ID: 715092
Cookbook: browseurl.jbs
Time: 16:12:07
Date: 03/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report https://amigodepatasbh.com.br/ff 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Signatures 3
Sigma Signatures 3
Snort Signatures 4
Joe Sandbox Signatures 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
Contacted URLs 7
World Map of Contacted IPs 7
Public IPs 7
Private 8
General Information 8
Warnings 8
Simulations 8
Behavior and APIs 8
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASNs 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 9
Network Behavior 9
Network Port Distribution 9
TCP Packets 9
UDP Packets 11
DNS Queries 11
DNS Answers 12
HTTP Request Dependency Graph 12
HTTPS Proxied Packets 12
Statistics 18
Behavior 18
System Behavior 19
Analysis Process: chrome.exePID: 5688, Parent PID: 2704 19
General 19
File Activities 19
Registry Activities 19
Analysis Process: chrome.exePID: 5880, Parent PID: 5688 19
General 19
File Activities 20
Analysis Process: chrome.exePID: 2828, Parent PID: 2704 20
General 20
Registry Activities 20
Disassembly 20

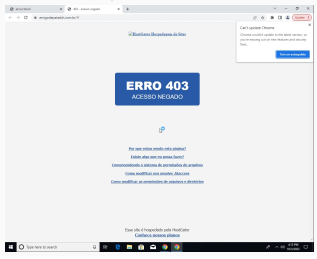
Windows Analysis Report

https://amigodepatasbh.com.br/ff

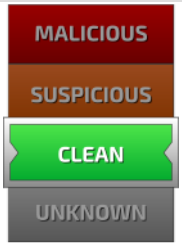
Overview

General Information

Sample URL:	http://https://amigodepatasbh.com.br/ff
Analysis ID:	715092
Infos:	



Detection

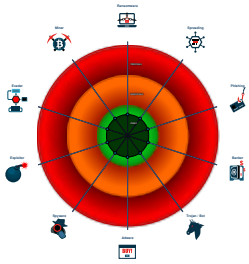


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64
- chrome.exe (PID: 5688 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 5880 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=1968 --field-trial-handle=1732,i,8218220987001890426,18157507330322035723,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 2828 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://amigodepatasbh.com.br/ff MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- cleanup

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

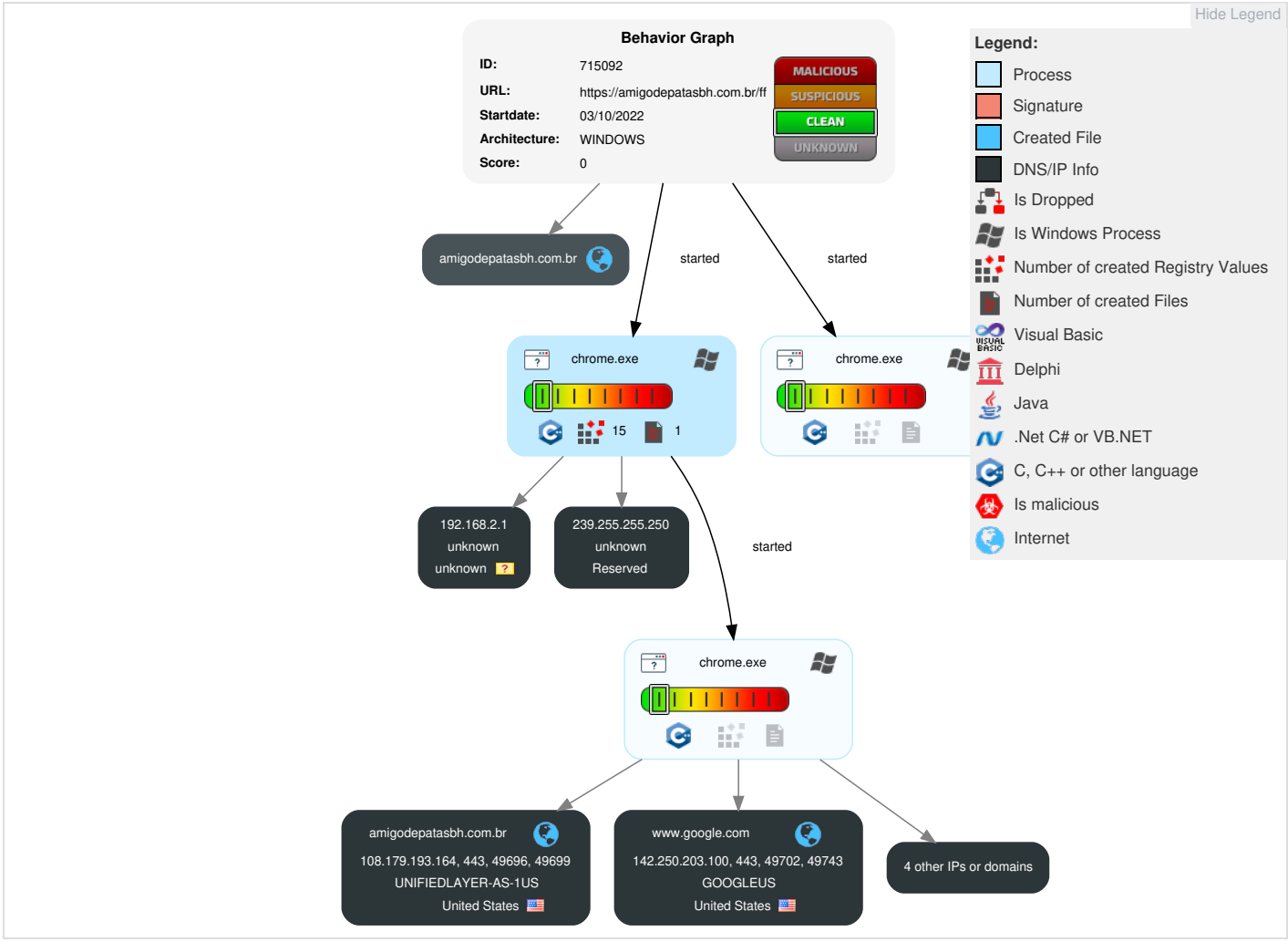
Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

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

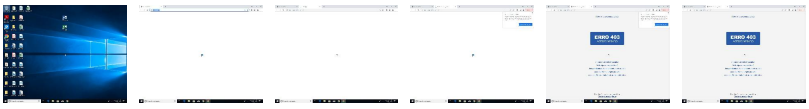
Behavior Graph

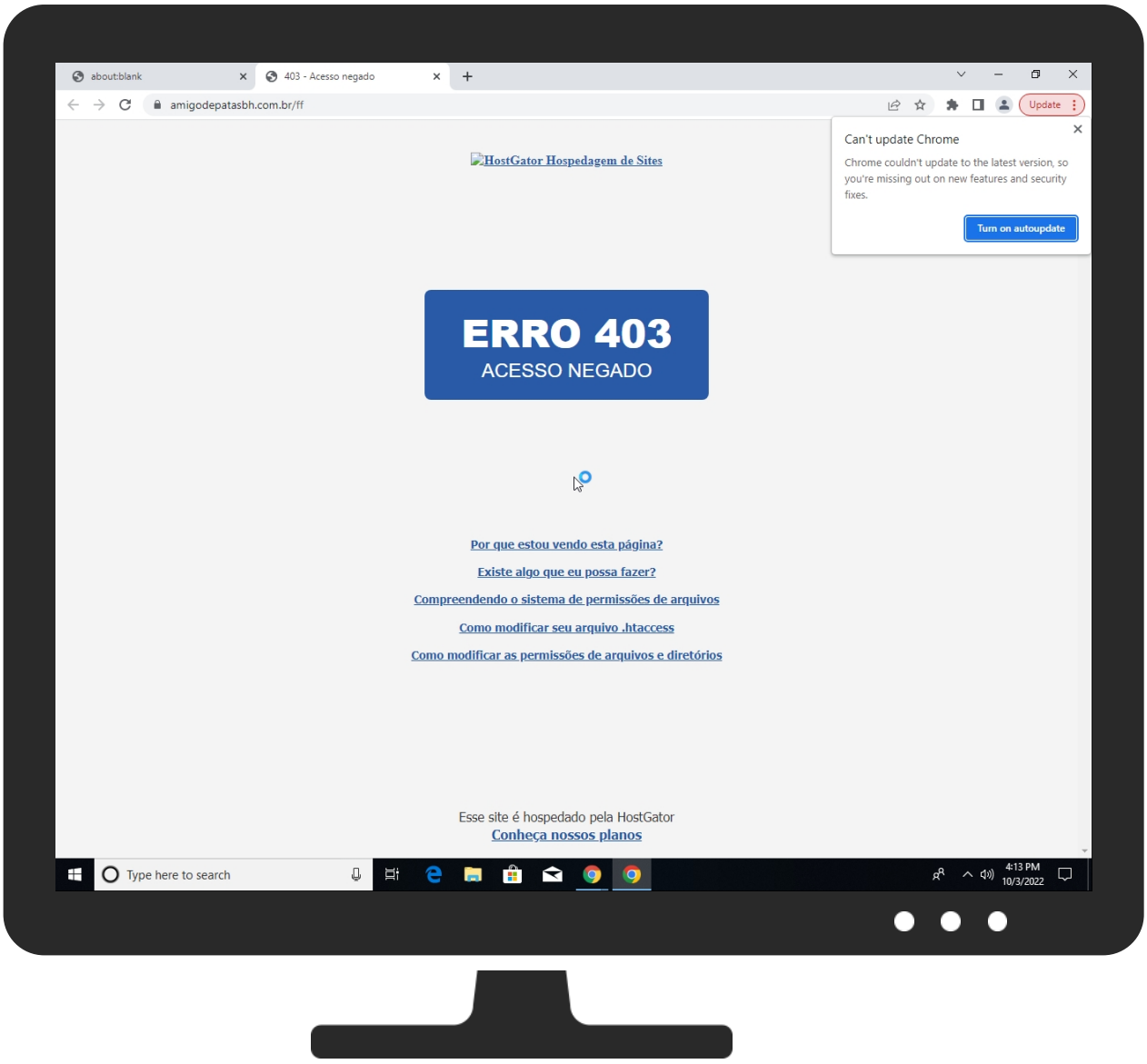


Screenshots

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://https://amigodepatasbh.com.br/ff	0%	Virustotal		Browse
http://https://amigodepatasbh.com.br/ff	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://amigodepatasbh.com.br/cgi-sys/js/jquery-1.11.2.min.js	0%	Avira URL Cloud	safe	
http://https://amigodepatasbh.com.br/cgi-sys/images/logo-403-page.png	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://amigodepatasbh.com.br/cgi-sys/images/favicon.png	0%	Avira URL Cloud	safe	

Domains and IPs

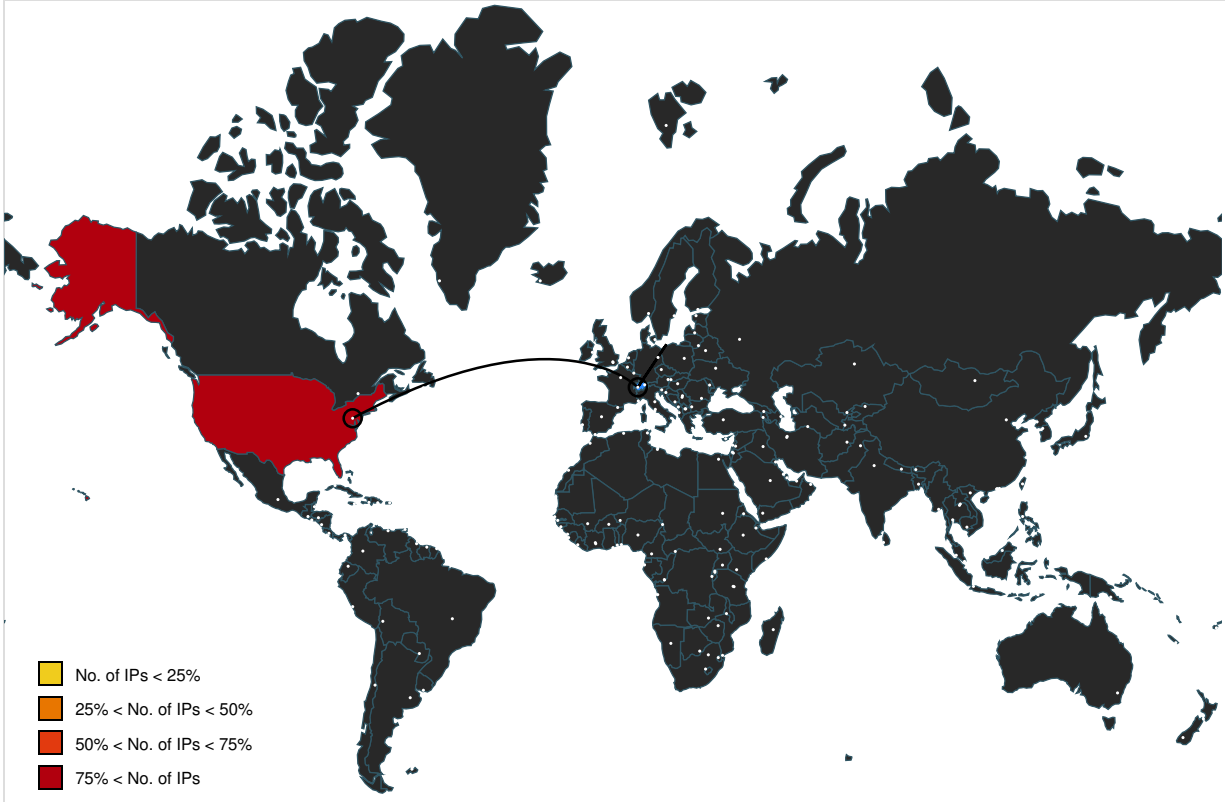
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.250.203.109	true	false		high
amigodepatasbh.com.br	108.179.193.164	true	false		unknown
www.google.com	142.250.203.100	true	false		high
clients.l.google.com	142.250.203.110	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://amigodepatasbh.com.br/ff	false		unknown
http://https://amigodepatasbh.com.br/ff	false		unknown
http://https://amigodepatasbh.com.br/cgi-sys/js/jquery-1.11.2.min.js	false	• Avira URL Cloud: safe	unknown
http://https://amigodepatasbh.com.br/cgi-sys/images/logo-403-page.png	false	• Avira URL Cloud: safe	unknown
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://amigodepatasbh.com.br/cgi-sys/images/favicon.png	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.203.100	www.google.com	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
108.179.193.164	amigodepatasbh.com.br	United States		46606	UNIFIEDLAYER-AS-1US	false
142.250.203.110	clients.l.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:	715092
Start date and time:	2022-10-03 16:12:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://amigodepatasbh.com.br/ff
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:	12
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:	CLEAN
Classification:	clean0.win@25/0@5/7
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): SgrmBroker.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.203.99, 34.104.35.123
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, edgedl.me.gvt1.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

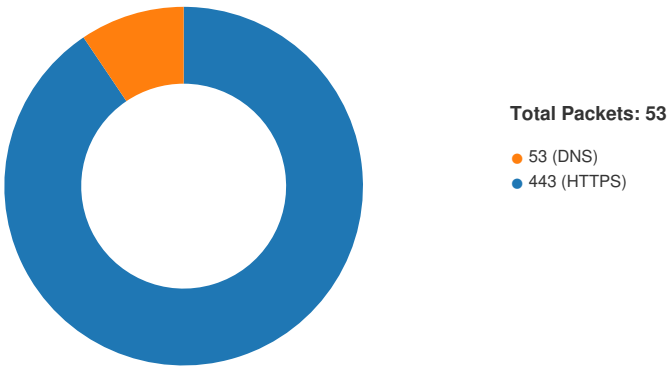
No created / dropped files found

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:13:09.618771076 CEST	49694	443	192.168.2.7	142.250.203.110

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:13:09.618839979 CEST	443	49694	142.250.203.110	192.168.2.7
Oct 3, 2022 16:13:09.618935108 CEST	49694	443	192.168.2.7	142.250.203.110
Oct 3, 2022 16:13:09.619122982 CEST	49695	443	192.168.2.7	142.250.203.109
Oct 3, 2022 16:13:09.619163990 CEST	443	49695	142.250.203.109	192.168.2.7
Oct 3, 2022 16:13:09.619235992 CEST	49695	443	192.168.2.7	142.250.203.109
Oct 3, 2022 16:13:09.623907089 CEST	49694	443	192.168.2.7	142.250.203.110
Oct 3, 2022 16:13:09.623951912 CEST	443	49694	142.250.203.110	192.168.2.7
Oct 3, 2022 16:13:09.624185085 CEST	49695	443	192.168.2.7	142.250.203.109
Oct 3, 2022 16:13:09.624206066 CEST	443	49695	142.250.203.109	192.168.2.7
Oct 3, 2022 16:13:09.625339985 CEST	49696	443	192.168.2.7	108.179.193.164
Oct 3, 2022 16:13:09.625405073 CEST	443	49696	108.179.193.164	192.168.2.7
Oct 3, 2022 16:13:09.625485897 CEST	49696	443	192.168.2.7	108.179.193.164
Oct 3, 2022 16:13:09.626153946 CEST	49696	443	192.168.2.7	108.179.193.164
Oct 3, 2022 16:13:09.626183987 CEST	443	49696	108.179.193.164	192.168.2.7
Oct 3, 2022 16:13:09.737982988 CEST	443	49695	142.250.203.109	192.168.2.7
Oct 3, 2022 16:13:09.751445055 CEST	443	49694	142.250.203.110	192.168.2.7
Oct 3, 2022 16:13:09.780873060 CEST	49695	443	192.168.2.7	142.250.203.109
Oct 3, 2022 16:13:09.795634985 CEST	49694	443	192.168.2.7	142.250.203.110
Oct 3, 2022 16:13:09.998224974 CEST	443	49696	108.179.193.164	192.168.2.7
Oct 3, 2022 16:13:10.000173092 CEST	49694	443	192.168.2.7	142.250.203.110
Oct 3, 2022 16:13:10.000236988 CEST	443	49694	142.250.203.110	192.168.2.7
Oct 3, 2022 16:13:10.000396013 CEST	49695	443	192.168.2.7	142.250.203.109
Oct 3, 2022 16:13:10.000432014 CEST	443	49695	142.250.203.109	192.168.2.7
Oct 3, 2022 16:13:10.001180887 CEST	49696	443	192.168.2.7	108.179.193.164
Oct 3, 2022 16:13:10.001235962 CEST	443	49696	108.179.193.164	192.168.2.7
Oct 3, 2022 16:13:10.001293898 CEST	443	49694	142.250.203.110	192.168.2.7
Oct 3, 2022 16:13:10.001379013 CEST	49694	443	192.168.2.7	142.250.203.110
Oct 3, 2022 16:13:10.006234884 CEST	443	49696	108.179.193.164	192.168.2.7
Oct 3, 2022 16:13:10.006237030 CEST	443	49695	142.250.203.109	192.168.2.7
Oct 3, 2022 16:13:10.006273031 CEST	443	49694	142.250.203.110	192.168.2.7
Oct 3, 2022 16:13:10.006382942 CEST	49695	443	192.168.2.7	142.250.203.109
Oct 3, 2022 16:13:10.006499052 CEST	49694	443	192.168.2.7	142.250.203.110
Oct 3, 2022 16:13:10.006504059 CEST	49696	443	192.168.2.7	108.179.193.164
Oct 3, 2022 16:13:10.736288071 CEST	49696	443	192.168.2.7	108.179.193.164
Oct 3, 2022 16:13:10.736342907 CEST	443	49696	108.179.193.164	192.168.2.7
Oct 3, 2022 16:13:10.736556053 CEST	443	49696	108.179.193.164	192.168.2.7
Oct 3, 2022 16:13:10.736974955 CEST	49696	443	192.168.2.7	108.179.193.164
Oct 3, 2022 16:13:10.737025976 CEST	443	49696	108.179.193.164	192.168.2.7
Oct 3, 2022 16:13:10.737111092 CEST	49695	443	192.168.2.7	142.250.203.109
Oct 3, 2022 16:13:10.737140894 CEST	443	49695	142.250.203.109	192.168.2.7
Oct 3, 2022 16:13:10.737730026 CEST	49694	443	192.168.2.7	142.250.203.110
Oct 3, 2022 16:13:10.737766027 CEST	443	49694	142.250.203.110	192.168.2.7
Oct 3, 2022 16:13:10.737957954 CEST	443	49695	142.250.203.109	192.168.2.7
Oct 3, 2022 16:13:10.738090992 CEST	49695	443	192.168.2.7	142.250.203.109
Oct 3, 2022 16:13:10.738132954 CEST	443	49695	142.250.203.109	192.168.2.7
Oct 3, 2022 16:13:10.738142014 CEST	49694	443	192.168.2.7	142.250.203.110
Oct 3, 2022 16:13:10.738153934 CEST	443	49694	142.250.203.110	192.168.2.7
Oct 3, 2022 16:13:10.738250971 CEST	443	49694	142.250.203.110	192.168.2.7
Oct 3, 2022 16:13:10.775610924 CEST	443	49694	142.250.203.110	192.168.2.7
Oct 3, 2022 16:13:10.775722027 CEST	49694	443	192.168.2.7	142.250.203.110
Oct 3, 2022 16:13:10.775749922 CEST	443	49694	142.250.203.110	192.168.2.7
Oct 3, 2022 16:13:10.775818110 CEST	443	49694	142.250.203.110	192.168.2.7
Oct 3, 2022 16:13:10.775876045 CEST	49694	443	192.168.2.7	142.250.203.110
Oct 3, 2022 16:13:10.787177086 CEST	49694	443	192.168.2.7	142.250.203.110
Oct 3, 2022 16:13:10.787206888 CEST	443	49694	142.250.203.110	192.168.2.7
Oct 3, 2022 16:13:10.796250105 CEST	443	49695	142.250.203.109	192.168.2.7
Oct 3, 2022 16:13:10.796330929 CEST	49695	443	192.168.2.7	142.250.203.109
Oct 3, 2022 16:13:10.796346903 CEST	443	49695	142.250.203.109	192.168.2.7
Oct 3, 2022 16:13:10.796514034 CEST	443	49695	142.250.203.109	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:13:10.796578884 CEST	49695	443	192.168.2.7	142.250.203.109
Oct 3, 2022 16:13:10.797718048 CEST	49695	443	192.168.2.7	142.250.203.109
Oct 3, 2022 16:13:10.797744036 CEST	443	49695	142.250.203.109	192.168.2.7
Oct 3, 2022 16:13:10.820744991 CEST	49696	443	192.168.2.7	108.179.193.164
Oct 3, 2022 16:13:10.901066065 CEST	443	49696	108.179.193.164	192.168.2.7
Oct 3, 2022 16:13:10.901134968 CEST	443	49696	108.179.193.164	192.168.2.7
Oct 3, 2022 16:13:10.901153088 CEST	443	49696	108.179.193.164	192.168.2.7
Oct 3, 2022 16:13:10.901199102 CEST	443	49696	108.179.193.164	192.168.2.7
Oct 3, 2022 16:13:10.901257038 CEST	49696	443	192.168.2.7	108.179.193.164
Oct 3, 2022 16:13:10.901309013 CEST	443	49696	108.179.193.164	192.168.2.7
Oct 3, 2022 16:13:10.901334047 CEST	49696	443	192.168.2.7	108.179.193.164
Oct 3, 2022 16:13:10.953160048 CEST	49699	443	192.168.2.7	108.179.193.164
Oct 3, 2022 16:13:10.953228951 CEST	443	49699	108.179.193.164	192.168.2.7
Oct 3, 2022 16:13:10.953331947 CEST	49699	443	192.168.2.7	108.179.193.164
Oct 3, 2022 16:13:10.968720913 CEST	49699	443	192.168.2.7	108.179.193.164
Oct 3, 2022 16:13:10.968763113 CEST	443	49699	108.179.193.164	192.168.2.7
Oct 3, 2022 16:13:10.979254007 CEST	49700	443	192.168.2.7	108.179.193.164
Oct 3, 2022 16:13:10.979316950 CEST	443	49700	108.179.193.164	192.168.2.7
Oct 3, 2022 16:13:10.979406118 CEST	49700	443	192.168.2.7	108.179.193.164
Oct 3, 2022 16:13:10.982249022 CEST	49700	443	192.168.2.7	108.179.193.164
Oct 3, 2022 16:13:10.982286930 CEST	443	49700	108.179.193.164	192.168.2.7
Oct 3, 2022 16:13:11.020703077 CEST	49696	443	192.168.2.7	108.179.193.164
Oct 3, 2022 16:13:11.046967030 CEST	443	49696	108.179.193.164	192.168.2.7
Oct 3, 2022 16:13:11.046993971 CEST	443	49696	108.179.193.164	192.168.2.7
Oct 3, 2022 16:13:11.047081947 CEST	443	49696	108.179.193.164	192.168.2.7
Oct 3, 2022 16:13:11.047096968 CEST	443	49696	108.179.193.164	192.168.2.7
Oct 3, 2022 16:13:11.047132015 CEST	49696	443	192.168.2.7	108.179.193.164
Oct 3, 2022 16:13:11.047142982 CEST	443	49696	108.179.193.164	192.168.2.7
Oct 3, 2022 16:13:11.047183037 CEST	49696	443	192.168.2.7	108.179.193.164
Oct 3, 2022 16:13:11.047198057 CEST	443	49696	108.179.193.164	192.168.2.7
Oct 3, 2022 16:13:11.047205925 CEST	49696	443	192.168.2.7	108.179.193.164
Oct 3, 2022 16:13:11.047244072 CEST	49696	443	192.168.2.7	108.179.193.164
Oct 3, 2022 16:13:11.195286989 CEST	49696	443	192.168.2.7	108.179.193.164
Oct 3, 2022 16:13:11.195362091 CEST	443	49696	108.179.193.164	192.168.2.7
Oct 3, 2022 16:13:11.245536089 CEST	49702	443	192.168.2.7	142.250.203.100
Oct 3, 2022 16:13:11.245613098 CEST	443	49702	142.250.203.100	192.168.2.7
Oct 3, 2022 16:13:11.245743036 CEST	49702	443	192.168.2.7	142.250.203.100
Oct 3, 2022 16:13:11.249059916 CEST	49702	443	192.168.2.7	142.250.203.100
Oct 3, 2022 16:13:11.249090910 CEST	443	49702	142.250.203.100	192.168.2.7
Oct 3, 2022 16:13:11.270061970 CEST	443	49699	108.179.193.164	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:13:09.396327972 CEST	59058	53	192.168.2.7	8.8.8.8
Oct 3, 2022 16:13:09.402843952 CEST	54875	53	192.168.2.7	8.8.8.8
Oct 3, 2022 16:13:09.417613983 CEST	59477	53	192.168.2.7	8.8.8.8
Oct 3, 2022 16:13:09.420639992 CEST	53	54875	8.8.8.8	192.168.2.7
Oct 3, 2022 16:13:09.443137884 CEST	53	59477	8.8.8.8	192.168.2.7
Oct 3, 2022 16:13:09.549377918 CEST	53	59058	8.8.8.8	192.168.2.7
Oct 3, 2022 16:13:11.200690985 CEST	56588	53	192.168.2.7	8.8.8.8
Oct 3, 2022 16:13:11.220202923 CEST	53	56588	8.8.8.8	192.168.2.7
Oct 3, 2022 16:13:14.385890961 CEST	50505	53	192.168.2.7	8.8.8.8
Oct 3, 2022 16:13:14.538032055 CEST	53	50505	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 3, 2022 16:13:09.396327972 CEST	192.168.2.7	8.8.8.8	0x463a	Standard query (0)	amigodepatasbh.com.br	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:13:09.402843952 CEST	192.168.2.7	8.8.8.8	0x6900	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:13:09.417613983 CEST	192.168.2.7	8.8.8.8	0x3e08	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:13:11.200690985 CEST	192.168.2.7	8.8.8.8	0xd4b5	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:13:14.385890961 CEST	192.168.2.7	8.8.8.8	0xb6e9	Standard query (0)	amigodepatasbh.com.br	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
Oct 3, 2022 16:13:09.420639992 CEST	8.8.8.8	192.168.2.7	0x6900	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Oct 3, 2022 16:13:09.420639992 CEST	8.8.8.8	192.168.2.7	0x6900	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:13:09.443137884 CEST	8.8.8.8	192.168.2.7	0x3e08	No error (0)	accounts.google.com		142.250.203.109	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:13:09.549377918 CEST	8.8.8.8	192.168.2.7	0x463a	No error (0)	amigodepatasbh.com.br		108.179.193.164	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:13:11.220202923 CEST	8.8.8.8	192.168.2.7	0xd4b5	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:13:14.538032055 CEST	8.8.8.8	192.168.2.7	0xb6e9	No error (0)	amigodepatasbh.com.br		108.179.193.164	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- amigodepatasbh.com.br
- clients2.google.com
- accounts.google.com
- https:

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49696	108.179.193.164	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:13:10 UTC	0	OUT	GET /ff HTTP/1.1 Host: amigodepatasbh.com.br Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 sec-ch-ua-platform: "Windows" Upgrade-Insecure-Requests: 1 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: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:13:10 UTC	5	IN	HTTP/1.1 403 Forbidden Date: Mon, 03 Oct 2022 14:13:10 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Thu, 15 Sep 2022 10:04:04 GMT Accept-Ranges: bytes Content-Length: 22122 Vary: Accept-Encoding Content-Type: text/html
2022-10-03 14:13:10 UTC	5	IN	Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 5d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 36 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0d 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 37 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0d 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 38 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0d 0a 3c 21 2d 2d 5b 69 66 20 67 74 20 49 45 20 38 5d 3e 3c 21 Data Ascii: <!doctype html>...[if lt IE 7]> <html class="no-js ie6 oldie" lang="en"> <![endif]-->...[if IE 7]> <html class="no-js ie7 oldie" lang="en"> <![endif]-->...[if IE 8]> <html class="no-js ie8 oldie" lang="en"> <![endif]-->...[if gt IE 8]><!
2022-10-03 14:13:11 UTC	13	IN	Data Raw: 70 74 73 20 69 6e 64 69 76 69 64 75 61 69 73 20 71 75 65 20 64 65 76 65 6d 20 73 65 72 20 65 78 65 63 75 74 61 64 6f 73 20 61 74 72 61 76 c3 a9 73 20 64 65 20 73 6f 6c 69 63 69 74 61 c3 a7 c3 b5 65 73 2e 20 41 6c 67 75 6e 73 20 64 65 73 74 65 73 20 73 c3 a3 6f 20 6d 61 69 73 20 66 c3 a1 63 65 69 73 20 64 65 20 65 6e 63 6f 6e 74 72 61 72 20 65 20 63 6f 72 72 69 67 69 72 20 64 6f 20 71 75 65 20 6f 75 74 72 6f 73 2e 3c 2f 70 3e 0d 0a 09 09 09 09 09 09 3c 68 34 3e 50 72 6f 70 72 69 65 64 61 64 65 20 64 65 20 41 72 71 75 69 76 6f 73 20 65 20 44 69 72 65 74 c3 b3 72 69 6f 73 3c 2f 68 34 3e 0d 0a 09 09 09 09 09 09 3c 70 3e 4f 20 73 65 72 76 69 64 6f 72 20 6e 6f 20 71 75 61 6c 20 76 6f 63 c3 aa 20 65 73 74 c3 a1 20 68 6f 73 70 65 64 61 64 6f 20 72 6f 64 61 Data Ascii: pts individuais que devem ser executados atravs de solicitaes. Alguns destes so mais fceis de encontrar e corrigir do que outros. Propriedade de Arquivos e Diretrios O servidor no qual voc est hospedado roda
2022-10-03 14:13:11 UTC	20	IN	Data Raw: 64 6f 73 20 63 65 6e c3 a1 72 69 6f 73 2c 20 65 20 61 66 65 74 61 20 64 69 72 65 74 61 6d 65 6e 74 65 20 6f 20 66 75 6e 63 69 6f 6e 61 6d 65 6e 74 6f 20 64 65 20 73 65 75 20 77 65 62 73 69 74 65 2e 3c 2f 70 3e 0d 0a 09 09 09 09 09 09 3c 70 3e 52 65 64 69 72 65 63 69 6f 6e 61 6d 65 6e 74 6f 73 20 65 20 72 65 65 73 63 72 69 74 61 73 20 64 65 20 55 52 4c 20 73 c3 a3 6f 20 64 75 61 73 20 64 69 72 65 74 69 76 61 73 20 63 6f 6d 75 6e 73 20 65 6e 63 6f 6e 74 72 61 64 61 73 20 6e 6f 20 2e 68 74 61 63 63 65 73 73 20 65 20 6d 75 69 74 6f 73 20 73 63 72 69 70 74 73 2c 20 63 6f 6d 6f 20 6f 20 57 6f 72 64 50 72 65 73 73 2c 20 44 72 75 70 61 6c 2c 20 4a 6f 6f 6d 6c 61 20 65 20 4d 61 67 65 6e 74 6f 2c 20 70 6f 72 20 65 78 65 6d 70 6c 6f 2c 20 61 64 69 63 69 6f 6e 61 Data Ascii: dos cenrios, e afeta diretamente o funcionamento de seu website. Redirecionamentos e reescritas de URL so duas diretivas comuns encontradas no .htaccess e muitos scripts, como o WordPress, Drupal, Joomla e Magento, por exemplo, adiciona

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.7	49694	142.250.203.110	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:13:10 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
2022-10-03 14:13:10 UTC	1	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-LgIM7TIOhRcqa-rH90-SKw' '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: Mon, 03 Oct 2022 14:13:10 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5754 X-Daystart: 25990 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
2022-10-03 14:13:10 UTC	2	IN	Data Raw: 32 63 39 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 35 34 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 32 35 39 39 30 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: 2c9<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" protocol="2.0" server="prod"><daystart elapsed_days="5754" elapsed_seconds="25990"/><app appid="nmmhkkegccagdldgiimedpiccmgmieda" cohort="1::" cohortname=""
2022-10-03 14:13:10 UTC	3	IN	Data Raw: 6d 78 76 59 6e 4d 76 4e 7a 49 30 51 55 46 58 4e 56 39 7a 54 32 52 76 64 55 77 79 4d 45 52 45 53 45 5a 47 56 6d 4a 6e 51 51 2f 31 2e 30 2e 30 2e 36 5f 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 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 Data Ascii: mxvYnMvNzI0QUFXNV9zT2RvdUwyMERESEZGVmJnQQ/1.0.0.6_nmmhkkegccagdldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" protected="0" si
2022-10-03 14:13:10 UTC	3	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.7	49695	142.250.203.109	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:13:10 UTC	1	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
2022-10-03 14:13:10 UTC	1	OUT	Data Raw: 20 Data Ascii:
2022-10-03 14:13:10 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: Mon, 03 Oct 2022 14:13:10 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/IdentityListAccountsHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-3a6F-DJLTKjduZ2nICNjeg' '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 Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-wow64=*, 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-WoW64, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Cross-Origin-Opener-Policy: same-origin 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
2022-10-03 14:13:10 UTC	5	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",[]]
2022-10-03 14:13:10 UTC	5	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.7	49699	108.179.193.164	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:13:11 UTC	26	OUT	GET /cgi-sys/js/jquery-1.11.2.min.js HTTP/1.1 Host: amigodepatasbh.com.br Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 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 sec-ch-ua-platform: "Windows" Accept: */* Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: script Referer: https://amigodepatasbh.com.br/ff Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 14:13:11 UTC	28	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:13:11 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Thu, 15 Sep 2022 10:04:05 GMT Accept-Ranges: bytes Content-Length: 95935 Vary: Accept-Encoding Content-Type: application/javascript
2022-10-03 14:13:11 UTC	28	IN	Data Raw: 2f 2a 21 20 6a 51 75 65 72 79 20 76 31 2e 31 31 2e 32 20 7c 20 28 63 29 20 32 30 30 35 2c 20 32 30 31 34 20 6a 51 75 65 72 79 20 46 6f 75 6e 64 61 74 69 6f 6e 2c 20 49 6e 63 2e 20 7c 20 6a 71 75 65 72 79 2e 6f 72 67 2f 6c 69 63 65 6e 73 65 20 2a 2f 0d 0a 21 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 6d 6f 64 75 6c 65 26 26 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 6d 6f 64 75 6c 65 2e 65 78 70 6f 72 74 73 3f 6d 6f 64 75 6c 65 2e 65 78 70 6f 72 74 73 3d 61 2e 64 6f 63 75 6d 65 6e 74 3f 62 28 61 2c 21 30 29 3a 66 75 6e 63 74 69 6f 6e 28 61 29 7b 69 66 28 21 61 2e 64 6f 63 75 6d 65 6e 74 29 74 68 72 6f 77 20 6e 65 77 20 45 72 72 6f 72 28 22 6a 51 75 65 72 79 20 72 65 71 75 69 72 65 73 20 61 20 77 69 Data Ascii: /*! jQuery v1.11.2 | (c) 2005, 2014 jQuery Foundation, Inc. | jquery.org/license */!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a wi
2022-10-03 14:13:11 UTC	38	IN	Data Raw: 7c 7c 43 29 3b 69 66 28 64 29 72 65 74 75 72 6e 20 64 3b 69 66 28 63 29 77 68 69 6c 65 28 63 3d 63 2e 6e 65 78 74 53 69 62 6c 69 6e 67 29 69 66 28 63 3d 3d 3d 62 29 72 65 74 75 72 6e 2d 31 3b 72 65 74 75 72 6e 20 61 3f 31 3a 2d 31 7d 66 75 6e 63 74 69 6f 6e 20 6d 62 28 61 29 7b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 62 29 7b 76 61 72 20 63 3d 62 2e 6e 6f 64 65 4e 61 6d 65 2e 74 6f 4c 6f 77 65 72 43 61 73 65 28 29 3b 72 65 74 75 72 6e 22 69 6e 70 75 74 22 3d 3d 63 26 26 62 2e 74 79 70 65 3d 3d 3d 61 7d 7d 66 75 6e 63 74 69 6f 6e 20 6e 62 28 61 29 7b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 62 29 7b 76 61 72 20 63 3d 62 2e 6e 6f 64 65 4e 61 6d 65 2e 74 6f 4c 6f 77 65 72 43 61 73 65 28 29 3b 72 65 74 75 72 6e 28 22 69 6e 70 75 74 22 3d 3d Data Ascii: ||C);if(d)return d;if(c)while(c=c.nextSibling)if(c===b)return-1;return a?1:-1}function mb(a){return function(b){var c=b.nodeName.toLowerCase();return"input"===c&&b.type===a}}function nb(a){return function(b){var c=b.nodeName.toLowerCase();return("input"==
2022-10-03 14:13:11 UTC	46	IN	Data Raw: 2c 66 5b 67 5d 29 2c 61 5b 64 5d 3d 21 28 63 5b 64 5d 3d 66 5b 67 5d 29 7d 29 3a 66 75 6e 63 74 69 6f 6e 28 61 29 7b 72 65 74 75 72 6e 20 65 28 61 2c 30 2c 63 29 7d 29 3a 65 7d 7d 2c 70 73 65 75 64 6f 73 3a 7b 6e 6f 74 3a 69 62 28 66 75 6e 63 74 69 6f 6e 28 61 29 7b 76 61 72 20 62 3d 5b 5d 2c 63 3d 5b 5d 2c 64 3d 68 28 61 2e 72 65 70 6c 61 63 65 28 52 2c 22 24 31 22 29 29 3b 72 65 74 75 72 6e 20 64 5b 75 5d 3f 69 62 28 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 2c 65 29 7b 76 61 72 20 66 2c 67 3d 64 28 61 2c 6e 75 6c 6c 2c 65 2c 5b 5d 29 2c 68 3d 61 2e 6c 65 6e 67 74 68 3b 77 68 69 6c 65 28 68 2d 2d 29 28 66 3d 67 5b 68 5d 29 26 26 28 61 5b 68 5d 3d 21 28 62 5b 68 5d 3d 66 29 29 7d 29 3a 66 75 6e 63 74 69 6f 6e 28 61 2c 65 2c 66 29 7b 72 65 74 75 72 6e 20 Data Ascii: ,f[g]),a[d]=!(c[d]=f[g])}):function(a){return e(a,0,c)}):e}},pseudos:{not:ib(function(a){var b=[],c=[],d=h(a.replace(R,"$1"));return d[u]?ib(function(a,b,c,e){var f,g=d(a,null,e,[]),h=a.length;while(h--)(f=g[h])&&(a[h]=!(b[h]=f))}):function(a,e,f){ return
2022-10-03 14:13:11 UTC	54	IN	Data Raw: 69 73 2e 70 75 73 68 53 74 61 63 6b 28 77 28 74 68 69 73 2c 61 7c 7c 5b 5d 2c 21 30 29 29 7d 2c 69 73 3a 66 75 6e 63 74 69 6f 6e 28 61 29 7b 72 65 74 75 72 6e 21 21 77 28 74 68 69 73 2c 22 73 74 72 69 6e 67 22 3d 3d 74 79 70 65 6f 66 20 61 26 26 74 2e 74 65 73 74 28 61 29 3f 6d 28 61 29 3a 61 7c 7c 5b 5d 2c 21 31 29 2e 6c 65 6e 67 74 68 7d 7d 29 3b 76 61 72 20 78 2c 79 3d 61 2e 64 6f 63 75 6d 65 6e 74 2c 7a 3d 2f 5e 28 3f 3a 5c 73 2a 28 3c 5b 5c 77 5c 57 5d 2b 3e 29 5b 5e 3e 5d 2a 7c 23 28 5b 5c 77 2d 5d 2a 29 29 24 2f 2c 41 3d 6d 2e 66 6e 2e 69 6e 69 74 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 76 61 72 20 63 2c 64 3b 69 66 28 21 61 29 72 65 74 75 72 6e 20 74 68 69 73 3b 69 66 28 22 73 74 72 69 6e 67 22 3d 3d 74 79 70 65 6f 66 20 61 29 7b 69 66 28 63 Data Ascii: is.pushStack(w(this,a||[],!0))},is:function(a){return!!w(this,"string"==typeof a&&t.test(a)?m(a):a||[],!1).length}});var x,y=a.document,z=/^(?:\s*(<[\w\W]+>)[^>]*|#([\w-]*))$/,A=m.fn.init=function(a,b){var c,d;if(!a)return this;if("string "==typeof a){if(c
2022-10-03 14:13:11 UTC	62	IN	Data Raw: 6e 75 6c 6c 3a 2b 63 2b 22 22 3d 3d 3d 63 3f 2b 63 3a 4d 2e 74 65 73 74 28 63 29 3f 6d 2e 70 61 72 73 65 4a 53 4f 4e 28 63 29 3a 63 7d 63 61 74 63 68 28 65 29 7b 7d 6d 2e 64 61 74 61 28 61 2c 62 2c 63 29 7d 65 6c 73 65 20 63 3d 76 6f 69 64 20 30 7d 72 65 74 75 72 6e 20 63 7d 66 75 6e 63 74 69 6f 6e 20 50 28 61 29 7b 76 61 72 20 62 3b 66 6f 72 28 62 20 69 6e 20 61 29 69 66 28 28 22 64 61 74 61 22 21 3d 3d 62 7c 7c 21 6d 2e 69 73 45 6d 70 74 79 4f 62 6a 65 63 74 28 61 5b 62 5d 29 29 26 26 22 74 6f 4a 53 4f 4e 22 21 3d 3d 62 29 72 65 74 75 72 6e 21 31 3b 0d 0a 72 65 74 75 72 6e 21 30 7d 66 75 6e 63 74 69 6f 6e 20 51 28 61 2c 62 2c 64 2c 65 29 7b 69 66 28 6d 2e 61 63 63 65 70 74 44 61 74 61 28 61 29 29 7b 76 61 72 20 66 2c 67 2c 68 3d 6d 2e 65 78 70 61 6e 64 Data Ascii: null:+c+""===c?+c:M.test(c)?m.parseJSON(c):c}catch(e){}m.data(a,b,c)}else c=void 0}return c}function P(a){var b;for(b in a)if(("data"!==b||!m.isEmptyObject(a[b]))&&"toJSON"!==b)return!1;return!0}function Q(a,b,d,e){if(m.acceptData(a)){var f,g,h=m.expand

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:13:11 UTC	69	IN	Data Raw: 6b 2e 5f 64 65 66 61 75 6c 74 2e 61 70 70 6c 79 28 6f 2e 70 6f 70 28 29 2c 63 29 3d 3d 3d 21 31 29 26 26 6d 2e 61 63 63 65 70 74 44 61 74 61 28 64 29 26 26 67 26 26 64 5b 70 5d 26 26 21 6d 2e 69 73 57 69 6e 64 6f 77 28 64 29 29 7b 6c 3d 64 5b 67 5d 2c 6c 26 26 28 64 5b 67 5d 3d 6e 75 6c 6c 29 2c 6d 2e 65 76 65 6e 74 2e 74 72 69 67 67 65 72 65 64 3d 70 3b 74 72 79 7b 64 5b 70 5d 28 29 7d 63 61 74 63 68 28 72 29 7b 7d 6d 2e 65 76 65 6e 74 2e 74 72 69 67 67 65 72 65 64 3d 76 6f 69 64 20 30 2c 6c 26 26 28 64 5b 67 5d 3d 6c 29 7d 72 65 74 75 72 6e 20 62 2e 72 65 73 75 6c 74 7d 7d 2c 64 69 73 70 61 74 63 68 3a 66 75 6e 63 74 69 6f 6e 28 61 29 7b 61 3d 6d 2e 65 76 65 6e 74 2e 66 69 78 28 61 29 3b 76 61 72 20 62 2c 63 2c 65 2c 66 2c 67 2c 68 3d 5b 5d 2c 69 3d 64 Data Ascii: k._default.apply(o.pop(),c)===!1)&&m.acceptData(d)&&g&&d[p]&&!m.isWindow(d)){l=d[g],l&&(d[g]=null) ,m.event.triggered=p;try{d[p]()}catch(r){}m.event.triggered=void 0,l&&(d[g]=l)}return b.result}},dispatch:function(a){a= m.event.fix(a);var b,c,e,f,g,h=[],i=d
2022-10-03 14:13:11 UTC	77	IN	Data Raw: 73 74 7c 64 65 74 61 69 6c 73 7c 66 69 67 63 61 70 74 69 6f 6e 7c 66 69 67 75 72 65 7c 66 6f 6f 74 65 72 7c 68 65 61 64 65 72 7c 68 67 72 6f 75 70 7c 6d 61 72 6b 7c 6d 65 74 65 72 7c 6e 61 76 7c 6f 75 74 70 75 74 7c 70 72 6f 67 72 65 73 73 7c 73 65 63 74 69 6f 6e 7c 73 75 6d 6d 61 72 79 7c 74 69 6d 65 7c 76 69 64 65 6f 22 2c 66 62 3d 2f 20 6a 51 75 65 72 79 5c 64 2b 3d 22 28 3f 3a 6e 75 6c 6c 7c 5c 64 2b 29 22 2f 67 2c 67 62 3d 6e 65 77 20 52 65 67 45 78 70 28 22 3c 28 3f 3a 22 2b 65 62 2b 22 29 5b 5c 5c 73 2f 3e 5d 22 2c 22 69 22 29 2c 68 62 3d 2f 5e 5c 73 2b 2f 2c 69 62 3d 2f 3c 28 3f 21 61 72 65 61 7c 62 72 7c 63 6f 6c 7c 65 6d 62 65 64 7c 68 72 7c 69 6d 67 7c 69 6e 70 75 74 7c 6c 69 6e 6b 7c 6d 65 74 61 7c 70 61 72 61 6d 29 28 28 5b 5c 77 3a 5d 2b 29 Data Ascii: st|details|figcaption|figure|footer|header|hgroup|mark|meter|nav|output|progress|section|summary|time|video" ,fb=/ jQuery\d+="(?:null|\d+)"/g,gb=new RegExp("<(?:"+eb+")[\\s/>]","i"),hb=/^\s+/,ib=/<(?!area|br|col|embed|hr|img|inpu t|link|meta|param)(([\w:]+)
2022-10-03 14:13:11 UTC	85	IN	Data Raw: 64 54 6f 28 62 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 29 2c 62 3d 28 43 62 5b 30 5d 2e 63 6f 6e 74 65 6e 74 57 69 6e 64 6f 77 7c 7c 43 62 5b 30 5d 2e 63 6f 6e 74 65 6e 74 44 6f 63 75 6d 65 6e 74 29 2e 64 6f 63 75 6d 65 6e 74 2c 62 2e 77 72 69 74 65 28 29 2c 62 2e 63 6c 6f 73 65 28 29 2c 63 3d 45 62 28 61 2c 62 29 2c 43 62 2e 64 65 74 61 63 68 28 29 29 2c 44 62 5b 5d 3d 63 29 2c 63 7d 21 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 61 3b 6b 2e 73 68 72 69 6e 6b 57 72 61 70 42 6c 6f 63 6b 73 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 69 66 28 6e 75 6c 6c 21 3d 61 29 72 65 74 75 72 6e 20 61 3b 61 3d 21 31 3b 76 61 72 20 62 2c 63 2c 64 3b 72 65 74 75 72 6e 20 63 3d 79 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 62 6f 64 79 22 29 Data Ascii: dTo(b.documentElement),b=(Cb[0].contentWindow||Cb[0].contentDocument).document,b.write(),b.close() ,c=Eb(a,b),Cb.detach()),Db[a]=c),c}!function(){var a;k.shrinkWrapBlocks=function(){if(null!=a)return a;a=!1;var b,c,d;return c=y.getElementsByTagName("body")
2022-10-03 14:13:11 UTC	93	IN	Data Raw: 21 30 29 7d 2c 68 69 64 65 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 56 62 28 74 68 69 73 29 7d 2c 74 6f 67 67 6c 65 3a 66 75 6e 63 74 69 6f 6e 28 61 29 7b 72 65 74 75 72 6e 22 62 6f 6f 6c 65 61 6e 22 3d 3d 74 79 70 65 6f 66 20 61 3f 61 3f 74 68 69 73 2e 73 68 6f 77 28 29 3a 74 68 69 73 2e 68 69 64 65 28 29 3a 74 68 69 73 2e 65 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 29 7b 55 28 74 68 69 73 29 3f 6d 28 74 68 69 73 29 2e 73 68 6f 77 28 29 3a 6d 28 74 68 69 73 29 2e 68 69 64 65 28 29 7d 29 7d 7d 29 3b 66 75 6e 63 74 69 6f 6e 20 5a 62 28 61 2c 62 2c 63 2c 64 2c 65 29 7b 72 65 74 75 72 6e 20 6e 65 77 20 5a 62 2e 70 72 6f 74 6f 74 79 70 65 2e 69 6e 69 74 28 61 2c 62 2c 63 2c 64 2c 65 29 0d 0a 7d 6d 2e 54 77 65 65 6e 3d 5a 62 2c 5a 62 2e 70 72 6f Data Ascii: !0)},hide:function(){return Vb(this)},toggle:function(a){return"boolean"==typeof a?a?this.show():this.hide() :this.each(function(){U(this)?m(this).show():m(this).hide()})}});function Zb(a,b,c,d,e){return new Zb.prototype.init(a,b ,c,d,e)}m.Tween=Zb,Zb.pro
2022-10-03 14:13:11 UTC	101	IN	Data Raw: 20 74 79 70 65 3d 27 63 68 65 63 6b 62 6f 78 27 2f 3e 22 2c 64 3d 62 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 61 22 29 5b 30 5d 2c 63 3d 79 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 73 65 6c 65 63 74 22 29 2c 65 3d 63 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 79 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 6f 70 74 69 6f 6e 22 29 29 2c 61 3d 62 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 69 6e 70 75 74 22 29 5b 30 5d 2c 64 2e 73 74 79 6c 65 2e 63 73 73 54 65 78 74 3d 22 74 6f 70 3a 31 70 78 22 2c 6b 2e 67 65 74 53 65 74 41 74 74 72 69 62 75 74 65 3d 22 74 22 21 3d 3d 62 2e 63 6c 61 73 73 4e 61 6d 65 2c 6b 2e 73 74 79 6c 65 3d 2f 74 6f 70 2f 2e 74 65 73 74 28 64 2e 67 65 74 41 74 74 72 69 62 75 74 Data Ascii: type='checkbox'/>",d=b.getElementsByTagName("a")[0],c=y.createElement("select"),e=c.appendChild(y .createElement("option")),a=b.getElementsByTagName("input")[0],d.style.cssText="top:1px",k.getSetAttribute="t" !==b.className,k.style=/top/.test(d.getAttribut
2022-10-03 14:13:11 UTC	108	IN	Data Raw: 7b 29 7c 28 7d 7c 5d 29 7c 22 28 3f 3a 5b 5e 22 5c 5c 5c 72 5c 6e 5d 7c 5c 5c 5b 22 5c 5c 5c 2f 62 66 6e 72 74 5d 7c 5c 5c 75 5b 5c 64 61 2d 66 41 2d 46 5d 7b 34 7d 29 2a 22 5c 73 2a 3a 3f 7c 74 72 75 65 7c 66 61 6c 73 65 7c 6e 75 6c 6c 7c 2d 3f 28 3f 21 30 5c 64 29 5c 64 2b 28 3f 3a 5c 2e 5c 64 2b 7c 29 28 3f 3a 5b 65 45 5d 5b 2b 2d 5d 3f 5c 64 2b 7c 29 2f 67 3b 6d 2e 70 61 72 73 65 4a 53 4f 4e 3d 66 75 6e 63 74 69 6f 6e 28 62 29 7b 69 66 28 61 2e 4a 53 4f 4e 26 26 61 2e 4a 53 4f 4e 2e 70 61 72 73 65 29 72 65 74 75 72 6e 20 61 2e 4a 53 4f 4e 2e 70 61 72 73 65 28 62 2b 22 22 29 3b 76 61 72 20 63 2c 64 3d 6e 75 6c 6c 2c 65 3d 6d 2e 74 72 69 6d 28 62 2b 22 22 29 3b 72 65 74 75 72 6e 20 65 26 26 21 6d 2e 74 72 69 6d 28 65 2e 72 65 70 6c 61 63 65 28 78 63 2c Data Ascii: {)|(}|])|"(?:[^"\\\r\n]|\["\\\bfnrt]|\u[\da-fA-F]{4})*"\s*:?|true|false|null|-?(?!0\d)\d+(?:\.\d+|)(?:[eE][+-]?\d+|)/g;m.pars eJSON=function(b){if(a.JSON&&a.JSON.parse)return a.JSON.parse(b+"");var c,d=null,e=m.trim(b+"");return e&&!m.t rim(e.replace(xc,
2022-10-03 14:13:11 UTC	116	IN	Data Raw: 74 7c 74 65 78 74 61 72 65 61 7c 6b 65 79 67 65 6e 29 2f 69 3b 66 75 6e 63 74 69 6f 6e 20 56 63 28 61 2c 62 2c 63 2c 64 29 7b 76 61 72 20 65 3b 69 66 28 6d 2e 69 73 41 72 72 61 79 28 62 29 29 6d 2e 65 61 63 68 28 62 2c 66 75 6e 63 74 69 6f 6e 28 62 2c 65 29 7b 63 7c 7c 52 63 2e 74 65 73 74 28 61 29 3f 64 28 61 2c 65 29 3a 56 63 28 61 2b 22 5b 22 2b 28 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 65 3f 62 3a 22 22 29 2b 22 5d 22 2c 65 2c 63 2c 64 29 7d 29 3b 65 6c 73 65 20 69 66 28 63 7c 7c 22 6f 62 6a 65 63 74 22 21 3d 3d 6d 2e 74 79 70 65 28 62 29 29 64 28 61 2c 62 29 3b 65 6c 73 65 20 66 6f 72 28 65 20 69 6e 20 62 29 56 63 28 61 2b 22 5b 22 2b 65 2b 22 5d 22 2c 62 5b 65 5d 2c 63 2c 64 29 7d 6d 2e 70 61 72 61 6d 3d 66 75 6e 63 74 69 6f 6e 28 61 2c Data Ascii: t|textarea|keygen)/i;function Vc(a,b,c,d){var e;if(m.isArray(b))m.each(b,function(b,e){c||Rc.test(a)?d(a,e):Vc(a+" ["+("object"==typeof e?b:"")+"]",e,c,d)});else if(c||"object"!==m.type(b))d(a,b);else for(e in b)Vc(a+"["+e+"]",b[e],c,d)}m. param=function(a,
2022-10-03 14:13:11 UTC	124	IN	Data Raw: 2e 24 3d 6d 29 2c 6d 7d 29 3b 0d 0a Data Ascii: .$=m),m});

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.7	49700	108.179.193.164	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:13:11 UTC	27	OUT	GET /cgi-sys/images/logo-403-page.png HTTP/1.1 Host: amigodepatasbh.com.br Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 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 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://amigodepatasbh.com.br/ff Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 14:13:11 UTC	36	IN	HTTP/1.1 404 Not Found Date: Mon, 03 Oct 2022 14:13:11 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Thu, 15 Sep 2022 10:04:08 GMT Accept-Ranges: bytes Content-Length: 2361 Vary: Accept-Encoding Content-Type: text/html
2022-10-03 14:13:11 UTC	36	IN	Data Raw: 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 70 74 2d 42 52 22 3e 0d 0a 20 20 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 38 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 66 6f 72 6d 61 74 2d 64 65 74 65 63 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 6c Data Ascii: <!DOCTYPE html><html lang="pt-BR"> <head> <meta charset="UTF-8"> <meta http-equiv="X-UA-Compatible" content="IE=edge"> <meta name="viewport" content="width=device-width, initial-scale=1"> <meta name="format-detection" content="tel

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.7	49705	108.179.193.164	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:13:12 UTC	124	OUT	GET /cgi-sys/images/favicon.png HTTP/1.1 Host: amigodepatasbh.com.br Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 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 sec-ch-ua-platform: "Windows" Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://amigodepatasbh.com.br/ff Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 14:13:13 UTC	125	IN	HTTP/1.1 404 Not Found Date: Mon, 03 Oct 2022 14:13:13 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Thu, 15 Sep 2022 10:04:08 GMT Accept-Ranges: bytes Content-Length: 2361 Vary: Accept-Encoding Content-Type: text/html
2022-10-03 14:13:13 UTC	125	IN	Data Raw: 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 70 74 2d 42 52 22 3e 0d 0a 20 20 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 38 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 66 6f 72 6d 61 74 2d 64 65 74 65 63 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 6c Data Ascii: <!DOCTYPE html><html lang="pt-BR"> <head> <meta charset="UTF-8"> <meta http-equiv="X-UA-Compatible" content="IE=edge"> <meta name="viewport" content="width=device-width, initial-scale=1"> <meta name="format-detection" content="tel

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.7	49711	108.179.193.164	443	C:\Program Files\Google\Chrome\Application\chrome.exe

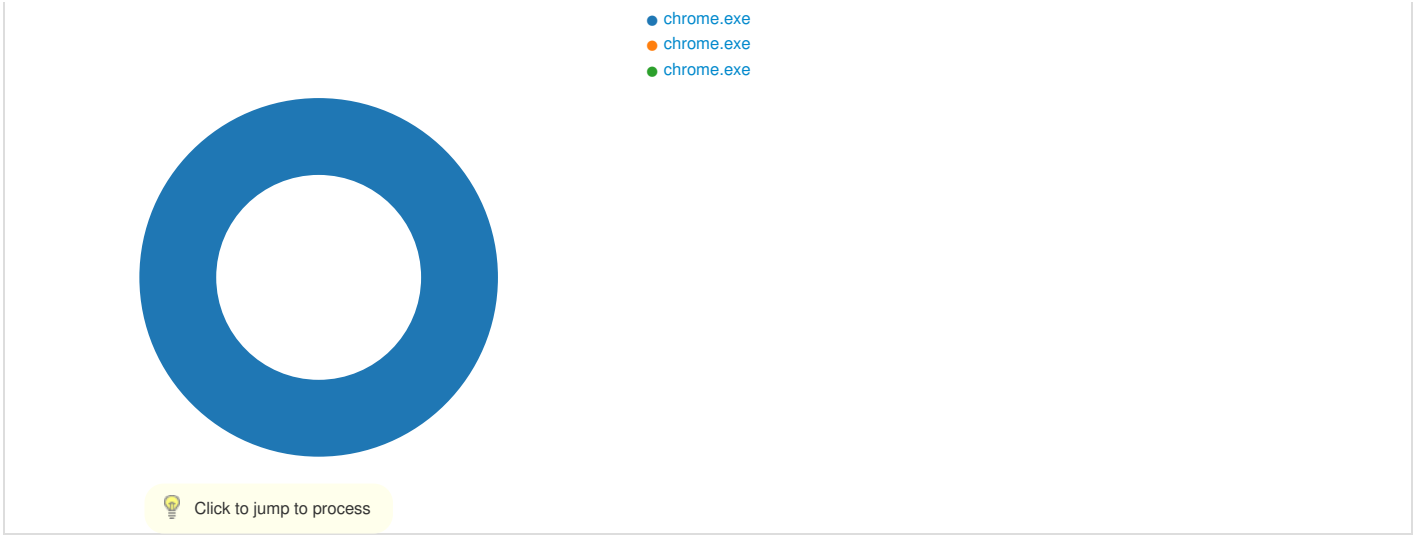
Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:13:15 UTC	127	OUT	GET /cgi-sys/images/logo-403-page.png HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: amigodepatasbh.com.br
2022-10-03 14:13:15 UTC	130	IN	HTTP/1.1 404 Not Found Date: Mon, 03 Oct 2022 14:13:15 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Thu, 15 Sep 2022 10:04:08 GMT Accept-Ranges: bytes Content-Length: 2361 Vary: Accept-Encoding Content-Type: text/html
2022-10-03 14:13:15 UTC	130	IN	Data Raw: 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 70 74 2d 42 52 22 3e 0d 0a 20 20 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 38 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 66 6f 72 6d 61 74 2d 64 65 74 65 63 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 6c Data Ascii: <!DOCTYPE html><html lang="pt-BR"> <head> <meta charset="UTF-8"> <meta http-equiv="X-UA-Compatible" content="IE=edge"> <meta name="viewport" content="width=device-width, initial-scale=1"> <meta name="format-detection" content="tel

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.7	49710	108.179.193.164	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 14:13:15 UTC	127	OUT	GET /cgi-sys/images/favicon.png HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: amigodepatasbh.com.br
2022-10-03 14:13:15 UTC	128	IN	HTTP/1.1 404 Not Found Date: Mon, 03 Oct 2022 14:13:15 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Thu, 15 Sep 2022 10:04:08 GMT Accept-Ranges: bytes Content-Length: 2361 Vary: Accept-Encoding Content-Type: text/html
2022-10-03 14:13:15 UTC	128	IN	Data Raw: 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 70 74 2d 42 52 22 3e 0d 0a 20 20 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 38 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 66 6f 72 6d 61 74 2d 64 65 74 65 63 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 6c Data Ascii: <!DOCTYPE html><html lang="pt-BR"> <head> <meta charset="UTF-8"> <meta http-equiv="X-UA-Compatible" content="IE=edge"> <meta name="viewport" content="width=device-width, initial-scale=1"> <meta name="format-detection" content="tel

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 5688, Parent PID: 2704

General

Target ID:	0
Start time:	16:13:04
Start date:	03/10/2022
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:	0x7ff7c2920000
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: 5880, Parent PID: 5688

General

Target ID:	1
Start time:	16:13:06
Start date:	03/10/2022
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=1968 --field-trial-handle=1732,i,8218220987001890426,18157507330322035723,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff7c2920000
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: **2828**, Parent PID: **2704**

General

Target ID:	2
Start time:	16:13:07
Start date:	03/10/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "https://amigodepatasbh.com.br/ff
Imagebase:	0x7ff7c2920000
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