ID: 383544
Cookbook: browseurl.jbs
Time: 22:21:36
Date: 07/04/2021
Version: 31.0.0 Emerald

Table of Contents

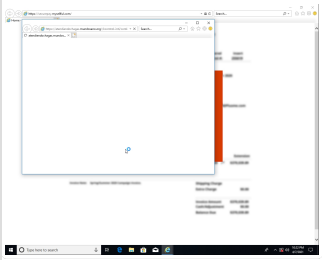
Analysis Report https://securepay.mysellful.com/

Overview

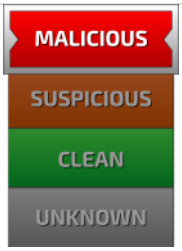
General Information

Sample URL:	http://https://securepay.mysellful.com/
Analysis ID:	383544
Infos:	

Most interesting Screenshot:



Detection



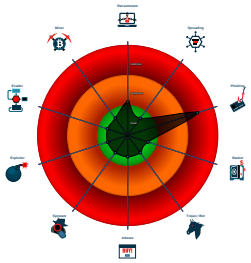
HTMLPhisher

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

Signatures

- Antivirus detection for URL or domain
- Yara detected HtmlPhish6
- Phishing site detected (based on im…
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 4460 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 2160 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4460 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 5576 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4460 CREDAT:82952 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

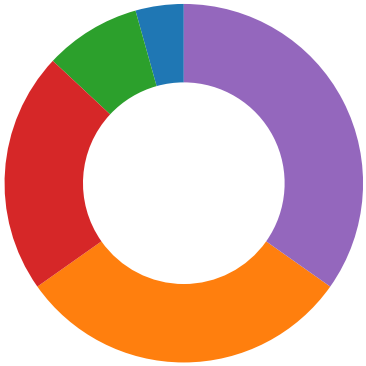
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\s[1].htm	JoeSecurity_HtmlPhish_6	Yara detected HtmlPhish_6	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\s[2].htm	JoeSecurity_HtmlPhish_6	Yara detected HtmlPhish_6	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Phishing:

Yara detected HtmlPhish6

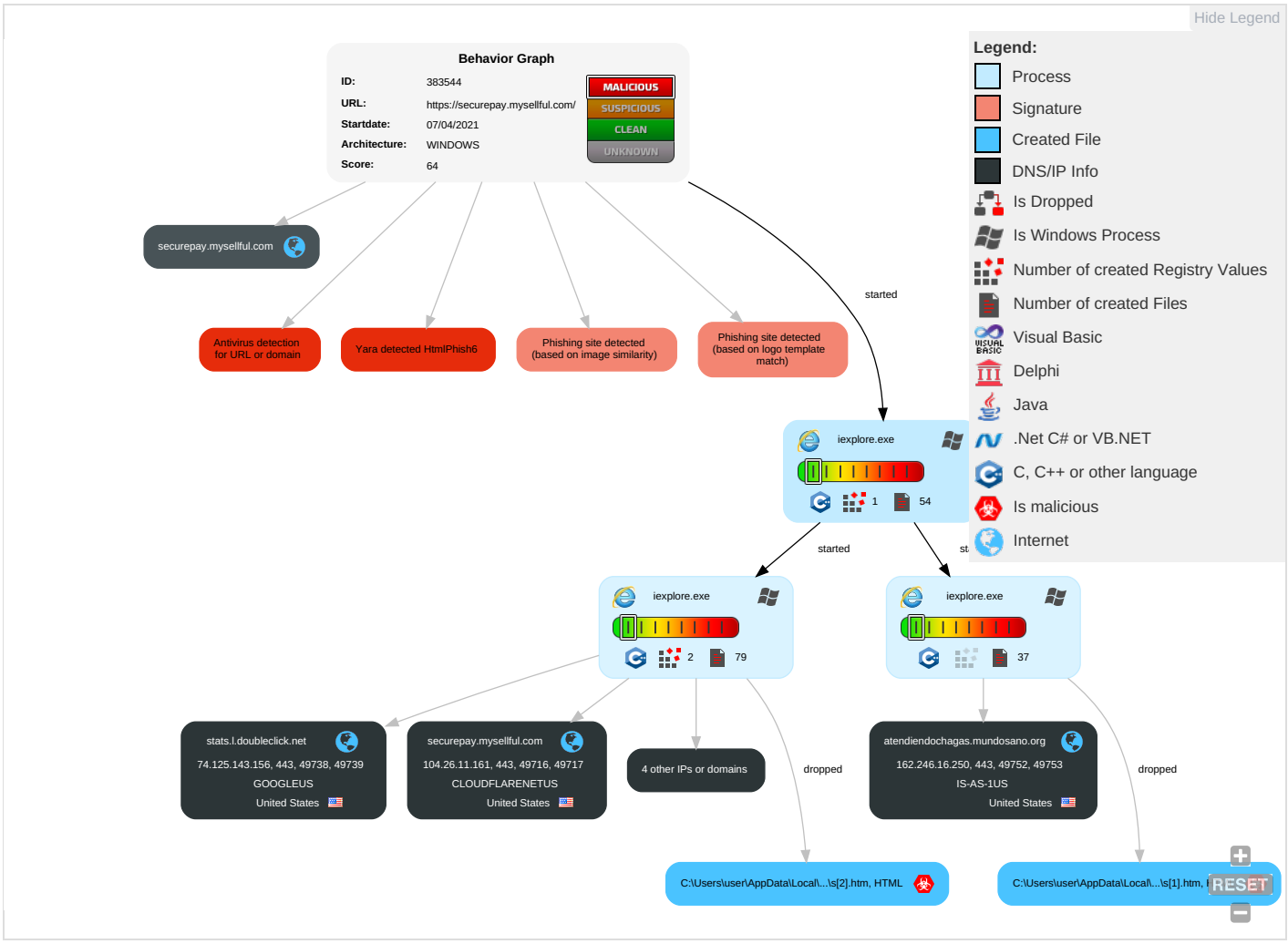
Phishing site detected (based on image similarity)

Phishing site detected (based on logo template match)

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	Impac
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partiti
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lockc
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	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data

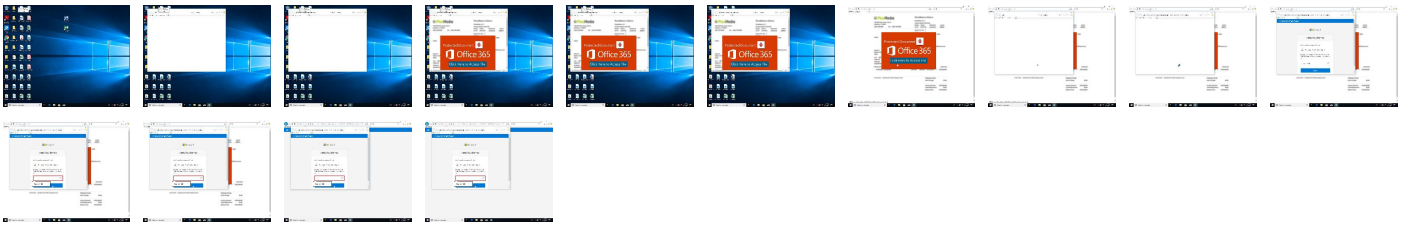
Behavior Graph

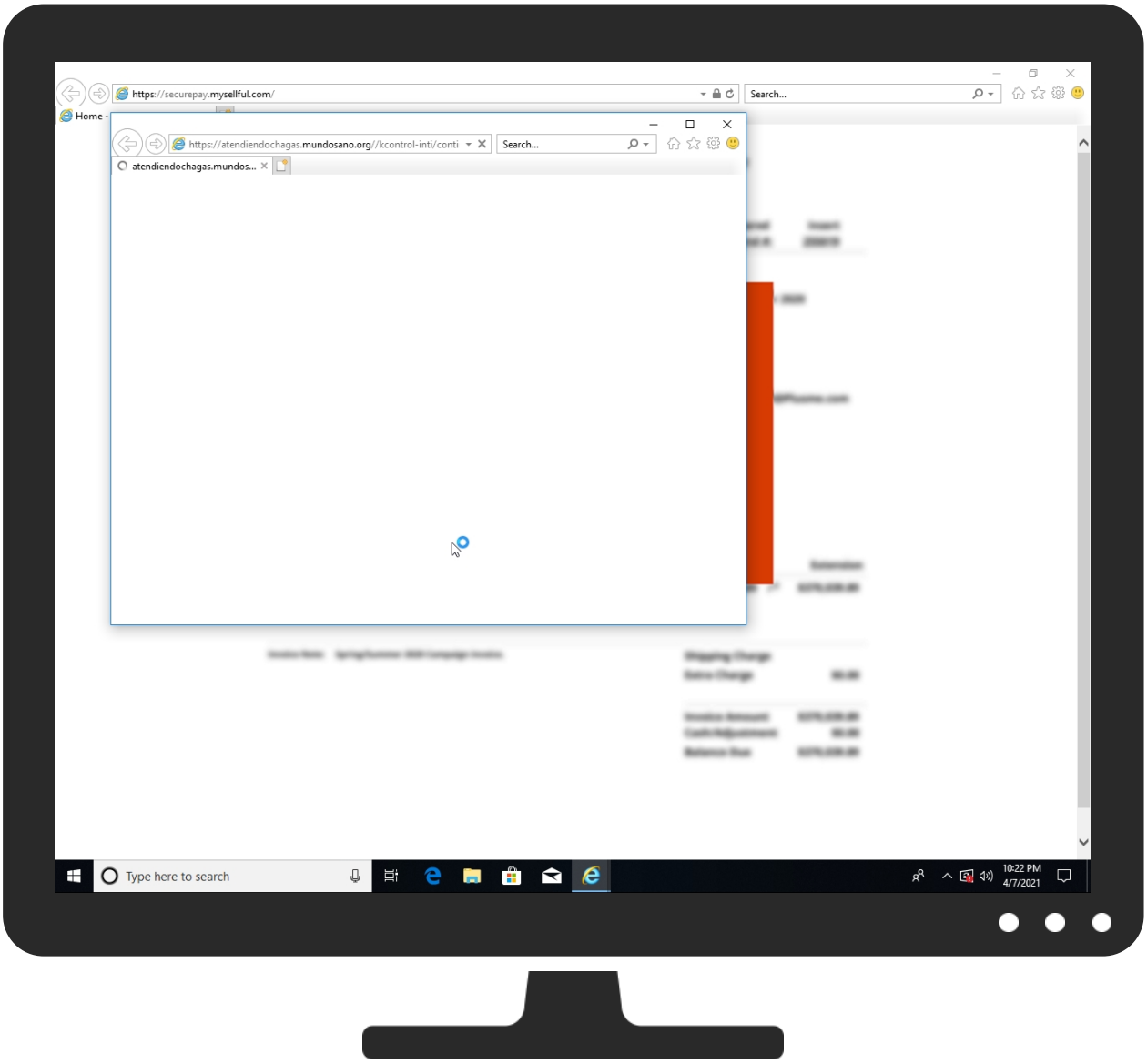


Screenshots

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://securepay.mysellful.com/	1%	Virustotal		Browse
http://https://securepay.mysellful.com/	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
atendiendochagas.mundosano.org	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
http://https://atendiendochagas.mundosano.org/kcontrol-inti/continue/new/s/?signin=d41d8cd98f00b204e9800998ecf8427e&auth=eb74f312212be18a263f555439392ab2f19be7815afbdfc1069c245ec67f3c3c7067c33f	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://atendiendochagas.mundosano.org//kcontrol-inti/continue/newRoot	0%	Avira URL Cloud	safe	
http://swiperjs.com	0%	URL Reputation	safe	
http://swiperjs.com	0%	URL Reputation	safe	
http://swiperjs.com	0%	URL Reputation	safe	
http://https://atendiendochagas.mundosano.org//kcontrol-inti/continue/new	0%	Avira URL Cloud	safe	
http://https://securepay.mysellful.com/b	0%	Avira URL Cloud	safe	
http://https://atendiendochagas.mundosano.org/kcontrol-inti/continue/new/	0%	Avira URL Cloud	safe	
http://https://cdn1.sellful.com/wp-content/cache/busting/google-tracking/ga-0a4e309b5f2d7439b4f8876b19f37fc	0%	Avira URL Cloud	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cdn1.sellful.com/wp-content/plugins/wp-rocket/assets/js/lazyload/11.0.6/lazyload.min.js	0%	Avira URL Cloud	safe	
http://https://atendiendochagas.mundosano.org//kcontrol-inti/continue/newas.mundosano.org/kcontrol-inti/con	0%	Avira URL Cloud	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://atendiendochagllful.com/b	0%	Avira URL Cloud	safe	
http://https://atendiendochagas.mundosano.org/kcontrol-inti/continue/new/s/?signin=d41d8cd98f00b204e9800998	0%	Avira URL Cloud	safe	
http://https://securepay.mysellful.com/Root	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
stateless.sellful.com	104.26.12.213	true	false		unknown
stats.l.doubleclick.net	74.125.143.156	true	false		high
atendiendochagas.mundosano.org	162.246.16.250	true	false	• 0%, Virustotal, Browse	unknown
www.google.ch	216.58.215.227	true	false		high
cdn1.sellful.com	104.26.13.213	true	false		unknown
securepay.mysellful.com	104.26.11.161	true	false		unknown
stats.g.doubleclick.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://atendiendochagas.mundosano.org/kcontrol-inti/continue/new/s/?signin=d41d8cd98f00b204e9800998ecf8427e&auth=eb74f312212be18a263f555439392ab2f19be7815afbdfc1069c245ec67f3c3c7067c33f	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://securepay.mysellful.com/	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://atendiendochagas.mundosano.org//kcontrol-inti/continue/newRoot	{70535A4C-982A-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://jquery.org/license	position.min-1.11.4[1].js.2.dr	false		high
http://swiperjs.com	swiper.min-5.3.6[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://twitter.com/intent/tweet?text=	share-link.min-3.1.1[1].js.2.dr	false		high
http://https://atendiendochagas.mundosano.org//kcontrol-inti/continue/new	~DF7A51840F262B8417.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://securepay.mysellful.com/b	~DF827A3CCA513061E4.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/antoinevastel/picasso-like-canvas-fingerprinting	api[1].js.2.dr	false		high
http://jqueryui.com	position.min-1.11.4[1].js.2.dr	false		high
http://api.jqueryui.com/position/	position.min-1.11.4[1].js.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://atendiendochagas.mundosano.org/kcontrol-inti/continue/new/	new[1].htm.7.dr	false	• Avira URL Cloud: safe	unknown
http://https://securepay.mysellful.com/	{67FCA281-982A-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false		unknown
http://https://cdn1.sellful.com/wp-content/cache/busting/google-tracking/ga-0a4e309b5f2d7439b4f8876b19f37fc	gtm-479609c18ecd923ecdd3ed096cb1cd91[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/embed/ID?autoplay=1	MC8R5KA7.htm.2.dr	false		high
http://https://elementor.com/hello-theme/?utm_source=wp-themes&utm_campaign=theme-uri&utm_medium=wp-dash	ccaf1bb7df93920b7090e89ad7f87719[1].css.2.dr	false		high
http://https://cct.google/taggy/agent.js	gtm-479609c18ecd923ecdd3ed096cb1cd91[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/kobizz/dialogs-manager/blob/master/LICENSE.txt	dialog.min-4.8.1[1].js.2.dr	false		high
http://https://cdn1.sellful.com/wp-content/plugins/wp-rocket/assets/js/lazyload/11.0.6/lazyload.min.js	MC8R5KA7.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://fontawesome.com/license/free	v4-shims.min-3.1.1[1].js.2.dr	false		high
http://https://fontawesome.com	v4-shims.min-3.1.1[1].js.2.dr	false		high
http://https://www.gnu.org/licenses/gpl-3.0.html	ccaf1bb7df93920b7090e89ad7f87719[1].css.2.dr	false		high
http://https://atendiendochagas.mundosano.org//kcontrol-inti/continue/newas.mundosano.org/kcontrol-inti/con	{70535A4C-982A-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.google.%/ads/ga-audiences	ga-0a4e309b5f2d7439b4f8876b19f37fc7[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://atendiendochagllful.com/b	{67FCA281-982A-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://atendiendochagas.mundosano.org/kcontrol-inti/continue/new/s/?signin=d41d8cd98f00b204e9800998	~DF827A3CCA513061E4.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://i.ytimg.com/vi/ID/hqdefault.jpg	MC8R5KA7.htm.2.dr	false		high
http://https://stats.g.doubleclick.net/j/collect	ga-0a4e309b5f2d7439b4f8876b19f37fc7[1].js.2.dr	false		high
http://https://securepay.mysellful.com/Root	{67FCA281-982A-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://elementor.com/?utm_source=wp-themes&utm_campaign=author-uri&utm_medium=wp-dash	ccaf1bb7df93920b7090e89ad7f87719[1].css.2.dr	false		high
http://https://www.pinterest.com/pin/create/button/?url=	share-link.min-3.1.1[1].js.2.dr	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.26.12.213	stateless.sellful.com	United States		13335	CLOUDFLARENETUS	false
104.26.11.161	securepay.mysellful.com	United States		13335	CLOUDFLARENETUS	false
162.246.16.250	atendiendochagas.mundosano.org	United States		19318	IS-AS-1US	false
74.125.143.156	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
104.26.13.213	cdn1.sellful.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383544
Start date:	07.04.2021
Start time:	22:21:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://securepay.mysellful.com/
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.phis.win@5/58@9/5
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://atendiendochagas.mundosano.org//kcontrol-inti/continue/new

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.42.151.234, 23.54.113.53, 40.88.32.150, 13.88.21.125, 23.60.220.29, 52.147.198.201, 172.217.168.10, 216.58.215.227, 172.217.168.78, 172.217.168.4, 88.221.16.97, 104.43.193.48, 20.82.210.154, 152.199.19.161, 23.10.249.26, 23.10.249.43, 51.103.5.186, 52.155.217.156 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, wns.notify.trafficmanager.net, go.microsoft.com, www.google.com, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www.google-analytics.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fonts.googleapis.com, client.wns.windows.com, fs.microsoft.com, www-google-analytics.l.google.com, fonts.gstatic.com, ie9comview.vo.msecnd.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{67FCA27F-982A-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	45768
Entropy (8bit):	1.9934580088962113
Encrypted:	false
SSDEEP:	192:rAZBVZo2XWcthifKYSzMzfKBQkD6EB3tbctIxauWFexafyYxat4uxKu3jxK+g:rwBb/mo+z+7Hoviy
MD5:	14A4CADDB82EC0E781777E9540CF67BE
SHA1:	FDD1D8AE005A0C2B12FBEE428D6574230E1CC568
SHA-256:	B9A57E10F8A7509B7772EB29C8C4A9824822BF25880560EB75808BE96D73CCBE
SHA-512:	915CD1CFC53FFEAC08529C0ED1AAAC272B9EF8CC78E53292618636F390F57DD343284409092771F6E948663E358EC1EC806531A4C344BFBE596F03349E0C9B9
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{67FCA281-982A-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	44580
Entropy (8bit):	2.1573209378759914
Encrypted:	false
SSDEEP:	192:rSZFQp6LkHj929vWNMR8TvA0tGz0YZ6zEjZFNG4n16Qxvtd3:rO6EQD04eaTA0kz0ULlZpn
MD5:	48ABD361C1E7AF1235DBCF825A658FFD
SHA1:	A2667BB84DD449F8C2F59FBB9E36271E641F3C93
SHA-256:	23A16B270E183C69DA64EA0229D7424769FEF466F8102A35D918FCE6418C79FD
SHA-512:	3AB2C6298474954FE85F5FFB38A6C55DFFA8C2AEA53DDA7EAD7F2444AB43E0F2C417DB35EBB84D7CBFD1169E46CD93547B1FB83280291ECE2A0066859B278FCC
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{70535A4C-982A-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	31880
Entropy (8bit):	2.035537912163108
Encrypted:	false
SSDEEP:	192:r+ZtQ86WkejN21WUMUn1ZDAi+UXqr1qbUg:rKyHXYEMBm7DL5Xqr1qz
MD5:	AC7FA7415DC1FD0F06E1C73270CFFF97
SHA1:	856F3003777909A3EF7DDB6BB3A9094C0F88D13D
SHA-256:	A1357FC570883FD6BCF0AF4BB84313C72AA7F6D9D44C2759DC1CAF96ACBEF91D
SHA-512:	7B07EC6097811E88EFEA98A65ED75433A07F385F620123D1E226448F1D556C6BC480588B23F68CB6B6B2744A5E80637152FB559AA646628F4C60F593F457B7F2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{70535A4C-982A-11EB-90E6-ECF4BB82F7E0}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{70535A4D-982A-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.565539420426121
Encrypted:	false
SSDEEP:	48:IwGGcprHGwpacG4pQkGrapbS7GQpKm1xG7HpRPTGIpG:raZRQ86yBS1AZTtA
MD5:	2E5D0E625F4F8D24E88D38350C3F5C76
SHA1:	B32E3918530AFE574D665497266BC47E3D68D155
SHA-256:	26F16C139274B01EDB4CA9375A9D39D937CBECC24E87FB050E4E3221A579F4CA
SHA-512:	6F4F154D9642719BD3B836C9C4D1FB02C470F1B5F8614CA213F8C2A68F19E6D300CE98FCEA677AB784744D6C4CDB73E1B41C463F25B99914137F61A3CBEB3B0B
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	4028
Entropy (8bit):	5.2943615654303535
Encrypted:	false
SSDEEP:	96:UYgS7NAYgWNkYgLNuYggNwYgCNpYgMNlOS7NhOWNROLNKCOgNbOCNGOMNyOS7NIB:937NBlNtkN7PNRpNuTNz7NFNUNKcN3Ni
MD5:	775906B0B3B1AB6C28A494E1C39BAD70
SHA1:	EA02161815087057FAAD5AD45C8AFC53A3C5E4AD
SHA-256:	1A8242357B58770FCA34F6B86921FF5BAFB8C0F536891E7A86A04451350A544C
SHA-512:	DC54EDA99FD2154E13C87360B51026873EB82ACDA3DC5EC5D05A903F765D2C6698A217E7C711A640A35AC73AAF3A30F1BE6D409871A260C9B56BD76FE902184
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Roboto%3A100%2C100italic%2C200%2C200italic%2C300%2C300italic%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic%2C800%2C800italic%2C900%2C900italic%7CRoboto+Slab%3A100%2C100italic%2C200%2C200italic%2C300%2C300italic%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic%2C800%2C800italic%2C900%2C900italic&ver=5.2.9
Preview:	@font-face {. font-family: 'Roboto';. font-style: italic;. font-weight: 100;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOiCnqEu92Fr1Mu51QrEzAdKQ.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: italic;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOjCnqEu92Fr1Mu51TjASc6CsI.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: italic;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOkCnqEu92Fr1Mu51xIIzQ.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: italic;. font-weight: 500;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOjCnqEu92Fr1Mu51S7ACc6CsI.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: italic;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOjCnqEu92Fr1Mu51TzBic6CsI.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: italic;. font-weight: 900;. src: url(http

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\css[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	188
Entropy (8bit):	5.119072399147113
Encrypted:	false
SSDEEP:	3:0SYWFFWlIYCiF15RI5XwDKLRIHDfFTo/TfqzrZqcdJ2dTi8EuRlGlL+9JYARNin:0IFFm15+56ZTo/Tizlpd0celdJNin
MD5:	4CFC4658F748E1FC67D2EA27F9B3692F
SHA1:	82C520D112F48E337E99DF00067BFAA75D0F9CA2
SHA-256:	ABC5A61E85F95E54C925FE9589099AD680912480E7C97052AF0496CBC6D111B8
SHA-512:	BFDDD6D4E0225EF444FD621B2CC20D022C02E30AB3E8AACA197E8F6304AA95E8C253815C6DC329646E5F39BBAF0B953A0667B296D15AB6BCECE788D1BFDC614B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Open+Sans:600

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\css[2].css	
Preview:	@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 600;. src: url(https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UNirkOUuhv.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\dialog.min-4.8.1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	10863
Entropy (8bit):	5.1613915002906126
Encrypted:	false
SSDEEP:	192:sEPwJdswSRibO6JSplZn41SFzpYK2p7ESa/Tl9w0uV6uSnotk+nWEdpTARHrLG4/:FH6JElZn4WpYKC7E5rI9oV6ultk6tIe6
MD5:	58BAF0F238D7AFC7AB926B8D51E5B559
SHA1:	8515E5F578269E29C048450F78C107935D325DFF
SHA-256:	2989E0B9E836CB9DE3274D641EC6A58C2052F039E790DDD59B22303930BFDEEB
SHA-512:	A15D0799C93D0C93789582D5330BDA9AEB5332A2EF4917FE0F6A758EA77A1231B976DC960BA17D0038BD16ACB34C62400EC4213AB458D1B301FB6141958FA00
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn1.sellful.com/wp-content/cache/busting/3146/wp-content/plugins/elementor/assets/lib/dialog/dialog.min-4.8.1.js
Preview:	/*! dialogs-manager v4.8.1 | (c) Kobi Zaltzberg | https://github.com/kobizz/dialogs-manager/blob/master/LICENSE.txt . 2020-08-17 18:55 */.!function(a,b){"use strict";var c={widgetsTypes:{},createWidgetType:function(b,d,e){e||(e=this.Widget);var f=function(){e.apply(this,arguments)},g=f.prototype=new e(b);return g.types=g.types.concat([b]),a.extend(g,d),g.constructor=f,f.extend=function(a,b){return c.createWidgetType(a,b,f)},f},addWidgetType:function(a,b,c){return b&&b.prototype instanceof this.Widget?this.widgetsTypes[a]=b:this.widgetsTypes[a]=this.createWidgetType(a,b,c)},getWidgetType:function(a){return this.widgetsTypes[a]}};c.Instance=function(){var b=this,d={},e={},f=function(){d.body=a("body")},g=function(b){var c={classPrefix:"dialog",effects:{show:"fadeIn",hide:"fadeOut"}};a.extend(e,c,b);this.createWidget=function(a,d){var e=c.getWidgetType(a),f=new e(a);return d=d||{},f.init(b,d),f},this.getSettings=function(a){return a?e[a]:Object.create(e)},this.init=function(a){return g(a

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\frontend-modules.min-3.1.1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with LF, NEL line terminators
Category:	downloaded
Size (bytes):	64914
Entropy (8bit):	5.3578444056002485
Encrypted:	false
SSDEEP:	1536:ODFdqcFjyAlENEeDq6/9m59Clae6dxx7A6htTF38tzfFKQt4RcSS/Yq31pC:2qcFjy5Yq3TC
MD5:	2AA14A960A066B954DFACB7CE9B6D192
SHA1:	525BBDDC67ADDA7E9B1960FF5AAC621922ABDEB3
SHA-256:	DEA0AD73F4973782017880F1DCE0AF21A946D0E21A07DF4C5B98ECED5EBB40B1
SHA-512:	95941BD8FD973B2D49AEC7F12031E452A07352EE3BECF2D4012D021584B77337C9EE25D40718EE99BA1234EECB9B3DE52BC3C2545407073F1062C2B650D2319
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn1.sellful.com/wp-content/cache/busting/3146/wp-content/plugins/elementor/assets/js/frontend-modules.min-3.1.1.js
Preview:	/*! elementor - v3.1.1 - 31-01-2021 */.(self.webpackChunkelementor=self.webpackChunkelementor||[]).push([[354],{9396:(t,e,r)=>{t.exports=r(9862)},5091:(t,e,r)=>{t.exports=r(7060)},8401:(t,e,r)=>{t.exports=r(9043)},7394:(t,e,r)=>{t.exports=r(3679)},3587:(t,e,r)=>{t.exports=r(7092)},2055:(t,e,r)=>{t.exports=r(8473)},3452:(t,e,r)=>{t.exports=r(671)},8274:(t,e,r)=>{t.exports=r(7629)},3493:(t,e,r)=>{t.exports=r(3966)},4176:(t,e,r)=>{t.exports=r(4969)},5499:(t,e,r)=>{t.exports=r(990)},8282:(t,e,r)=>{t.exports=r(6760)},1281:(t,e,r)=>{t.exports=r(9280)},9363:(t,e,r)=>{t.exports=r(9551)},93:(t,e,r)=>{t.exports=r(2194)},8852:t=>{t.exports=function _assertThisInitialized(t){if(void 0===t)throw new ReferenceError("this hasn't been initialised - super() hasn't been called");return t}},1959:t=>{t.exports=function _classCallCheck(t,e){if(!(t instanceof e))throw new TypeError("Cannot call a class as a function")}},846:(t,e,r)=>{var n=r(5499),o=r(6870),i=r(898);function _construct(e,r,s){return i()?t.e

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\frontend.min-3.1.1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	80963
Entropy (8bit):	5.241137249036391
Encrypted:	false
SSDEEP:	1536:rQeCyqmeXKVZVb9/ql1xz8rQ3SeugaB7r3WggqYZ3RSo+fY9QHqD+fxX5YlakVCg:0RTcv+0PZfP
MD5:	DCE958AFB428DD3DC78F203EF99BAE42
SHA1:	36EC6A22853E4212CFA7D150E9486200C943FE63
SHA-256:	26D2072B425A61E1ED81ED2B3F254888531E62060C7C4B3C788FFB925A8C864E
SHA-512:	FA90CC9502E52FB631BD7C691EC6C3A9A7B81FC479C7B7F5FE0ABF94B8BD3A1375D0C65067AE342F35981E4937740E11BAFBC37CF51FE655C50316DC066B34 2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn1.sellful.com/wp-content/cache/busting/3146/wp-content/plugins/elementor/assets/js/frontend.min-3.1.1.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\frontend.min-3.1.1[1].js	
Preview:	/*! elementor - v3.1.1 - 31-01-2021 */.(self.webpackChunkelementor=self.webpackChunkelementor||[]).push([[819],{5453:(e,t,n)=>{e.exports=n(6802)},4680:(e,t,n)=> {e.exports=n(1792)},1888:(e,t,n)=>{e.exports=n(2555)},2009:(e,t,n)=>{e.exports=n(2771)},2937:(e,t,n)=>{e.exports=n(7841)},8923:(e,t,n)=>{e.exports=n(5948)},5657: (e,t,n)=>{e.exports=n(1995)},3220:(e,t,n)=>{e.exports=n(9485)},2292:e=>{e.exports=function _arrayLikeToArray(e,t){(null==t||t>e.length)&&(t=e.length);for(var n=0,i=new A rray(t);n<t;n++)i[n]=e[n];return i}},9479:(e,t,n)=>{var i=n(9396);e.exports=function _arrayWithHoles(e){if(i(e))return e}},9117:(e,t,n)=>{var i=n(3220);function asyncGene ratorStep(e,t,n,o,r,a,s){try{var l=e[a](s),d=l.value}catch(e){return void n(e)}l.done?t(d):i.resolve(d).then(o,r)}e.exports=function _asyncToGenerator(e){return function(){var t=this,n=arguments;return new i((function(i,o){var r=e.apply(t,n);function _next(e){asyncGeneratorStep(r,i,o,_next,_throw,"next",e)}function _throw(e){asyncGenerato

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\gtm-479609c18ecd923ecdd3ed096cb1cd91[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	99212
Entropy (8bit):	5.521881513645312
Encrypted:	false
SSDEEP:	1536:JoUK1bOl+0E+HlUnK+sCEOkKQfn2zeWgzvC6sruTAin1U9aKPh52QsnyAC7iHg:JoUKxu+04nvs+SWnrRiLhg
MD5:	7EDF89BCE763DAE748007CC1141380D7
SHA1:	C60F42B0D042E5D3A07A2EBA19C2ADCC1963DB3F
SHA-256:	F823A747AEE70B21C44208FC0B5413A7512557E5188A2AA64529241A5B4C4E4E
SHA-512:	BFBEB4D2D7D2742D60602A8F99E713B6A1F459E11E2493488F14C0CD65B2C6E3F2CC84FF4593F2A1E9FF46BA66F6D9C71C84B533A88A9E2907704107652F19C5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn1.sellful.com/wp-content/cache/busting/3146/gtm-479609c18ecd923ecdd3ed096cb1cd91.js
Preview:	.// Copyright 2012 Google Inc. All rights reserved..(function(){..var data = {."resource": {. "version":"1",. . "macros":[{. "function":"__e". },{. "function":"__cid". }],. "tags":[{. "function":"__rep",. "once_per_event":true,. "vtp_containerId":["macro",1],. "tag_id":1. }],. "predicates":[{. "function":"_eq",. "arg0":["mac ro",0],. "arg1":"gtm.js". }],. "rules":[. [["if",0],["add",0]]].},."runtime":[].....};../*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var aa ,ba=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}},ca=function(a){var b="undefined"!=typeof Symbol&&Symbol.iterator& &a[Symbol.iterator];return b?b.call(a):{next:ba(a)}},da="function"==typeof Object.create?Object.create:function(a){var b=function(){};b.prototype=a;return new b},ea;.if(" function"==typeof Object.setPrototypeOf)ea=Object.setPrototypeOf;else{var ia;a:{var ja={a:!0},ma={};

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\jet-blocks.min-1.2.4[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	13937
Entropy (8bit):	5.194590837918052
Encrypted:	false
SSDEEP:	192:1LJbl09ztPA/QhP0RBA2CbGtg0eXpzNxUV6a5xF6+ZhkcEWLs44W1cu2WzaB6Dmt:1wxAQB6DmRht
MD5:	A4F2716EEDDAAB1AB3F91DF8A53743BD
SHA1:	864F3205952350B27668E1FBEB300173FA1BFD9F
SHA-256:	42123FA141C9B3B24EA7AFA9028E5407324018F168CB68CA04FA46D51180E89F
SHA-512:	1412B997FD3791682783DF8682ADF9FD610AE9F2B97113C0B1C9E44807D68019D699C608E5E236042112A7F0AD51B6593A8D9DC335C5C7D086842DE577F77CFB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn1.sellful.com/wp-content/cache/busting/3146/wp-content/plugins/jet-blocks/assets/js/jet-blocks.min-1.2.4.js
Preview:	!function(h,m,o){"use strict";var c={init:function(){var e={"jet-nav-menu.default":c.navMenu,"jet-search.default":c.searchBox,"jet-auth-links.default":c.authLinks,"jet-ha mburger-panel.default":c.hamburgerPanel,"jet-blocks-cart.default":c.refreshCart};h.each(e,function(e,t){m.hooks.addAction("frontend/element_ready/"+e,t)}),h(doc ument).on("click.jetBlocks",".jet-search__popup-trigger",c.searchPopupSwitch).on("click.jetBlocks",".jet-search__popup-close",c.searchPopupSwitch),m.hooks.addAc tion("frontend/element_ready/section",c.setStickySection),h(document).on("ready",c.stickySection)},refreshCart:function(e){if(o&&window.JetBlocksEditor&&window. JetBlocksEditor.activeSection){var t=window.JetBlocksEditor.activeSection;-1!==["cart_list_style","cart_list_items_style","cart_buttons_style"].indexOf(t)?e.find(".jet-blocks- cart").addClass("jet-cart-hover"):e.find(".jet-blocks-cart").removeClass("jet-cart-hover"),h(".widget_shopping_cart_content").empty(),h(document.body).trigger("wc_fr agment_ref

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\jet-elements.min-2.5.5[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	61303
Entropy (8bit):	5.457784118707286
Encrypted:	false
SSDEEP:	1536:oZRoxSpg4k8S5LugZRopr2oKzm+Hs3xeDz:oZjS5Urr3xeDz
MD5:	AA0D6562E66188D42D8B4EB243D5AEAE
SHA1:	269ED4B11B57DB0B520CEA0F5895EAABF778F022
SHA-256:	56DD17B91E80F419356B9519459F99E939F846BAB801BE32A15719293131DE4C
SHA-512:	85FB2C7490D4D909225F8C49E113C5ADEA299E9967D2CAA9B2F58BF2D43EBD433A5A82BA4A461C63750BC8393375C3AE76EE93F83D7426D206DBF5D39B549B 4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\jet-elements.min-2.5.5[1].js	
IE Cache URL:	http://https://cdn1.sellful.com/wp-content/cache/busting/3146/wp-content/plugins/jet-elements/assets/js/jet-elements.min-2.5.5.js
Preview:	!function(e,t){"use strict";var i={init:function(){var a={"jet-carousel.default":i.widgetCarousel,"jet-circle-progress.default":i.widgetProgress,"jet-map.default":i.widgetMap,"jet-countdown-timer.default":i.widgetCountdown,"jet-posts.default":i.widgetPosts,"jet-animated-text.default":i.widgetAnimatedText,"jet-animated-box.default":i.widgetAnimatedBox,"jet-images-layout.default":i.widgetImagesLayout,"jet-slider.default":i.widgetSlider,"jet-testimonials.default":i.widgetTestimonials,"jet-image-comparison.default":i.widgetImageComparison,"jet-instagram-gallery.default":i.widgetInstagramGallery,"jet-scroll-navigation.default":i.widgetScrollNavigation,"jet-subscribe-form.default":i.widgetSubscribeForm,"jet-progress-bar.default":i.widgetProgressBar,"jet-portfolio.default":i.widgetPortfolio,"jet-timeline.default":i.widgetTimeLine,"jet-table.default":i.widgetTable,"jet-dropbar.default":i.widgetDropbar,"jet-video.default":i.widgetVideo,"jet-audio.default":i.widgetAudio,"jet-horizontal-timeline.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\pdf[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	6830
Entropy (8bit):	7.849424154989951
Encrypted:	false
SSDEEP:	192:n6ND9AxRGozwHD0Ksf+GQUAU6Z0WoYGoKUcsgYRU:6xWRXwHmtfYGLUYIU
MD5:	F1E3F187F7C23FA8D1555004F3800356
SHA1:	E71E52A142E754399AE39EF38584789B66E9EA00
SHA-256:	DB307FCEF7F95139689007D7A623B340EC21282BD421C4E4B2BA09078F230545
SHA-512:	BD568B1C92D7C3B586E2EA7E9C47B08FD1171FF6615FA4F670F12950DC62315B58E6BB5336F50B111FF42B27558398DFF9715054A8E44F0A8B9CD1541F0BC07D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://atendiendochagas.mundosano.org/kcontrol-inti/continue/new/s/files/pdf.png
Preview:	.PNG.....IHDR.....\r.f... cHRM..z&.....u0...`.:....p..Q<....bKGD.....7IDATx..K....j.[....{..&....V6....np3...-.. $.qF..0.a....a6y.....&D.g.#.....;..aC..q.5.k....n..SU.T...Oj.[..w.....:.....Nz....P.0..,.....b`..X.....`10..,.....b`..X.....U.@...?...Dfs..S....".....y.I.'q.s...^.9.....u.~qnn.....p.....?\u..Pz..&.>.E....)O....zzz.?..k.q#...;0..`Y...jaA.....S.\HF...#"...".dY:.O./..@.C).....f.I...<..;o.9..0... ..B....I..&`.4...|..1..9z...o.E...P..h...R..P.q...l....1....8....$..v.....q.q.j6.4555Vw.g..=:TJ.....v\.6.%.).H(...._'. ._.>.f...s].&.....j.U]..?2..-..rs....U.....7T0._.p..<.....*.4.".|S...C....L@=...Q..(,.^.S...`?@...f...1x.....w.6.~....F.....7....{.\....z..B.....d..;.....F.&.... 3\.T.....q..Fcq...9|.&....A.....<.....{..L 3,. ..1a...!(.`- .F.ASK&px..<p...D...d....*W~g].....h.j.0.Y.....d...4dK. .F...`.Y`j..\.7SQ{_.f.AS.....\....S..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\preloaded-elements-handlers.min-3.1.1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	37256
Entropy (8bit):	5.259484656179558
Encrypted:	false
SSDEEP:	768:0b49qeNT6bqYu4LqGaHWTo3dk5bqKWypqI1Qad+q7jukqgN8O8IDyq1HP3f69WmQ:0b4VKqYu4LqzHWTo3dSqKWypqI1Qad+W
MD5:	ED8DE4F9A94259E5BC6E81D7857C76E4
SHA1:	0F9330D1551934BF28E3AFC4BD63366DF88E9CA7
SHA-256:	420AD608FCB00C75B037C32408D72FABD863EB70B707A36F93DD00F4BDA513E9
SHA-512:	BA1C334DEB4F5333E304BF7EFF82ECBC070E7E032369E351153DEA28C23AE80281541173 92EA1FC7E847F40C19EB6B1495C84CFEE5C7145696521D35A9B7379
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn1.sellful.com/wp-content/cache/busting/3146/wp-content/plugins/elementor/assets/js/preloaded-elements-handlers.min-3.1.1.js
Preview:	/*! elementor - v3.1.1 - 31-01-2021 */.(self.webpackChunkelementor=self.webpackChunkelementor||[]).push([[995,209,745,120,192,520,181,791,268,357],{2937:(e,t,n)=>{e.exports=n(7841)},3774:(e,t,n)=>{e.exports=n(5966)},5315:(e,t,n)=>{e.exports=n(9406)},3220:(e,t,n)=>{e.exports=n(9485)},9117:(e,t,n)=>{var r=n(3220);function asyncGeneratorStep(e,t,n,i,a,o,s){try{var l=e[o](s),u=l.value}catch(e){return void n(e)}l.done?t(u):r.resolve(u).then(i,a)}e.exports=function _asyncToGenerator(e){return function(){var t=this,n=arguments;return new r((function(r,i){var a=e.apply(t,n);function _next(e){asyncGeneratorStep(a,r,i,_next,_throw,"next",e)}function _throw(e){asyncGeneratorStep(a,r,i,_next,_throw,"throw",e)}_next(void 0)}))}}},8042:(e,t,n)=>{var r=n(7394);e.exports=function _defineProperty(e,t,n){return t in e?r(e,t,{value:n,enumerable:!0,configurable:!0,writable:!0}):e[t]=n,e}},4899:(e,t,n)=>{var r=n(7394),i=n(2937),a=n(3774),o=n(3587),s=n(5315),l=n(3452),u=n(8042);function ownKeys(e,t){var n=l

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\swiper.min-5.3.6[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	139153
Entropy (8bit):	5.2146927200642335
Encrypted:	false
SSDEEP:	1536:Fj2qhgxfeuGMfoqi2ZLjK8ieVlLXCiiSsWRLK7A3dnaKBjY4vHgZsUOUTqiqpBgA:wxoo6desFshaKi+HgZsUOUTqiqM37ER
MD5:	15BB2B8491FC7E84137D65F610E1685A
SHA1:	CD76B70A5426893E9C022B9A75C50A7C1348E2D0
SHA-256:	B23F49F504FAA32AAC548B6662FFD64412F6738496FAB8BE38DA46C5B7121804
SHA-512:	95C05110B29101C84DF71C54172269F478D9CD14965B3DE987613E11E0F1CCF01C1B7D2BF290D97EF11373F24DCCD677F8710E1555D332903181F469D0F2B0BB
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\swiper.min-5.3.6[1].js	
IE Cache URL:	http://https://cdn1.sellful.com/wp-content/cache/busting/3146/wp-content/plugins/elementor/assets/lib/swiper/swiper.min-5.3.6.js
Preview:	/**. * Swiper 5.3.6. * Most modern mobile touch slider and framework with hardware accelerated transitions. * http://swiperjs.com. *. * Copyright 2014-2020 Vladimir Kharlampidi. *. * Released under the MIT License. *. * Released on: February 29, 2020. */..!function(e,t){"object"==typeof exports&&"undefined"!=typeof module?module.exports=t():"function"==typeof define&&define.amd?define(t):(e=e||self).Swiper=t()}(this,(function(){"use strict";var e="undefined"==typeof document?{body:{},addEventListener:function(){},removeEventListener:function(){},activeElement:{blur:function(){},nodeName:""},querySelector:function(){return null},querySelectorAll:function(){return []},getElementById:function(){return null},createEvent:function(){return{initEvent:function(){}}},createElement:function(){return{children:[],childNodes:[],style:{},setAttribute:function(){},getElementsByTagName:function(){return[]}}},location:{hash:""}}:document,t="undefined"==typeof window?{document:e,navigator:{userAgent:""}},

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\wu-visit-counter.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	451
Entropy (8bit):	4.887002620324048
Encrypted:	false
SSDEEP:	12:sE5OWQdRVMq3osE2jlYcW7hpQzXQXwlx8XQ1RFw3KeGXr7dzkZGXYMCjJn:sE5EBBEilYVVJwAXURFw3/GXr7Fk8XYr
MD5:	BD2D3003A2FF56FFE8D773738166C4E8
SHA1:	038E00D4CC39EC3B07034BDE7D183488A327D93D
SHA-256:	E0D101D1C3EAA67495D8A04D1D4A2D84B02B44CE6C9B060C323A5534CD83D59C
SHA-512:	AF545977FE96BCE0F8CCFF024BC101EB6E3E7BF218D173EEEE1D2694FF20CB0E69C1D05BA3300234A6B205CD7D5079FCBBA34F05427BFB5FEA43100493A9E541
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn1.sellful.com/wp-content/plugins/wp-ultimo/assets/js/wu-visit-counter.min.js
Preview:	!function(n){var o,t=!1,i=function(){return console.log("Counting Visit..."),n.ajax({type:"GET",url:wu_visit_counter.ajaxurl,data:{action:"wu_count_visits",code:wu_visit_counter.code}}).done(function(){t=!0,console.log("Visit registered.")})};setTimeout(function(){console.log("Listening for unloads..."),n(window).on("unload",function(){"null"==typeof o&&(t||(o=i()))})},3e3),n(document).ready(function(){setTimeout(function(){o=i()},1e4)})}(jQuery);

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\KFOiCnqEu92Fr1Mu51QrEzAdKQ[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 21776, version 1.1
Category:	downloaded
Size (bytes):	21776
Entropy (8bit):	7.972467440478283
Encrypted:	false
SSDEEP:	384:G+oO9eMm6IbA7qJx9w3/TVd3fr5KjEid8pTN4TbOwyFPhgGRw9:zl9eMm6eKsHwpdPr5K+Pu6wsPaGRU
MD5:	E21019768EE6D334593AA1EBCA028ACF
SHA1:	DFE80B4CB13F47ECED9236E33AB360DB41711B0C
SHA-256:	75D75439F2A7EA1851A3E5B621320B9DFA1399861D2EC6D443A3C2919B93AFB7
SHA-512:	CFE0237C61D61CD630A1F9E05C2A00DEE1C2006811ADAB19162F2BCB890E2F126054EC01131CD2642D2D2398C0F56C7D2D9A25A56C2BAD6FF4BC6FB21029C9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOiCnqEu92Fr1Mu51QrEzAdKQ.woff
Preview:	wOFF.....U.....GDEF.....G...d....GPOS.....!GSUB.....OS/2...L...O...`t..'cmap.....#cvt .....H...H.2..fpgm.....3...._...gasp...0.....glyf...<..A...u....hdmx..M....q.....#.&head..Np...6...6.|.hhea..N....#...$.}.[hmtx..N.....rQ.loca..QX..... .._maxp..SP... ... .4..name..Sp..... G= post..TL..... .a.dprep..Td.....+6.x...1..P.....PB..U.=I.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x...l\..F..3...N..q)..a|.....^..33..c.....p"y.iT....<Gg...!.3...T1...{.g0.u.y.....m.|.k..NF.....mox.;...7&.Y..C.R_[.T.c..-.=...9:...a*j.G.....O.Q".6...>...(?...~...._2:..K4....S%...jbr).....*....e.U..-..X.3.ILQ....z..!.f:...<.W.#...e.c=...&6...lc;;..3<.s<....H.i2..N..t..)Ns...#`..".).[...._..T..T.....+l..=..O.....Z..F...r..eM.f.Y.....-...r.\.s6.r.,...:.<$..#.I..F.$.2#.e..].[.....yR...e.|{..O..`)..U.0.e.50.Z.b../cM..i.&O._..+.Y.W...;z....j.p._.o..[CL.)n'.UGx..>).X..MJ..Fr..v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\KFOjCnqEu92Fr1Mu51TLBCc6Csl[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 22360, version 1.1
Category:	downloaded
Size (bytes):	22360
Entropy (8bit):	7.975733480737877
Encrypted:	false
SSDEEP:	384:afBIIA0zhsqLW3UAI+x+VH9cxS8XwZtyOOCiKCu5s7YRKWIrfu/oiQfTO4TPg:aG0zhsqLSUAI+xi2s8XwZtuKJzE6/qfg
MD5:	C2E42D1EAC2DE2B58A2358686E6ED73C
SHA1:	24760369053031DF1F2BE831E067E3D9E37F0B3A
SHA-256:	B31B421BAFE532F6B6BDBB6F680FB11BD3968F23C7FE09A29B1A22F4C8DD2A7E
SHA-512:	BFB71B0B6DE51CD1E643733A14B5CD4342F4E93A1732E9AAF6F3A6012DD85EEC5F660F409474C55751B28D122BA202875A325D72F0B7CF327660577C7C1DC9D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOjCnqEu92Fr1Mu51TLBCc6Csl.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\KFOjCnqEu92Fr1Mu51TLBCc6CsI[1].woff	
Preview:	wOFF.....WX.....h.....GDEF.....G...d....GPOS.....oGSUB.....OS/2...p...O...`v...cmap.....#cvt .....Z...Z...=fpgm...4...3.....#.gasp...h..... ...glyf...t..C...t..,..hdmx..O....n....25$8head..Pl...6...6.G.Whhea..P....#...$.H..hmtx..P.....B(Cloca..Sd.....maxp..Ud... ... .4..name..U.....>.post..Vd..... .a.dprep..V |.....8...Cx...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x....%Y....Wm=..mo..k.m....rl...m.g"^..../..[.}.S...\.mD...1..G>..giz...=C..}.y....|o..c.x.R.r"B.....m ...../.&./6..5D.AGX.....)<'.)....?.... .Y4>|1...ES.Gc...FO.>$.../...}RCl..T.zD..uZ4~D.._OK.$.Z.(..JR...\..\..\..\.\.....*'n..6:x...b,..$...?.g:./y.iLg.3..l.0.y.g..X..V...d.#O...0....b7{..> .n.iD.V....." e.\A..OR.kwp.].....6p..."ZE..%...e.u3..L..V...W.7b..L.3.L1K...Ts..$6.-b.....9...b@..!1,...v.C....{...dox.G(...|a%E:.Fn.Nn.^n.....Sf..E)...k....<g..){....|.....DT..N....H y.F.Jez....._?7.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\KFOjCnqEu92Fr1Mu51TzBic6CsI[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 21656, version 1.1
Category:	downloaded
Size (bytes):	21656
Entropy (8bit):	7.971138981009303
Encrypted:	false
SSDEEP:	384:vfqIIA0zh/VF0+5SLHCK+yo5HHx/KnMpljPSiQZxLZtspfA9JaXWWyBuM9rgaSJV:vJ0zh/VFv0Hm15HHtKnalaiQfZtsp49o
MD5:	147F4E11CE73A22AAC9C6C2822290953
SHA1:	EEFEA89A9C36F8B1A7CA99372A7E0E05C92EADD6
SHA-256:	A22585CFD64238EF14B1B383B5B9A8BAD7C89E354C09FC0886067E876687A38C
SHA-512:	3D7ADA26B281864CE394CB49974A9EA59D28FA8C2EFB006DF31DCAE66DB4684223BDB42B8234A5135BF1B4F834E91DE415E44558EB2CF2346086C8879397058
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOjCnqEu92Fr1Mu51TzBic6CsI.woff
Preview:	wOFF.....T.....GDEF.....G...d....GPOS.....oGSUB.....OS/2...p...O...`u...cmap.....#cvt .....J...J..,ofpgm...$...3....c...gasp...X.....glyf... d..@...o.H.6.hdmx..MD...n.....,..0head..M....6...6...`hhea..M....#...$....hmtx..N.....1)loca..P.....maxp..R.... ... .4..name..R..... .=$post..S..... .a.dprep..S.....9 ..Bx...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x....%Y....Wm=..mo..k.m....rl...m.g"^..../..[.}.S...\.mD...1..G>..giz...=C..}.y....\|o..c.x.R.r"B.....m...../.&. /6..5D.AGX.....)<'.)....?.... .Y4>\|1...ES.Gc...FO.>$.../...}RCl..T.zD..uZ4~D.._OK.$.Z.(..JR...\..\..\..\.\.....*'n..6:x...b,..$...?.g:./y.iLg.3..l.0.y.g..X..V...d.#O...0....b7{..>.n.iD.V....." e.\A..OR.kwp.].....6p..."ZE..%...e.u3..L..V...W.7b..L.3.L1K...Ts..$6.-b.....9...b@..!1,...v.C....{...dox.G(...|a%E:.Fn.Nn.^n.....Sf..E)...k....<g..){....|.....DT..N....Hy.F.Jez....._? 7.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\KFOkCnqEu92Fr1MmgVxIIzQ[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20424, version 1.1
Category:	downloaded
Size (bytes):	20424
Entropy (8bit):	7.973322748597765
Encrypted:	false
SSDEEP:	384:UaoO8n3eceZ+fUC1WCz8P+IgjhYSHA/fFb4+hQC:Bl8nOcBfUqT/jOgAiC
MD5:	04B7FD97F88B82DCCCE5EC446CCC29E6
SHA1:	9A3C1CE2EAB659A91AF7016570287428CC82C458
SHA-256:	A38AD0B609E4D2039D18B0F9DC89E9060F2E2E05F2F42764A6A93354346A6C37
SHA-512:	4B71614F447F4E250AB8060026BA002F3F0DAA9286F207AA4B0652201D9053BD72865C09D1AB90155CF932E17D5897D7A1F659C98F1B1AACFDF6397D6DB47DA8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOkCnqEu92Fr1MmgVxIIzQ.woff
Preview:	wOFF.....O.....GDEF.....G...d....GPOS.....!GSUB.....OS/2...L...P...`t..{cmap.....#cvt .....H...H.2..fpgm.....3...._...gasp...0.....glyf... <..<...q....Lhdmx..H....q...."&.(head..l@...6...6.G..hhea..Ix... ...$...whmtx..I....y.....lCloca..L.....X.;.maxp..N.... ... .4..name..N4.....x..9.post..O..... .m.dprep..O..... +6.x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x...l\..F..3...N..q)..a\|....^..33..c.....p"y.iT....<Gg...!.3...T1...{.g0.u.y.....m.\|.k..NF.....mox.;...7&.Y.. C.R_[.T.c..-.=...9:...a*j.G.....O.Q".6...>...(?...~...._.2:..K4....S%...jbr).....*....e.U..-..X.3.ILQ....z..!.f:...<.W.#...e.c=...&6...lc;;..3<.s<....H.i2..N..t..)Ns...#`..".).[...._.T..T... ..+l..=..O.....Z..F...r..eM.f.Y.....-...r.\.s6.r..,...:.<$..#.l..F.$.2#.e..].[.....yR...e.\{.O..`)..U.0.e.50.Z.b../cM..i.&O._..+.Y.W...;z....j.p._.o..[CL.)n'.UGx..>).X..MJ..Fr..v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\api[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	35662
Entropy (8bit):	5.289565799540458
Encrypted:	false
SSDEEP:	768:eIEo7x4VqTHUlEulsfi+P1u0C9tJXTPDbYYFfct/1VMp9JddY8PmE4k7DgGSB:e2yYYac1TssM
MD5:	6C6281C15CBC981BC05942BAC40BCD7E
SHA1:	6015D314D852ECC0C0158731D8E06724805E38E5
SHA-256:	0D3118E306C6A26F1D2EFCB698984E6922C5E7E155C94A84760E36E5592A3C11
SHA-512:	7DB423D081304661C5981C6FC6D37CE2F32DBE8B8C38A9D2791DBD6110DB36261FA249A1662F667B58AA5B1A88446AD65D90B6EFBBEE0DA1378BD39BB1FE0D B2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://securepay.mysellful.com/cdn-cgi/bm/cv/669835187/api.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\api[1].js	
Preview:	/**. * @license. * Copyright (c) 2015 Andr. Cruz <amdfcruz@gmail.com>. * Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the 'Software'), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:. * The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.. * THE SOFTWARE IS PROVIDED 'AS IS', WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	15526
Entropy (8bit):	5.721275823828831
Encrypted:	false
SSDEEP:	384:Ox5T7PuUyxgg2Ctjo/kohz2YDDD1fSCRdVl37Sm9:OjT7GDxgg2GE/kohz2YDDD1fS8oh9
MD5:	63DF83784CADD3A339B776520600C21A
SHA1:	69BB829612F3E3CB2F521323945C9284A2B0DCDE
SHA-256:	2EE69AEF3AFB10B368BDE9FEA7E97CC75C030C890E3D2B8DC4AD19D498234DBF
SHA-512:	FC1C4F31A0817471D1D2CA8ADEA7F3C39B67B0EA688CC58EB4F6C68F5F6558E236B9D3D2D8BA95EE296CFBF3C0197CE54DFECADBCCCE1B7497542FEE2914 1D5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://atendiendochagas.mundosano.org/kcontrol-inti/continue/new/s/files/css.css
Preview:	html {...line-height: 1.15;...-ms-text-size-adjust: 100%;...-webkit-text-size-adjust: 100%..}..body {...height: 100%;...margin: 0..}..article, aside, footer, header, nav, section { ...display: block..}..h1 {...font-size: 2em;...margin: .67em 0..}..figcaption, figure, main {...display: block..}..figure {...margin: 1em 40px..}..hr {...box-sizing: content-box;.. .height: 0;...overflow: visible..}..pre {...font-family: monospace, monospace;...font-size: 1em..}..a {...background-color: transparent;...-webkit-text-decoration-skip: objects..}. .abbr[title] {...border-bottom: none;...text-decoration: underline;...text-decoration: underline dotted..}..b, strong {...font-weight: inherit..}..b, strong {...font-weight: bolder ..}..code, kbd, samp {...font-family: monospace, monospace;...font-size: 1em..}..dfn {...font-style: italic..}..mark {...background-color: #ff0;...color: #000..}..small {...font-size: 80%..}..sub, sup {...font-size: 75%;...line-height: 0;...position: relative;...vertical-align: b

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\ga-0a4e309b5f2d7439b4f8876b19f37fc7[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	48759
Entropy (8bit):	5.5215063523389265
Encrypted:	false
SSDEEP:	768:/yR3fYFBLbfsce5XqY1TyPnHpX/KWY3SoavPVRhwmCgYUD0lgEw0stZc:/y9gZfA5h1UHpXxY3Soiuw0sU
MD5:	0A4E309B5F2D7439B4F8876B19F37FC7
SHA1:	7AC30F933A2B889EDBE5D3449F4EC90049B0E2A9
SHA-256:	F79723478F4C48501CD49AC52B81D6244A6562B9D3F08CE8AB208A8B8878D4C4
SHA-512:	891337D9CD308331BD0166BAA7C99C2B856D47F0ADE8AF596F71AFFC962546BBE0952554C51CC9A10E28BB4CEE3648AEC819D83A8935E69E95F53F5CBF141C 4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn1.sellful.com/wp-content/cache/busting/google-tracking/ga-0a4e309b5f2d7439b4f8876b19f37fc7.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var n=this||self,p=function(a,b){a=a.split(".");var c=n;a[0]in c||"undefin ed"==typeof c.execScript||c.execScript("var "+a[0]);for(var d;a.length&&(d=a.shift());)a.length||void 0===b?c=c[d]&&c[d]!==Object.prototype[d]?c[d]:c[d]={}:c[d]=b};var q= {},r=function(){q.TAGGING=q.TAGGING||[];q.TAGGING[1]=!0};var t=function(a,b){for(var c in b)b.hasOwnProperty(c)&&(a[c]=b[c])},v=function(a){for(var b in a)if(a. hasOwnProperty(b))return!0;return!1};var x=/^(?:(?:https?|mailto|ftp):|[^:/?#]*(?:[/?#]|$))/i;var y=window,z=document,A=function(a,b){z.addEventListener?z.addEventListene r(a,b,!1):z.attachEvent&&z.attachEvent("on"+a,b)};var B=/:[0-9]+$/,C=function(a,b,c){a=a.split("&");for(var d=0;d<a.length;d++){var e=a[d].split("=");if(decodeURIComponen t(e[0]).replace(/\+/g," ")===b)return b=e.slice(1).join("="),c?b:decodeURIComponent(b).replace(/\+/g," ")}},F=function(a,b){b&&(b=String(b).toLowerCase());if("p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\jet-blog.min-2.2.9[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	8501
Entropy (8bit):	5.0870306196602
Encrypted:	false
SSDEEP:	192:lKkO7xbWHSmyPEidPddSWneQAm9g3AFS7e78Q:lKh1myPEid+yeTm9TFi2p
MD5:	BDB89C23157E96CE0A6978293CE0EBFA
SHA1:	B4D7C5D9FAE848643FB9B283D424626A71D50D01
SHA-256:	047370A77F43B356CC417AFAF4B959E9B2C47F7DCFF73271A99EFAC3F25E665C
SHA-512:	C50E0D50C0CB0A96829D81FF3B76DE15388E51DC0B7350AEB3D6268613F1DCCBBBBE1AB8C9053CEB57BF4FD02A72ADB57E30729A5C37323FB5DF56C5C0667 7E
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\jet-blog.min-2.2.9[1].js	
Reputation:	low
IE Cache URL:	http://https://cdn1.sellful.com/wp-content/cache/busting/3146/wp-content/plugins/jet-blog/assets/js/jet-blog.min-2.2.9.js
Preview:	if(!function(c,i,a){"use strict";var o={YT:null,init:function(){var t={"jet-blog-smart-listing.default":o.initSmartListing,"jet-blog-smart-tiles.default":o.initSmartTiles,"jet-blog-text-ticker.default":o.initTextTicker,"jet-blog-video-playlist.default":o.initPlayList};c.each(t,function(t,e){i.hooks.addAction("frontend/element_ready/"+t,e)})},initPlayList:function(i){void 0!==YT.Player?o.initPlayListCb(i,YT):c(document).on("JetYouTubeIframeAPIReady",function(t,e){o.initPlayListCb(i,e)})},initPlayListCb:function(t,e){null===o.YT&&(o.YT=e),t.hasClass("players-initialized")||(t.addClass("players-initialized"),o.switchVideo(t.find(".jet-blog-playlist__item.jet-blog-active")),t.on("click.JetBlog",".jet-blog-playlist__item",function(){t.find(".jet-blog-playlist__canvas").addClass("jet-blog-canvas-active"),o.switchVideo(c(this))})),t.on("click.JetBlog",".jet-blog-playlist__canvas-overlay",o.stopVideo))},initTextTicker:function(t){var r=null,d=t.find(".jet-text-ticker__posts"),e=d.data("typing")

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\lazyload.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	5273
Entropy (8bit):	5.071642558938907
Encrypted:	false
SSDEEP:	96:IncwFK9HqOq0tioPJUQuyhaFBx7Plpr2AVS1h3os81YwgDJf/55haS5OXqfQ9zm6:M9YH9qEJDcrx7Pll2qSPfRtDhaGOX79T
MD5:	B906C7B5D31EFDE9C615DE31CF4C089C
SHA1:	721540E4BABC25B6F245B92AEEF70E993E408D80
SHA-256:	FD9B21475370627E77A6988F76C0BF93A005F9E66C4F2E9FD62E5C2DE5976DC9
SHA-512:	EF912F012E72F697157368BC68636BA86CA945342A894378B08AEFFC12E95809B17E204EE9E397A59BAD7CF1B22CA7E4E85904FF81541837B8120DBDEBBCE062
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn1.sellful.com/wp-content/plugins/wp-rocket/assets/js/lazyload/11.0.6/lazyload.min.js
Preview:	function _extends(){return(_extends=Object.assign||function(t){for(var e=1;e<arguments.length;e++){var n=arguments[e];for(var o in n)Object.prototype.hasOwnProperty.call(n,o)&&(t[o]=n[o])}return t}).apply(this,arguments)}function _typeof(t){return(_typeof="function"==typeof Symbol&&"symbol"==typeof Symbol.iterator?function(t){return typeof t}:function(t){return t&&"function"==typeof Symbol&&t.constructor===Symbol&&t!==Symbol.prototype?"symbol":typeof t})(t)}!function(t,e){"object"===("undefined"==typeof exports?"undefined":_typeof(exports))&&"undefined"!=typeof module?module.exports=e():"function"==typeof define&&define.amd?define(e):t.LazyLoad=e()}(this,function(){"use strict";var t="undefined"!=typeof window,e=t&&!("onscroll"in window)||"undefined"!=typeof navigator&&/(gle|ing|ro)bot|crawl|spider/i.test(navigator.userAgent),n=t&&"IntersectionObserver"in window,o=t&&"classList"in document.createElement("p"),r={elements_selector:"img",container:e||t?document:null,threshold:300,threshol

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\logo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 226 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	3331
Entropy (8bit):	7.927896166439245
Encrypted:	false
SSDEEP:	96:zHjOKn3csE3x5liVsCo4GcPIZpV6x5cge8oo9:zDOK3zE3x5TCwcP4LQNeq
MD5:	EF884BDEDEF280DF97A4C5604058D8DB
SHA1:	6F04244B51AD2409659E267D308B97E09CE9062B
SHA-256:	825DE044D5AC6442A094FF95099F9F67E9249A8110A2FBD57128285776632ADB
SHA-512:	A083381C53070B65B3B8A7A7293D5D2674D2F6EC69C0E19748823D3FDD6F527E8D3D31D311CCEF8E26FC531770F101CDAF95F23ECC990DB405B5EF48B0C91B2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://atendiendochagas.mundosano.org/kcontrol-inti/continue/new/s/files/logo.png
Preview:	.PNG.....IHDR.....0.....sRGB.....IDATx..=w....G.z..L.4fN.k\dS..._`.....r...~.F..e._.RZ.0.K.\..CB...1.{qq/..^|.G..o.....?....Or.....y~....]..V.a.mM...M.\k*H..@B`s.$"n...)!.@"b#4. !.9...7.u...hD ....T.....:EJ.4"..X.....<\|.pgkk+....>~.....pju1i"b.J.&!.!...=T....k..D7.....O.<.?}...../..(.`0..!.C..'.?..e..~.....l6...._.x1rmR...$|E...l.WKDH...f..... ...Y.0R....>...{...-..o.....,...E./....._....eM.Q....@Q...w sp5.9..l.W)...Pq... .]..B..).../M.G.g....].V...5$<.....Eb.9.....>LYAk.Z.k..b..]N%>}4a....4!S...t..d..<.8AH+.../r...._...!qt.:q..fR.:..KW..._...T...5..>.0!.hq.rbND\...XR..,2.uX..Q.b...wQ.....g..X...F...~.....ikZE...UA....V.I!..]..Mm..R.....~k.VC.n..V.*B#W...\..yI.3.....2.....6c....2J....,g..5O1.s.4V2.....f..K..Obf\....;.w...\|.F>F>6_z..P.dU<.wVV.....?.q.?&.....O.>....l.S.upp....59.C_.....fJ.M.={v,.....]Y_....n.?UF....v<.$..AD...p.....:$r =p...C.k.3....n.v..~.TGd!...l.W...s..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\s[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17394
Entropy (8bit):	3.324079896074607
Encrypted:	false
SSDEEP:	384:rKp84GZw7WZ1v5jBi1FnJICqWqjbTSIHaTPqsHkEiroLOweZnZq5fy6CJP:r+WfhjDUS
MD5:	474A9980C4D204E7D4B593832B226BEA
SHA1:	DBDB72D920A55C1AB76FDA122271C9986C8F9389
SHA-256:	163589FCFF3F5D67836D8DF3EC13D11E561E93C25B9679D3BA92B98F9D34EABF

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\s[1].htm	
SHA-512:	DFC58C88418F96A98009D0FF7BF626C5679A20BD63B0FE20C7B792D6EB95CD26C3206978DAB6DE70DA6CDDEAA612663C3972BAB5930DC84ADF1820F407A5E 14
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_6, Description: Yara detected HtmlPhish_6, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\s[1].htm, Author: Joe Security
Reputation:	low
Preview:	..<script type="text/javascript">....document.write(unescape('%3c%6d%65%74%61%20%63%68%61%72%73%65%74%3d%22%55%54%46%2d%38%22%20%6 e%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%2e%30%2c%20%6d%61%78%69%6d%75%6d%2d%73%63 %61%6c%65%3d%31%2e%30%2c%20%6d%69%6e%69%6d%75%6d%2d%73%63%61%6c%65%3d%31%2e%30%2c%20%75%73%65%72%2d%73%63%61%6 c%61%62%6c%65%3d%6e%6f%22%3e%0d%0a%09%3c%74%69%74%6c%65%3e%56%61%6c%69%64%61%74%69%6f%6e%3c%2f%74%69%74%6c%65% 3e%0d%0a%09%3c%6c%69%6e%6b%20%72%65%6c%3d%22%73%74%79%6c%65%73%68%65%65%74%20%70%72%65%66%65%74%63%68%22%20%68 %72%65%66%3d%22%68%74%74%70%73%3a%2f%2f%66%6f%6e%74%73%2e%67%6f%6f%67%6c%65%61%70%69%73%2e%63%6f%6d%2f%63%73%7 3%3f%66%61%6d%69%6c%79%3d%4f%70%65%6e%2b%53%61%6e%73%3a%36%30%30%22%3e%0d%0a%09%3c%6c%69%6e%6b%20%72%65%6c%3d% 22%73%74%79%6c%65%73%68%65%65%74%22%20%68%72%65%66%3d%22%2e%2f%66%69%6c%65%73%2f%63%73%73%2e%63%73%7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\s[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17394
Entropy (8bit):	3.324079896074607
Encrypted:	false
SSDEEP:	384:rKp84GZw7WZ1v5jBi1FnJICqWqjbTSIHaTPqsHkEiroLOweZnZq5fy6CJP:r+WfhjDUS
MD5:	474A9980C4D204E7D4B593832B226BEA
SHA1:	DBDB72D920A55C1AB76FDA122271C9986C8F9389
SHA-256:	163589FCFF3F5D67836D8DF3EC13D11E561E93C25B9679D3BA92B98F9D34EABF
SHA-512:	DFC58C88418F96A98009D0FF7BF626C5679A20BD63B0FE20C7B792D6EB95CD26C3206978DAB6DE70DA6CDDEAA612663C3972BAB5930DC84ADF1820F407A5E 14
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_6, Description: Yara detected HtmlPhish_6, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\s[2].htm, Author: Joe Security
Reputation:	low
Preview:	..<script type="text/javascript">....document.write(unescape('%3c%6d%65%74%61%20%63%68%61%72%73%65%74%3d%22%55%54%46%2d%38%22%20%6 e%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%2e%30%2c%20%6d%61%78%69%6d%75%6d%2d%73%63 %61%6c%65%3d%31%2e%30%2c%20%6d%69%6e%69%6d%75%6d%2d%73%63%61%6c%65%3d%31%2e%30%2c%20%75%73%65%72%2d%73%63%61%6 c%61%62%6c%65%3d%6e%6f%22%3e%0d%0a%09%3c%74%69%74%6c%65%3e%56%61%6c%69%64%61%74%69%6f%6e%3c%2f%74%69%74%6c%65% 3e%0d%0a%09%3c%6c%69%6e%6b%20%72%65%6c%3d%22%73%74%79%6c%65%73%68%65%65%74%20%70%72%65%66%65%74%63%68%22%20%68 %72%65%66%3d%22%68%74%74%70%73%3a%2f%2f%66%6f%6e%74%73%2e%67%6f%6f%67%6c%65%61%70%69%73%2e%63%6f%6d%2f%63%73%7 3%3f%66%61%6d%69%6c%79%3d%4f%70%65%6e%2b%53%61%6e%73%3a%36%30%30%22%3e%0d%0a%09%3c%6c%69%6e%6b%20%72%65%6c%3d% 22%73%74%79%6c%65%73%68%65%65%74%22%20%68%72%65%66%3d%22%2e%2f%66%69%6c%65%73%2f%63%73%73%2e%63%73%7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\share-link.min-3.1.1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	2578
Entropy (8bit):	5.177015723485366
Encrypted:	false
SSDEEP:	48:mPTblyuvUkJipDUGr207o/9QZOF1JzOTPUzGbe2yhL4rXpDeiUkLTj7fWfPfpC7X:mPnlyuv/IpDUGr20KqZOFPOzUb2nrXpZ
MD5:	9BB8540493A7FE11B229870EB37BE165
SHA1:	D77F17CB9057DC8F622B8C0BF23F6ACB739B3B8E
SHA-256:	4A7EE62EB33F3BBB66C2151E5CAC6BF4904E28302EFC36128F3E3CCAE6FDE580
SHA-512:	FB245059108EE476BFBCA60A96D401C2796EE44B646E0874D41B5FDB1204A66E3BEC6A4AB8E155E50489B3ADF48BD609683B3D1C020B9F39D084A915F837777
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn1.sellful.com/wp-content/cache/busting/3146/wp-content/plugins/elementor/assets/lib/share-link/share-link.min-3.1.1.js
Preview:	(function(a){window.ShareLink=function(b,c){var d,e={},f=function(a){var b=a.substr(0,e.classPrefixLength);return b===e.classPrefix?a.substr(e.classPrefixLength):null},g= function(a){d.on("click",function(){h(a)})},h=function(a){var b="";if(e.width&&e.height){var c=screen.width/2-e.width/2,d=screen.height/2-e.height/2;b="toolbar=0,status=0 ,width="+e.width+",height="+e.height+",top="+d+",left="+c}var f=ShareLink.getNetworkLink(a,e),g=/^https?:\/\/.test(f),h=g?"":"_self";open(f,h,b)},i=function(){a.each(b.c lassList,function(){var a=f(this);if(a)return g(a),!1})},j=function(){a.extend(e,ShareLink.defaultSettings,c),["title","text"].forEach(function(a){e[a]=e[a].replace("#","")}),e.cla ssPrefixLength=e.classPrefix.length},k=function(){d=a(b)};(function(){j(),k(),i()})()},ShareLink.networkTemplates={twitter:"https://twitter.com/intent/tweet?text={text}\x 20{url}",pinterest:"https://www.pinterest.com/pin/create/button/?url={url}&media={image}",facebook:"https://www.facebook.com/sharer.php?u={u

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\MC8R5KA7.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\MC8R5KA7.htm	
Category:	downloaded
Size (bytes):	23111
Entropy (8bit):	5.290380324630683
Encrypted:	false
SSDEEP:	384:oaiTh2gpHvHO5H9AO6jogtqJ6JPJeJuWJAJTtWJ6JPJeJS/N5uYu7nTgdePPqvmJ:oaiTbpPu5H9AnGJ6JPJeJuWJAJgJ6JPO
MD5:	A1195EB5C3C6D7B2258505A0B11FC1A2
SHA1:	96DC8419032CD521DA33E4AD76DCFBCABCB157AE
SHA-256:	C401366641ABCD9E1856FC7D2641CF14F77CE5A9009C5C378E9E50ABDAA95CC4
SHA-512:	2E36F4C65D359BF76F6860579C2F24EECF94AF55EA8156C595D822E18F7E7C65E0B618F676959F9CAA023F4556DB483BF49A9FCD439FA22EC0B214CA85C6C06
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://securepay.mysellful.com/
Preview:	<!doctype html><html lang="en-US" prefix="og: http://ogp.me/ns#"><head><meta charset="UTF-8"><meta name="viewport" content="width=device-width, initial-scale=1"><link rel="profile" href="https://gmpg.org/xfn/11"><meta http-equiv="x-dns-prefetch-control" content="on"><link rel="preconnect" crossorigin href="//stateless.sellful.com" /><link rel="preconnect" href="//cdn1.sellful.com" /><link rel="preconnect" crossorigin href="//fonts.googleapis.com" /><link rel="preconnect" crossorigin href="//ajax.googleapis.com" /><link rel="preconnect" crossorigin href="//apis.google.com" /><link rel="preconnect" crossorigin href="//google-analytics.com" /><link rel="preconnect" crossorigin href="//www.google-analytics.com" /><link rel="preconnect" crossorigin href="//ssl.google-analytics.com" /><link rel="dns-prefetch" href="//youtube.com" /><link rel="preconnect" crossorigin href="//fonts.gstatic.com" /><link rel="preconnect" crossorigin href="//fonts.gstatic.com/s/" /><style>#ub_global_footer_conten

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\admin-ajax[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	very short file (no magic)
Category:	downloaded
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://securepay.mysellful.com/dashboard/admin-ajax.php?action=wu_count_visits&code=6132cfcf5a
Preview:	1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\c6561660-new-remittance-785x800[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 785 x 800, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	152673
Entropy (8bit):	**7.990638263266791**
Encrypted:	**true**
SSDEEP:	3072:ytxeTRjbnkb3i/XeBAtdnmng/v2WQfWQTm7uffXYwvZ1oMEhvW/:y6TRHW+1AyGWIPboMEhS
MD5:	F3ABDCA15BFA18336CFC35F883491739
SHA1:	335C15AA3E10703589CE0CF0F64A9A373120F235
SHA-256:	67DFDFB4D1A369156EB7F956AE26B1FCE3634AC737DCEEFF5DAD5DAEDB0CE6BC
SHA-512:	2290035BE750566C90B946BBB16B58A8F76A553EFCF1DD49B9E289E7D8AA5AA11492E859A3BB8A7B150AABE19C056E4F803E792219763F348F137D207069E49C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://stateless.sellful.com/2021/04/c6561660-new-remittance-785x800.png
Preview:	.PNG.....IHDR..... .....#x9..T(IDATx..}ac.6.,.....?...E.x.@.4..L..nrG.\..Q.)u.,....;.X.b..+V..2x..+V.X.b...V.X.b..+.fZ.b..+V.X.i..+V.X.ba..+V.X.b...V.X.b..+.fZ.b..+V.X.i..+V .X.b..L+V.X.b...3.X.b..+V,.b..+V.X.0..+V.X.b..L+V.X.b...3.X.b..+V,.b..+V.X.8...}..._..^...b..+V.X...L>.....?.]....y..x.??H,...?t_t..+V.X..wl..Jr.]`...../...v?.._p.|.?.....#.]0t.?..... ....f.gc.O.....U.3n.....}.tr',;..}....~..6..}./...._.....?1._.p.p9..Z0-.....v..;._D..X.|..,.....M1....?..Lk.8./..s..}.>.*O..Y*W,..;...w'2.....x.....h|.i./.....9.....9..A....{..c.`.oq.b...S. ".l.>..Oa.8xz...G..P..9.....>YFZ....F...,O.$3.....n.0%.....0...>O..Mwx:r<>?..%.>..i...b^....9.).@.f..$.....3Pp.. l.=....s.....F....U .'.6.<._.....>..u...../...K.....u.?.8..w 3wr....'O.....V.]...L._...s..]..B...sm.@.V...i...a.]...7yb..{...jb...*.5..< ..x..+....Ot.3..P..! H.@,..T.....S.....#'#R.g..6.;....D|.|.=~.V.vQ...N`....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\ccaf1bb7df93920b7090e89ad7f87719[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	962960
Entropy (8bit):	4.9838251465791545
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\ccaf1bb7df93920b7090e89ad7f87719[1].css	
SSDEEP:	24576:0akeSkXmBQ2hXTtK0sBCwRgwIsrS26LTFTF:xkeSkXmBQSXTSgwO
MD5:	94547D32CD5E7AFFFDF394055C5C767D
SHA1:	10E65A16AD492DFEF08374373BCAED3559159D61
SHA-256:	3BFA9CA8A9F68321B95EABB8E2401C2725C76E967A9C2A560C4C2014C351DA11
SHA-512:	93977CD46D315E8123831E3D37E081159F88821203B940267188DD60EAC8B957862C09F1D868621237C40607D683849DAEAF8947088B3C869C209FB57351E436
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn1.sellful.com/wp-content/cache/min/3146/ccaf1bb7df93920b7090e89ad7f87719.css
Preview:	.wp-block-audio figcaption{margin-top:.5em;margin-bottom:1em;color:#555d66;text-align:center;font-size:13px}.wp-block-audio audio{width:100%;min-width:300px}.block-editor-block-list__layout .reusable-block-edit-panel{align-items:center;background:#f8f9f9;color:#555d66;display:flex;flex-wrap:wrap;font-family:-apple-system,BlinkMacSystemFont,Segoe UI,Roboto,Oxygen-Sans,Ubuntu,Cantarell,Helvetica Neue,sans-serif;font-size:13px;top:-14px;margin:0 -14px;padding:8px 14px;position:relative;border:1px dashed rgba(145,151,162,.25);border-bottom:none}.block-editor-block-list__layout .block-editor-block-list__layout .reusable-block-edit-panel{margin:0 -14px;padding:8px 14px}.block-editor-block-list__layout .reusable-block-edit-panel .reusable-block-edit-panel__spinner{margin:0 5px}.block-editor-block-list__layout .reusable-block-edit-panel .reusable-block-edit-panel__info{margin-right:auto}.block-editor-block-list__layout .reusable-block-edit-panel .reusable-block-edit-panel__label{margin-right:8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\frontend.min-3.0.5[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with LF, NEL line terminators
Category:	downloaded
Size (bytes):	172226
Entropy (8bit):	5.177850445576503
Encrypted:	false
SSDEEP:	1536:fUoTZWLyt96lLV35l00ytezfURlR/TgXrCn2kCA79hJUWpyLBYAyXEaan7Jd8dFS:fUoTZIymlEv6vGylDddi5knbM
MD5:	64A17E19546A8EAEB7449982967CFA69
SHA1:	B777FF3056A8DD8C79F93C0125F21EC3909C9802
SHA-256:	65115988F62E8284EBC9BBD735C7DE493F47ED8EA5A266FDDB4C86D4997472FB
SHA-512:	C3F3B69EF730C492AC5FED2313A334F72CA0C317EA9F3224A5BC780D18B766EFD4EEB1F4DAA024BBE0837A842E63B75C9E0A144A6E8FC4EA2A940E55950769 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn1.sellful.com/wp-content/cache/busting/3146/wp-content/plugins/elementor-pro/assets/js/frontend.min-3.0.5.js
Preview:	/*! elementor-pro - v3.0.5 - 23-09-2020 */.!function(e){var t={};function n(i){if(t[i])return t[i].exports;var r=t[i]={i:i,l:!1,exports:{}};return e[i].call(r.exports,r,r.exports,n),r.l=!0,r .exports}n.m=e,n.c=t,n.d=function(e,t,i){n.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:i})},n.r=function(e){"undefined"!=typeof Symbol&&Symbol.toString Tag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},n.t=function(e,t){if(1&t&&(e=n(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var i=Object.create(null);if(n.r(i),Object.defineProperty(i,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var r in e)n.d(i,r,function(t){return e[t]}.bind(null,r));return i},n.n=function(e){var t=e&&e.__esModule?function(){return e.default}:function(){return e};return n.d(t," a",t),t},n.o=function(e,t){return Object.prototype.hasOwnProperty.call(e,t)},n.p="",n(n.s=474)}([function(e,t,n){e.exports=n(113)},function(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\jet-tricks-frontend-1.2.12[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	20554
Entropy (8bit):	5.001175704365427
Encrypted:	false
SSDEEP:	384:vPiXLzLL3fu7Dlof01DlwZtWSHyk5hAoALTKAI7NEdoALTwI3aoALTKpmlQLH83y:vPovHIDsSIktBHAoALTKPKdoALTzaoAn
MD5:	61EE94A46DB07B5D0ADDD2F1CB20AF10
SHA1:	513E714A9FA59ACBBE436EA70EAE7EC8DD5B87C1
SHA-256:	340CB3133FD2998435B655096B9DDFC1F24DB65D66F296A7369643C4256273B9
SHA-512:	604270F1291B03C65E85E4B3FC106D60FE7F7A73F110E55D668A502164F40D6A0FAC23A2A753F46BD3DCDE1B9FA34A44ABDC38E66A3864AF63F3315B3997B3E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn1.sellful.com/wp-content/cache/busting/3146/wp-content/plugins/jet-tricks/assets/js/jet-tricks-frontend-1.2.12.js
Preview:	(function($, elementor) {...'use strict';...var JetTricks = {....init: function() {....elementor.hooks.addAction('frontend/element_ready/section', JetTricks.elementorSection); ....elementor.hooks.addAction('frontend/element_ready/column', JetTricks.elementorColumn);....elementor.hooks.addAction('frontend/element_ready/widget', JetTricks.elementorWidget);.....var widgets = {.....'jet-view-more.default' : JetTricks.widgetViewMore,.....'jet-unfold.default' : JetTricks.widgetUnfold,.....'jet-hotspots.default' : JetTricks.widgetHotspots....};.....$.each(widgets, function(widget, callback) {.....elementor.hooks.addAction('frontend/element_ready/' + widget, callback);....});...},....elementorSection: function($scope) {....var $target = $scope,.....sectionId = $scope.data('id'),.....editMode = Boolean(elementor.isEditMode()),.....settings = {};.....if (window.JetTricksSettings && window.JetTricksSettings.elements_data.sections.hasOwnProperty(section

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\jquery-1.12.4-wp[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	96873
Entropy (8bit):	5.372169393547772
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\jquery-1.12.4-wp[1].js	
SSDEEP:	1536:HYE1fGBiByJsbfXXeRJ/shgWCeLLccJdZVHk04ssx+/mvaSIFSet43tpXJIGVyp3:fsAg0psxTva/FSeKy2bDD5a98Hrq
MD5:	49EDCCEA2E7BA985CADC9BA0531CBED1
SHA1:	F8747F8EE704D9AF31D0950015E01D3F9635B070
SHA-256:	1DB21D816296E6939BA1F42962496E4134AE2B0081E26970864C40C6D02BB1DF
SHA-512:	F766DF685B673657BDF57551354C149BE2024385102854D2CA351E976684BB88361EAE848F11F714E6E5973C061440831EA6F5BE995B89FD5BD2D4559A0DC4A6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn1.sellful.com/wp-content/cache/busting/3146/wp-includes/js/jquery/jquery-1.12.4-wp.js
Preview:	/*! jQuery v1.12.4 | (c) jQuery Foundation | jquery.org/license | WordPress 2019-05-16 */.!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 window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProperty,l={},m="1.12.4",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?a<0?this[a+this.length]:this[a]:e.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a){return n.each(this,a)},map:function(a){return this.pushStack(n.map(this,fu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\jquery-migrate.min-1.4.1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	10056
Entropy (8bit):	5.308628526814024
Encrypted:	false
SSDEEP:	192:kZrk/GNyd31svs7wkX8KzJcqSDdAcHX4YE5NLR:srhNyNO0kkMKzFSDdAcIYwLR
MD5:	7121994EEC5320FBE6586463BF9651C2
SHA1:	90532AFF6D4121954254CDF04994D834F7EC169B
SHA-256:	48EB8B500AE6A38617B5738D2B3FAEC481922A7782246E31D2755C034A45CD5D
SHA-512:	B74A2F03C64E883B9A34DE43690429327DFB4AA230A7A6AFCA8150A16E3D84E98461245FF264C26368D9904562CC34FE219F71F951D364FA5C68C039B76776CD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn1.sellful.com/wp-content/cache/busting/3146/wp-includes/js/jquery/jquery-migrate.min-1.4.1.js
Preview:	/*! jQuery Migrate v1.4.1 | (c) jQuery Foundation and other contributors | jquery.org/license */."undefined"==typeof jQuery.migrateMute&&(jQuery.migrateMute=!0),function(a,b,c){function d(c){var d=b.console;f[c]||(f[c]=!0,a.migrateWarnings.push(c),d&&d.warn&&!a.migrateMute&&(d.warn("JQMIGRATE: "+c),a.migrateTrace&&d.trace&&d.trace()))}function e(b,c,e,f){if(Object.defineProperty)try{return void Object.defineProperty(b,c,{configurable:!0,enumerable:!0,get:function(){return d(f),e},set:function(a){d(f),e=a}})}catch(g){}a._definePropertyBroken=!0,b[c]=e}a.migrateVersion="1.4.1";var f={};a.migrateWarnings=[],b.console&&b.console.log&&b.console.log("JQMIGRATE: Migrate is installed"+(a.migrateMute?"":" with logging active")+", version "+a.migrateVersion),a.migrateTrace===c&&(a.migrateTrace=!0),a.migrateReset=function(){f={},a.migrateWarnings.length=0},"BackCompat"===document.compatMode&&d("jQuery is not compatible with Quirks Mode");var g=a("<input/>",{size:1}).attr("size")&&a.attrFn,h=a.att

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\new[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	274
Entropy (8bit):	5.103985734252342
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwol6hEr6VX16hu9nPhoA2Lc+Q6Q+KqD:J0+ox0RJWWPh5ET
MD5:	0E241B8D33B2AE011B112941747BA154
SHA1:	1F027D10066871A789A960053D74B17B81843920
SHA-256:	2F3D726E8D6811D028A298E3BF49D01FBC0D12AD6D91993EE16CA5BDEC111295
SHA-512:	011C5578E3BEA4EBF8DE11F141F0044AEB7AF3608DB15B1545C4EF23A3B5B8187D7888978C76C87B48D1ED44DF28203D37395617F075254B8CE67D6D1EC7A9C
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>301 Moved Permanently</title>.</head><body>. Moved Permanently . The document has moved here. .</body></html>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\v4-shims.min-3.1.1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	15055
Entropy (8bit):	4.548869590540711
Encrypted:	false
SSDEEP:	192:bP6Vw28fajqZFSJtd4fxVOT2iQsVJqYqV5PnX9dUWFjWqh2P9e93f7POD3o:OX8fajqZFwtdykZwRXcoWI2P9o7S3o
MD5:	7A5DEA0A705CC2F4CD87DBAAA6666BC6
SHA1:	678BC6F750F13ADB29BBC158EB0D9CD813B736FA
SHA-256:	97CF1307C16A437B77B5F7F5C9BC0B985D0745A14BE5A279019ACA5A3432E264

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\v4-shims.min-3.1.1[1].js	
SHA-512:	7C19D0EDC28FE8733075534DE6176483416BB3535F37B7607536AEA2DDF9C5591D864225049C9A74735C1DAF44C72688D91C1133BB018683ADE11F16EA596807
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn1.sellful.com/wp-content/cache/busting/3146/wp-content/plugins/elementor/assets/lib/font-awesome/js/v4-shims.min-3.1.1.js
Preview:	/*!. * Font Awesome Free 5.15.1 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license/free (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */.var l,a;l=this,a=function(){"use strict";var l={},a={};try{"undefined"!=typeof window&&(l=window),"undefined"!=typeof document&&(a=document)}catch(l){}var e=(l.navigator||{}).userAgent,r=void 0===e?"":e,n=l,o=a,u=(n.document,!!o.documentElement&&!!o.head&&"function"==typeof o.addEventListener&&o.createElement,~r.indexOf("MSIE")||r.indexOf("Trident/"),"___FONT_AWESOME___"),t=function(){try{return"production"===process.env.NODE_ENV}catch(l){return!1}}();var f=n||{};f[u]||(f[u]={}),f[u].styles||(f[u].styles={}),f[u].hooks||(f[u].hooks={}),f[u].shims||(f[u].shims=[]);var i=f[u],s=[["glass",null,"glass-martini"],["meetup","fab",null],["star-o","far","star"],["remove",null,"times"],["close",null,"times"],["gear",null,"cog"],["trash-o","far","trash-alt"],["file-o","far","file"],["clock-o","far","clock"],["arro

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\webpack.runtime.min-3.1.1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	4626
Entropy (8bit):	5.358820430051677
Encrypted:	false
SSDEEP:	96:BcQS4KssNLRu/QLXluU/MxV/LUVHwK2U2fdkGltCX:fS4kPJLNMxdQeTFHk
MD5:	7423529C58B1A1BF4EE735F7AFBB59BD
SHA1:	52D72A236F4925E5BD2C0A173A03C7CA8A92BBA8
SHA-256:	E9286A9B5C5047627AFB876EBE1C90933EE1C438164D529D01D80C4636C4B405
SHA-512:	820F4F987F67BC271BB7C098E21BED9F14F5528D6DBD30F62E90F5D331AA9475434EA54602F24BC80EBE7FF4E673059D7E4493049064B029BAC463826609D039
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn1.sellful.com/wp-content/cache/busting/3146/wp-content/plugins/elementor/assets/js/webpack.runtime.min-3.1.1.js
Preview:	/*! elementor - v3.1.1 - 31-01-2021 */.(()=>{"use strict";var e,r,_={},t={};function __webpack_require__(e){if(t[e])return t[e].exports;var r=t[e]={exports:{}};return _[e](r,r.exports,__webpack_require__),r.exports}__webpack_require__.m=_,__webpack_require__.t=function(e,r){if(1&r&&(e=this(e)),8&r)return e;if(4&r&&"object"==typeof e&&e&&e.__esModule)return e;var _=Object.create(null);__webpack_require__.r(_);var t={};if(2&r&&"object"==typeof e&&e)for(const r in e)t[r]=()=>e[r];return t.default=()=>e,__webpack_require__.d(_,t),_},__webpack_require__.d=(e,r)=>{for(var _ in r)__webpack_require__.o(r,_)&&!__webpack_require__.o(e,_)&&Object.defineProperty(e,_,{enumerable:!0,get:r[_]})},__webpack_require__.f={},__webpack_require__.e=e=>Promise.all(Object.keys(__webpack_require__.f).reduce(((r,_)=>(__webpack_require__.f[_](e,r),r)),[])),__webpack_require__.u=e=>209===e?"accordion.959b6d3705116b2a55b1.bundle.min.js":745===e?"alert.f4e7a6df1283698dea78.bundle.min.js":120===e?"counter.99f87b466b

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\KFOjCnqEu92Fr1Mu51S7ACc6CsI[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 22080, version 1.1
Category:	downloaded
Size (bytes):	22080
Entropy (8bit):	7.970620647480227
Encrypted:	false
SSDEEP:	384:BfnIIA0zhdg/5oXRAZDRsZObG141wGUaBgKYADioTCgZM6+HJtWjbmMbQMbL2nNQ:B00zhdW7ZDRsR141wYAoTCGUptzMbqnu
MD5:	FA8878D8872A2AC4BEB377CDAE15566A
SHA1:	34EE72B0E553C3EFA41A7E0DF4EB710596469A10
SHA-256:	8411023A027610AEB3DC333438E12A17222163AE78817C5395DA04548ED30150
SHA-512:	112ED53A4A18EB3378A57B154566C0F1AF438FF400EBE453253F5E2465B6A07370B447736EACB99114ED43E05CAE5A3A019BE6886D50EB15FA1E2D6F35D9AFBA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOjCnqEu92Fr1Mu51S7ACc6CsI.woff
Preview:	wOFF.....V@.....0.....GDEF.....G...d....GPOS.....oGSUB.....OS/2...p...N...`t..dcmap.....#cvt .....\...\1..Mfpgm...4...2.....$.gasp...h.....glyf...t..Bf..s...hdmx..N....l....(/./head..OH...6...6...vhhea..O....#...$....hmtx..O.....*:8loca..R@.....*.imaxp..T8... ... .4..name..TX.....!.>gpost..U4..... .a.dprep..UL.....X9..x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x....%Y....Wm=..mo..k.m....rl...m.g"^..../..[.}.S...\.mD...1..G>..giz...=C..}.y....|o..c.x.R.r"B.....m.../../&./6..5D.AGX.....)<'.)....?.... .Y4>|1...ES.Gc...FO.>$.../...}RCl..T.zD..uZ4~D.._OK.$.Z.(..JR...\..\..\..\.\.....*'n..6:x...b,..$...?.g:./y.iLg.3..l.0.y.g..X..V...d.#O...0....b7{..>.n.iD.V....." e.\A..OR.kwp.].....6p..."ZE..%...e.u3..L..V...W.7b..L.3.L1K...Ts..$6.-b.....9...b@..!1,...v.C....{...dox.G(...|a%E:.Fn.Nn.^n.....Sf..E)...k....<g..){....|.....DT..N....Hy.F.Jez....._?7.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\KFOjCnqEu92Fr1Mu51TjASc6CsI[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 22280, version 1.1
Category:	downloaded
Size (bytes):	22280
Entropy (8bit):	7.9727639867534075
Encrypted:	false
SSDEEP:	384:P9oOx7sdtvlKnxdf5DGTHz3uPGia2ghi4OEiO+KdRialMgTC3YS95HbcW8Y:1lZsdKnxdBDwz++ia2l4OEi7KCquoS9J
MD5:	6E949B62AF2E8B6F705E35EE4DBC17F4
SHA1:	31BC06C0C932EC0176F42C6864C58D7450BBF97E

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\KFOjCnqEu92Fr1Mu51TjASc6Csl[1].woff	
SHA-256:	917A5159BE44DE9A82072F6A1C52EF645844D6BEDF42F8FD1549CD99D6DB2CC5
SHA-512:	109EF637EF3C4FB1670DD328466BF1507F0E92D97153A71CA045F3F17F924CC92FF75777B3730CF722825C755D646A796F429F50973C64B543AA13C174D8921B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOjCnqEu92Fr1Mu51TjASc6Csl.woff
Preview:	wOFF.....W.....x.....GDEF.....G...d....GPOS.....!GSUB.....OS/2...L...N...`t6.<cmap.....#cvt .....X...X/...fpgm.....4.....".gasp...@..... ....glyf...L..C`..tP>.e%hdmx..O....m....$+.-head..P....6...6...mhhea..PT...#...$...zhmtx..Px.....3J.loca..S.....maxp..U.... ... .4..name..U0.....>.post..V..... .a.dprep..V $.....?.1 .x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x...l\..F..3...N..q)..a|.....^..33..c.....p"y.iT....<Gg...!.3...T1...{.g0.u.y.....m.|.k..NF.....mox. ;...7&.Y..C.R_[.T.c..-.=...9:...a*j.G.....O.Q".6...>...(?...~...._.2:..K4....S%...jbr).....*....e.U..-..X.3.ILQ....z..!.f:...<.W.#...e.c=...&6...lc;;..3<.s<....H.i2..N..t..)Ns...#`..".).[... ._.T..T.....+l..=..O.....Z..F...r..eM.f.Y.....-...r.\.s6.r..,...:.<$..#.l..F.$.2#.e..].[.....yR...e.|{..O..`)..U.0.e.50.Z.b../cM..i.&O._..+.Y.W...;z....j.p._.o..[CL.)n'.UGx..>).X..MJ..Fr..v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\KFOkCnqEu92Fr1Mu51xIIzQ[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 22036, version 1.1
Category:	downloaded
Size (bytes):	22036
Entropy (8bit):	7.974581575530646
Encrypted:	false
SSDEEP:	384:WhoOtWgD0GjcBsPSQSQhzT8EeFVJDOFKA3t1pLXhj8gGddsbnDX1F:4l30GI/cRMzqKA91pNj89WnDX1F
MD5:	522AECAD450B10CE647739BC8D9AA1C6
SHA1:	6C3528F1BDD5B980F41BDCD1D9FCD812FE0C6D61
SHA-256:	2B5FB1F0EE063320196A64157AE9A949BB4656BC48604914175F1EDA636DCE07
SHA-512:	33AAAE71C92278EE04102EE59B3856DB9EB7C6F187EC35BBD302492619CA47811FF379A2B469DAF670407ADEA10B3BCF56A7B883CD1241447957471263CF95B3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOkCnqEu92Fr1Mu51xIIzQ.woff
Preview:	wOFF.....V.....x.....GDEF.....G...d....GPOS.....!GSUB.....OS/2...L...O...`t..Rcmap.....#cvt .....R...R..-.fpgm.....4....s...gasp...<.....glyf.. .H..Bd..rp}..hdmx..N....m....#-.,head..O....6...6...ehhea..OT...#...$....hmtx..Ox.....cC.loca..R..... |.maxp..T.... ... .4..name..T0.....:.post..U..... .a.dprep..U .....D. .].x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x...l\..F..3...N..q)..a|.....^..33..c.....p"y.iT....<Gg...!.3...T1...{.g0.u.y.....m.|.k..NF.....mox.;...7&.Y.. C.R_[.T.c..-.=...9:...a*j.G.....O.Q".6...>...(?...~...._.2:..K4....S%...jbr).....*....e.U..-..X.3.ILQ....z..!.f:...<.W.#...e.c=...&6...lc;;..3<.s<....H.i2..N..t..)Ns...#`..".).[....._.T..T... ..+l..=..O.....Z..F...r..eM.f.Y.....-...r.\.s6.r..,...:.<$..#.l..F.$.2#.e..].[.....yR...e.|{..O..`)..U.0.e.50.Z.b../cM..i.&O._..+.Y.W...;z....j.p._.o..[CL.)n'.UGx..>).X..MJ..Fr..v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\KFOlCnqEu92Fr1MmEU9fBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20532, version 1.1
Category:	downloaded
Size (bytes):	20532
Entropy (8bit):	7.966425322589798
Encrypted:	false
SSDEEP:	384:tfEIIA0zhnegvIQxhXmqd8lpP/FwL0cV8yP1JSRHbNHlZL7qwZkoEu3HTbpXcyKd:tr0zhnewHxRmqd8PdwLLeR/ZLGwZLbTA
MD5:	DA2721C68B4BC80DB8D4C404F76B118C
SHA1:	3A32E8B7EFBC9DFB52F024D657B8C8C0A80E5804
SHA-256:	BD811625271ACCA47F7DAC48B460F13E08EE947B2A8E17E278C4D5CCB5D9323C
SHA-512:	5110656E41A261BD2A06F8B5B2A362FF8836B4289E1DE0777D83DB8E9D709C4C4248B67653A28FA47AD4AE823021ADBFC587900E142BF6887C2A7C936F7F4C33
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmEU9fBBc-.woff
Preview:	wOFF.....P4.....l.....GDEF.....G...d....GPOS.....oGSUB.....OS/2...p...Q...`t...cmap.....#cvt .....\...\1..Kfpgm...8...2.....$.gasp...l.....glyf... x..<e..n..W..hdmx..H....m....+1.3head..IP...6...6...rhhea..I.... ...$....hmtx..I.....S.loca..L8.....maxp..N4... ... .4..name..NT.....:.post..O0..... .m.dprep..OD.....S.. .)x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x....%Y....Wm=..mo..k.m....rl...m.g"^..../..[.}.S...\.mD...1..G>..giz...=C..}.y....|o..c.x.R.r"B.....m...../.&./ 6..5D.AGX....)<'.)....?.... .Y4>|1...ES.Gc...FO.>$.../...}RCl..T.zD..uZ4~D._OK.$.Z.(..JR...\..\..\..\.\.....*'n..6:x...b,..$...?.g:./y.iLg.3..l.0.y.g..X..V...d.#O...0....b7{..>.n.iD.V....." e.\A..OR.kwp.].....6p..."ZE..%...e.u3..L..V...W.7b..L.3.L1K...Ts..$6.-b.....9...b@..!1,...v.C....{...dox.G(...|a%E:.Fn.Nn.^n.....Sf..E)...k....<g..){....|.....DT..N....Hy.F.Jez....._? 7.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\KFOlCnqEu92Fr1MmSU5fBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20404, version 1.1
Category:	downloaded
Size (bytes):	20404
Entropy (8bit):	7.970248785137973
Encrypted:	false
SSDEEP:	384:8uFoOxqigBacqKz8RGLv6K5a+jZ/rFSyeM5B8r/WjRy0BsM16t/PJ:PFlIvUKz8R+t5N53eGar/gY0Bv6tp
MD5:	BF0F407102FAF3A0B521D3B545F547A5
SHA1:	CA357CD0DE5DD0242E8EFACFB8D24AB60FDC86AB
SHA-256:	855A06974032BB69157D469ABA6F63440E8BE47C421F45C3F396F4E0B87B6DE8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\KFOlCnqEu92Fr1MmSU5fBBc-[1].woff	
SHA-512:	85359028F7FE49B1DF90B72E48DC7DE4B21F1B65E8BF109595705A3F4EAF9FA79854B5AEF060FE266291C5ECE9D04FCEAD1DE09BAA2C5E20601E1579212520C8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmSU5fBBc-.woff
Preview:	wOFF.....O.....x.....GDEF.....G...d....GPOS.....!GSUB.....OS/2...L...P...`t6..cmap.....#cvt .....X...X/...fpgm.....4.....".gasp...@.....glyf.. .L..<'..m..]5Yhdmx..Ht...m....),..head..H....6...6.Y.ihhea..I.... ...$....hmtx..I<.....Dd.loca..K.....maxp..M.... ... .4.\name..M.....|..9.post..N..... .m.dprep..N.....:z /.Wx...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x...l\..F..3...N..q)..a\|.....^..33..c.....p"y.iT....<Gg...!.3...T1...{.g0.u.y.....m.\|.k..NF.....mox.;...7&.Y.. C.R_[.T.c..-.=...9:...a*j.G.....O.Q".6...>...(?...~...._.2:..K4....S%...jbr).....*....e.U..-..X.3.ILQ....z..!.f:...<.W.#...e.c=...&6...lc;;..3<.s<....H.i2..N..t..)Ns...#`..".).[...._.T..T... ..+l..=..O.....Z..F...r..eM.f.Y.....-...r.\.s6.r..,...:.<$..#.l..F.$.2#.e..].[.....yR...e.\{.O..`)..U.0.e.50.Z.b../cM..i.&O._..+.Y.W...;z....j.p._.o..[CL.)n'.UGx..>).X..MJ..Fr..v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\KFOlCnqEu92Fr1MmWUlfBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20396, version 1.1
Category:	downloaded
Size (bytes):	20396
Entropy (8bit):	7.974131663185347
Encrypted:	false
SSDEEP:	384:SfXdUIIA0zhyKR28ePpAwxZ5M3py8wtshtdf45DEVTGdYb7H2Q/VEgm:Svdj0zhbRmjIQ8wtsV4lEVGdY3/i/
MD5:	68D6DABFE54E245E7D5D5C16C3C4B1A9
SHA1:	7FDAB895EAEBECEDB3FB5473EAB94A1B292CEF19
SHA-256:	A01A632E56731A854F35701AA8C3A6A19A113290D9032FF9048F8064C45383BD
SHA-512:	44EB151F85178A2F9600E85AD43FAE470FABE0F247C9A03E67931B36028E600C7550D9DE2D69B3576A06577A5DEAF54822EE4BDC9DCBB47588D1972C8A959D4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmWUlfBBc-.woff
Preview:	wOFF.....O.....GDEF.....G...d....GPOS.....oGSUB.....OS/2...p...Q...`u...cmap.....#cvt .....H...H+~..fpgm...$...3...._...gasp...X..... ...glyf...d..< ..l..C^]hdmx..H....m....03#7head..H....6...6...\hhea..I,... ...$.&..hmtx..IL.....".J.loca..K.....maxp..M.... ... .4..name..M.....~..9.post..N..... .m.dprep..N.....)* v60x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x....%Y....Wm=..mo..k.m....rl...m.g"^..../..[.}.S...\.mD...1..G>..giz...=C..}.y....|o..c.x.R.r"B.....m...../.&. /6..5D.AGX.....)<'.)....?.... .Y4>|1...ES.Gc...FO.>$.../...}RCl..T.zD..uZ4~D._OK.$.Z.(..JR...\..\..\..\.....*'n..6:x...b,..$...?.g:./y.iLg.3..l.0.y.g..X..V...d.#O...0....b7{..>.n.iD.V....." e.\A..OR.kwp.].....6p..."ZE..%...e.u3..L..V...W.7b..L.3.L1K...Ts..$6.-b.....9...b@..!1,...v.C....{...dox.G(...|a%E:.Fn.Nn.^n.....Sf..E)...k....<g..)....|.....DT..N....Hy.F.Jez....._? 7.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\KFOlCnqEu92Fr1MmYUtfBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20412, version 1.1
Category:	downloaded
Size (bytes):	20412
Entropy (8bit):	7.970834733902595
Encrypted:	false
SSDEEP:	384:af5t4IIA0zhLqV6fCjKK/bF+ituwbilrCG36/C4odv4QobGOo8y0rO+:arn0zhLqnDFbuwb0rCGPdv4QoKOByf+
MD5:	64BBA9C4E8156C152050C657E9D24BF1
SHA1:	90ECF87091FAABE7BC0FF54A43828FA4DD483278
SHA-256:	D33864E01E5103EBE439732BB606E694C73B6851F24DA25D41901EB17CB5D98E
SHA-512:	2456A688A4C51759293E482D434A324BA81EFAC9DC203226007C256D468E424A88C678D1B8BCAD9E3950C6AC4F7FF76CACAD71A730709A600CA45569586910C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmYUtfBBc-.woff
Preview:	wOFF.....O.....|.....GDEF.....G...d....GPOS.....oGSUB.....OS/2...p...O...`v...cmap.....#cvt .....Z...Z...=fpgm...4...3.....#.gasp...h.....glyf... t..<...lL....hdmx..H....n....47(;head..H....6...6...Rhhea..I,... ...$.]..hmtx..IL.....,A.loca..K.....Bs.maxp..M.... ... .4..name..M.....\|..9.post..N..... .m.dprep..N.....8...Cx...1.. P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x....%Y....Wm=..mo..k.m....rl...m.g"^..../..[.}.S...\.mD...1..G>..giz...=C..}.y....\|o..c.x.R.r"B.....m...../.&. /6..5D.AGX.....)<'.)....?.... .Y4>\|1...ES.Gc...FO.>$.../...}RCl..T.zD..uZ4~D._OK.$.Z.(..JR...\..\..\..\.....*'n..6:x...b,..$...?.g:./y.iLg.3..l.0.y.g..X..V...d.#O...0....b7{..>.n.iD.V....." e.\A..OR.kwp.].....6p..."ZE..%...e.u3..L..V...W.7b..L.3.L1K...Ts..$6.-b.....9...b@..!1,...v.C....{...dox.G(...|a%E:.Fn.Nn.^n.....Sf..E)...k....<g..)....|.....DT..N....Hy.F.Jez....._? 7.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\KFOmCnqEu92Fr1Mu4mxM[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20332, version 1.1
Category:	downloaded
Size (bytes):	20332
Entropy (8bit):	7.970235088150752
Encrypted:	false
SSDEEP:	384:U0iwaxoOUPVkOJJSu6SsCKTIRDqG9oHKwZh98OSv+MsgkAOY:75mlUmOSu1guh+fZhLSxkAr
MD5:	DC3E086FC0C5ADDC09702E111D2ADB42
SHA1:	B1138B84FF19EAC5F43C4202297529D389BD09B7
SHA-256:	EA50AC7FDDB61A5CE248A7F8B3A31A98FE16285E076B16E6DA6B4E10910724BB

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\KFOmCnqEu92Fr1Mu4mxM[1].woff	
SHA-512:	10123C785C396CF0844751A014413ECF4D058AD0C00CAAEF5F8FFEF504C370F03EACD0B3C2A49211EEE0877B7AE7D0EF6E01264F04FC910C2660584B5E943BE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOmCnqEu92Fr1Mu4mxM.woff
Preview:	wOFF.....Ol.....x.....GDEF.....G...d....GPOS.....!GSUB.....OS/2...L...P...`t...cmap.....#cvt .....T...T+...fpgm.....5....w.`.gasp...@.....glyf.. .L..;...m.&.x.hdmx..H....m...././.head..H....6...6.j.zhhea..H.... ...$....hmtx..H.....]uloca..Kp.....m,maxp..Mp... ... .4..name..M.....t.U9.post..N`..... .m.dprep..Nt.....I .f..x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x...l\..F..3...N..q)..a\.....^..33..c.....p"y.iT....<Gg...!.3...T1...{.g0.u.y.....m.|.k..NF.....mox.;...7&.Y. .C.R_[.T.c..-.=...9:...a*j.G.....O.Q".6...>...(?...~...._.2:..K4....S%...jbr).....*....e.U..-..X.3.ILQ....z..!.f:...<.W.#...e.c=...&6...lc;;..3<.s<....H.i2..N..t..)Ns...#`..").{...._.T..T.. ...+l..=..O.....Z..F...r..eM.f.Y.....-...r.\.s6.r..,...:.<$..#.l..F.$.2#.e..].[.....yR...e.|{..O..`)..U.0.e.50.Z.b../cM..i.&O._..+.Y.W...;z....j.p._.o..[CL.)n'.UGx..>).X..MJ..Fr..v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\jet-tabs-frontend.min-1.1.7[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	7481
Entropy (8bit):	5.0298003069756305
Encrypted:	false
SSDEEP:	96:kZa+oLlasGlMZoDJ0Vq5uvcWtCWNLXACWNWD+bIbYf+GTEGTj9b9REAk8aEQELEv:4oLlarMBWWGTn/hPyJM5PM5e7g
MD5:	1A3B3BDF021E39D1CEB582804793620B
SHA1:	823A875AA14387C45DA64842E8E883EC1F50069F
SHA-256:	8F66B0245A0249DF24108EECA809057C74121739DEA7F8A4FB35AE0B1180E41A
SHA-512:	BAE766BE1D85A84C5C9AB3E23829D109F4B18E4BBD0ECC7BBB18DAD140DED9E2B01547B5F8EA8789C2A5F3A7FC13E69E61285474046EEF3472987D6A6AB27A 6A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn1.sellful.com/wp-content/cache/busting/3146/wp-content/plugins/jet-tabs/assets/js/jet-tabs-frontend.min-1.1.7.js
Preview:	!function(f,o,t){"use strict";var e={init:function(){var t={"jet-tabs.default":e.tabsInit,"jet-accordion.default":e.accordionInit,"jet-image-accordion.default":e.imageAccordionInit ,"jet-switcher.default":e.switcherInit};f.each(t,function(t,e){o.hooks.addAction("frontend/element_ready/"+t,e)})},tabsInit:function(o){var i,t=f(".jet-tabs",o).first(),a=t.data("i d"),c=f(window),e=f(".jet-tabs__control-wrapper",t).first(),s=f(".jet-tabs__content-wrapper",t).first(),r=f("> .jet-tabs__control",e),d=f("> .jet-tabs__content",s),n=t.data("settin gs")||{},l=null,g=window.location.hash||!1,h=!!g&&g.replace("#","").split("&");if("click"===n.event?r.on("click.jetTabs",function(){var t=f(this),e=+t.data("tab")-1;clearInterval(l),v(e)}):"ontouchend"in window||"ontouchstart"in window?(r.on("touchstart",function(t){i=f(window).scrollTop()}),r.on("touchend",function(t){var e=f(this),o=+e.data("tab")- 1;if(i!==f(window).scrollTop())return!1;clearInterval(l),v(o)})):r.on("mouseenter",function(t){var e=f(this)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\jquery.sticky.min-3.0.5[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	6595
Entropy (8bit):	5.001833104960226
Encrypted:	false
SSDEEP:	192:y4C8yiXSZPQfaNkLjEMHJx8vqOS5Z3N71jgiqM1xocYjtCDIoiL3:y4xyiXSZPVNkvEMHf8itN71ciqM16c9k
MD5:	E16A8821E5F099C3A619889EA7CF0399
SHA1:	A38E0C736AAF0B019B29B63B00E68C1381502217
SHA-256:	A48DEA362116D7516A2CF97066A32758D353760EE02DBF900DDFF86B02A16473
SHA-512:	41CF1EABFCD3B4752EE9FD1A7E7F5719249053BCAD871254A9D9821E016B40A2FBC29797DC14035CDA01628FAD879C2FDA47337853219F31250B9C7020D43CF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn1.sellful.com/wp-content/cache/busting/3146/wp-content/plugins/elementor-pro/assets/lib/sticky/jquery.sticky.min-3.0.5.js
Preview:	(function($){var Sticky=function(element,userSettings){var $element,isSticky=false,isFollowingParent=false,isReachedEffectsPoint=false,elements={},settings;var defaultSettings={to:"top",offset:0,effectsOffset:0,parent:false,classes:{sticky:"sticky",stickyActive:"sticky-active",stickyEffects:"sticky-effects",spacer:"sticky-spacer"}};var in itElements=function(){$element=$(element).addClass(settings.classes.sticky);elements.$window=$(window);if(settings.parent){if("parent"===settings.parent){elemen ts.$parent=$element.parent()}else{elements.$parent=$element.closest(settings.parent)}}};var initSettings=function(){settings=jQuery.extend(true,defaultSettings,userSettin gs)};var bindEvents=function(){elements.$window.on({scroll:onWindowScroll,resize:onWindowResize})};var unbindEvents=function(){elements.$window.off("scroll",onW indowScroll).off("resize",onWindowResize)};var init=function(){initSettings();initElements();bindEvents();checkPosition()};var backupCSS=function($elementBackup CSS,backup

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\position.min-1.11.4[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	6527
Entropy (8bit):	5.3218491668096926
Encrypted:	false
SSDEEP:	96:b23MB+YiLvmF7EoSrOJa8KKlLfWh0b1lo4frg4iGl6HPOpajlg6q4R6PUlutKH7O:b7eu7pa8fgEqouPNlguAp0bFH7r8f
MD5:	1C4A13EDEC1958817E83433AEAA42F62
SHA1:	851D4F36AC29A54F9AEB865E4772E10B941252D3
SHA-256:	49AF6B83569C5E8C707E93884D9BA619B402F0A115925951301E2E3C844F0AD8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\position.min-1.11.4[1].js	
SHA-512:	DD435E86BE26572719B209BB009522C97CDA4BF1D99CD3B1A777EDDFE55892250C3EE21CD3E6D693E0752B5F5A36C51ED2ABA10783B4E47A062645B64885045A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn1.sellful.com/wp-content/cache/busting/3146/wp-includes/js/jquery/ui/position.min-1.11.4.js
Preview:	/*!. * jQuery UI Position 1.11.4. * http://jqueryui.com. *. * Copyright jQuery Foundation and other contributors. * Released under the MIT license.. * http://jquery.org/license. *. * http://api.jqueryui.com/position/. */.!function(a){"function"==typeof define&&define.amd?define(["jquery"],a):a(jQuery)}(function(a){return function(){function b(a,b,c){return[parseFloat(a[0])*(n.test(a[0])?b/100:1),parseFloat(a[1])*(n.test(a[1])?c/100:1)]}function c(b,c){return parseInt(a.css(b,c),10)||0}function d(b){var c=b[0];return 9===c.nodeType?{width:b.width(),height:b.height(),offset:{top:0,left:0}}:a.isWindow(c)?{width:b.width(),height:b.height(),offset:{top:b.scrollTop(),left:b.scrollLeft()}}:c.preventDefault?{width:0,height:0,offset:{top:c.pageY,left:c.pageX}}:{width:b.outerWidth(),height:b.outerHeight(),offset:b.offset()}}a.ui=a.ui||{};var e,f,g=Math.max,h=Math.abs,i=Math.round,j=/left|center|right/,k=/top|center|bottom/,l=/[\+\-]\d+(\.[\d]+)?%?/,m=/^\w+/,n=/%$/,o=a.fn.position;a.position={scr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\waypoints.min-4.0.2[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	12198
Entropy (8bit):	5.031745242580206
Encrypted:	false
SSDEEP:	192:GngaW9ELBD26z861V/CvJiVKIsvfT+6EdpEsBpP9Qwo7Q4a99RfuzqXppc4mmm9t:Ggz9kBD26861V/wsVKIsvTEdpEsnmwoz
MD5:	3819C3569DA71DAEC283A75483735F7E
SHA1:	ECD40A5CC6F0B76200C454CA880210DC301CFAB8
SHA-256:	214674CC77ABA35AB3567B88E2739FD08E8E96C61D279559AD61874069683EA0
SHA-512:	2710655DFF46653DAEB3A6E3F6D36F885E51D5B375738EE353ACA40C6F66AE1A7DECE57039D58747012ED9EA2822191143C06F270123B8CC580F6A41B8E8AEF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn1.sellful.com/wp-content/cache/busting/3146/wp-content/plugins/elementor/assets/lib/waypoints/waypoints.min-4.0.2.js
Preview:	!function(){"use strict";function Waypoint(options){if(!options)throw new Error("No options passed to Waypoint constructor");if(!options.element)throw new Error("No element option passed to Waypoint constructor");if(!options.handler)throw new Error("No handler option passed to Waypoint constructor");this.key="waypoint-"+keyCounter,this.options=Waypoint.Adapter.extend({},Waypoint.defaults,options),this.element=this.options.element,this.adapter=new Waypoint.Adapter(this.element),this.callback=options.handler,this.axis=this.options.horizontal?"horizontal":"vertical",this.enabled=this.options.enabled,this.triggerPoint=null,this.group=Waypoint.Group.findOrCreate({name:this.options.group,axis:this.axis}),this.context=Waypoint.Context.findOrCreateByElement(this.options.context),Waypoint.offsetAliases[this.options.offset]&&(this.options.offset=Waypoint.offsetAliases[this.options.offset]),this.group.add(this),this.context.add(this),allWaypoints[this.key]=this,keyCounter+=1}var keyCounter=0,allW

C:\Users\user\AppData\Local\Temp\dat3A40.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 2532, version 2.24904
Category:	modified
Size (bytes):	2532
Entropy (8bit):	7.627755614174705
Encrypted:	false
SSDEEP:	48:WGMiY6eIlk7QuaqrjRh4pi6j4fN6+XRsnBBpr+bes:WRBLIIoQuHfRh4pi6sfPGnDFs
MD5:	10600F6B3D9C9BE2D2B2CE58D2C6508B
SHA1:	421CA4369738433E33348785FE776A0C839605D5
SHA-256:	29B7A9358ABDC68C51DB5A5AF4A4F4E2E041A67527ADEE2366B1F84F116FE9A5
SHA-512:	B6C04F3068EB7DAC8F782BDED0FE815B4FE5A9BECCF0B561D6CEAEAA7365919A39710B2D1AD58D252330476AA836629B3C62C84FABFA6DC4BCF1C8F055D66C1C
Malicious:	false
Reputation:	low
Preview:	wOFF.....aH.....OS/2...D...H...`1Wp.cmap.....l...b..ocvt ..... ...*....fpgm.....Y...gasp.....glyf.....Whead.....2...6.tJ.hhea.....$....hmtx.....loca.....X.hmaxp...,..... .y..name...L.....Mpost...D..... .Q.}prep...X.....x...x.c`aog.....:....Q.B3_dHc..`e.bdb... .`@..`.....,9.|...V...)00...C..x.c```f.`..F.....|... .....\..K..n.,..g`@.I|.8"vYl....p...0.....x.c.b.e(`h`X.....x.....x.]..N.@..s$..'@:!.u*C....K$.%%...J.....n..b.....|.s...|v..G*)V.7.....!O.6eaL.yV.e.j..kN..M.h....Lm....-b....p.N.m.v.....U<..#...O.}.K..,V..&...^...L.c.x.....?ug..l9e..Ns.D....D...K.....m..A.M....a.....g.P..`....d.....x..R.K.1...$....g-.B.Vq..m..Z..T..@\t.E...7X...:.).c... ].{.Q.['...`.^...&....{y<..N....t...6..f....\.K1..Z}{.eA-..x.{....0P7p.....l.....E...r....EVQ.....Q_.4.A.Z..;...PGs.o..Eo...{t...a.P.~...b,Dz.}.OXdp."d4."C.X..&,u.g.....r.c..j

C:\Users\user\AppData\Local\Temp\datF3B1.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 2532, version 2.24904
Category:	modified
Size (bytes):	2532
Entropy (8bit):	7.627755614174705
Encrypted:	false
SSDEEP:	48:WGMiY6eIlk7QuaqrjRh4pi6j4fN6+XRsnBBpr+bes:WRBLIIoQuHfRh4pi6sfPGnDFs
MD5:	10600F6B3D9C9BE2D2B2CE58D2C6508B
SHA1:	421CA4369738433E33348785FE776A0C839605D5
SHA-256:	29B7A9358ABDC68C51DB5A5AF4A4F4E2E041A67527ADEE2366B1F84F116FE9A5

C:\Users\user\AppData\Local\Temp\datF3B1.tmp	
SHA-512:	B6C04F3068EB7DAC8F782BDED0FE815B4FE5A9BECCF0B561D6CEAEAA7365919A39710B2D1AD58D252330476AA836629B3C62C84FABFA6DC4BCF1C8F055D66C1C
Malicious:	false
Reputation:	low
Preview:	wOFF.....aH.....OS/2...D...H...`1Wp.cmap.....l...b..ocvt ..... ...*....fpgm.....Y...gasp.....glyf.....Whead.....2...6.tJ.hhea.....$....hmtx.....loca.....X.hmaxp...,..... .y..name...L.....Mpost...D..... .Q.}prep...X.....x...x.c`aog.....:....Q.B3_dHc..`e.bdb... .`@..`.....,9.\|...V...)00...C..x.c```f.`..F.....\|... .....\..K..n.,..g`@.\|.8"vYl.....p...0.....x.c.b.e(`h`X.....x.....x.].N.@..s$..'@:!.u*C....K$.%%...J.....n..b.....\|.s...\|v..G*)V.7.....!O.6eaL.yV.e.j..kN..M.h....Lm....-b....p.N.m.v.....U<..#...O.}.K..,V..&...^...L.c.x.....?ug..l9e..Ns.D....D...K.....m..A.M....a.....g.P..`....d.....x..R.K.1...$....g-.B.Vq..m..Z..T..@\t.E...7X...:.).c... ].{.Q.[7'...`.^...&....{y<..N.....t...6..f....\.K1..Z}{.eA-..x.{....0P7p.....l.....E...r....EVQ.....Q_.4.A.Z..;...PGs.o..Eo...{t...a.P.~...b,Dz.}.OXdp."d4."C.X..&,u.g.....r.c..j

C:\Users\user\AppData\Local\Temp\~DF0A2A2977AA5B8124.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF7A51840F262B8417.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	41625
Entropy (8bit):	0.7241172419077708
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+npLCJucOxcO0BOoFvOoFXAtOoFpOoFnOoF6HOoFNvD:kBqoxKAuqR+npLCJubKjdXqr1q
MD5:	B194237E369C3EFEA1DD3B523486D9E7
SHA1:	B672BB3691A94B2DE671AAC4E96B625F5ED69E26
SHA-256:	28C3CEFDB7AE04FDC597B88C33E74D4BE4CE7B193573F480361225345CFC44F4
SHA-512:	4A865B2BFDD5BD941B526260C41101370B8121D8FF6EE70CDF1FDDEF5C4E784E55ADE82E923F1B6BBC53CF09FA73D25C262637DE5A60A81BA25524091847C25
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF827A3CCA513061E4.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	46925
Entropy (8bit):	0.9058593529263693
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+XZbS5pg040lOGxpQDn16Qx:kBqoxKAuqR+XZbS5pg040lOqi
MD5:	D42FC5B8267C2A66D266198C42197588
SHA1:	CA13CB6B924B323771E5E81535888E210030DB2A
SHA-256:	CC3A05FEE26D68C93BFE11A8448AF8D897DADD87AA4C3A45A9E854551BA10A50
SHA-512:	C6DB2B03BFB49D0FC09E53D7861C01068116E7E24B3FCC4596C1156B73791C1E84B2E4C1F9C8D20AA11698CCF03425AC199DB6BD58E620B66628EECED49A101
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DF827A3CCA513061E4.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFDB692E0DABAF91D0.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13349
Entropy (8bit):	0.6732701015783877
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lln9lln9loV9lo19lWZUoFZbM:kBqoIeAxHM
MD5:	89F5139BEA455C2D7D25734F22E6FE50
SHA1:	1A8C2714ABAF7ECF412BA09F0C57E63941BEBD74
SHA-256:	C96250606C29D3812A1A43436AF7BEE1688FCA3E87B61294A2C30D0D13BB2392
SHA-512:	91EC7879A411A5CC23849815FEF7D43E047C80ACAF2E58717285E3E37F21C1C7995705FE38BDEF5391AF0ED2F56B78ACAA1107EA06C0CF88D2CFA477AA073D 8
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

Network Port Distribution

Total Packets: 119

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 22:22:30.448779106 CEST	49716	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:30.450076103 CEST	49717	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:30.570919991 CEST	443	49717	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:30.571074009 CEST	49717	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:30.693100929 CEST	49717	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:30.797226906 CEST	443	49716	104.26.11.161	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 22:22:30.797357082 CEST	49716	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:30.797972918 CEST	49716	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:30.808461905 CEST	443	49717	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:30.812117100 CEST	443	49717	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:30.812163115 CEST	443	49717	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:30.812232018 CEST	49717	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:30.814184904 CEST	49717	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:30.848321915 CEST	49717	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:30.854614973 CEST	49717	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:30.854837894 CEST	49717	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:30.964782000 CEST	443	49717	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:30.964936972 CEST	443	49717	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:30.965039015 CEST	49717	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:30.965209007 CEST	443	49717	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:30.965708017 CEST	49717	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:30.966954947 CEST	49717	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:30.970510006 CEST	443	49717	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:30.970535040 CEST	443	49717	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:30.971056938 CEST	49717	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:31.011818886 CEST	443	49717	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:31.082037926 CEST	443	49717	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:31.147654057 CEST	443	49716	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:31.153456926 CEST	443	49716	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:31.153506994 CEST	443	49716	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:31.153567076 CEST	49716	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:31.153615952 CEST	49716	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:31.189640999 CEST	443	49717	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:31.189666986 CEST	443	49717	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:31.189678907 CEST	443	49717	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:31.189687014 CEST	443	49717	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:31.189704895 CEST	443	49717	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:31.189726114 CEST	443	49717	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:31.189742088 CEST	49717	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:31.189790964 CEST	49717	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:31.189819098 CEST	49717	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:31.192013025 CEST	443	49717	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:31.192039967 CEST	443	49717	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:31.192105055 CEST	49717	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:31.192131042 CEST	49717	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:31.194219112 CEST	443	49717	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:31.194305897 CEST	49717	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:31.232623100 CEST	49716	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:31.236427069 CEST	49716	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:31.396075010 CEST	49718	443	192.168.2.7	104.26.13.213
Apr 7, 2021 22:22:31.397675991 CEST	49719	443	192.168.2.7	104.26.13.213
Apr 7, 2021 22:22:31.398654938 CEST	49720	443	192.168.2.7	104.26.13.213
Apr 7, 2021 22:22:31.437386990 CEST	49723	443	192.168.2.7	104.26.13.213
Apr 7, 2021 22:22:31.469400883 CEST	49724	443	192.168.2.7	104.26.13.213
Apr 7, 2021 22:22:31.471045017 CEST	49725	443	192.168.2.7	104.26.13.213
Apr 7, 2021 22:22:31.473450899 CEST	49717	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:31.581001043 CEST	443	49716	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:31.583225965 CEST	443	49716	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:31.583255053 CEST	443	49716	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:31.583318949 CEST	49716	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:31.583359957 CEST	49716	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:31.584032059 CEST	49716	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:31.584604979 CEST	443	49716	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:31.584918022 CEST	443	49716	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:31.584985971 CEST	49716	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:31.589698076 CEST	443	49717	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:31.593632936 CEST	443	49719	104.26.13.213	192.168.2.7
Apr 7, 2021 22:22:31.593765020 CEST	49719	443	192.168.2.7	104.26.13.213
Apr 7, 2021 22:22:31.594459057 CEST	49719	443	192.168.2.7	104.26.13.213
Apr 7, 2021 22:22:31.599055052 CEST	443	49718	104.26.13.213	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 22:22:31.599133968 CEST	49718	443	192.168.2.7	104.26.13.213
Apr 7, 2021 22:22:31.599841118 CEST	49718	443	192.168.2.7	104.26.13.213
Apr 7, 2021 22:22:31.600389004 CEST	443	49717	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:31.600518942 CEST	49717	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:31.600524902 CEST	443	49717	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:31.600575924 CEST	49717	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:31.600754023 CEST	443	49717	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:31.600789070 CEST	443	49717	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:31.600806952 CEST	49717	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:31.600830078 CEST	49717	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:31.602593899 CEST	443	49717	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:31.602646112 CEST	443	49717	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:31.602684975 CEST	49717	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:31.602721930 CEST	49717	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:31.605351925 CEST	443	49717	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:31.605429888 CEST	49717	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:31.605459929 CEST	443	49717	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:31.605511904 CEST	49717	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:31.608031034 CEST	443	49717	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:31.608069897 CEST	443	49717	104.26.11.161	192.168.2.7
Apr 7, 2021 22:22:31.608105898 CEST	49717	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:31.608127117 CEST	49717	443	192.168.2.7	104.26.11.161
Apr 7, 2021 22:22:31.666222095 CEST	443	49725	104.26.13.213	192.168.2.7
Apr 7, 2021 22:22:31.666316986 CEST	49725	443	192.168.2.7	104.26.13.213
Apr 7, 2021 22:22:31.666951895 CEST	49725	443	192.168.2.7	104.26.13.213
Apr 7, 2021 22:22:31.741997004 CEST	443	49720	104.26.13.213	192.168.2.7
Apr 7, 2021 22:22:31.742151022 CEST	49720	443	192.168.2.7	104.26.13.213
Apr 7, 2021 22:22:31.754622936 CEST	49720	443	192.168.2.7	104.26.13.213
Apr 7, 2021 22:22:31.781842947 CEST	443	49723	104.26.13.213	192.168.2.7
Apr 7, 2021 22:22:31.781981945 CEST	49723	443	192.168.2.7	104.26.13.213

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 22:22:21.097249985 CEST	63668	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:21.112400055 CEST	53	63668	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:21.242180109 CEST	54640	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:21.263341904 CEST	53	54640	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:22.215538025 CEST	58739	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:22.227956057 CEST	53	58739	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:22.909481049 CEST	60338	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:22.922755957 CEST	53	60338	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:24.455060005 CEST	58717	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:24.469839096 CEST	53	58717	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:25.266320944 CEST	59762	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:25.279947042 CEST	53	59762	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:26.360039949 CEST	54329	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:26.376730919 CEST	53	54329	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:27.604932070 CEST	58052	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:27.618017912 CEST	53	58052	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:28.018101931 CEST	54008	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:28.036384106 CEST	53	54008	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:28.285816908 CEST	59451	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:28.299582005 CEST	53	59451	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:29.141805887 CEST	52914	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:30.144201994 CEST	52914	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:30.436769962 CEST	53	52914	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:30.436796904 CEST	53	52914	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:31.332946062 CEST	64569	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:31.372749090 CEST	53	64569	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:31.406598091 CEST	52816	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:31.420141935 CEST	53	52816	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:33.346479893 CEST	50781	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:34.116445065 CEST	54230	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 22:22:34.129534006 CEST	53	54230	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:34.141232014 CEST	54911	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:34.163623095 CEST	53	54911	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:34.354475021 CEST	50781	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:34.374286890 CEST	53	50781	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:35.033653975 CEST	49958	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:35.047275066 CEST	53	49958	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:36.432656050 CEST	50860	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:36.447026014 CEST	53	50860	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:36.969053984 CEST	50452	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:37.008287907 CEST	53	50452	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:37.244966984 CEST	59730	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:37.250227928 CEST	59310	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:37.258914948 CEST	53	59730	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:37.264255047 CEST	53	59310	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:37.524648905 CEST	51919	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:37.538871050 CEST	53	51919	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:38.366089106 CEST	64296	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:38.385289907 CEST	53	64296	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:39.056340933 CEST	56680	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:39.069106102 CEST	53	56680	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:40.326116085 CEST	58820	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:40.338433027 CEST	53	58820	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:41.009813070 CEST	60983	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:41.022342920 CEST	53	60983	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:44.276968002 CEST	49247	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:44.297084093 CEST	53	49247	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:44.898049116 CEST	52286	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:45.571949959 CEST	53	52286	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:46.926276922 CEST	56064	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:46.939625978 CEST	53	56064	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:48.548099995 CEST	63744	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:48.561424017 CEST	53	63744	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:49.892529964 CEST	61457	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:49.907902956 CEST	53	61457	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:50.921454906 CEST	58367	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:50.944678068 CEST	53	58367	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:53.285141945 CEST	60599	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:53.300179005 CEST	53	60599	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:57.769819975 CEST	59571	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:57.782869101 CEST	53	59571	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:58.002757072 CEST	52689	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:58.015573978 CEST	53	52689	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:58.701379061 CEST	50290	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:58.713850021 CEST	53	50290	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:58.786317110 CEST	60427	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:58.799658060 CEST	53	60427	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:59.012726068 CEST	52689	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:59.025633097 CEST	53	52689	8.8.8.8	192.168.2.7
Apr 7, 2021 22:22:59.714608908 CEST	50290	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:22:59.729726076 CEST	53	50290	8.8.8.8	192.168.2.7
Apr 7, 2021 22:23:00.011640072 CEST	52689	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:23:00.024596930 CEST	53	52689	8.8.8.8	192.168.2.7
Apr 7, 2021 22:23:00.730509043 CEST	50290	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:23:00.752983093 CEST	53	50290	8.8.8.8	192.168.2.7
Apr 7, 2021 22:23:02.351576090 CEST	52689	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:23:02.364634037 CEST	53	52689	8.8.8.8	192.168.2.7
Apr 7, 2021 22:23:02.749933004 CEST	50290	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:23:02.763684034 CEST	53	50290	8.8.8.8	192.168.2.7
Apr 7, 2021 22:23:03.958374977 CEST	56209	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:23:04.634875059 CEST	53	56209	8.8.8.8	192.168.2.7
Apr 7, 2021 22:23:06.355966091 CEST	52689	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:23:06.370362043 CEST	53	52689	8.8.8.8	192.168.2.7
Apr 7, 2021 22:23:06.763026953 CEST	50290	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 22:23:06.775548935 CEST	53	50290	8.8.8.8	192.168.2.7
Apr 7, 2021 22:23:11.014693022 CEST	59582	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:23:11.036672115 CEST	53	59582	8.8.8.8	192.168.2.7
Apr 7, 2021 22:23:12.602880955 CEST	60949	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:23:12.617038012 CEST	53	60949	8.8.8.8	192.168.2.7
Apr 7, 2021 22:23:13.590917110 CEST	60949	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:23:13.603322983 CEST	53	60949	8.8.8.8	192.168.2.7
Apr 7, 2021 22:23:14.606479883 CEST	60949	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:23:14.619482040 CEST	53	60949	8.8.8.8	192.168.2.7
Apr 7, 2021 22:23:16.430238962 CEST	58542	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:23:16.456943035 CEST	53	58542	8.8.8.8	192.168.2.7
Apr 7, 2021 22:23:16.622251987 CEST	60949	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:23:16.636049986 CEST	53	60949	8.8.8.8	192.168.2.7
Apr 7, 2021 22:23:20.638232946 CEST	60949	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:23:22.274838924 CEST	53	60949	8.8.8.8	192.168.2.7
Apr 7, 2021 22:23:22.407684088 CEST	59179	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:23:22.423801899 CEST	53	59179	8.8.8.8	192.168.2.7
Apr 7, 2021 22:23:25.547008991 CEST	60927	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:23:25.565629005 CEST	53	60927	8.8.8.8	192.168.2.7
Apr 7, 2021 22:23:40.264508963 CEST	57854	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:23:40.348750114 CEST	53	57854	8.8.8.8	192.168.2.7
Apr 7, 2021 22:23:40.687227011 CEST	62026	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:23:40.772105932 CEST	53	62026	8.8.8.8	192.168.2.7
Apr 7, 2021 22:23:41.159405947 CEST	59453	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:23:41.234596968 CEST	53	59453	8.8.8.8	192.168.2.7
Apr 7, 2021 22:23:41.543239117 CEST	62468	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:23:41.557147980 CEST	53	62468	8.8.8.8	192.168.2.7
Apr 7, 2021 22:23:42.227324963 CEST	52563	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:23:42.301630020 CEST	53	52563	8.8.8.8	192.168.2.7
Apr 7, 2021 22:23:42.707890987 CEST	54721	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:23:42.722757101 CEST	53	54721	8.8.8.8	192.168.2.7
Apr 7, 2021 22:23:43.020591021 CEST	62826	53	192.168.2.7	8.8.8.8
Apr 7, 2021 22:23:43.033844948 CEST	53	62826	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 7, 2021 22:22:29.141805887 CEST	192.168.2.7	8.8.8.8	0x452c	Standard query (0)	securepay.mysellful.com	A (IP address)	IN (0x0001)
Apr 7, 2021 22:22:30.144201994 CEST	192.168.2.7	8.8.8.8	0x452c	Standard query (0)	securepay.mysellful.com	A (IP address)	IN (0x0001)
Apr 7, 2021 22:22:31.332946062 CEST	192.168.2.7	8.8.8.8	0x89a	Standard query (0)	cdn1.sellful.com	A (IP address)	IN (0x0001)
Apr 7, 2021 22:22:34.141232014 CEST	192.168.2.7	8.8.8.8	0x71b8	Standard query (0)	stateless.sellful.com	A (IP address)	IN (0x0001)
Apr 7, 2021 22:22:36.969053984 CEST	192.168.2.7	8.8.8.8	0x2fbd	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Apr 7, 2021 22:22:37.250227928 CEST	192.168.2.7	8.8.8.8	0xb43f	Standard query (0)	www.google.ch	A (IP address)	IN (0x0001)
Apr 7, 2021 22:22:44.898049116 CEST	192.168.2.7	8.8.8.8	0x8794	Standard query (0)	atendiendo chagas.mundosano.org	A (IP address)	IN (0x0001)
Apr 7, 2021 22:22:58.786317110 CEST	192.168.2.7	8.8.8.8	0x5505	Standard query (0)	securepay.mysellful.com	A (IP address)	IN (0x0001)
Apr 7, 2021 22:23:03.958374977 CEST	192.168.2.7	8.8.8.8	0x6600	Standard query (0)	atendiendo chagas.mundosano.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 7, 2021 22:22:30.436769962 CEST	8.8.8.8	192.168.2.7	0x452c	No error (0)	securepay.mysellful.com		104.26.11.161	A (IP address)	IN (0x0001)
Apr 7, 2021 22:22:30.436769962 CEST	8.8.8.8	192.168.2.7	0x452c	No error (0)	securepay.mysellful.com		104.26.10.161	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 7, 2021 22:22:30.436769962 CEST	8.8.8.8	192.168.2.7	0x452c	No error (0)	securepay.mysellful.com		172.67.73.36	A (IP address)	IN (0x0001)
Apr 7, 2021 22:22:30.436796904 CEST	8.8.8.8	192.168.2.7	0x452c	No error (0)	securepay.mysellful.com		104.26.10.161	A (IP address)	IN (0x0001)
Apr 7, 2021 22:22:30.436796904 CEST	8.8.8.8	192.168.2.7	0x452c	No error (0)	securepay.mysellful.com		172.67.73.36	A (IP address)	IN (0x0001)
Apr 7, 2021 22:22:30.436796904 CEST	8.8.8.8	192.168.2.7	0x452c	No error (0)	securepay.mysellful.com		104.26.11.161	A (IP address)	IN (0x0001)
Apr 7, 2021 22:22:31.372749090 CEST	8.8.8.8	192.168.2.7	0x89a	No error (0)	cdn1.sellful.com		104.26.13.213	A (IP address)	IN (0x0001)
Apr 7, 2021 22:22:31.372749090 CEST	8.8.8.8	192.168.2.7	0x89a	No error (0)	cdn1.sellful.com		104.26.12.213	A (IP address)	IN (0x0001)
Apr 7, 2021 22:22:31.372749090 CEST	8.8.8.8	192.168.2.7	0x89a	No error (0)	cdn1.sellful.com		172.67.68.1	A (IP address)	IN (0x0001)
Apr 7, 2021 22:22:34.163623095 CEST	8.8.8.8	192.168.2.7	0x71b8	No error (0)	stateless.sellful.com		104.26.12.213	A (IP address)	IN (0x0001)
Apr 7, 2021 22:22:34.163623095 CEST	8.8.8.8	192.168.2.7	0x71b8	No error (0)	stateless.sellful.com		104.26.13.213	A (IP address)	IN (0x0001)
Apr 7, 2021 22:22:34.163623095 CEST	8.8.8.8	192.168.2.7	0x71b8	No error (0)	stateless.sellful.com		172.67.68.1	A (IP address)	IN (0x0001)
Apr 7, 2021 22:22:37.008287907 CEST	8.8.8.8	192.168.2.7	0x2fbd	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Apr 7, 2021 22:22:37.008287907 CEST	8.8.8.8	192.168.2.7	0x2fbd	No error (0)	stats.l.doubleclick.net		74.125.143.156	A (IP address)	IN (0x0001)
Apr 7, 2021 22:22:37.008287907 CEST	8.8.8.8	192.168.2.7	0x2fbd	No error (0)	stats.l.doubleclick.net		74.125.143.155	A (IP address)	IN (0x0001)
Apr 7, 2021 22:22:37.008287907 CEST	8.8.8.8	192.168.2.7	0x2fbd	No error (0)	stats.l.doubleclick.net		74.125.143.157	A (IP address)	IN (0x0001)
Apr 7, 2021 22:22:37.008287907 CEST	8.8.8.8	192.168.2.7	0x2fbd	No error (0)	stats.l.doubleclick.net		74.125.143.154	A (IP address)	IN (0x0001)
Apr 7, 2021 22:22:37.264255047 CEST	8.8.8.8	192.168.2.7	0xb43f	No error (0)	www.google.ch		216.58.215.227	A (IP address)	IN (0x0001)
Apr 7, 2021 22:22:45.571949959 CEST	8.8.8.8	192.168.2.7	0x8794	No error (0)	atendiendochagas.mundosano.org		162.246.16.250	A (IP address)	IN (0x0001)
Apr 7, 2021 22:22:58.799658060 CEST	8.8.8.8	192.168.2.7	0x5505	No error (0)	securepay.mysellful.com		104.26.10.161	A (IP address)	IN (0x0001)
Apr 7, 2021 22:22:58.799658060 CEST	8.8.8.8	192.168.2.7	0x5505	No error (0)	securepay.mysellful.com		172.67.73.36	A (IP address)	IN (0x0001)
Apr 7, 2021 22:22:58.799658060 CEST	8.8.8.8	192.168.2.7	0x5505	No error (0)	securepay.mysellful.com		104.26.11.161	A (IP address)	IN (0x0001)
Apr 7, 2021 22:23:04.634875059 CEST	8.8.8.8	192.168.2.7	0x6600	No error (0)	atendiendochagas.mundosano.org		162.246.16.250	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 7, 2021 22:22:30.812163115 CEST	104.26.11.161	443	192.168.2.7	49717	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Wed Aug 04 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Apr 7, 2021 22:22:31.153506994 CEST	104.26.11.161	443	192.168.2.7	49716	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Wed Aug 04 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Apr 7, 2021 22:22:31.794702053 CEST	104.26.13.213	443	192.168.2.7	49719	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sat Jul 11 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Sun Jul 11 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Apr 7, 2021 22:22:31.809123039 CEST	104.26.13.213	443	192.168.2.7	49718	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sat Jul 11 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Sun Jul 11 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Apr 7, 2021 22:22:31.866132021 CEST	104.26.13.213	443	192.168.2.7	49725	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sat Jul 11 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Sun Jul 11 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Apr 7, 2021 22:22:32.104548931 CEST	104.26.13.213	443	192.168.2.7	49720	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sat Jul 11 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Sun Jul 11 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 7, 2021 22:22:32.135126114 CEST	104.26.13.213	443	192.168.2.7	49723	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sat Jul 11 02:00:00 CEST 2020	Sun Jul 11 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Apr 7, 2021 22:22:32.162162066 CEST	104.26.13.213	443	192.168.2.7	49724	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sat Jul 11 02:00:00 CEST 2020	Sun Jul 11 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Apr 7, 2021 22:22:34.224149942 CEST	104.26.12.213	443	192.168.2.7	49733	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sat Jul 11 02:00:00 CEST 2020	Sun Jul 11 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Apr 7, 2021 22:22:34.544238091 CEST	104.26.12.213	443	192.168.2.7	49732	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sat Jul 11 02:00:00 CEST 2020	Sun Jul 11 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Apr 7, 2021 22:22:37.062088013 CEST	74.125.143.156	443	192.168.2.7	49739	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Mar 16 20:28:05 CET 2021	Tue Jun 08 21:28:04 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 7, 2021 22:22:37.062187910 CEST	74.125.143.156	443	192.168.2.7	49738	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Mar 16 20:28:05 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jun 08 21:28:04 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Apr 7, 2021 22:22:45.845652103 CEST	162.246.16.250	443	192.168.2.7	49753	CN=atendiendochagas.mundosano.org CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sun Mar 21 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sun Jun 20 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Apr 7, 2021 22:22:45.845690966 CEST	162.246.16.250	443	192.168.2.7	49752	CN=atendiendochagas.mundosano.org CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sun Mar 21 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sun Jun 20 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 7, 2021 22:23:04.832465887 CEST	162.246.16.250	443	192.168.2.7	49765	CN=atendiendochagas.mundosano.org CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sun Mar 21 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sun Jun 20 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Apr 7, 2021 22:23:04.832659960 CEST	162.246.16.250	443	192.168.2.7	49764	CN=atendiendochagas.mundosano.org CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sun Mar 21 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sun Jun 20 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior

iexplore.exe
iexplore.exe
iexplore.exe

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 4460 Parent PID: 792

General

Start time:	22:22:27
Start date:	07/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff70b860000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 2160 Parent PID: 4460

General

Start time:	22:22:27

Start date:	07/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4460 CREDAT:17410 /prefetch:2
Imagebase:	0x11a0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 5576 Parent PID: 4460

General

Start time:	22:22:41
Start date:	07/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4460 CREDAT:82952 /prefetch:2
Imagebase:	0x11a0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly