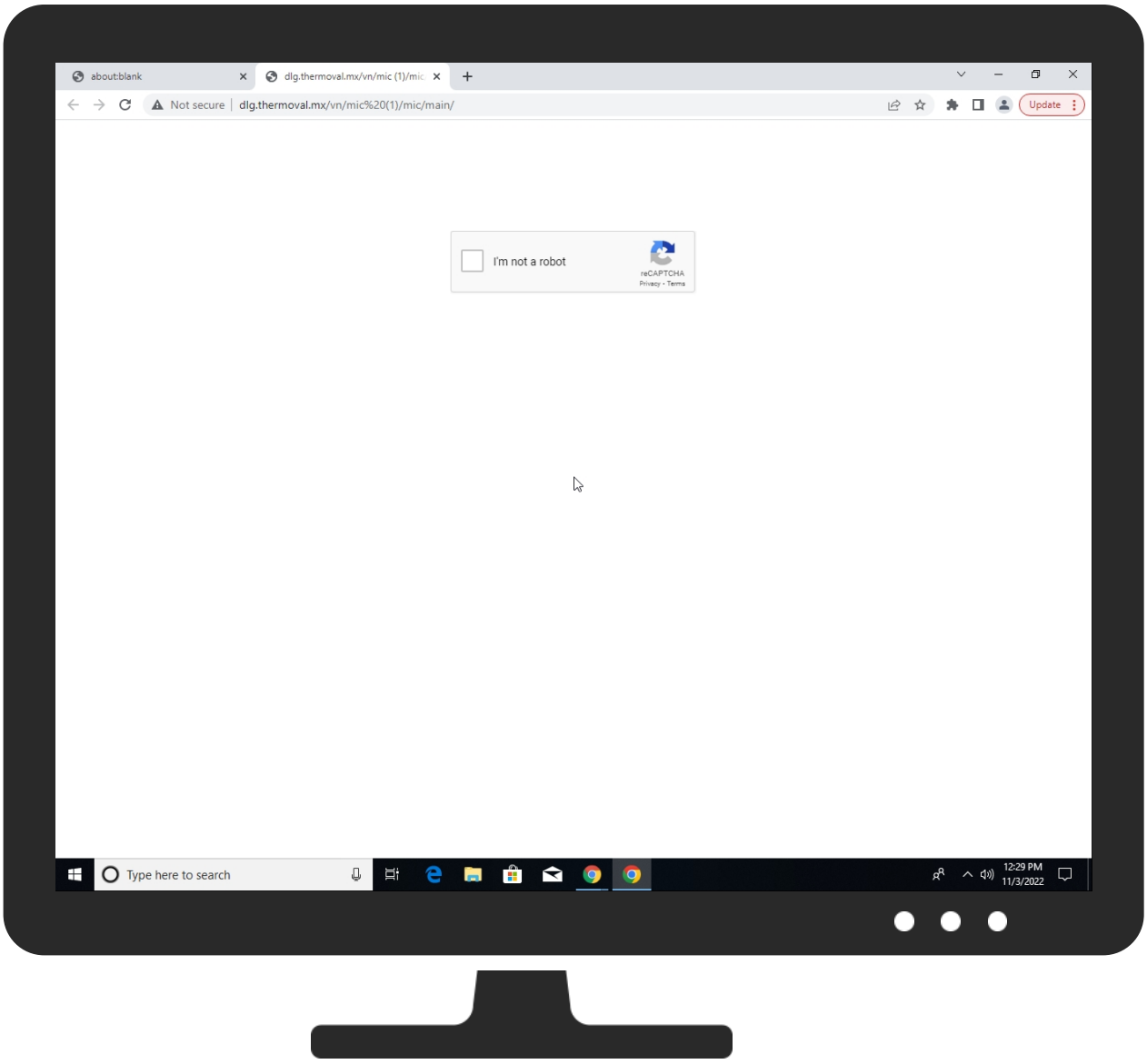


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://dlg.thermoval.mx/vn/mic%20(1)/mic/?e=amxnQGRsZy5kaw==	0%	Virustotal		Browse
http://dlg.thermoval.mx/vn/mic%20(1)/mic/?e=amxnQGRsZy5kaw==	0%	Avira URL Cloud	safe	
http://dlg.thermoval.mx/vn/mic%20(1)/mic/?e=amxnQGRsZy5kaw==	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://dlg.thermoval.mx/vn/mic%20(1)/mic/main/	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	
http://dlg.thermoval.mx/vn/mic%20(1)/mic/main	0%	Avira URL Cloud	safe	
http://dlg.thermoval.mx/favicon.ico	0%	Avira URL Cloud	safe	
http://dlg.thermoval.mx/vn/mic%20(1)/mic/main	0%	Virustotal		Browse

Domains and IPs

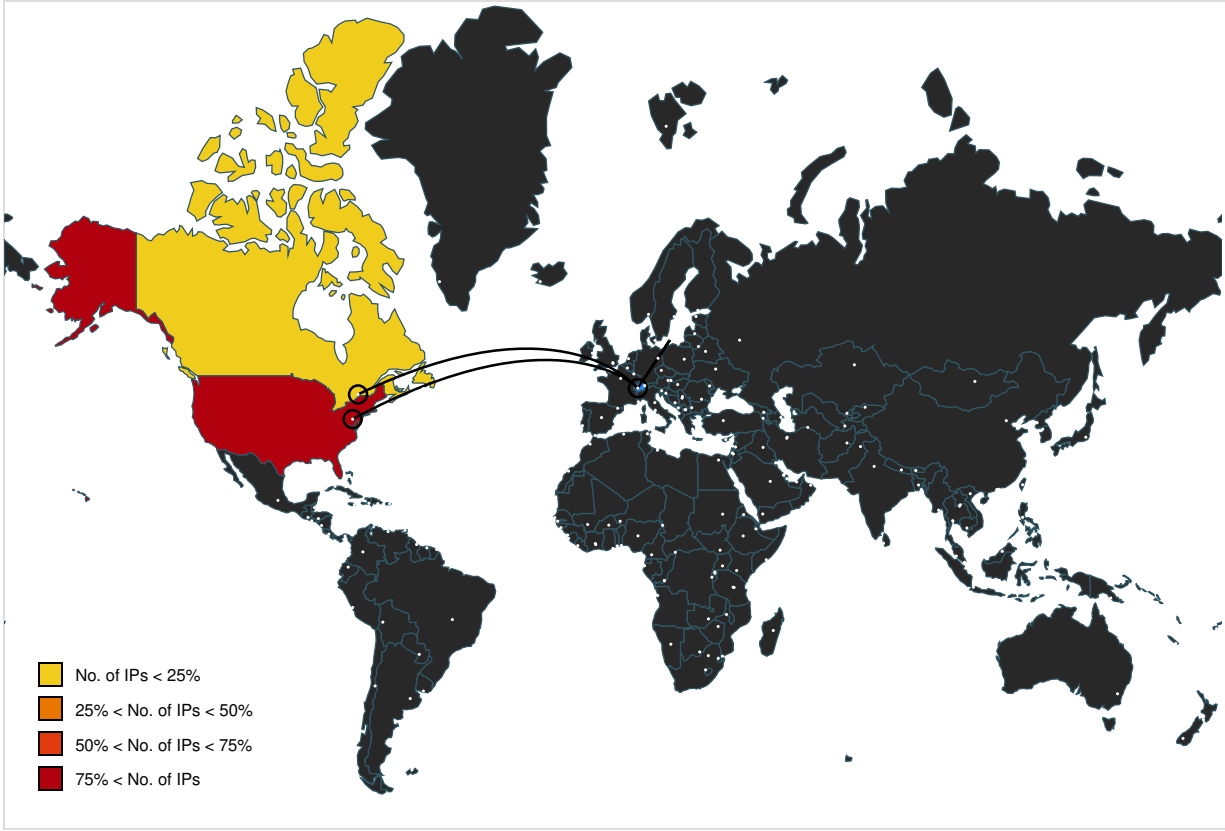
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
stackpath.bootstrapcdn.com	104.18.10.207	true	false		high
accounts.google.com	142.251.143.141	true	false		high
www.google.com	142.251.143.132	true	false		high
clients.l.google.com	142.251.143.174	true	false		high
dlg.thermoval.mx	192.99.62.61	true	false		unknown
clients2.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.google.com/recaptcha/api2/bframe?hl=en&v=Ixi5IiChXmIG6rRkjUa1qXHT&k=6LfKT9YiAAAAALqPYG6r5x-vNt62pf39FWtZjSeQ	false		high
http://dlg.thermoval.mx/vn/mic%20(1)/mic/main	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://dlg.thermoval.mx/vn/mic%20(1)/mic/main/	true	• SlashNext: Credential Stealing type: Phishing & Social Engineering	unknown
http://dlg.thermoval.mx/vn/mic%20(1)/mic/?e=amxnQGRsZy5kaw==	true		unknown
http://https://www.google.com/recaptcha/api2/webworker.js?hl=en&v=Ixi5IiChXmIG6rRkjUa1qXHT	false		high
http://dlg.thermoval.mx/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/recaptcha/api.js	false		high
http://https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css	false		high
http://https://www.google.com/recaptcha/api2/anchor?ar=1&k=6LfKT9YiAAAAALqPYG6r5x-vNt62pf39FWtZjSeQ&co=aHR0cDovL2RsZy50aGVybW92YWwubXg6ODA.&hl=en&v=Ixi5IiChXmIG6rRkjUa1qXHT&size=normal&cb=rqirtg7im98e	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://www.google.com/recaptcha/api2/anchor?ar=1&k=6LfKT9YiAAAAALqPYG6r5x-vNt62pf39FWtZjSeQ&co=aHR0cDovL2RsZy50aGVybW92YWwubXg6ODA.&hl=en&v=Ixi5IiChXmIG6rRkjUa1qXHT&size=normal&cb=rqirtg7im98e	false		high
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://dlg.thermoval.mx/vn/mic%20(1)/mic/main/	true	• SlashNext: Credential Stealing type: Phishing & Social Engineering	unknown
http://https://www.google.com/recaptcha/api2/bframe?hl=en&v=Ixi5IiChXmIG6rRkjUa1qXHT&k=6LfKT9YiAAAAALqPYG6r5x-vNt62pf39FWtZjSeQ	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.18.10.207	stackpath.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
192.99.62.61	dlg.thermoval.mx	Canada		16276	OVHFR	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.251.143.132	www.google.com	United States		15169	GOOGLEUS	false
142.251.143.141	accounts.google.com	United States		15169	GOOGLEUS	false
142.251.143.174	clients.l.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:	736954
Start date and time:	2022-11-03 12:28:45 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://dlg.thermoval.mx/vn/mic (1)/mic/?e=amxnQGRsZy5kaw==
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:	5
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.phis.win@25/0@6/8
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.251.143.163, 34.104.35.123, 142.251.143.131, 142.251.143.202, 142.251.143.106, 142.251.143.138, 142.251.143.170
- Excluded domains from analysis (whitelisted): edgedl.me.gvt1.com, content-autofill.googleapis.com, fonts.gstatic.com, update.googleapis.com, ctldl.windowsupdate.com, clientservices.googleapis.com, www.gstatic.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

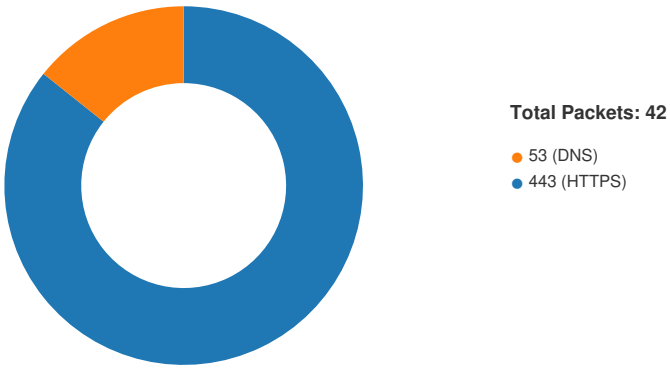
No created / dropped files found

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:29:48.807007074 CET	49698	443	192.168.2.5	142.251.143.141
Nov 3, 2022 12:29:48.807094097 CET	443	49698	142.251.143.141	192.168.2.5
Nov 3, 2022 12:29:48.807789087 CET	49699	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:29:48.807841063 CET	443	49699	142.251.143.174	192.168.2.5
Nov 3, 2022 12:29:48.808912039 CET	49698	443	192.168.2.5	142.251.143.141
Nov 3, 2022 12:29:48.809052944 CET	49699	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:29:48.810471058 CET	49698	443	192.168.2.5	142.251.143.141
Nov 3, 2022 12:29:48.810508013 CET	443	49698	142.251.143.141	192.168.2.5
Nov 3, 2022 12:29:48.826536894 CET	49699	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:29:48.826591969 CET	443	49699	142.251.143.174	192.168.2.5
Nov 3, 2022 12:29:48.902770042 CET	443	49698	142.251.143.141	192.168.2.5
Nov 3, 2022 12:29:48.903244972 CET	49701	80	192.168.2.5	192.99.62.61
Nov 3, 2022 12:29:48.904176950 CET	49698	443	192.168.2.5	142.251.143.141
Nov 3, 2022 12:29:48.904216051 CET	443	49698	142.251.143.141	192.168.2.5
Nov 3, 2022 12:29:48.905174971 CET	49702	80	192.168.2.5	192.99.62.61
Nov 3, 2022 12:29:48.908874989 CET	443	49698	142.251.143.141	192.168.2.5
Nov 3, 2022 12:29:48.908996105 CET	49698	443	192.168.2.5	142.251.143.141
Nov 3, 2022 12:29:48.911382914 CET	443	49699	142.251.143.174	192.168.2.5
Nov 3, 2022 12:29:48.914360046 CET	49699	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:29:48.914442062 CET	443	49699	142.251.143.174	192.168.2.5
Nov 3, 2022 12:29:48.915100098 CET	443	49699	142.251.143.174	192.168.2.5
Nov 3, 2022 12:29:48.915185928 CET	49699	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:29:48.916436911 CET	443	49699	142.251.143.174	192.168.2.5
Nov 3, 2022 12:29:48.916501045 CET	49699	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:29:49.007479906 CET	80	49701	192.99.62.61	192.168.2.5
Nov 3, 2022 12:29:49.007647038 CET	49701	80	192.168.2.5	192.99.62.61
Nov 3, 2022 12:29:49.008526087 CET	49701	80	192.168.2.5	192.99.62.61
Nov 3, 2022 12:29:49.009196997 CET	80	49702	192.99.62.61	192.168.2.5
Nov 3, 2022 12:29:49.009337902 CET	49702	80	192.168.2.5	192.99.62.61
Nov 3, 2022 12:29:49.091870070 CET	49703	443	192.168.2.5	142.251.143.132
Nov 3, 2022 12:29:49.091936111 CET	443	49703	142.251.143.132	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:29:49.092036963 CET	49703	443	192.168.2.5	142.251.143.132
Nov 3, 2022 12:29:49.097603083 CET	49703	443	192.168.2.5	142.251.143.132
Nov 3, 2022 12:29:49.097639084 CET	443	49703	142.251.143.132	192.168.2.5
Nov 3, 2022 12:29:49.112878084 CET	80	49701	192.99.62.61	192.168.2.5
Nov 3, 2022 12:29:49.183114052 CET	443	49703	142.251.143.132	192.168.2.5
Nov 3, 2022 12:29:49.198966980 CET	49703	443	192.168.2.5	142.251.143.132
Nov 3, 2022 12:29:49.199048042 CET	443	49703	142.251.143.132	192.168.2.5
Nov 3, 2022 12:29:49.205454111 CET	443	49703	142.251.143.132	192.168.2.5
Nov 3, 2022 12:29:49.205720901 CET	49703	443	192.168.2.5	142.251.143.132
Nov 3, 2022 12:29:49.214911938 CET	80	49701	192.99.62.61	192.168.2.5
Nov 3, 2022 12:29:49.220045090 CET	80	49701	192.99.62.61	192.168.2.5
Nov 3, 2022 12:29:49.220200062 CET	49701	80	192.168.2.5	192.99.62.61
Nov 3, 2022 12:29:49.402169943 CET	49701	80	192.168.2.5	192.99.62.61
Nov 3, 2022 12:29:49.482338905 CET	49698	443	192.168.2.5	142.251.143.141
Nov 3, 2022 12:29:49.482400894 CET	443	49698	142.251.143.141	192.168.2.5
Nov 3, 2022 12:29:49.482739925 CET	443	49698	142.251.143.141	192.168.2.5
Nov 3, 2022 12:29:49.483298063 CET	49698	443	192.168.2.5	142.251.143.141
Nov 3, 2022 12:29:49.483331919 CET	443	49698	142.251.143.141	192.168.2.5
Nov 3, 2022 12:29:49.484028101 CET	49699	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:29:49.484071016 CET	443	49699	142.251.143.174	192.168.2.5
Nov 3, 2022 12:29:49.484349966 CET	443	49699	142.251.143.174	192.168.2.5
Nov 3, 2022 12:29:49.484391928 CET	49699	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:29:49.484412909 CET	443	49699	142.251.143.174	192.168.2.5
Nov 3, 2022 12:29:49.490647078 CET	49703	443	192.168.2.5	142.251.143.132
Nov 3, 2022 12:29:49.490693092 CET	443	49703	142.251.143.132	192.168.2.5
Nov 3, 2022 12:29:49.490986109 CET	443	49703	142.251.143.132	192.168.2.5
Nov 3, 2022 12:29:49.506547928 CET	80	49701	192.99.62.61	192.168.2.5
Nov 3, 2022 12:29:49.543323994 CET	443	49699	142.251.143.174	192.168.2.5
Nov 3, 2022 12:29:49.543488026 CET	49699	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:29:49.543534040 CET	443	49699	142.251.143.174	192.168.2.5
Nov 3, 2022 12:29:49.543569088 CET	443	49699	142.251.143.174	192.168.2.5
Nov 3, 2022 12:29:49.543617964 CET	49699	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:29:49.544300079 CET	80	49701	192.99.62.61	192.168.2.5
Nov 3, 2022 12:29:49.553594112 CET	49699	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:29:49.553627968 CET	443	49699	142.251.143.174	192.168.2.5
Nov 3, 2022 12:29:49.559475899 CET	443	49698	142.251.143.141	192.168.2.5
Nov 3, 2022 12:29:49.559640884 CET	49698	443	192.168.2.5	142.251.143.141
Nov 3, 2022 12:29:49.559689999 CET	443	49698	142.251.143.141	192.168.2.5
Nov 3, 2022 12:29:49.559828997 CET	443	49698	142.251.143.141	192.168.2.5
Nov 3, 2022 12:29:49.559901953 CET	49698	443	192.168.2.5	142.251.143.141
Nov 3, 2022 12:29:49.584745884 CET	49698	443	192.168.2.5	142.251.143.141
Nov 3, 2022 12:29:49.584789038 CET	443	49698	142.251.143.141	192.168.2.5
Nov 3, 2022 12:29:49.597019911 CET	49701	80	192.168.2.5	192.99.62.61
Nov 3, 2022 12:29:49.598272085 CET	49703	443	192.168.2.5	142.251.143.132
Nov 3, 2022 12:29:49.598303080 CET	443	49703	142.251.143.132	192.168.2.5
Nov 3, 2022 12:29:49.690905094 CET	49701	80	192.168.2.5	192.99.62.61
Nov 3, 2022 12:29:49.696825027 CET	49703	443	192.168.2.5	142.251.143.132
Nov 3, 2022 12:29:49.795140028 CET	80	49701	192.99.62.61	192.168.2.5
Nov 3, 2022 12:29:49.891505003 CET	80	49701	192.99.62.61	192.168.2.5
Nov 3, 2022 12:29:49.891551971 CET	80	49701	192.99.62.61	192.168.2.5
Nov 3, 2022 12:29:49.891701937 CET	49701	80	192.168.2.5	192.99.62.61
Nov 3, 2022 12:29:49.896554947 CET	80	49701	192.99.62.61	192.168.2.5
Nov 3, 2022 12:29:49.996674061 CET	49703	443	192.168.2.5	142.251.143.132
Nov 3, 2022 12:29:49.996726990 CET	443	49703	142.251.143.132	192.168.2.5
Nov 3, 2022 12:29:50.074249983 CET	49705	443	192.168.2.5	104.18.10.207
Nov 3, 2022 12:29:50.074321032 CET	443	49705	104.18.10.207	192.168.2.5
Nov 3, 2022 12:29:50.074429989 CET	49705	443	192.168.2.5	104.18.10.207
Nov 3, 2022 12:29:50.080435038 CET	49705	443	192.168.2.5	104.18.10.207
Nov 3, 2022 12:29:50.080471992 CET	443	49705	104.18.10.207	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:29:50.096889019 CET	49701	80	192.168.2.5	192.99.62.61
Nov 3, 2022 12:29:50.129040003 CET	443	49705	104.18.10.207	192.168.2.5
Nov 3, 2022 12:29:50.145890951 CET	443	49703	142.251.143.132	192.168.2.5
Nov 3, 2022 12:29:50.146152020 CET	443	49703	142.251.143.132	192.168.2.5
Nov 3, 2022 12:29:50.146246910 CET	49703	443	192.168.2.5	142.251.143.132
Nov 3, 2022 12:29:50.178133011 CET	49705	443	192.168.2.5	104.18.10.207
Nov 3, 2022 12:29:50.178175926 CET	443	49705	104.18.10.207	192.168.2.5
Nov 3, 2022 12:29:50.179775000 CET	49703	443	192.168.2.5	142.251.143.132
Nov 3, 2022 12:29:50.179812908 CET	443	49703	142.251.143.132	192.168.2.5
Nov 3, 2022 12:29:50.182622910 CET	443	49705	104.18.10.207	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:29:47.165843964 CET	61893	53	192.168.2.5	8.8.8.8
Nov 3, 2022 12:29:47.167749882 CET	60649	53	192.168.2.5	8.8.8.8
Nov 3, 2022 12:29:47.191386938 CET	53	61893	8.8.8.8	192.168.2.5
Nov 3, 2022 12:29:47.195754051 CET	53	60649	8.8.8.8	192.168.2.5
Nov 3, 2022 12:29:48.605357885 CET	49724	53	192.168.2.5	8.8.8.8
Nov 3, 2022 12:29:48.623624086 CET	60649	53	192.168.2.5	8.8.8.8
Nov 3, 2022 12:29:48.651177883 CET	53	60649	8.8.8.8	192.168.2.5
Nov 3, 2022 12:29:48.720166922 CET	53	49724	8.8.8.8	192.168.2.5
Nov 3, 2022 12:29:48.886029005 CET	65323	53	192.168.2.5	8.8.8.8
Nov 3, 2022 12:29:48.913223982 CET	53	65323	8.8.8.8	192.168.2.5
Nov 3, 2022 12:29:49.998810053 CET	56751	53	192.168.2.5	8.8.8.8
Nov 3, 2022 12:29:50.021548986 CET	53	56751	8.8.8.8	192.168.2.5

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Nov 3, 2022 12:29:48.651316881 CET	192.168.2.5	8.8.8.8	d020	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 3, 2022 12:29:47.165843964 CET	192.168.2.5	8.8.8.8	0x9ea3	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:29:47.167749882 CET	192.168.2.5	8.8.8.8	0x8325	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:29:48.605357885 CET	192.168.2.5	8.8.8.8	0x53b1	Standard query (0)	dlg.thermoval.mx	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:29:48.623624086 CET	192.168.2.5	8.8.8.8	0x8325	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:29:48.886029005 CET	192.168.2.5	8.8.8.8	0x1ca0	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:29:49.998810053 CET	192.168.2.5	8.8.8.8	0xd88e	Standard query (0)	stackpath.bootstrapcdn.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
Nov 3, 2022 12:29:47.191386938 CET	8.8.8.8	192.168.2.5	0x9ea3	No error (0)	accounts.google.com		142.251.143.141	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:29:47.195754051 CET	8.8.8.8	192.168.2.5	0x8325	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 3, 2022 12:29:47.195754051 CET	8.8.8.8	192.168.2.5	0x8325	No error (0)	clients.l.google.com		142.251.143.174	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:29:48.651177883 CET	8.8.8.8	192.168.2.5	0x8325	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false

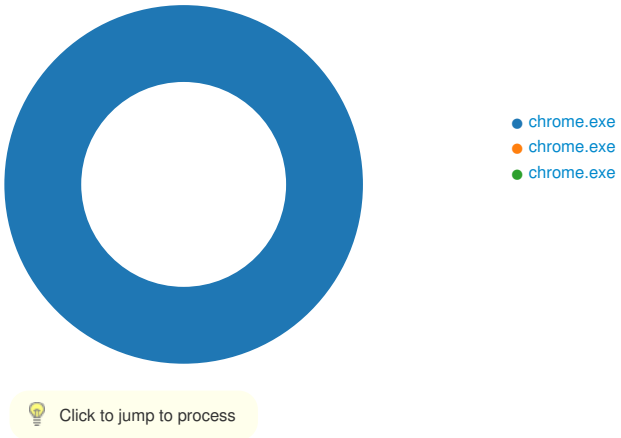
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 3, 2022 12:29:48.651177883 CET	8.8.8.8	192.168.2.5	0x8325	No error (0)	clients.l.google.com		142.251.143.174	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:29:48.720166922 CET	8.8.8.8	192.168.2.5	0x53b1	No error (0)	dlg.thermoval.mx		192.99.62.61	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:29:48.913223982 CET	8.8.8.8	192.168.2.5	0x1ca0	No error (0)	www.google.com		142.251.143.132	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:29:50.021548986 CET	8.8.8.8	192.168.2.5	0xd88e	No error (0)	stackpath.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:29:50.021548986 CET	8.8.8.8	192.168.2.5	0xd88e	No error (0)	stackpath.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- accounts.google.com
- clients2.google.com
- dlg.thermoval.mx
  - www.google.com
  - stackpath.bootstrapcdn.com
- https:

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 5008, Parent PID: 3924

General

Target ID:	0
Start time:	12:29:40
Start date:	03/11/2022
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:	0x7ff7d31b0000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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: **5248**, Parent PID: **5008**

General

Target ID:	1
Start time:	12:29:42
Start date:	03/11/2022
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=1660 --field-trial-handle=1632,i,5625803513214026422,4861494269649546728,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff7d31b0000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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: **3712**, Parent PID: **3924**

General

Target ID:	2

Start time:	12:29:42
Start date:	03/11/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "http://dlg.thermoval.mx/vn/mic%20(1)/mic/?e=amxnQGRsZy5kaw==
Imagebase:	0x7ff7d31b0000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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