ID: 363628
Cookbook: browseurl.jbs
Time: 00:12:30
Date: 05/03/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report https://05tns.csb.app/ 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Signature Overview 4
AV Detection: 5
Phishing: 5
Compliance: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 11
Public 12
General Information 13
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 14
Domains 15
ASN 15
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
Static File Info 47
No static file info 48
Network Behavior 48
Snort IDS Alerts 48
Network Port Distribution 48
TCP Packets 48
UDP Packets 50
ICMP Packets 52
DNS Queries 53
DNS Answers 54
HTTP Request Dependency Graph 57
HTTP Packets 57
HTTPS Packets 62
Code Manipulations 79

Copyright null 2021

Statistics 79
Behavior 79
System Behavior 79
Analysis Process: iexplore.exe PID: 6884 Parent PID: 800 80
General 80
File Activities 80
Registry Activities 80
Analysis Process: iexplore.exe PID: 6928 Parent PID: 6884 80
General 80
File Activities 80
Registry Activities 81
Disassembly 81

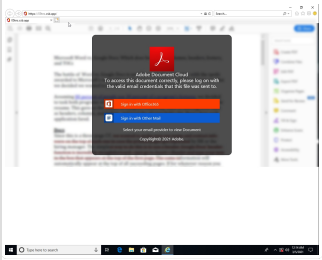
Analysis Report https://05tns.csb.app/

Overview

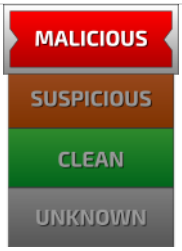
General Information

Sample URL:	http://https://05tns.csb.app/
Analysis ID:	363628
Infos:	

Most interesting Screenshot:



Detection



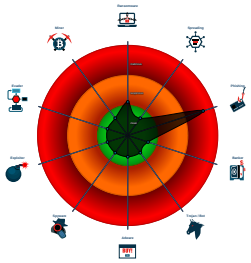
HTMLPhisher

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Phishing site detected (based on fav…
- Phishing site detected (based on sh…
- Yara detected HtmlPhish_7
- Found iframes
- HTML body contains low number of …
- HTML title does not match URL
- None HTTPS page querying sensitiv…
- Unusual large HTML page

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6884 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6928 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6884 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

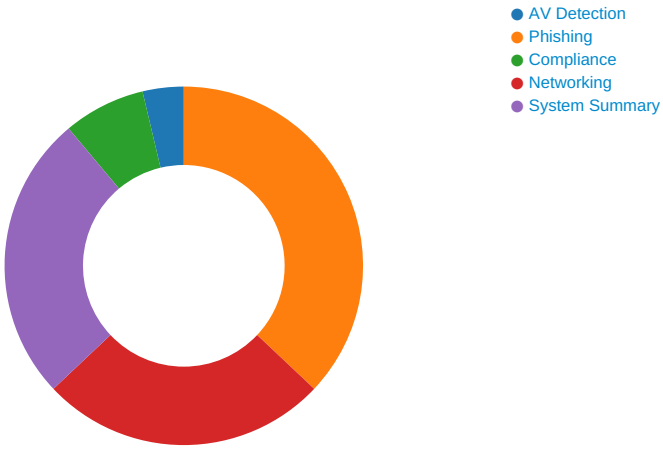
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Phishing:

Phishing site detected (based on favicon image match)

Phishing site detected (based on shot template match)

Yara detected HtmlPhish_7

Compliance:

Uses new MSVCR Dlls

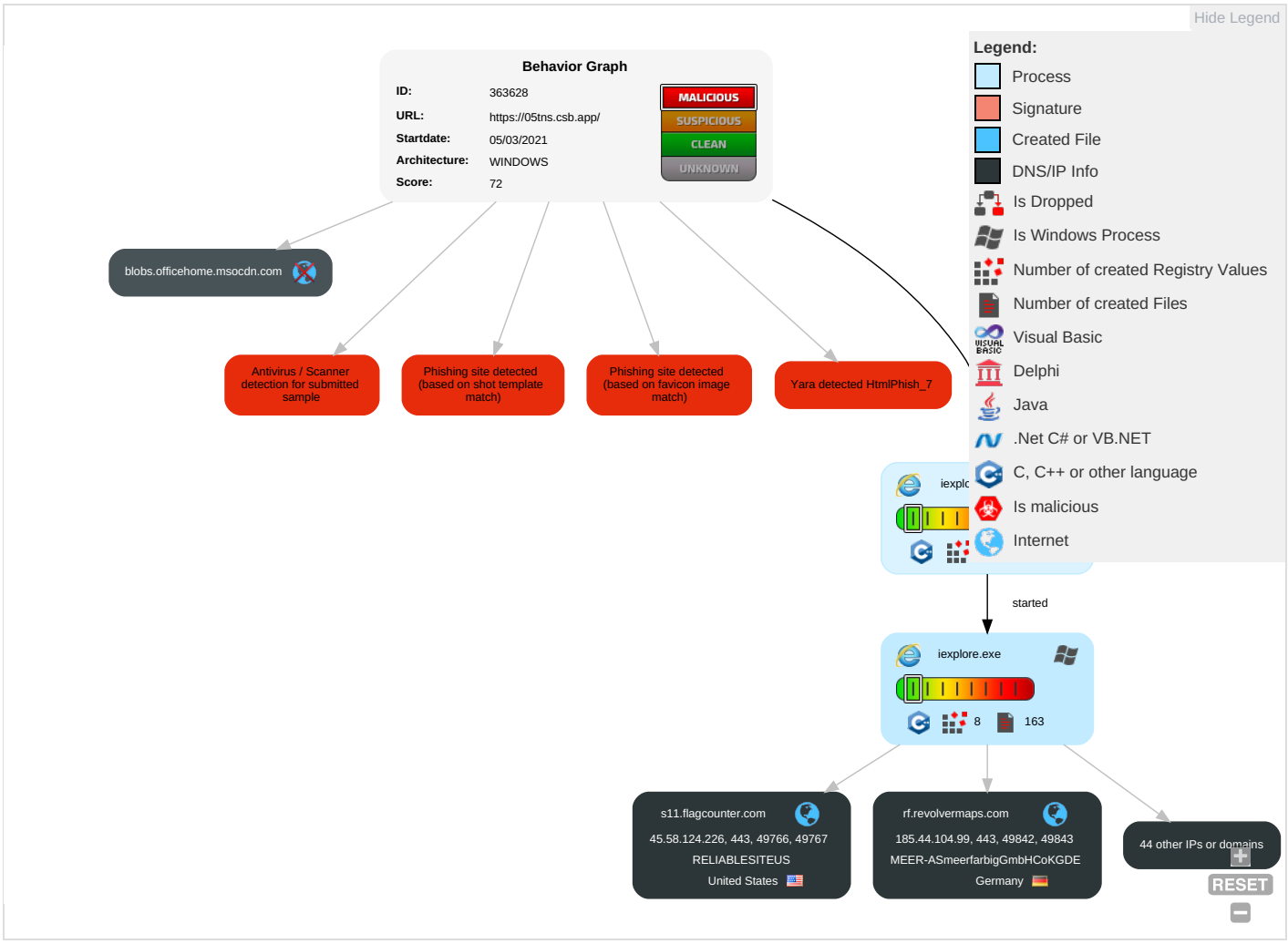
Uses secure TLS version for HTTPS connections

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
Drive-by Compromise 1	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
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 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
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 4	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 3	SIM Card Swap	

Behavior Graph

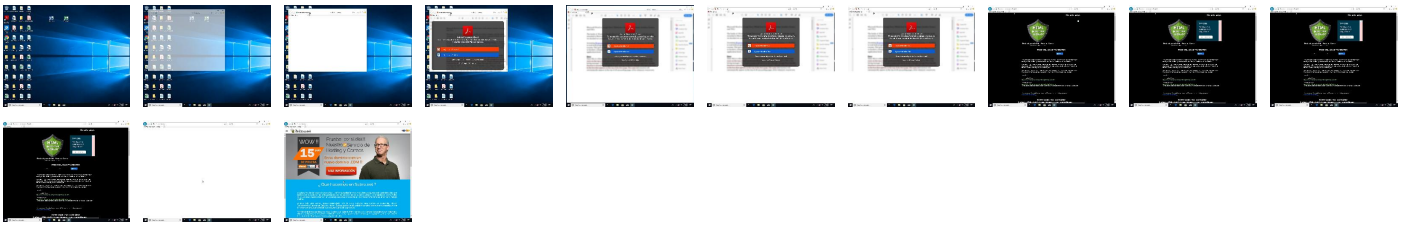
Copyright null 2021

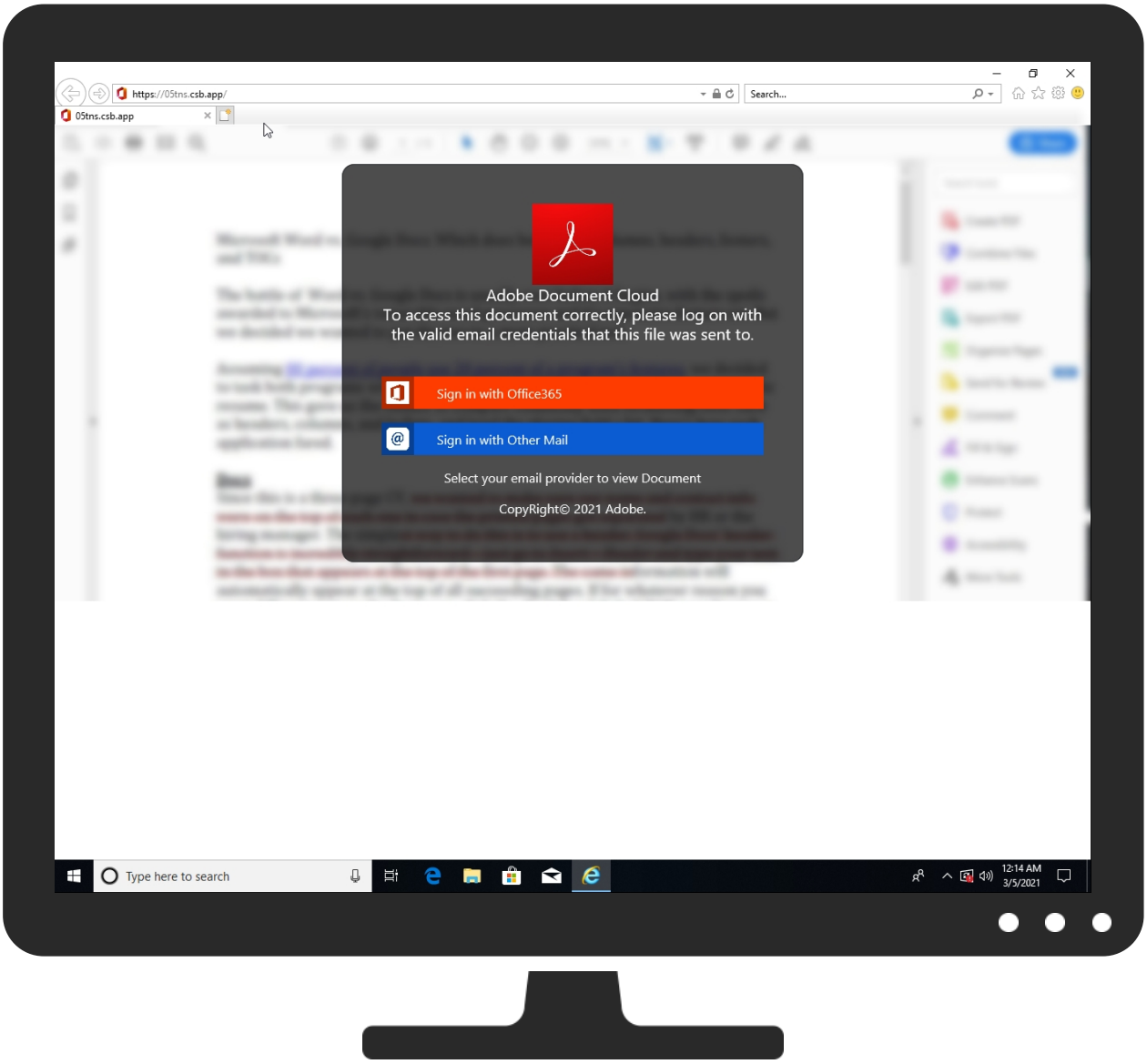


Screenshots

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://05tns.csb.app/	0%	Avira URL Cloud	safe	
http://https://05tns.csb.app/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.broofa.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.broofa.com	0%	URL Reputation	safe	
http://www.broofa.com	0%	URL Reputation	safe	
http://www.htmlprotection.kom.gt	0%	Avira URL Cloud	safe	
http://https://blobs.officehome.msocdn.com/images/content/images/favicon-8f211ea639.ico	0%	Avira URL Cloud	safe	
http://https://c.sharethis.mgr.consensu.org/is_eu	0%	Avira URL Cloud	safe	
http://https://www.internalfb.com/intern/invariant/	0%	URL Reputation	safe	
http://https://www.internalfb.com/intern/invariant/	0%	URL Reputation	safe	
http://https://www.internalfb.com/intern/invariant/	0%	URL Reputation	safe	
http://www.phpprotection.kom.gt	0%	Avira URL Cloud	safe	
http://hospitalesprivadospsiquiatricosdeguatemala.com	0%	Avira URL Cloud	safe	
http://https://www.sabro.net/favicon.pngv	0%	Avira URL Cloud	safe	
http://www.cayville.com/	0%	Avira URL Cloud	safe	
http://https://05tns.csb.app/N	0%	Avira URL Cloud	safe	
http://medicosdeguatemala.com/neurologos.htm	0%	Avira URL Cloud	safe	
http://www.htmlprotection.kom.gt/testpsw.jpg	0%	Avira URL Cloud	safe	
http://https://05tns.csb.app/Root	0%	Avira URL Cloud	safe	
http://sanatorioretirodemaria.com	0%	Avira URL Cloud	safe	
http://https://c.sharethis.mgr.consensu.org/cmp.js	0%	Avira URL Cloud	safe	
http://s1.smartaddon.com/s13.png	0%	Avira URL Cloud	safe	
http://www.hacepaginas.com/plantillas/plantilla7/index.htm	0%	Avira URL Cloud	safe	
http://https://c.sharethis.mgr.consensu.org/cmp-v2.js	0%	Avira URL Cloud	safe	
http://https://www.sabro.net/n.kom.gt/	0%	Avira URL Cloud	safe	
http://https://www.sabro.net/n.kom.gt/tton_count&show_faces=false&width=150&action=like&font=verdana&colors	0%	Avira URL Cloud	safe	
http://www.caxardelavega.es/	0%	Avira URL Cloud	safe	
http://www.smartaddon.com/?share	0%	Avira URL Cloud	safe	
http://www.protegerphp.com	0%	Avira URL Cloud	safe	
http://www.sabro.net	0%	Avira URL Cloud	safe	
http://s1.smartaddon.com/share_addon.js	0%	Avira URL Cloud	safe	
http://hospitalesantialcoholicosydrogadictosdeguatemala.com	0%	Avira URL Cloud	safe	
http://com.net.gt/pagar.cgi?hash=239876sfdg8734lkjsap93um5cp9w358gqwtc9q23lk4sunf8632bc87359nsdgcgni	0%	Avira URL Cloud	safe	
http://www.protegerjavascript.com	0%	Avira URL Cloud	safe	
http://www.htmlprotection.kom.gt/favicon.ico	0%	Avira URL Cloud	safe	
http://https://www.sabro.net/bysabro2.png	0%	Avira URL Cloud	safe	
http://hospitalespsiquiatricosguatemala.com	0%	Avira URL Cloud	safe	
http://https://blobs.officehome.msocdn.com/images/content/images/favicon-8f211ea639.ico~	0%	Avira URL Cloud	safe	
http://dreddymongue.com	0%	Avira URL Cloud	safe	
http://www.ofuscarphp.com	0%	Avira URL Cloud	safe	
http://www.sabro.net/	0%	Avira URL Cloud	safe	
http://www.javascriptprotection.kom.gt	0%	Avira URL Cloud	safe	
http://https://fburl.com/debugjs.	0%	URL Reputation	safe	
http://https://fburl.com/debugjs.	0%	URL Reputation	safe	
http://https://fburl.com/debugjs.	0%	URL Reputation	safe	
http://sanatoriospsiquiatricosdeguatemala.com	0%	Avira URL Cloud	safe	
http://https://05tns.csb.app/ion.kom.gt/Root	0%	Avira URL Cloud	safe	
http://s1.smartaddon.com/s8.png	0%	Avira URL Cloud	safe	
http://https://05tns.csb.app/n.kom.gt/Root	0%	Avira URL Cloud	safe	
http://www.htmlprotection.kom.gt/protect-html-code.jpg	0%	Avira URL Cloud	safe	
http://neuropsiquiatrasdeguatemala.com	0%	Avira URL Cloud	safe	
http://https://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://www.protegerhtml.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.googletagservices.com	172.217.22.194	true	false		high
c.statcounter.com	172.67.38.97	true	false		high
rf.revolvermaps.com	185.44.104.99	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
httplogserver-lb.global.unified-prod.sharethis.net	52.29.155.194	true	false		unknown
www.htmlprotection.kom.gt	107.161.189.250	true	false		unknown
tagr-gcp-odr-euw4.mookie1.com	34.98.67.61	true	false		high
cdnjs.cloudflare.com	104.16.18.94	true	false		high
cm.g.doubleclick.net	172.217.20.226	true	false		high
www.statcounter.com	104.22.53.65	true	false		high
id.rlcdn.com	34.120.207.148	true	false		high
ipv4.imgur.map.fastly.net	151.101.112.193	true	false		unknown
star-mini.c10r.facebook.com	185.60.216.35	true	false		high
pagead46.l.doubleclick.net	172.217.22.194	true	false		high
d2znr2yi078d75.cloudfront.net	13.224.193.72	true	false		high
us-u.openx.net	35.244.159.8	true	false		high
tag-terraform-elb-1705565586.eu-central-1.elb.amazonaws.com	3.123.210.158	true	false		high
sabro.net	107.161.189.250	true	false		unknown
s11.flagcounter.com	45.58.124.226	true	false		high
partnerad.l.doubleclick.net	142.250.186.34	true	false		high
dlaj66hdiarg7.cloudfront.net	143.204.90.102	true	false		high
googleads.g.doubleclick.net	172.217.23.34	true	false		high
pugm-lhr.pubmatic.com	185.64.190.78	true	false		high
d3oiwf0xhhk8m1.cloudfront.net	143.204.90.122	true	false		high
05tns.csb.app	104.18.26.114	true	false		unknown
d1r0ldx4ccoewq.cloudfront.net	143.204.90.62	true	false		high
blobs.officehome.msocdn.com	unknown	unknown	false		unknown
www.sabro.net	unknown	unknown	false		unknown
ka-f.fontawesome.com	unknown	unknown	false		high
buttons-config.sharethis.com	unknown	unknown	false		high
image6.pubmatic.com	unknown	unknown	false		high
d.agkn.com	unknown	unknown	false		high
adservice.google.co.uk	unknown	unknown	false		unknown
platform-cdn.sharethis.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
token.rubiconproject.com	unknown	unknown	false		high
platform-api.sharethis.com	unknown	unknown	false		high
s1.smartaddon.com	unknown	unknown	false		unknown
www.facebook.com	unknown	unknown	false		high
odr.mookie1.com	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high
maxcdn.bootstrapcdn.com	unknown	unknown	false		high
l.sharethis.com	unknown	unknown	false		high
i.imgur.com	unknown	unknown	false		high
c.sharethis.mgr.consensu.org	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.htmlprotection.kom.gt/testpsw.jpg	false	• Avira URL Cloud: safe	unknown
http://s11.flagcounter.com/count/tsG8/bg_FFFFFF/txt_000000/border_CCCCCC/columns_2/maxflags_12/viewers_0/labels_0/pageviews_0/flags_0/	false		high
http://www.htmlprotection.kom.gt/	true		unknown
http://https://05tns.csb.app/	true		unknown
http://https://www.sabro.net/	true		unknown
http://www.htmlprotection.kom.gt/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://www.sabro.net/	false	• Avira URL Cloud: safe	unknown
http://www.htmlprotection.kom.gt/protect-html-code.jpg	false	• Avira URL Cloud: safe	unknown
http://www.htmlprotection.kom.gt/	false		unknown

URLs from Memory and Binaries

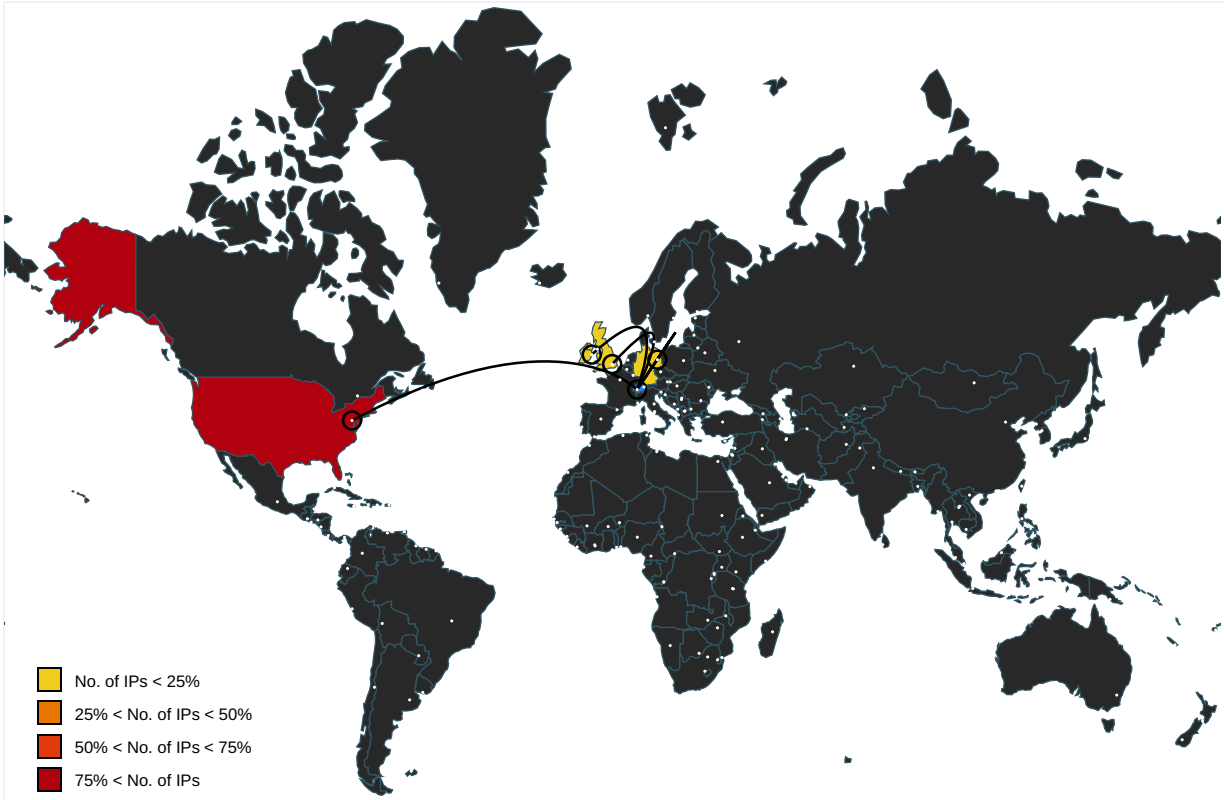
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.youtube.com/channel/UCScMHRHqDV8t6ioSd5rfGnw	NBGQBKNS.htm.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-6373591680915711&output=html&adk=1812272	{518CDF0B-7D3F-11EB-90EB-ECF4BBEA1588}.dat.1.dr, ~DF4503A7332C97782D.TMP.1.dr	false		high
http://www.broofa.com	element_main[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.htmlprotection.kom.gt	NBGQBKNS.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://blobs.officehome.msocdn.com/images/content/images/favicon-8f211ea639.ico	imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://s11.flagcounter.com/count/GkpN/bg_111111/txt_777777/border_111111/columns_2/maxflags_10/view	jquery.23.10__[1].js.2.dr	false		high
http://https://api.whatsapp.com/send?phone=50250004770&text=Necesito	menux_[1].js.2.dr	false		high
http://https://api.whatsapp.com/send?phone=50250004770&text=(sabro.net	jquery.23.10__[1].js.2.dr	false		high
http://jasm73.awardspace.com/	NBGQBKNS.htm.2.dr	false		high
http://https://buttons-config.sharethis.com/js/	sharethis[1].js.2.dr	false		high
http://https://c.sharethis.mgr.consensu.org/is_eu	sharethis[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://scripts.sil.org/OFLhttp://scripts.sil.org/OFLRalewayCopyright	Raleway-Regular[1].ttf.2.dr	false		high
http://https://05tns.csb.app/	{518CDF0B-7D3F-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true		unknown
http://https://api.whatsapp.com/send?phone=50250004770&text=(chat	jquery.23.10__[1].js.2.dr	false		high
http://https://fontawesome.com	free.min[1].css.2.dr	false		high
http://https://www.internalfb.com/intern/invariant/	hbC1ovHPP4z[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.phpprotection.kom.gt	NBGQBKNS.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/twbs/bootstrap/graphs/contributors)	bootstrap.min[1].js.2.dr	false		high
http://info.flagcounter.com/tsG8	NBGQBKNS.htm.2.dr	false		high
http://https://www.linkedin.com/sharing/share-offsite/?url=http%3A%2F%2Fwww.sabro.net	jquery.23.10__[1].js.2.dr	false		high
http://www.youtube.com/embed/	jquery.23.10__[1].js.2.dr	false		high
http://https://sharethis.com/platform/share-buttons?	sharethis[1].js.2.dr	false		high
http://https://statcounter.com/p4123447/visitor/	jquery.23.10__[1].js.2.dr	false		high
http://hospitalesprivadospsiquiatricosdeguatemala.com	jquery.23.10__[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.ampproject.org/amp4ads-host-v0.js	f[1].txt0.2.dr	false		high
http://opensource.org/licenses/MIT).	popper.min[1].js.2.dr	false		high
http://scripts.sil.org/OFLhttp://scripts.sil.org/OFL	Raleway-Regular[1].ttf.2.dr	false		high
http://https://s11.flagcounter.com/count/FxTm/bg_171717/txt_ffffff/border_171717/columns_3/maxflags_12/view	menux_[1].js.2.dr	false		high
http://https://www.sabro.net/favicon.pngv	imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.sabro.net/	A0JQBACH.htm.2.dr, {518CDF0B-7D3F-11EB-90EB-ECF4BBEA1588}.dat.1.dr, IGI3DLXG.htm.2.dr	false		unknown
http://www.cayville.com/	NBGQBKNS.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://scripts.sil.org/OFLhttp://scripts.sil.org/OFLRaleway	Raleway-Regular[1].ttf.2.dr	false		high
http://https://05tns.csb.app/N	{518CDF0B-7D3F-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true	• Avira URL Cloud: safe	unknown
http://medicosdeguatemala.com/neurologos.htm	jquery.23.10__[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://platform-cdn.sharethis.com	sharethis[1].js.2.dr	false		high
http://https://i.imgur.com/oBtBCMa.png	jquery.23.10__[1].js.2.dr	false		high
http://https://twitter.com/monge_eddy?s=03	jquery.23.10__[1].js.2.dr	false		high
http://https://05tns.csb.app/Root	{518CDF0B-7D3F-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true	• Avira URL Cloud: safe	unknown
http://https://googleads.g.doubleclick.net/pagead/html/r20210303/r20190131/zrt_lookup.html	{518CDF0B-7D3F-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false		high
http://https://platform-api.sharethis.com/powr.js?platform=sharethis	sharethis[1].js.2.dr	false		high
http://https://www.instagram.com/retiro_de_maria__/	jquery.23.10__[1].js.2.dr	false		high
http://sanatorioretirodemaria.com	jquery.23.10__[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.googletagservices.com/activeview/js/current/osd.js	f[1].txt0.2.dr	false		high
http://https://c.sharethis.mgr.consensu.org/cmp.js	sharethis[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://s1.smartaddon.com/s13.png	NBGQBKNS.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.hacepaginas.com/plantillas/plantilla7/index.htm	NBGQBKNS.htm.2.dr	false	• Avira URL Cloud: safe	unknown

Copyright null 2021

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://c.sharethis.mgr.consensu.org/cmp-v2.js	sharethis[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://googleads.g.doubleclick.net/pagead/drt/si	{518CDF0B-7D3F-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false		high
http://https://www.sabro.net/n.kom.gt/	~DF4503A7332C97782D.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	bootstrap.min[1].js.2.dr, bootstrap.min[1].css.2.dr	false		high
http://googleads.g.doubleclick.net	f[1].txt0.2.dr	false		high
http://https://www.sabro.net/n.kom.gt/tton_count&show_faces=false&width=150&action=like&font=verdana&colors	~DF4503A7332C97782D.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://www.caxardelavega.es/	NBGQBKNS.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.smartaddon.com/?share	NBGQBKNS.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.protegerphp.com	menux_[1].js.2.dr, IGI3DLXG.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.sabro.net	jquery.23.10__[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ka-f.fontawesome.com	585b051251[1].js.2.dr	false		high
http://s1.smartaddon.com/share_addon.js	NBGQBKNS.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://hospitalesantialcoholicosydrogadictosdeguatemala.com	jquery.23.10__[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://com.net.gt/pagar.cgi?hash=239876sfdg8734lkjsap93um5cp9w358gqwtc9q23lk4sunf8632bc87359nsdgcgni	NBGQBKNS.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://statcounter.com/	jquery.23.10__[1].js.2.dr	false		high
http://www.protegerjavascript.com	menux_[1].js.2.dr, IGI3DLXG.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.linkedin.com/in/dr-eddy-monge-019030135/	jquery.23.10__[1].js.2.dr	false		high
http://https://www.sabro.net/bysabro2.png	menux_[1].js.2.dr, jquery.23.10__[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://fontawesome.com/license/free	free.min[1].css.2.dr	false		high
http://s11.flagcounter.com/count/tsG8/bg_FFFFFF/txt_000000/border_CCCCCC/columns_2/maxflags_12/viewe	NBGQBKNS.htm.2.dr	false		high
http://https://platform-cdn.sharethis.com/img/share-this-logo%402x.png	sharethis[1].js.2.dr	false		high
http://https://attestation.android.com	f[4].txt.2.dr, f[1].txt.2.dr	false		high
http://hospitalespsiquiatricosguatemala.com	jquery.23.10__[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://blobs.officehome.msocdn.com/images/content/images/favicon-8f211ea639.ico~	imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-6373591680915711&output=html&h=250&slot	{518CDF0B-7D3F-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false		high
http://dreddymongue.com	jquery.23.10__[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.ofuscarphp.com	menux_[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.statcounter.com/counter/counter.js	jquery.23.10__[1].js.2.dr	false		high
http://www.javascriptprotection.kom.gt	NBGQBKNS.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	f[4].txt.2.dr, rx_lidar[1].js.2.dr	false		high
http://https://fburl.com/debugjs.	hbC1ovHPP4z[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://s05.flagcounter.com/count2/AMuf/bg_171717/txt_ffffff/border_171717/columns_3/maxflags_12/vie	menux_[1].js.2.dr	false		high
http://sanatoriospsiquiatricosdeguatemala.com	jquery.23.10__[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://05tns.csb.app/ion.kom.gt/Root	{518CDF0B-7D3F-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true	• Avira URL Cloud: safe	unknown
http://s1.smartaddon.com/s8.png	NBGQBKNS.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.ampproject.org/rtv/%	f[1].txt0.2.dr	false		high
http://https://googleads.g.doubleclick.net	f[1].txt0.2.dr	false		high
http://https://05tns.csb.app/n.kom.gt/Root	{518CDF0B-7D3F-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true	• Avira URL Cloud: safe	unknown
http://www.youtube.com/v/ZO2YrkezStQ&hl=es_ES&fs=1&autoplay=1	jquery.23.10__[1].js.2.dr	false		high
http://https://kit.fontawesome.com	585b051251[1].js.2.dr	false		high
http://neuropsiquiatrasdeguatemala.com	jquery.23.10__[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://getbootstrap.com)	bootstrap.min[1].js.2.dr, bootstrap.min[1].css.2.dr	false	• Avira URL Cloud: safe	low
http://https://c.statcounter.com/4123447/0/7ac0b739/1/	jquery.23.10__[1].js.2.dr	false		high
http://https://www.youtube.com/user/dreddymonge/videos	jquery.23.10__[1].js.2.dr	false		high
http://www.protegerhtml.com	menux_[1].js.2.dr, IGI3DLXG.htm.2.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
143.204.90.102	dlaj66hdiarg7.cloudfront.net	United States		16509	AMAZON-02US	false
52.29.155.194	httplogserver-lb.global.unified-prod.sharethis.net	United States		16509	AMAZON-02US	false
143.204.90.62	d1r0ldx4ccoewq.cloudfront.net	United States		16509	AMAZON-02US	false
143.204.90.122	d3oiwf0xhhk8m1.cloudfront.net	United States		16509	AMAZON-02US	false
45.58.124.226	s11.flagcounter.com	United States		23470	RELIABLESITEUS	false
3.123.210.158	tag-terraform-elb-1705565586.eu-central-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
107.161.189.250	www.htmlprotection.kom.gt	United States		33182	DIMENOCUS	false
35.244.159.8	us-u.openx.net	United States		15169	GOOGLEUS	false
172.217.23.34	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
172.67.38.97	c.statcounter.com	United States		13335	CLOUDFLARENETUS	false
151.101.112.193	ipv4.imgur.map.fastly.net	United States		54113	FASTLYUS	false
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
13.224.193.72	d2znr2yi078d75.cloudfront.net	United States		16509	AMAZON-02US	false
172.217.20.226	cm.g.doubleclick.net	United States		15169	GOOGLEUS	false
142.250.186.34	partnerad.l.doubleclick.net	United States		15169	GOOGLEUS	false
185.64.190.78	pugm-lhr.pubmatic.com	United Kingdom		62713	AS-PUBMATICUS	false
34.120.207.148	id.rlcdn.com	United States		15169	GOOGLEUS	false
172.217.22.194	www.googletagservices.com	United States		15169	GOOGLEUS	false
185.60.216.35	star-mini.c10r.facebook.com	Ireland		32934	FACEBOOKUS	false
104.22.53.65	www.statcounter.com	United States		13335	CLOUDFLARENETUS	false
104.18.26.114	05tns.csb.app	United States		13335	CLOUDFLARENETUS	false
34.98.67.61	tagr-gcp-odr-euw4.mookie1.com	United States		15169	GOOGLEUS	false
185.44.104.99	rf.revolvermaps.com	Germany		34549	MEER-ASmeerfarbigGmbHCoKGDE	false

Copyright null 2021

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	363628
Start date:	05.03.2021
Start time:	00:12:30
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://05tns.csb.app/
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:	7
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:	mal72.phis.win@3/113@36/23
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: http://www.htmlprotection.kom.gt/ • Browsing link: http://www.sabro.net/

Copyright null 2021

Warnings:	Show All • Exclude process from analysis (whitelisted): ielowutil.exe, backgroundTaskHost.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.139.144, 104.42.151.234, 88.221.62.148, 172.217.23.42, 209.197.3.24, 209.197.3.15, 216.58.207.170, 104.18.23.52, 104.18.22.52, 172.64.202.28, 172.64.203.28, 104.43.193.48, 23.218.209.132, 52.255.188.83, 172.217.22.206, 142.250.185.194, 51.11.168.160, 216.58.207.130, 172.217.22.195, 172.217.23.33, 172.217.23.68, 69.173.144.139, 69.173.144.165, 69.173.144.138, 152.199.19.161, 20.54.26.129, 52.155.217.156, 205.185.216.42, 205.185.216.10 • Excluded domains from analysis (whitelisted): cds.s5x3j6q5.hwcdn.net, arc.msn.com.nsatc.net, ka-f.fontawesome.com.cdn.cloudflare.net, pixel.rubiconproject.net.akadns.net, partner.googleadservices.com, adservice.google.com, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, go.microsoft.com, e12520.g.akamaiedge.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, www.google.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, www.gstatic.com, au-bg-shim.trafficmanager.net, kit.fontawesome.com.cdn.cloudflare.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fonts.googleapis.com, ajax.googleapis.com, ie9comview.vo.msecnd.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, cds.d2s7q6s2.hwcdn.net, pagead2.googlesyndication.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, www3.l.google.com, translate.googleapis.com, tpc.googlesyndication.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, translate.google.com, cds.j3z9t3p6.hwcdn.net, wildcard.officehome.msocdn.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtDeviceIoControlFile calls found. • VT rate limit hit for: https://05tns.csb.app/

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\DOMStore\E5F0NRSV\www.htmlprotection.kom[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4477
Entropy (8bit):	4.783064408319448
Encrypted:	false
SSDEEP:	96:uQO/QOi8QO4QOEQOJxQOuMQQOHQO/QOi8QO4QOEQOJxQOuMQQOHQOnQO/QOi8QOU:8FiSuKNuMW9FiSuKNuMW9dFiSuKNuMWr
MD5:	72493A93B01F1FF7B968DF4BC974E405
SHA1:	FEE897A6CCB96BFCC4DF96D0F39007A2D4FC9A40
SHA-256:	5D49AAE119234F8B1DB456B77880969D5E9E68AB15E143B0BF7473076A6C8273
SHA-512:	B341A298DEB32DE5E293EE56FD2A11376B67EB40B145B98F06AD8FB44DD2F8263C3621756F53AE92714E81257D25AE8AB2B06BB47C24E8B5BE0753959B8D89E6
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="goog_pem_mod" value="792" ltime="568614336" htime="30871884" /></root><root><item name="goog_pem_mod" value="792" ltime="568614336" htime="30871884" /><item name="google_experiment_mod47" value="194" ltime="568614336" htime="30871884" /><item name="google_experiment_mod34" value="348" ltime="568614336" htime="30871884" /><item name="google_experiment_mod53" value="907" ltime="568614336" htime="30871884" /><item name="google_experiment_mod36" value="758" ltime="568614336" htime="30871884" /><item name="google_experiment_mod37" value="873" ltime="568614336" htime="30871884" /><item name="google_experiment_mod44" value="38" ltime="568614336" htime="30871884" /></root><root><item name="goog_pem_mod" value="792" ltime="568614336" htime="30871884" /><item name="google_experiment_mod47" value="194" ltime="568614336" htime="30871884" /><item name="google_experiment_mod34" value="348" ltime="568614336" htime="30871884" /><item name="google_experiment_mod53" value=

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\URW0GA4Q\www.sabro[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	257
Entropy (8bit):	4.855971561134019
Encrypted:	false
SSDEEP:	6:JFK1rUFF0HYJqqrJP9NuQOKw1rFK1rUF49MFGkqqOJawQOKwb:JsrUAHs7XNuQO5rsULF57OlwQO3
MD5:	5D3EBCFA6AA5CA139054B19DA92C9FDC
SHA1:	B08E5C941DE28B0333CCB2296D1CDFB0DDD7532D
SHA-256:	8725AAA91F67CD9306B775F249FBE9CE8DD872E9AF93FE2FB78212F299C02EE8
SHA-512:	D21F65B4F9AEAEC3DBC66DDA3F58CC01460EBADC753B7A169CDD6B6135A2B0FDF8A54D1301E78CE78858E577E0B607D7CC50BFF2CAD94390D5C48FE67CFFE7D
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="__sharethis_local_storage_test__" value="hello world" ltime="697574336" htime="30871884" /></root><root></root><root><item name="sc_medium_source" value="{"d":1614899684}" ltime="697934336" htime="30871884" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{518CDF09-7D3F-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{518CDF09-7D3F-11EB-90EB-ECF4BBEA1588}.dat	
Size (bytes):	30296
Entropy (8bit):	1.849782747790178
Encrypted:	false
SSDEEP:	192:rtZHZE2OLWXt6ifvOMzM6UBsaDusfdOxjX:rD5TV9DmHJ9S
MD5:	35BD377F602050427217728D4745FB62
SHA1:	BC1A8EA3AB7CE4C0B1C18277450BA91442B6653B
SHA-256:	28FDE6F8EBBA7855465C6BB70E1F326ECEA1E4E8CEB1B49126E04E5BA30CE208
SHA-512:	8E3C1092D8F954873677AE97608B6F114A17E44A3DCB3887D24C659ABD6FFA9FE8A4F8C473BBC16DF0FACA65F10A010F0B469B0524067998030E2789697F8B7E
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\{518CDF0B-7D3F-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	232886
Entropy (8bit):	3.6944488023813413
Encrypted:	false
SSDEEP:	768:DT2ssuT2sscT2ssDk9qq5jx16Xq5jx1zT2sswT2ssFT2ssX2ssD2ss92ss1k9AjW:8q716Xq713Goq716Xq713G7
MD5:	214A1701B9EFA9F15DC113DCDEC30F2D
SHA1:	8139BDE58F61DB990B01225E4241568475187101
SHA-256:	E83ECE27C9F49ED1C1419061B26A5EA9C2C76E70FF001EDD24363DB6C1A848E5
SHA-512:	5CB62A9E210AC158A5824C5C264396C1A0FA434FBB757CF59423D75D6FBFE774964E0A3C069ABD057A8CC104132C2EF6DE5343F87E80A232A23665A90FE1835
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\{5A362815-7D3F-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5659639908782597
Encrypted:	false
SSDEEP:	48:Iw0GcpruGwpasG4pQwGrapbSpZGQpKNG7HpRRaTGIpG:roZGQs6OBSpzAsTReA
MD5:	40BA13B1A4BC19F84520265387FD39FF
SHA1:	F515E0AB49BF0DE67E5299DA831A3051B805CC76
SHA-256:	076F5D7496F80C1BBCF9AB1C3B027CB1767B5DB469AE0BFBADDCDF2E553F40D0
SHA-512:	714D9B172110BC764166FEF9A150FFBFAF0C04FEA1488AC55B5FCEB00D47443EF7E025D88276BC9F2A20377D8E6EDAD5A04552913D81668D993BA1DDA8D4BB 9
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	10762
Entropy (8bit):	5.091045047326189
Encrypted:	false
SSDEEP:	96:RoLnMvyyT8b1q+qoX4WCKiBpEaaproKGTI8tKepwznmky33N5H0qMf:RINb1q+q4aBarxB8tKDYnN5H0qMf
MD5:	7E4159994C47B5ADF290303693EB117B
SHA1:	C47F4DE85ACFBFF9D603E0634954B40A73696947
SHA-256:	B5895C999B6670E4263C0EA76342AE4AB5B80356C28A422CEE21539A27C4D572

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
SHA-512:	F74A1AA86AB7059FBA3A21855D8021CBF515926B1DB81956E8BF5954033FA9E27744CF95E08A95FF121D2475AB2FD646E5CDA9513B04299336874D1F5A3033FA
Malicious:	false
Reputation:	low
Preview:	P.h.t.t.p.s.:././.b.l.o.b.s...o.f.f.i.c.e.h.o.m.e...m.s.o.c.d.n...c.o.m./.i.m.a.g.e.s./.c.o.n.t.e.n.t./.i.m.a.g.e.s./.f.a.v.i.c.o.n.-.8.f.2.1.1.e.a.6.3.9...i.c.o..... ....(... ...@..... ....$.. ...@.' .....0.. +..%.....&..:.;.@..... .....9$..6"..1...+...%.....;..;..;..;..;.`.;.....@(.;%..6"..1...+...%.....;..;..;..;..;..;..;..;..;.p..... .....F,.0E+..@)..;%..6"..1...,...&... .....;..;..;..;..;..;..;..;..;.....F,..E+..@)..;%..6"..1...,...&... .....;..;..;..;..;..;..;..;..;..;..;..;..;.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\585b051251[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	10866
Entropy (8bit):	5.182477446178365
Encrypted:	false
SSDEEP:	192:BBHN42S+9SZRvACpiIthFzoXnemF+shSGnZ+PPxQDqv7jh81Q5l8OcchIlzbCn:HRCfhFzevnEZ/h81Q5l8OsE
MD5:	4B900F0AF3BBDA85E1077C8EC8C83831
SHA1:	7E7015965195F25AFA3A47BE2108278AD6A0A4AC
SHA-256:	7943D6D067DB8587E9FB675F0D2CC78D6C90C91B187CF8642A3F52FF91381685
SHA-512:	2CD82E0DCD1381447522CFFD610136513323E5D2980FAE730801FE8BBA580FF7FDF9CB8D2E9AC794D6F2FB59C724EDA71BECE7CAA72C775BC963E1A54B30EB CB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://kit.fontawesome.com/585b051251.js
Preview:	window.FontAwesomeKitConfig = {"asyncLoading":{"enabled":true},"autoA11y":{"enabled":true},"baseUrl":"https://ka-f.fontawesome.com","baseUrlKit":"https://kit.fo ntawesome.com","detectConflictsUntil":null,"iconUploads":{},"id":132286382,"license":"free","method":"css","minify":{"enabled":true},"token":"585b051251","v4Fon tFaceShim":{"enabled":false},"v4shim":{"enabled":true},"version":"5.15.2"};.!function(t){"function"==typeof define&&define.amd?define("kit-loader",t):t()}((function(){"use strict";function t(e){return(t="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})(e)}function e(t,e,n){return e in t?Object.defineProperty(t,e,{value:n,enumerable:!0,configurable:!0,writ able:!0}):t[e]=n,t}function n(t,e){var n=Object.keys(t);if(Object.getOwnPropertySymbols){var r=Object.getOwnPropertySymbols(t);e&&(r=r.filter((function(e){return Object.g

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\9560678631816622811[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 300 x 250, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	4752
Entropy (8bit):	7.905322416694388
Encrypted:	false
SSDEEP:	96:yJUHzEekMxFsdJmWe+lXFog0ZMUSZg98yx7Y5TXLfKxwp:KX+xCmG/UkaFE5TXbKxwp
MD5:	7E206AC275BA7456CC45EE2FD27D6FEA
SHA1:	E2460E14733D12FE614830AE85FF00EC43E217F1
SHA-256:	F9E931C78E401B497EBE22947734CAA29CCFD79D2473AF8A8E680B2FAAC5BF9F
SHA-512:	B554D03EF6FC48FD4FC817A7AB98A9BD6691B01897EA384B48AACFE425C093218CA5093C716DE78E5EFFF15BA4334D8C5C11E287DAC3655ACAF59F283EC43E 0D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/simgad/9560678631816622811?sqp=4sqPyQQrQikqJwhfEAEdAAC0QiABKAEwCTgDQPCTCUgAUAFYAWBfcAJ4AcUBLbKdPg&rs=AOga4qkQRHh7HP5T2gUr0tLF_9TMMPg_wQ
Preview:	.PNG.....IHDR...,.....,.....PLTE.9M..... M^.....@`o`t..... L^.CU..... Rc...`.....0Vg/25`s.....Pjw.....L^0Vf...kmo@jzp}..FX...p~.....CV...`.....kmp...MOS... Pjx.....p.....026...MPS.....o~....Pw....>ADPv.0^o.EX.....MOR0^n.....p....._t.p}.MPR.....\^a!#'.....z{~...@jy...025...!$'...Pw....z{}\^`y{~.../26.RcPv. #'.....o.....z\|~.....?@D..... Qco..@kz_.....jlo....._`>@DkloE.0A....IDATx.._....%[.V....c.l..+...B .%.p. ..4Ws'M.4.....e....F.....]k..F.[9...'.{BH..a!,.....BBX..a !,.....BX..a!,.....BX..a!,.....BX....H..V..[.?..e5.....BJ.4.d{...Z/$.s.wM..A...s..<..U$....F.{.ng..s8....i..ohZ.e..z.....^8...$7...'..$Mj.z..86:..uE...?....G.V&.J=.....O'3....i.+./;.2.B*;.;..... J/h....Z.k....z.L.j^.hM>4.,J1-..(....64.jF8,.$377..a.....}. 0..9.u`]....9,..Q.....sS.....+R>[....`A%v.7.....J.rU..t:=RoY....>L.W5m..:....^...X..^..`...k

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\A0JQBACH.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	230
Entropy (8bit):	5.090627889035541
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwol6hEr6VX16hu9nPjLVR+KqD:J0+ox0RJWWPiT
MD5:	EBF88D84B8CDA6A4EFFF23DEF85C4E71
SHA1:	E28114F56774CBFF3E3D6D8794F1FD2442B8C63D
SHA-256:	9E69E65F5036CED77306A086CFA20244A76E740DF28EF0A01C8BDBFF985E286A
SHA-512:	45B6A9F10D919A3521CB68EA65932652E7A7C08794BD076AF631FD6FF63D9C5E9B331795C3C02F2264545210C1F8B68D3C7A0D0B75C9B0A78C519FA76B5650D8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\A0JQBACH.htm	
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\2WF3MMUU\XAV7EGKH.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	exported SGML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	3584499
Entropy (8bit):	3.073243234012029
Encrypted:	false
SSDEEP:	768:T0+0v+0b0v+09mZQOtK/8Qxbbyb+bb5bbw+bb0bR+bbubb/+bbIzbm+bbI/bT+bA:T0Rs+0RsC
MD5:	C710470393D9103B9C1F2FD0CFAB6B51
SHA1:	E60E1DD6773CDE765E7D76AD7693924646818A3E
SHA-256:	78209F63D344F8130FD4D32ACEB75EDD4E6AC82C553AD1AEDDFDFAFA0C38B1FC
SHA-512:	E793BAB6DC38FDB95F422287C7B62A0183E54DEC4DC23CBD0F047C056D9C6282FF74182DAE3A3BC28B9CC4B47DBAE3315B5E978860859EDDB57793F01DC56AB
Malicious:	false
Reputation:	low
Preview:	.... ##. ### ###. ### THIS WEBPAGE WAS PROTECTED AT: www.htmlprotection.kom.gt ###. ### ###. ## ##################################.....TG9yZW0gaXBzdW0gZG9sb3Igc2l0IGFtZXQsIGNvbnNlY3RldHVlciBhZGlwaXNjaW5nIGVsaXQsIHNlZCBkaWFtIG5vbnVtbXkgb.mliaCBldWlzbW9kIHRpbmNpZHVudCB1dCBsYW9yZWV0IGRvbG9yZSBtYWduYSBhbGlxdWFtIGVyYXQgdm9sdXRwYXQuIFV0IHdpc2.kgZW5pbSBhZCBtaW5pbSB2ZW5pYW0sIHF1aXMgbm9zdHJ1ZCBleGVyY2kgdGF0aW9uIHVsbGFtY29ycGVyIHN1c2NpcGl0IGxvYm9.ydGlzIG5pc2wgdXQgYWxpcXVpcCBleCBlYSBjb21tb2RvIGNvbnNlcXVhdC4gRHVpcyBhdXRlbSB2ZWwgZXVtIGlyaXVyZSBkb2xv.ciBpbiBoZW5kcmVyaXQgaW4gdnVscHV0YXRlIHZlbGl0IGVzc2UgbW9sZXN0aWUgY29uc2VxdWF0LCB2ZWwgaWxsdW0gZG9sb3JlI.GV

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\ads[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	62284
Entropy (8bit):	6.1219462480367755
Encrypted:	false
SSDEEP:	1536:Jxc3z9+e69OVpfCRxCZ6BHEiVn+aMDWewKb5:JxcD9Z69GpwB5V+aMHwe5
MD5:	B3C5F9CB0085D740C1002177998827EA
SHA1:	0510BB393423A780D47DBD0C2E1B75D348D76BB3
SHA-256:	38BBC4D6A46F4654914B7E468603E01E9B772FBC155D099769E2496F34F82E9D
SHA-512:	3979F241C26CD570B049C61C32B1ECDDA1F3A761BC5A4C7E7FA5374ED5CB3DDDD18D38C52201FDB4BDD65C19B3E08CFCC8F4446C1AB2C97DA6E07AC7648BD2D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-6373591680915711&output=html&h=250&slotname=9454352660&adk=3430002613&adf=1314770583&pi=t.ma~as.9454352660&w=250&lmt=1614899672&url=http%3A%2F%2Fwww.htmlprotection.kom.gt%2F&flash=29.0.0&wgl=1&adsid=ChEIgKeCggYQ6quMiYul5rvRARIvAD5jN23CnTlAjBbaP0KlHQMXatMuye_Jt8cDEXFEc6rZMonxjOBau1U4XQ6VvAM&dt=1614899671622&bpp=20&bdt=701&idt=641&shv=r20210303&cbv=r20190131&ptt=5&saldr=sa&abxe=1&cookie=ID%3Db85e1f3cdfd063ee-22ca798fa8ba00a8%3AT%3D1614899617%3ART%3D1614899617%3AS%3DALNI_MZjBCCxQhf4gdmXmPjgCpdTTZ97pQ&prev_slotnames=9454352660%2C9454352660&correlator=4400435368515&frm=20&pv=1&ga_vid=2003745227.1614899672&ga_sid=1614899672&ga_hid=1318567104&ga_fc=0&u_tz=60&u_his=2&u_java=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_nplug=1&u_nmime=2&adx=648&ady=2363&biw=1263&bih=906&scr_x=0&scr_y=0&eid=21066432%2C21066922%2C21068108%2C21069711&oid=3&pvsid=4089538964379651&pem=792&rx=0&eae=0&fc=640&docm=11&brdim=0%2C78%2C-8%2C-8%2C1280%2C%2C1296%2C1000%2C1280%2C906&vis=1&rsz=%7Cm%7Cebr%7Cp&abl=XS&pfx=0&fu=8192&bc=1&ifi=3&uci=a!3&btvi=2&xpc=DbpAEryMgX&p=http%3A//www.htmlprotection.kom.gt&dtd=805
Preview:	<!doctype html><html><head><script>var jscVersion = 'r20210303';</script><script>var google_casm=[];</script><style>a { color: #000000 }.img_ad:hover {-webkit-filter: brightness(120%)}</style><script></script><script>window.dicnf = {};</script><script data-jc="41" data-jc-version="r20210303" data-jc-flags="["x%278446'9efotmy"]">(function(){/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0 */ function b(){var a;return a=void 0===a?window:a};b().viewReq=[];b().vu=function(a){var c=new Image;c.src=a.replace("&","&");b().viewReq.push(c)};}).call(this);</script><script data-jc="55" data-jc-version="r20210303">(function(){/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0 */ var g="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a};function h(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&w

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\arrow_right[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	565
Entropy (8bit):	4.489859281890485
Encrypted:	false
SSDEEP:	12:t4IRMXV+DtAOjFQWUFTnQFsUdFMDwolio8pnQFsU0gAvF:t4IuXV+BkNFTnQuwoynQWgAvF

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\arrow_right[1].svg	
MD5:	9928D025BD5792B718EE0A185F62E67C
SHA1:	16406D7B5B6D383B12859B853CF6CB7E3733E33D
SHA-256:	1BAE747C7FD090F56608956A97C870391E1C43F89D24D5766129B75628985C1E
SHA-512:	AE02F45454A4FB7B4D05CB5CCCA4BB5BD0D86909916BD78BA300B009CFCC5E71B89A812EA2E650B0D2EB9065D78D512180C4F8843E7DFF3109D3FB68E4810E7F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://platform-cdn.sharethis.com/img/arrow_right.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" fill="#fff" preserveAspectRatio="xMidYMid meet" height="1em" width="1em" viewBox="0 0 40 40">. <g>. <path d="m22.3 2 1.4q0 0.3-0.2 0.5l-10.4 10.4q-0.3 0.3-0.6 0.3t-0.5-0.3l-1.1-1.1q-0.2-0.2-0.2-0.5t0.2-0.5l8.8-8.8-8.8-8.7q-0.2-0.3-0.2-0.6t0.2-0.5l1.1-1.1q0.3-0.2 0.5-0.2t0.6 0.2l10.4 10.4q0.2 0.2 0.2 0.5z m8.6 0q0 0.3-0.3 0.5l-10.4 10.4q-0.2 0.3-0.5 0.3t-0.5-0.3l-1.1-1.1q-0.2-0.2-0.2-0.5t0.2-0.5l8.8-8.8-8.8-8.7q-0.2-0.3-0.2-0.6t0.2-0.5l1.1-1.1q0.2-0.2 0.5-0.2t0.5 0.2l10.4 10.4q0.3 0.2 0.3 0.5z"></path>. </g>.</svg>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\bootstrap.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	48944
Entropy (8bit):	5.272507874206726
Encrypted:	false
SSDEEP:	768:9VG5R15WbHVKZrycEHSYro34CrSLB6WU/6DqBf4l1B:9VIRuo53XiwWTvl1B
MD5:	14D449EB8876FA55E1EF3C2CC52B0C17
SHA1:	A9545831803B1359CFEED47E3B4D6BAE68E40E99
SHA-256:	E7ED36CEEE5450B4243BBC35188AFABDFB4280C7C57597001DE0ED167299B01B
SHA-512:	00D9069B9BD29AD0DAA0503F341D67549CCE28E888E1AFFD1A2A45B64A4C1BC460D81CFC4751857F991F2F4FB3D2572FD97FCA651BA0C2B0255530209B182F2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js
Preview:	/*!. * Bootstrap v4.0.0 (https://getbootstrap.com). * Copyright 2011-2018 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors). * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquery"),require("popper.js")):"function"==typeof define&&define.amd?define(["exports","jquery","popper.js"],e):e(t.bootstrap={},t.jQuery,t.Popper)}(this,function(t,e,n){"use strict";function i(t,e){for(var n=0;n<e.length;n++){var i=e[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(t,i.key,i)}}function s(t,e,n){return e&&i(t.prototype,e),n&&i(t,n),t}function r(){return(r=Object.assign||function(t){for(var e=1;e<arguments.length;e++){var n=arguments[e];for(var i in n)Object.prototype.hasOwnProperty.call(n,i)&&(t[i]=n[i])}return t}).apply(this,arguments)}e=e&&e.hasOwnProperty("default")?e.default:e,n=n&&n.hasOwnProp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\cookie_push_onload[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	1174
Entropy (8bit):	5.74166936214599
Encrypted:	false
SSDEEP:	24:hY6t2eJJBewfHDdUg8EcvjHODQMJXeK+C6uS/MLmeK+C6uSGymWAuDSXeMzCUtVv:9V4goLHODS1CTXT1CTVyPyCM6Nu
MD5:	2FE2B1F17888E326B010A8CDA72D48D3
SHA1:	59CBBEEDE4C472024C482BAE8529144119BBBD27
SHA-256:	9A9B7FB32E01FD70747F32EFDBD0472FD681C85EEBB0C42D10C7A514820A0062
SHA-512:	30BE2E73020EB97A67709E47DED40E999D352DA9B94EDD946D1315BDA65AD616AAA3CDFCFA675D061E4ED4AE1BAE3F0D245908D44411B2425C49B4345D2F6607
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html>.<head>. <title></title>. <script type="text/javascript">(function(){var f=null,g=null;function l(a){var b="";n(a,function(a){b+=String.fromCharCode(a)});return b}function n(a,b){function c(b){for(;e<a.length;){var c=a.charAt(e++),d=g[c];if(null!=d)return d;if(!/^[\s\xa0]*$/.test(c))throw Error("Unknown base64 encoding at char: "+c);}return b}p();for(var e=0;;){var d=c(-1),m=c(0),h=c(64),k=c(64);if(64===k&&-1===d)break;b(d<<2|m>>4);64!=h&&(b(m<<4&240|h>>2),64!=k&&b(h<<6&192|k))}}.function p(){if(!f){f={};g={};for(var a=0;65>a;a++)f[a]="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=".charAt(a),g[f[a]]=a,62<=a&&(g["ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789-_".charAt(a)]=a)}};function q(){for(var a=window.location.hash.substring(1).split("","),b=0;b<a.length;b++){var c=l(a[b]),e=window;e.google_image_requests||(e.google_image_requests=[]);var d=e.document.createElement("img");d.src=c;e.google_image_requests.push(d)}}var r=!1;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\cookie_push_onload[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1174
Entropy (8bit):	5.74166936214599
Encrypted:	false
SSDEEP:	24:hY6t2eJJBewfHDdUg8EcvjHODQMJXeK+C6uS/MLmeK+C6uSGymWAuDSXeMzCUtVv:9V4goLHODS1CTXT1CTVyPyCM6Nu
MD5:	2FE2B1F17888E326B010A8CDA72D48D3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\cookie_push_onload[2].htm	
SHA1:	59CBBEEDE4C472024C482BAE8529144119BBBD27
SHA-256:	9A9B7FB32E01FD70747F32EFDBD0472FD681C85EEBB0C42D10C7A514820A0062
SHA-512:	30BE2E73020EB97A67709E47DED40E999D352DA9B94EDD946D1315BDA65AD616AAA3CDFCFA675D061E4ED4AE1BAE3F0D245908D44411B2425C49B4345D2F66 07
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pagead2.googlesyndication.com/pagead/s/cookie_push_onload.html
Preview:	<!DOCTYPE html>.<html>.<head>. <title></title>. <script type="text/javascript">(function(){var f=null,g=null;function l(a){var b="";n(a,function(a){b+=String.fromCharCo de(a)});return b}function n(a,b){function c(b){for(;e<a.length;){var c=a.charAt(e++),d=g[c];if(null!=d)return d;if(!/^[\s\xa0]*$/.test(c))throw Error("Unknown base64 encoding at char: "+c);}return b}p();for(var e=0;;){var d=c(-1),m=c(0),h=c(64),k=c(64);if(64===k&&-1===d)break;b(d<<2|m>>4);64!=h&&(b(m<<4&240|h>>2),64!=k&&b(h<<6&192|k))}}.f unction p(){if(!f){f={};g={};for(var a=0;65>a;a++)f[a]="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=".charAt(a),g[f[a]]=a,62<=a&& (g["ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789-_".charAt(a)]=a)}};function q(){for(var a=window.location.hash.substring(1).split(",",b=0;b<a.length;b++){var c=l(a[b]),e=window;e.google_image_requests||(e.google_image_requests=[]);var d=e.document.createElement("img");d.src=c;e.google_ima ge_requests.push(d)}}var r=!1;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\element_main[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	256226
Entropy (8bit):	5.4774099335172455
Encrypted:	false
SSDEEP:	3072:0Pp0vOR/B/WRPMgDQ1H3mmrbZ0FGxW2EvM02ed+Do29vqnyP5:0PpuORp2MbZ0FGI2E8edsD9vqyB
MD5:	1BA8F1D626C12BAE2734585A8B495EC9
SHA1:	0DCC95B169A5887D2ED27AA1BBF3A411FB547B15
SHA-256:	CA537B74A51C73D56A401EA7D361AD32F692558AB321B86A8FB0979F2927712C
SHA-512:	940C8ED49753BFCC3CD95B961AFD5B985EE3977FC107FECEF83C402CEA3B02F37E299F0456EB4F65299EB4A62C6CA48279B494F7180C678BC450854269F3372
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://translate.googleapis.com/element/TE_20210224_00/e/js/element/element_main.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var aa="' style="background-image:url(',ba="-disabled",ca="-document.getEl ementById('",da="/translate_a/t",ea="/translate_suggestion?client=",fa='</button> </td></tr><tr id="',ha='</td><td class="goog-te-banner-margin"></td> <td nowrap> <button id="',ia='<head><meta http-equiv="Content-Type" content="text/html; charset=UTF8"><link rel="stylesheet" type= "text/css" href="',ja="Component already rendered",g="DIV",ka="Edge",la="Google Website Translator",.ma="IFRAME",na="INPUT",oa="INTERNAL_SERVER_ERROR" ,pa="Not available",qa="Opera",ra="POST",sa="SPAN",ta="Symbol.iterator",ua="TEXTAREA",va="Unable to set parent component",wa="[goog.net.IframeIo] Unable to send, already active.",xa="about:invalid#zClosurez",ya="about:invalid#zSoyz",za="absolute",Aa="action",Ba="activedescendant",Ca="activity-form-container",Da="alt-ed ited",Ea="array",Fa="auto",Ga=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\f[1].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	98070
Entropy (8bit):	5.597766641016475
Encrypted:	false
SSDEEP:	1536:e022FRu33NKEmw/4NN1wxk9PnNGgQBX/sDCRw6zLr7AcahYGB1Yid7l5:+cIfmTZ9PYBh/sG6S7Evj7l5
MD5:	934312710DEC04F2E7FED694F850A076
SHA1:	FAEB9642C548AA8FBCD56AEDDF947E30CEC00A52
SHA-256:	4ED6D183A1851A29CD11C6AAB18604259B904D876CA3994923C336AB4C6F194E
SHA-512:	B8A5C89F1389288C738DE7F22E65686A6F55E5C1A05BDB3D8A064F4C40433EFCA82D35D2458A7E71E613ADC757264B7BEED4B0BB28FB01876BB52B968146F66
Malicious:	false
Reputation:	low
IE Cache URL:	http://pagead2.googlesyndication.com/pagead/show_ads.js
Preview:	(function(sttc){/* . . Copyright The Closure Library Authors. . SPDX-License-Identifier: Apache-2.0 .*/ .var q;function aa(a){var b=0;return function(){return b<a.length? {done:!1,value:a[b++]}:{done:!0}}}var ba="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)retur n a;a[b]=c.value;return a}; .function ca(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");}var ea=ca(this),fa="function"===typeof Symbol&&"symbol"===typeof Symbol("x"),r={},ha={};function t(a,b){var c=ha[b];if(null==c)return a[b];c=a[c];return void 0!==c?c:a[b]} .function v(a,b,c){if(b)a:{var d=a.sp lit(".");a=1===d.length;var e=d[0],f,!a&&e in r?f=r:f=ea;for(e=0;e<d.length-1;e++){var g=d[e];if(!(g in f))break a;f=f[g]}d=d[d.length-1];c=fa&&"es6"===c?f[d]:n

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\f[2].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	196
Entropy (8bit):	5.462605300203498
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\f[2].txt	
SSDEEP:	6:tDpuP3ha5u0fe1vEEprbsRdp+q1hQLdV2rP8C:9p55umEvEEp3sRP3QptC
MD5:	0410DC2D3446412323FFC3BA008FC67C
SHA1:	192C37F9F6A829A50E21EB16A7DC1E15D5E032E1
SHA-256:	38570A41AE790E351E2F451C18FC847EA5E3DD78E5457F150FE4AD502F659F16
SHA-512:	0F84FEE68042639BEB0558D43F6691A5D7B292B41311C41D6602B66BAF080DE6E8DCAFC3384237D228428AC047DA08AC50DB735E91B14DBB9D5442C3D2A461E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://partner.googleadservices.com/gampad/cookie.js?domain=www.htmlprotection.kom.gt&callback=_gfp_s_&client=ca-pub-6373591680915711
Preview:	_gfp_s_({"_cookies_":[{"_value_":"ID=b85e1f3cdfd063ee-22ca798fa8ba00a8:T=1614899617:RT=1614899617:S=ALNI_MZjBCCxQhf4gdmXmPjgCpdTTZ97pQ","_expires_":1648595617,"_path_":"/","_domain_":"kom.gt"}]});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\favicon[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	2166
Entropy (8bit):	7.864313413638801
Encrypted:	false
SSDEEP:	48:1elLb7crze15Ep7sTH/3gmvz1R3SDiNBzYW8HPiM0:1epwznmky33N5H0qM0
MD5:	6143FC132462E60949837DAAEE6F248D
SHA1:	FDC004D9743D008B14EF2D4F9A48256F82504479
SHA-256:	921B2058C99152F7DFA6ED68EC73CF56B581D43A719E0918C997FCAD0FCDE7F8
SHA-512:	0D03284EC167777A489BC25337F4535789A93F0947573A83FD05BA980BA922C8ED14E92233DBA674A4E80B2AAA10254B9C65073FE20BE5424B3F3E843CB4695C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.sabro.net/favicon.png
Preview:	.PNG.....IHDR... ... .szz....=IDATXG..{PT...w...A.....f....j*.h.1.-X.j0.#.....Q...".....X...HA.#(".FCty.DVa.uw.=.s[.6ct....;{.....;...Fttt...Wi4.....j.}....#Gb..8t.....?5.m....b4.....(.X..@dd$..t...D~~>.Y3...o.@.V..V..\...].....$%%.....m.....Z...>|X.sA.....3..'x..[.B.....l....6..e. n.$&&..OC*.b.....3.l.2444`..hoo'._...../ZZZ....)(--.H$.-[0v.XL.<.z .S.NEbb"....h4.s.....3SSS..l6455...:..'54Xrr29v...b16o./F!V.Z..s."...j.....-....*.bBXX..+W.eff..r.9.};jkk...Y.fY5...B!6n...#22.+V...Ky..g#//....I.8..D..{.0!!...2e..!p:.....0.2"". .&4.....D"A[[.. U&55..... &..~x..J.*MOOOY.h.....A__...jkk.T*Q\\.+.q..)....*F.....WJTT.....O..)%%.J.....L&.!.b..\..'q..a...p..SC.,.....b. 66.....4..KK.....|.2..=...B^..7n.....<@?h ?..d.....T.:..o.....~.....=.I.M.....P>....F.....y....r).....+ T..<...."...&..tA.....~)@TT.W\\.P..A%..~.../_..Y. .H!..8...!...w.....1...v...#.t>.....;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\flags_0[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 150 x 129, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	9132
Entropy (8bit):	7.960001488754323
Encrypted:	false
SSDEEP:	96:fUtmnta3kNzGsTGmpAOYCcXm2D6p4qCZUBU2ERju3Zl3qrpnMSllQFfr+/hQ6Guo:5lG7mpbc2U6K8ARjkjEGSlKNrqDFC0G
MD5:	3976F189072CD4A0983E72A6679EFE4A
SHA1:	839B4A8741F51511C243C4EFB1A887D025BEA9DC
SHA-256:	75AC1C0FDBD972F75361FF2E851C17F1B0A75CA31DD290DA0ABAEE9694C1188C
SHA-512:	064B93E1A3A036D1B5567DEBD33D6EFD2910B0E4521B6B641CDF0882EDB83EE0D6CB14802CE018734A1997C9C39419295D59B3D35BEBA3940E0AA78E4120AAC
Malicious:	false
Reputation:	low
IE Cache URL:	http://s11.flagcounter.com/count/tsG8/bg_FFFFFF/txt_000000/border_CCCCCC/columns_2/maxflags_12/viewers_0/labels_0/pageviews_0/flags_0/
Preview:	.PNG.....IHDR.....tRNS.....#&E.. .IDATx..}.P\...g....9..6.aC.d..!&3..;.h..m.oFQ....H5.6.b'v.oF..k2^.R.....csS.....F.....(..B`....<.gw.....{vCHX....9.....<.9...>.j.....uX. |..y....-[.~...~..\3....vA.....o...z.....n.....y.3.....T...t.L_|.J.R.T.?...c..v{KKKww.UK..<>>~.....@h.'.=.PEEEOO...;.CJ....2p....d2.....Z....k.....O~r......./.d.....V.^..h4z...(..... .....8E...g.5.L&....W_1...W..x<.....j...===.v.....8.%%%??..}D.....7n...,..+...k.....iii%%%....3.r.{.9A.JJJ.....f..._z.%.r.f3K...d)---.%..L&?.H_.<.t.....N..SBBBss.....<.#.e .U.~3@A.f.....J.....`....O.R..;w.....;..:tH1.#G..{.'..(.,..>.._z....7.|322.....a.eee.|..U.~3@A.....nc.....Q.....~...+WX..._}.U..&/./..G../t8.La...R.m.X...J^..;.....F.y..[..<y.....#n...C.=... @||...>.@...{.##.?....bfEtuuMLL.`.0Cnn..By.].v.....b.n...cuuu.L&.....^{.o....w.....\..4.@...&..F~....7....(.0;;.....?q...WA...{.?....fv.....C.+&###&&.@KK..x..iv

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\googlelogo_color_42x16dp[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 42 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	910
Entropy (8bit):	7.7455040862049085
Encrypted:	false
SSDEEP:	24:do/cXeTrHaRodw+UWNhsGzRSIhAugV7unmH4ifkx08v5:K/cXeqadLUWNhNzRSMXgV7unbisx08B
MD5:	EFA6BB2BFE459BC6F4BDAFA3DB0383F6
SHA1:	52D15CE52FE50643E542C17812DE43F4ED1B6EE0
SHA-256:	6318394F737C66F0E2CCFCD88E3935C6667633A1B95FA29FBA2B75431D55EEF2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\googlelogo_color_42x16dp[1].png	
SHA-512:	E23C04D8997F5C2F92070E09261B7EE50D9DF8753F45CF66F604F0874FFA8D99E947C97C528EC02A2C3FBE8E43D840B343A7D0225532980D5DA95031216415B7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/images/branding/googlelogo/1x/googlelogo_color_42x16dp.png
Preview:	.PNG.....IHDR...*.....`'"....UIDATx..T...=.Mm.....&[....Sl..m.m....U....;.uf..frrr...v...U)...).....2Q..`.y.*...U.9..;..0.^.....B.....].h.^..... . L3....jQw..vB.D....<..P.4..|.B....d..?... ..Qv.....Dv..$...._|.*.@.....k....`..JG...$..T.y|T.....v.iH...yc6'...%..&.w.oI.ZS{..!6A@.Y.....a....U]..:....g-.....01F.....Q...k#..G\....~.+....z.>....F...}1[..~.9..r[.?..9.....2~....e."1.).} [.WW.{.r...|D..<7..t.M.`..S...8.ab..F ....n..S.:n.>1(g.p$.:k1..6...Y..@.5.8.0y.....R...;.K\. 0p...g.,r.E.....=.....!.^..Y!..D.Z.....aV.....;F.4...I.`^.L.VQ.....&...d....O.\...I).!1....{... ...K.f*.e ....L.....~.%IY(..Y.....NeA...?.^..2.C..^.....P....)T.&?.zm.Sl.b..I.D...%.{.B>X{.9Y..M..:).....EK..b.....}....|.o..]....GH?..3F.B(.:.....AdA.....Z... .L....)..@?...f.F....6..... u..oQfMC.....OC.1[3..j..j.G...&..D`.....@>...g....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\jquery.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	85578
Entropy (8bit):	5.366055229017455
Encrypted:	false
SSDEEP:	1536:EYE1JVoiB9JqZdXXe2pD3PgoIiulrUndZ6a4tfOR7WpfWBZ2BJda4w9W3qG9a986:v4J+OlfOhWppCW6G9a98Hr2
MD5:	2F6B11A7E914718E0290410E85366FE9
SHA1:	69BB69E25CA7D5EF0935317584E6153F3FD9A88C
SHA-256:	05B85D96F41FFF14D8F608DAD03AB71E2C1017C2DA0914D7C59291BAD7A54F8E
SHA-512:	0D40BCCAA59FEDECF7243D63B33C42592541D0330FEFC78EC81A4C6B9689922D5B211011CA4BE23AE22621CCE4C658F52A1552C92D7AC3615241EB640F8514B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js
Preview:	/*! jQuery v2.2.4 | (c) jQuery Foundation | jquery.org/license */.!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document? b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a 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="2.2.4",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uF EFF\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:func tion(){return e.call(this)},get:function(a){return null!=a?0>a?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,function(b,c){return a.call

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\lng_en[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 107 x 43, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	6595
Entropy (8bit):	7.9632855712117845
Encrypted:	false
SSDEEP:	96:00jPPkWwTXHNwAyWIlAQn9qUFGgq9wv3zEszYsEfIMrv8TebABpa0kmraVXOWOih:jaglAARgs8tIMY+VOWOih
MD5:	243AE66B0AB0DA84F6FF3230AA58C2CB
SHA1:	78B0A7CF120E5A996989D0CA18E7ADD0BE1D7922
SHA-256:	4F1FA8ED1AD7F48FE346D3C92A87D5E11E0D9F74E2CFBEE57B26C6F3E701912E
SHA-512:	548F5C02747F7CDDF52EEF9169F7D41C75E83B374AF280CDD00E4D98E53552024BD9604C22C3C0F6644BFDEAD0D9E65CD682CC26AEA95FE481FA8E8504A8F13
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.sabro.net/lng_en.png
Preview:	.PNG.....IHDR...k...+.....v`....IDATx..\.tUU.~I....tf..B"-=/.S..GA...@. $$.BL!.G...!..A...Q@..@H.!$.#HK...GgYFJ...}.}....,k..X.:.[.....N.....OS]...y.X..Z,]..Ks.@dT"F.&bTh <.".0sN6".....m..U..x..X..(.n<.E...)8b..gP...<d...._..U.?.U...P5....R.....u,.0..-@xh.....qQ.8w..aSr.]?...C..?..U..I.;x.i$....NO...e.\.a.....y$Hx&.X..I..L4..+.../..}..[t...%..+.....s. .C..#."5e&.....^.....~.....^!....;.X..N.....XLs.....D.4.....4j...6]A.....&..).V....J.u.,X.....w..K..z.]<.)r.,A..Y..6.]..@.....#:n).}.....1....._.....P8x.Af..q.....Wo\Gm....A.b..... ..o.1.....c...F.R.6.~....._...I.7>.eI;\|.#....?....2.BO....K?...E....^aD.h,[.....k8x....Xn.ee,.%.....E...{?..z...&..=.....k.....A.}..c...$..,T.k..I...z.....p.}".8`2..".6s-\.....$....W...X..n....2.^ .Qp.....7.....%[.B.%..B..\..o....'.....:P.....-Y.....R...4.....A..q..G..7`..(<Q.{.qd%!Q+V..?....-.;..G.....R..X..4._|.....r....6.G.."....H{.v(.`....cNp.{..|...Y.&X.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\logomini[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 238x50, frames 3
Category:	downloaded
Size (bytes):	8337
Entropy (8bit):	7.91522190821328
Encrypted:	false
SSDEEP:	192:U5OHUPUvPu+xutCE9vvpQ0o+7QqSuOG1dH5j0mUyZaM:DyeuZCE9J1h0yOGzH9cyZaM
MD5:	FA2F1E847EFCDE3A68C92C6C67E68B99
SHA1:	D0D87F7D37D1073BCB85DC6DFED68164254920AE
SHA-256:	9E0EEDF07584A1BE6957AD39EA79D7FAD34B2D8357A1541348CF98E862362EC6

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\logomini[1].jpg	
SHA-512:	D3F5062A9E1FBC1A17C37B9B36A85321E224CFDCB85C8F3EA478E9F4293E8B3D36C19994B790E2F9A0BE3BCDCDE11D7146E4B3B775B39C94B0575B5E7A9953F1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.sabro.net/logomini.jpg
Preview:	......JFIF.....C.....C.....2.....<.....!.1...A.. "Qaq...2...#B...$br.....3.....!.1."a.#AQq.2.....&B.....?.....L.....{.....9..y.<.....m...0..=._R.-.....Z.'2$.u..c..^uNG..o..6u.....Fo.^,..rD.. @ oo..?o...>..C..@TP.....o.....q.@}.....:.....:.....:.....:.....:.....8...q..>}.....ZU..d.I...7.z.&..H.@..S.R....P8....G#.....\m...i..A.39.*[{..>La.....c.bH...B.z....8.... .P.y.vw..=.uU..+=..N.?w....X....w...3..y!.m.;..4g._....s. ...a..(.. .g!TO.....C.y....y....%.....B...L>.@.....#..!.x..i7.....h.._H..8...%.<...7.@D<.....z.r.....ZKm$.....{l...>.....G."^? W<....!....z'...Oi......_.....x.Dx/....T.z.T."....`....!..!.....>.9....e..i.....OpU.@:.....:.....:.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\oBtBCMa[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 12, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	393
Entropy (8bit):	7.185956152171576
Encrypted:	false
SSDEEP:	12:6v/7W/6uBXvOo9j8aZ8gT6DUsgZha/teLvm8BeqN:iG/OC8Es4Bhwyvm8Bes
MD5:	86772E897A891CFC83B05856A358C303
SHA1:	DF7E59691057E91D8D00194B9AD5329863ABA16B
SHA-256:	1DB82561CAAEE375614049456BBCCFA6E005808ABD0B1456D2BFDAD04A9DBD89
SHA-512:	F61F9A9134E2E1449012F33C8696BCF07C40C11E4DBADD3FAD392A764D644D06CF6B8617439231C9FA0E5F2C88266627EEDA44E3C23B08B45F9B463760D4E38
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://i.imgur.com/oBtBCMa.png
Preview:	.PNG.....IHDR.....k.=.....sRGB.....gAMA.....a....3IDAT8O...K.@.....T."....{...GQ*D,T.Jk.M.I.IR+...'...X.~.....P(Rn.....|...>.8...B..f.2l....BG.\..=.....I..5..9$ .Qtyu.G..%?.~..B.....bi%G.....G.."....*.pW6.9k%?EW,,nP..4.....$.<>.>6t.>."=.L-...n.S/y....s.u..g.]1.....2.@*..7+.....|.%t..d.^..]~....B.....O.Q..t}.'.E.].....s@...o.!.K.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\portal-v2[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	2106
Entropy (8bit):	5.172740393508721
Encrypted:	false
SSDEEP:	48:F7CpDuMY6wRQAQl07kFUZ3Hwx1RnKKHP2NsTr4sDE9oNeCVb:F7snIQ5LRKKHPusAGcC9
MD5:	411E427F4CDD3BE20C16AE94D6EFB2C6
SHA1:	2B5131D31CC7D8B0B14B24670E7C99120D7C37AF
SHA-256:	AC84513C4C5EA7E4458E91C46E33BA71B56E19FABF93CC079FFCB01A975C2E3D
SHA-512:	94516FF9BD5DA56D23B610894D7A96818F535ADA063A200CE26D100C4B8843D48FEC25F66D6DF8B0F5D273F5ECDB6842DBDC199576BB0980994ADC87A0C55D4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.sharethis.mgr.consensu.org/portal-v2.html
Preview:	<html>. <head>. <script></script>. </head>. <body>. <script type="text/javascript">. !function(e){var t={};function n(o){if(t[o])return t[o].exports;var r=t[o]={i:o,l:!1,exports:{}};return e[o].call(r.exports,r,r.exports,n),r.l=!0,r.exports}n.m=e,n.c=t,n.d=function(e,t,o){n.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:o})},n.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&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 o=Object.create(null);if(n.r(o),Object.defineProperty(o,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var r in e)n.d(o,r,function(t){return e[t]}.bind(null,r));return o},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="/"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\s[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	143
Entropy (8bit):	5.079318363208902
Encrypted:	false
SSDEEP:	3:Ply9JL/ZSGKHjJMzVJu+1vK3VYrSLIzECAXhxMAFjWAEtv0Gb:TJL/sGeMRJVSOGLIoDXhxVFjWAEd0Gb
MD5:	E4E31B474D3E0B577B3C8856E91F8659
SHA1:	A81311F7FCFA9B6B23A24D4E5C976D5F75B1B9B7
SHA-256:	18088C10E79C926292732AF98A0CE470E90F3FBCBA4BB4896AB3310C2D94E421
SHA-512:	A07961EB39C4CD4E39EE19E2C675E64E5BA5367DAA18E2F76A23772ABD62F46B002E6BE8FB0F35A70616941178FACC8DF579C4A68E5811B74313C12806AAFAE3
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\s[1].htm	
Reputation:	low
Preview:	<!DOCTYPE HTML PUBLIC>.<html>. <head>. <meta http-equiv="refresh" content="0;url=https://www.google.com/pagead/drt/ui" />. </head>.</html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\s[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	143
Entropy (8bit):	5.079318363208902
Encrypted:	false
SSDEEP:	3:PIy9JL/ZSGKHjJMzVJu+1vK3VYrSLIzECAXhxMAFjWAEtv0Gb:TJL/sGeMRJVSOGLIoDXhxVFjWAEd0Gb
MD5:	E4E31B474D3E0B577B3C8856E91F8659
SHA1:	A81311F7FCFA9B6B23A24D4E5C976D5F75B1B9B7
SHA-256:	18088C10E79C926292732AF98A0CE470E90F3FBCBA4BB4896AB3310C2D94E421
SHA-512:	A07961EB39C4CD4E39EE19E2C675E64E5BA5367DAA18E2F76A23772ABD62F46B002E6BE8FB0F35A70616941178FACC8DF579C4A68E5811B74313C12806AAFAE3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/drt/s?v=r20120211
Preview:	<!DOCTYPE HTML PUBLIC>.<html>. <head>. <meta http-equiv="refresh" content="0;url=https://www.google.com/pagead/drt/ui" />. </head>.</html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\sabro-diseno-de-paginas-web-guatemala[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 240 x 180, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	3855
Entropy (8bit):	7.833382088287725
Encrypted:	false
SSDEEP:	96:EGp9/d6FIxjUMQS5D6h4XvGO9WVkiPuwSQI3gv04V2:T9/d6FIZRn6SeMIPuwWws7
MD5:	9F11201E821850B0C669C29DBDB81775
SHA1:	DF49196073E167FE66AAF07383A61178BC594E5D
SHA-256:	1C2D56A5365FB8EF709EC39E82D22DB24819CAB74D9DCDF8AD783E36879740A9
SHA-512:	AC1442B1CF7CF3BC7F2AA06BF7DB6F0F2AE190CC22EBBF3CA8B02EF02162CA11F532791B7AE433AD5496C03912862E1557DDE4FE53F53F5A7DDD3ABEF031E25
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.sabro.net/sabro-diseno-de-paginas-web-guatemala.png
Preview:	.PNG.....IHDR.....IDATx....s....p....A.....*....3U....h....`..(.".`..r.j...!..%.h8....s.....f..=.=...dE..1...>....wF.^..~.<...w.a.is.....l`.a..a..a..f.....l`.l`.a..a.....f.Pk..L@z.p..8l.....:...D.....).?E.u._...(...v...o.!`&..P....M~...E....."`S..GA~.....?..f.=....GT...k..h..G.,#`r.s"`..8.@...d.F...5..C.4....r.M.....\...p.*..b.].L.}.L..<=.[.;..Er...o_. k...M.14E....S,...[..<.Ge..4.n..`iq|...+J.3..od..k>..p.^.c.PwY..RX/!...#....?...rZ...q.!`.D...2..#.Z.t../..bJ-.....L?.....8.....z..U.+=..~.9.&.pF....9].WW*...n.g....='.|.-..'.y....;:.8{....+.T..+..K..gl.:..R.J...s!..]f;.G3...<....{t....G.Z.....s.....X.....&`.....Y.&`.%`.f.....%`....G....7.....o./.=6.....B..q.c+.X6.S.\.....&.M...."."..&`VZ.sO..."#`.f%...W.$...r=...,`.8..jb{...fc.....&`Vs.?y....ezbuu...O....&.j.....e.....^b.....~a..wxUkwq.x..u..,CG...H.X4.....".."`.f..,.q5..0#-`..N.....6GoCA....I.Z....E...,^.....s+.H.l..S9]...ah.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\sabro-portafolio-apps[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 240 x 180, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	7107
Entropy (8bit):	7.906727176645508
Encrypted:	false
SSDEEP:	192:aMddkc3L8bdzV/j2KZMMYizSnUYCFegD82rFBIa5:jdeqmj2K61SSnCegD8+Fma5
MD5:	A4E82319553ECBA8CCA671B8BF83D2A0
SHA1:	B4260394507E6599EC5CE206901273151CAAA3E7
SHA-256:	D40D73A75B5DE0685BE8D41EE1513B58A0D6300558356AF48D1ED0DF0222141F
SHA-512:	4CB54E5F99498BF1A7FCC369822665DE090F089CD755C3841655479D4F4CDE7099CD57A0381D8AFF60F6B4F07FDB847B73D728EE7E1604EE18ED4A2F926D0AA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.sabro.net/sabro-portafolio-apps.png
Preview:	.PNG.....IHDR.....IDATx....\M...pk%..Kd..3.1...Q.,...2.Yg..2.clc..1..X....#.J..J..JQ2.>..}...SJ...}../u;.{=...y.9.yN)ppp.l..&..`.....sp0`.....988.0.....`.....spp0`.....98.0.....x..5RRS..$Ym...'.OJBl|<.GF .N....I..#.n(".".$....yn...#6..a.a..U...!..z/.Q..x..(^_...qJ.^.x...#^.z....R.kF.=J.`.I.....7..'.O..5...Q...zn..E..^.^+^.j...q.>{.QE.....!..D..K.>K.EL.=.....~..N...O.....F..bKCL..[..3@.....O.....2'il{>...1`..q.4.....;.....mE_.c.....d.....+..Q.Y.....K..w...,?.Cn....3.b?.%7....G...AI_...5.`..f.%2.#".....FTL....##...:'.Vq..P.1...H.B...~F.a...`...O..x.8....E..G!1"4K.G.3.7.J.....c~.~...{...~(.\.Q..!.dN.....~..~.W...-..}#.w.,.X.%.....~nvI.jZ..W.I..1...:...?.M....g..k...wC.p.2/.....=...M..8]....='...M.%....K_.T..G.0.."}c1`.\...\<..3`.....d....3`...0.....|o....u..P.t.,Y.Z5..kw.....-.....L.2h.....X.....Q..Q#....~.:::.....QRF.?8.c.....v..!e%==...`.....v3g.F`p..VU..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\sabro-portafolio-websites[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 240 x 180, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	10394
Entropy (8bit):	7.94213158570221
Encrypted:	false
SSDEEP:	192:ZUr8EJANnHfeyg0HVBEqOpLsJR9xn7i6V9oqvgS00lJggBTaQSHtPphTw:BE2Nn/eynXPO5q9xe7S3lJvTaQgtPzw
MD5:	9B53C0FFFD84F449A67B4E4802B76A4D
SHA1:	86EF70C26FF24F2855629DB2D8C5AAACFABF7617
SHA-256:	958C167603A5C20EC1FCE102D2BF8E222B543637E170805E687D87E713428512
SHA-512:	575DB54C00AA43C5EC157C9D3894EE1E1C371ACB8C0FF7D3D13BC16B2D90884E2DD3C28DE30CBFE6237E032EF33C35C8EDB4FA5E3F2DB60EDAB47BBB392C137C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.sabro.net/sabro-portafolio-websites.png
Preview:	.PNG.....IHDR.....(aIDATx..w.W.....z...I...$L.s...^.4.:.4.....t&F.....fj...B..cfB..4.$...n.....`....y.$...>.$.A...-.{....T.....[..?.....`666.....fcc.....`666.....fcc.....`666.....fcc.....`666.....fccc.Cm.n.B.....oe.;`..7.P.V.....,i.*.+..`..---...&..zT.V.F....7.....F.Un.?.....f../....f...|`.`..X.....\...j....t....zBbY.....2. .Xb.{.....2..V.jU*\.^...+%PQ.v{.A!..y.gb....u.u.u.D....c.{...b..!.e...@..Qu.....3.u;./.....O....`.....:Ay..&.....g.....2..p.B\..v*..j.k...".w5.5.....;..e...>?.....Rv.njf....J.v...f..R.*u'@..:-4:M.y.ju ..g1....@.P.....J.q.y.;.0.....h...1k..&. ...N2ij.`_..i.v.....4..6.....)....=.....S.;.Lf*.@..}...e(.D..8.Q\']8.3.aq8.t.).X.]p.i.p.h.)=....cYH.@e..,.....w..i.v%.lW.8.....+.p2.._....L..L.J.W..X..mc..]AcL.?.EL..K ....rj,..NBA...e.x._..Igv.....\.E|.d.f&nE.....%r...3.7...6....N.3.k..X,{..E._lGlOlWl?..'....''...\.....^D,..1.{mcQ.f....pW..Y....n.,..e;e..JJ.....~.-.7..)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\top1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 1366x500, frames 3
Category:	downloaded
Size (bytes):	420419
Entropy (8bit):	7.983264892723544
Encrypted:	false
SSDEEP:	6144:968o9D7nb+uNgwTTSqVxpDZBJ5asa53srmendRsXGwx1ukZMoJCLk2Ox9wzXVKus:9foVng2zDBJ5NQensXdx1ukZ0g2GalnK
MD5:	2582FC487CC7B3FA9C52F9CA9CFF2CCB
SHA1:	B7447DE100AF53BC4E67D7603909BC288B0F8596
SHA-256:	9CE408F46573A7AD238689C57446C01BF4DDA3BA94D52837B87757184540610D
SHA-512:	5609E9BCC9F2D10A7C5D8CD07CD46C6B7C58C0314E250DE277B69F1446A2284BB2329D2CD9ABE7E10CA420E77BAB5004141B88A971110DF404BBE80E150FD4A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.sabro.net/top1.jpg
Preview:	.....JFIF.....C.....C.....V.....'.....!1..A..Qa.."q.....#2.BR....$b.....%&345CSTVr...'(678DEFGUW.....Xcevw.....9Hdfgstu...)Y....h...Ix.....{.....!1..AQ..aq.."....2.R...#%&BUb..$345678TVrv.....CFWu.....'DEGdet...s.....()Scfw....X.g.....?.....X.../..||..?..._o..T-J..t.....u}._5C.wW..6....|..d...._o..7...X*.....).y..8*.....)..'"..Xo.M.:...%Z.Oq.8"u....U$.jw.O.....>6.&w.__.*..o.....L.I@.[.....N.Q....E.....{.~..*...rA..?...T..-....X..pD..x...Ukk.?7....\.. .....&..H..R../t...N.^{`..!:^.z}..`.....}pD...pA.....[k.....=.....o....uP...[. ...M..I...m.#.r.V.....?.....GM..).....F.6..N.6.*m.o.....k....<..`.....~....y.r.t.....=.....(t.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\5cdcc6fcdc07bd0012082264[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):	961
Entropy (8bit):	4.828983694144011
Encrypted:	false
SSDEEP:	12:qcLFvWB/SZJHRQmjPnZKMtiVmD0oEuZhCUoHYUOxlM0M7ROHi0kc+28Wbs:qcdWBSZJxhFkmD0fHlH0goy28cs
MD5:	E6EE5C366EA07E79EB6B4BDA3AD7EF3E
SHA1:	FE5F31FAFA664D5AD5CCB9C724329555458CBE15
SHA-256:	932C5D89241C7D9539F4AD859FDB99375389D24193F5DE35BCFAB85B05B0061E
SHA-512:	C7E40708E6074E48F382A9C3A4C9F332A497DE436C7F3F75592126D02B4D272FCAF824BE405A2813570E339CD5897A565685503AD5AE318A800726E0ADDF13EE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://buttons-config.sharethis.com/js/5cdcc6fcdc07bd0012082264.js
Preview:	window.__sharethis__.init({"ts":1591127116115,"gdpr-compliance-tool":{"enabled":false,"ts":1591127115710,"updated_at":1591127115710},"gdpr-compliance-tool-v2":{"enabled":true,"ts":1591127114407,"updated_at":1591127114407},"inline-share-buttons":{"enabled":false,"alignment":"center","color":"social","font_size":12,"has_spacing":true,"labels":"cta","langauge":"en","min_count":10,"networks":["facebook","twitter","pinterest","email","sms","sharethis"],"num_networks":6,"padding":10,"radius":4,"show_total":true,"size":32,"size_label":"small","spacing":8,"use_native_counts":true,"ts":1558346452003,"updated_at":1558346452003},"sticky-share-buttons":{"alignment":"right","enabled":true,"labels":"cta","min_count":"10","radius":"4px","mobile_breakpoint":"1024","top":"160px","show_mobile":true,"show_total":false,"show_desktop":true,"show_mobile_buttons":true,"use_native_counts":false,"spacing":0,"language":"en","ts":1557972733004,"updated_at":1557972733004}});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\OqOE21UvWe3[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit gray+alpha, non-interlaced
Category:	downloaded
Size (bytes):	400
Entropy (8bit):	6.584211645324161
Encrypted:	false
SSDEEP:	12:6v/7P+UhU2RGLJ31m9q/NPkIzS+TmxEMXr:+6UGN3gkNxzjiEMb
MD5:	B85D112F813E876DC294B4263CE4D333
SHA1:	CA55B0C604D89034EE0249024983F7570EA2F8BB
SHA-256:	ED91FBB0CD9308F91F8E1FD93942C94EE850FC4161ED788B16F801B743C70B9B
SHA-512:	07DF881DC463F96F412DB4DBB8DB94BE66492C1E130AC2997D9ECA21DAFC23944A962A44F893F96895550EB10691F627579501E17A853A3C8A8C3861656E9506
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.facebook.com/rsrc.php/v3/y5/r/OqOE21UvWe3.png
Preview:	.PNG.....IHDR.....7.....gAMA.....a.... cHRM..z&.....u0..`..:....p..Q<....bKGD.....tIME..... .`.....IDAT(....B1.D/H.ttT....L.....h...%.AH_.<.....n.M..Y...Z_+.4.4.....3.....[J\h,C.....M..exA$.p..H....gm.f...=...$).u.zd..D4T..tx.....%tEXtdate:create.2019-02-26T15:32:06-08:00J..L...%tEXtdate:modify.2019-02-26T15:32:06-08:00;\@.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\activeview[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	126
Entropy (8bit):	2.9881439641616536
Encrypted:	false
SSDEEP:	3:CUXPQE/xlEqjdfXPQE/xlEqjdfXPQE/xlEy:1QEoqh3QEoqh3QEoy
MD5:	7EDD19F8419144CEA07BFBE8887B944E
SHA1:	49D47C4F9EAFC111ED241D743F09D73C3A12F5C4
SHA-256:	605627E07A397426E1FDB473A8B69F252EB192CC953C266199DE9E5E63629F68
SHA-512:	19034777E93BFAAF0A80256EDFAED658D544E8EF9139C24C7FBBDE8CEAA9FFA5319558D33897DC692233784C147CAE7A9A5D80335A9206407ED0F15077BCE95A
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D.;GIF89a.....!.....,.....D.;GIF89a.....!.....,.....D.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\ads[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	63185
Entropy (8bit):	6.132406834988483
Encrypted:	false
SSDEEP:	1536:Jxc3z9+JGVVNVCRxLzNNNA+KiVn+aWLQhWDRpmM:JxcD9GV+aWFd0M
MD5:	45D0848C1E16D85F9F2312A0389F3C00
SHA1:	D688588BAF00015AD2F71A367AE08833A2E67CBD
SHA-256:	071BF5EA76B2CF23C9D816B3B7F12A4F2B5748883E5FDAD44810994047B3873B
SHA-512:	3C2C3E8257BEFF1E92883F596235EA7D574572D1F7D6019BED7DF9522980F08DB6D4550759027B1BB265DF6611B4441A1B704C555EC4EFBCE7804BDF234890C1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-6373591680915711&output=html&h=250&slotname=9454352660&adk=1294191884&adf=615884932&pi=t.ma~as.9454352660&w=250&lmt=1614899672&url=http%3A%2F%2Fwww.htmlprotection.kom.gt%2F&flash=29.0.0&wgl=1&dt=1614899671426&bpp=61&bdt=504&idt=423&shv=r20210303&cbv=r20190131&ptt=5&saldr=sa&abxe=1&correlator=4400435368515&frm=20&pv=2&ga_vid=2003745227.1614899672&ga_sid=1614899672&ga_hid=1318567104&ga_fc=0&u_tz=60&u_his=2&u_java=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_nplug=1&u_nmime=2&adx=676&ady=75&biw=1263&bih=906&scr_x=0&scr_y=0&eid=21066432%2C21066922%2C21068108%2C21069711&oid=3&pvsid=4089538964379651&pem=792&rx=0&eae=0&fc=640&docm=11&brdim=0%2C78%2C-8%2C-8%2C1280%2C%2C1296%2C1000%2C1280%2C906&vis=1&rsz=d%7C%7Ce%7C&abl=CS&pfx=0&fu=8192&bc=1&ifi=1&uci=a!1&xpc=wGHJNxAEDu&p=http%3A//www.htmlprotection.kom.gt&dtd=627
Preview:	<!doctype html><html><head><script>var jscVersion = 'r20210303';</script><script>var google_casm=[];</script><style>a { color: #000000 }.img_ad:hover {-webkit-filter: brightness(120%)}</style><script></script><script>window.dicnf = {};</script><script data-jc="41" data-jc-version="r20210303" data-jc-flags="["x%278446'9efotmy"]">(function(){/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0 */ function b(){var a;return a=void 0===a?window:a};b().viewReq=[];b().vu=function(a){var c=new Image;c.src=a.replace("&","&");b().viewReq.push(c)};}).call(this);</script><script data-jc="55" data-jc-version="r20210303">(function(){/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0 */ var g="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a};function h(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&w

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\bootstrap.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\bootstrap.min[1].css	
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	144877
Entropy (8bit):	5.049937202697915
Encrypted:	false
SSDEEP:	1536:GcoqwrUPyDHU7c7TcDEBi82NcuSELL4d/+oENM6HN26Q:VoPgPard2oENM6HN26Q
MD5:	450FC463B8B1A349DF717056FBB3E078
SHA1:	895125A4522A3B10EE7ADA06EE6503587CBF95C5
SHA-256:	2C0F3DCFE93D7E380C290FE4AB838ED8CADFF1596D62697F5444BE460D1F876D
SHA-512:	93BF1ED5F6D8B34F53413A86EFD4A925D578C97ABC757EA871F3F46F340745E4126C48219D2E8040713605B64A9ECF7AD986AA8102F5EA5ECF9228801D962F5D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css
Preview:	/*!. * Bootstrap v4.0.0 (https://getbootstrap.com). * Copyright 2011-2018 The Bootstrap Authors. * Copyright 2011-2018 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */:root{--blue:#007bff;--indigo:#6610f2;--purple:#6f42c1;--pink:#e83e8c;--red:#dc3545;--orange:#fd7e14;--yellow:#ffc107;--green:#28a745;--teal:#20c997;--cyan:#17a2b8;--white:#fff;--gray:#6c757d;--gray-dark:#343a40;--primary:#007bff;--secondary:#6c757d;--success:#28a745;--info:#17a2b8;--warning:#ffc107;--danger:#dc3545;--light:#f8f9fa;--dark:#343a40;--breakpoint-xs:0;--breakpoint-sm:576px;--breakpoint-md:768px;--breakpoint-lg:992px;--breakpoint-xl:1200px;--font-family-sans-serif:-apple-system,BlinkMacSystemFont,"Segoe UI",Roboto,"Helvetica Neue",Arial,sans-serif,"Apple Color Emoji","Segoe UI Emoji","Segoe UI Symbol";--font-family-monospace:SFMono-Regular,Menlo,Monaco,Consolas,"Liberation Mono","Courier New",monospace}*,::after,::before{box-sizing:border-box}html{font-family:sans

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\c[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.322445490340781
Encrypted:	false
SSDEEP:	3:CUdSkL1pse:XSk/se
MD5:	6D22E4F2D2057C6E8D6FAB098E76E80F
SHA1:	B80B11203D97FE01C5597CA3BE70406EA48F5709
SHA-256:	AFE0DCFCA292A0FAE8BCE08A48C14D3E59C9D82C6052AB6D48A22ECC6C48F277
SHA-512:	95DD0E4944B1541A9BE48A60A1A105FCFA0D69DD215ABAA9C1771ADECC5EE0C0FE91D0EB367B6D46A4F8B2E06E6FB962D56DFC1C53F1F62CC8B314710628CB1E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://rf.revolvermaps.com/js/c.php?i=5jvn1rlqz5o
Preview:	GIF89a.....!.....,.....L..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\counter[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):	39159
Entropy (8bit):	5.450542019923853
Encrypted:	false
SSDEEP:	768:dhstO8lVCA45/zUVdlcb6ddbt8utYKmypUX8f/5DB1YSMv13ROXqWiQRKt33JDYE:t8HdjljYZDYXFXUHDlf
MD5:	4DA07DBD600A063A57AEAD6EFF67D2C8
SHA1:	F47EF75ED972F3CFF7742D07D3AFACC47BABB8A7
SHA-256:	C5086D4F97BC3EE70971C51E89FA6AE25FF054ACCEC7C4E890B1083EE7BCC9AB
SHA-512:	4E77F636AA87FD3AF056D1CBCB3FF112981E347D44BB4CD1BF6660CC216835503EAD6EC77A99041CEAC602F92E16136711B9D5CDACFE29AA3E3444853DD0B69
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.statcounter.com/counter/counter.js
Preview:	var _statcounter=function(_1){var _2=false;function is_admin_project(_3){return [12225189,11548023,11878871,12214659,981359,9560334,6709687,9879613,4124138,204609,10776808,11601825].indexOf(_3)!==-1}try{var _4;var _5=1;if(typeof _1!=="undefined"&&_1.record_pageview){_4=_1;_5=_4._get_script_num()+1}else{if(typeof _1==="undefined"){_4=function(){};_4._pending_tags={}}else{if(_1.start_recording){_4=_1;if(_1._pageview_tags_in){_1=_1._pageview_tags_in}}else{_4=function(){}}if(Object.prototype.toString.call(_1)==="[object Array]"){_4._pending_tags=_1}else{_4._pending_tags={}}}_4._session_increment_calculated={};_4._returning_values={};_4._security_codes={}}_4.push=function(_6){_4._pending_tags=[_6]};var _7=true;var _8=false;if(typeof performance!=="undefined"){try{_8=Math.round(performance.now())}catch(ex){_8=false}}var _9=false;if(document.currentScript&&document.currentScript.src&&document.currentScript.src.indexOf("statcounter.com")!==-1){_9=document.currentScript.src}var _a=-1;var _b="";

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\f[1].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\f[1].txt	
Category:	downloaded
Size (bytes):	3570
Entropy (8bit):	5.433747245733649
Encrypted:	false
SSDEEP:	96:pat/JchW7gzohyEdpziJJcCMLt4ybMnuxO:KWWRJMcCMLJMnAO
MD5:	90EBDC2C7CE40D88EF44C2429FFB0B2B
SHA1:	6C3065AD08F7F547943D16151E6FB77EC195A24F
SHA-256:	6F18EACF38D920481D5A45AB4B0A38F7011AB25EF4ED80272EBDC509B9D30B82
SHA-512:	AF709AFE2188906B052D5386CC1D1C69309BDF2E7DCB1F594AE9EFA04E2114673C9BE13FBF7A1FE17B39638EC5FB3F3416D46435A43D5D0FB12B51374D08E7E9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/pagead/js/r20210303/r20110914/client/window_focus.js
Preview:	(function(){/* . . Copyright The Closure Library Authors. . SPDX-License-Identifier: Apache-2.0 .*/ .var e="function"==typeof Object.create?Object.create:function(a){function b(){}b.prototype=a;return new b},g;if("function"==typeof Object.setPrototypeOf)g=Object.setPrototypeOf;else{var h;a:{var k={a:!0},l={};try{l.__proto__=k;h=l.a;break a}catch(a){}h=!1}g=h?function(a,b){a.__proto__=b;if(a.__proto__!==b)throw new TypeError(a+" is not extensible");return a}:null}var m=g; .function n(a,b){a.prototype=e(b.prototype);a.prototype.constructor=a;if(m)m(a,b);else for(var d in b)if("prototype"!=d)if(Object.defineProperties){var c=Object.getOwnPropertyDescriptor(b,d);c&&Object.defineProperty(a,d,c)}else a[d]=b[d];a.s=b.prototype};function p(a,b,d){a.addEventListener&&a.addEventListener(b,d,!1)};function q(a,b,d){if(Array.isArray(b))for(var c=0;c<b.length;c++)q(a,String(b[c]),d);else null!=b&&d.push(a+(""===b?"":"="+encodeURIComponent(String(b))))};function r(a,b){a.google_image_requests||(a.goo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\f[2].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	17802
Entropy (8bit):	5.501945784371487
Encrypted:	false
SSDEEP:	384:yERXqwTwsyiD72wZtOwKqJmlS9vhNa7i22:NRXqwTwziTKwm8vhNa7q
MD5:	0677886684B59CE870AEEAB9ECCDFB1E
SHA1:	7D541A6582FB8F382ECDD2C62505C3543A8684E3
SHA-256:	7CA55FBF08002A5A09DD1508BBD174F2C8C292D2CA430C7F9DD69E39AB9CCD84
SHA-512:	7ED166757AFC8BD24F7EBDE9757DCBD0E0070F30393743DA3819DF8FEADF2FB95039A42261258F05DAE2BB24CA79C458EB647FCFF129A1E63DB3B133F8FEA5CE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/pagead/js/r20210303/r20110914/client/qs_click_protection.js
Preview:	(function(){/* . . Copyright The Closure Library Authors. . SPDX-License-Identifier: Apache-2.0 .*/ .function ba(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}var ca="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a}; .function da(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");}var ea=da(this);function l(a,b){if(b)a:{var c=ea;a=a.split(".");for(var d=0;d<a.length-1;d++){var e=a[d];if(!(e in c))break a;c=c[e]}a=a[a.length-1];d=c[a];b=b(d);b!=d&&null!=b&&ca(c,a,{configurable:!0,writable:!0,value:b})}} .function p(a){var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];return b?b.call(a):{next:ba(a)}}function fa(a){if(!(a instanceof Arr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\facebook[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	301
Entropy (8bit):	5.031371107984661
Encrypted:	false
SSDEEP:	6:tI9mc4sliuImRzAyAYXV6ZqRITSFUeHN2cINgrYepshWLKoEV2Ws:t4IRMXV+Ds0cIN3Y3LKoF
MD5:	C6E9BE45643E197CE1DB1D7E24A99ADC
SHA1:	D7338E398BB0F7A9082D24F121140D2CF9E88859
SHA-256:	768D97EC0916217AE82C70AEDA3A61B9B0DAB344EDC4A3240A4F7CD94AF00307
SHA-512:	8033A55B544066ACEB01404F0102D7651E9D731EBC04A164A831FC32006F826F4169929DA42363D818B93CFA3A04B3568E26621B26B73D1CDF00FAAE23887345
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://platform-cdn.sharethis.com/img/facebook.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" fill="#fff" preserveAspectRatio="xMidYMid meet" height="1em" width="1em" viewBox="0 0 40 40">. <g>. <path d="m21.7 16.7h5v5h-5v11.6h-5v-11.6h-5v-5h5v-2.1c0-2 0.6-4.5 1.8-5.9 1.3-1.3 2.8-2 4.7-2h3.5v5h-3.5c-0.9 0-1.5 0.6-1.5 1.5v3.5z"></path>. </g>.</svg>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\favicon-8f211ea639[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 3 icons, 32x32, 32 bits/pixel, 24x24, 32 bits/pixel
Category:	downloaded
Size (bytes):	7886

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\favicon-8f211ea639[1].ico	
Entropy (8bit):	3.9210304844654047
Encrypted:	false
SSDEEP:	48:gUf/M1nRyuOaT8w8LnSqhIIIgItcSol4oFChIi4+pEaagyUchEhDVIisoZ51u:RnMvyyT8b1q+x4WCKiBpEaapFGTI8tu
MD5:	8F211EA639E8777ABEB1AB7A8871580C
SHA1:	D6427CE52782D6B07118817E71A7E5192CA72F8C
SHA-256:	E588BDE3EB80B349B069BCBB10520E49F9AA6F38001CE651F396269DE3499549
SHA-512:	A8CFFCB96C7265EDAD2333A2B1270382DDF7E3C364118662A4562D0E77C73E4CFC56B1655DE0438932BCCD36219B1340A9050EB8F6705D24999C9456963BD2A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://blobs.officehome.msocdn.com/images/content/images/favicon-8f211ea639.ico
Preview:	....6......... .... .h...f...(... ...@..... ....$.. ...@.'. ....0.. +..%...........&...;..;.@...9$..6".1...+...%...............;...;..;...;..;.`.;.. ....@(.;%..6"..1...+...%...............;...;..;...;...;...;...;..;.p..F,.0E+..@)..;%..6"..1...,...&... ....;...;..;...;...;..;...;...;...;.. ....F,..E+..@)..;%..6"..1...,...&... ....;...;..;...;...;..;...;...;...;..F,..E+..@)..;%..6"..1...,...&... ....;...;..;...;...;..;...;...;...;..........................

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\hbC1ovHPP4z[1].js</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>ASCII text, with very long lines</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>510483</td></tr>
<tr><td>Entropy (8bit):</td><td>5.408397522764541</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>6144:LuWbMPGwHPtjxiNg3rlLw/QExWydXb1hPGMZafF/f/x25c7vLYr:aWHcxiGUQExWyp4x7vLYr</td></tr>
<tr><td>MD5:</td><td>47647B65D539467568A549A336FE594D</td></tr>
<tr><td>SHA1:</td><td>6E70021ACB4F9CC3E1236F418069DECCE7DE032B</td></tr>
<tr><td>SHA-256:</td><td>67DD5F9B9466E13F8372F8B04DF5336DBA6C90EB842105982D8AC7E9754AD70C</td></tr>
<tr><td>SHA-512:</td><td>B53C6FD9FA74B8A964534BB7AD4134EDBAAC6B6CF94727F16AFCFAE12CE7FD025F65B9F7EB13D9C89AC4486A1914B371A08B29151E61E2848133C4FFD3E382
DD</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>Preview:</td><td>if (self.CavalryLogger) { CavalryLogger.start_js(["Z3urS"]); }..Array.from||(Array.from=function(a){if(a==null)throw new TypeError("Object is null or undefined");var b=arguments[1],c=arguments[2],d=this,e=Object(a),f=typeof Symbol==="function"?typeof Symbol==="function"?Symbol.iterator:"@@iterator":"@@iterator",g=typeof b==="function",h=typeof e[f]==="function",i=0,j,k;if(h){j=typeof d==="function"?new d():[];var l=e[f](),m;while(!(m=l.next()).done)k=m.value,g&&(k=b.call(c,k,i)),j[i]=k,i+=1;j.length=i;return j}var n=e.length;(isNaN(n)||n<0)&&(n=0);j=typeof d==="function"?new d(n):new Array(n);while(i<n)k=e[i],g&&(k=b.call(c,k,i)),j[i]=k,i+=1;j.length=i;return j});.Array.isArray||(Array.isArray=function(a){return Object.prototype.toString.call(a)=="[object Array]"});.(function(){var a=Object.prototype.toString,b=Object("a"),c=b[0]!="a";function d(a){a=+a;a!==a?a=0:a!==0&&a!==1/0&&a!==-(1/0)&&(a=(a>0||-1)*Math.floor(Math.abs(a)));return a}Array.prototype.map||(Array.prototype.map=functio</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\jquery-3.2.1.slim.min[1].js</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>ASCII text, with very long lines</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>69597</td></tr>
<tr><td>Entropy (8bit):</td><td>5.369216080582935</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:qNhEyjjTikEJO4edXXe9J578go6MWX2xkjVe4c4j2ll2Ac7pK3F71QDU8CuT:Exc2yjq4j2uYnQDU8CuT</td></tr>
<tr><td>MD5:</td><td>5F48FC77CAC90C4778FA24EC9C57F37D</td></tr>
<tr><td>SHA1:</td><td>9E89D1515BC4C371B86F4CB1002FD8E377C1829F</td></tr>
<tr><td>SHA-256:</td><td>9365920887B11B33A3DC4BA28A0F93951F200341263E3B9CEFD384798E4BE398</td></tr>
<tr><td>SHA-512:</td><td>CAB8C4AFA1D8E3A8B7856EE29AE92566D44CEEAD70C8D533F2C98A976D77D0E1D314719B5C6A473789D8C6B21EBB4B89A6B0EC2E1C9C618FB1437EBC77D3A
269</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://code.jquery.com/jquery-3.2.1.slim.min.js</td></tr>
<tr><td>Preview:</td><td>/*! jQuery v3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_evalUrl,-event/ajax,-effects,-effects/Tween,-effects/animatedSelector | (c) JS Foundation and other contributors | jquery.org/license */.!function(a,b){"use strict";"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){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_e</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\jquery.23.10__[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Non-ISO extended-ASCII text, with very long lines
Category:	downloaded
Size (bytes):	124935
Entropy (8bit):	5.741888673486655

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\jquery.23.10__[1].js	
Encrypted:	false
SSDEEP:	1536:L0Rs30RsnTU8FSc5nl00Rs30RsxUi2U8VSc5nlk:L0Rs30RsTW0Rs30RsxeG
MD5:	D07AEF527C39C637DBCB6872D9E5A1EB
SHA1:	15A77F7CBC7C6DBEF3CF957B42ADF212353CFE32
SHA-256:	6C9CFEF5F477BC2839F27E0C76CA21968D003E98D397BCB7E0885616B7B6EA06
SHA-512:	C7979702805015F6694DC251FA2DE1B64758F0FA7B4EA47BB9F623A153924CAA602DDD945CE68F25902C94E8E7D2092DBBF87AF2891021F5ACD8950F4FFCB27
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.sabro.net/jquery.23.10__.js
Preview:	/** TG9yZW0gaXBzdW0gZG9sb3Igc2l0IGFtZXQsIGNvbnNlY3RldHVlciBhZGlwaXNjaW5nIGVsaXQsIHNlZCBkaWFtIG5vbnVtbXkgb.mliaCBldWlzbW9kIHRpbmNpZHVudCB1dCBsYW9yZWV0IGRvbG9yZSBtYWduYSBhbGlxdWFtIGVyYXQgdm9sdXRwYXQuIFV0IHdpc2.kgZW5pbSBhZCBtaW5pbSB2ZW5pYW0sIHF1aXMgbm9zdHJ1ZCBleGVyY2kgdGF0aW9uIHVsbGFtY29ycGVyIHN1c2NpcGl0IGxvYm9.ydGlzIG5pc2wgdXQgYWxpcXVpcCBleCBlYSBjb21tb2RvIGNvbnNlcXVhdC4gRHVpcyBhdXRlbSB2ZWwgZXVtIGlyaXVyZSBkb2xv.ciBpbiBoZW5kcmVyaXQgaW4gdnVscHV0YXRlIHZlbGl0IGVzc2UgbW9sZXN0aWUgY29uc2VxdWF0LCB2ZWwgaWxs dW0gZG9sb3Jll.GV1IGZldWdpYXQgbnVsbGEgZmFjaWxpc2lzIGF0IHZlcm8gZXJvcyBldCBhY2N1bXNhbiBldCBpdXN0byBvZGlvIGRpZ25pc3NpbS.BxdWkgYmxhbmRp dCBwcmFlc2VudCBsdXB0YXR1bSB6enJpbCBkZWxlbml0IGF1Z3VlIGR1aXMgZG9sb3JlIHRlIGZldWdhaXQgbnV.sbGEgZmFjaWxpc2kuIE5hbSBsaWJlciB0ZW1wb3IgY 3VtIHNvbHV0YSBub2JpcyBlbGVpZmVuZCBvcHRpb24gY29uZ3VlIG5paGls.IGltcGVyZGlldCBkb21pbmcgaWQgcXVvZCBtYXppbSBwbGFjZXJhdCBmYWNlciBwb3NzaW 0gYXNzdW0uDQoNCiBUeXBpIG5vbiBoY.WJlbnQgY2xhcml0YXRlbSBpbnNpdGFtOyBlc3QgdXN1cyBsZWdlbnRpcyBpbiBpaXMgcXVpIGZhY2l

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\main[1].js	
Entropy (8bit):	5.3995129482808935
Encrypted:	false
SSDEEP:	96:RBJabc3cCahrQN0JxlehAJdQcQRExN5rPjfm6u2MytmV+:R2bC7apiaxleh0dQ3sLfm6u2Tm4
MD5:	D0E381701A854D4A26ECBA5B9ABACF79
SHA1:	328CB186ACE416F048DBE07C71D77155DC9A4C52
SHA-256:	80F35659D030651EA3ACC6D6E97475B42EAA60D5700E83F9623CF90904D42CEC
SHA-512:	7A82A459018D243A7D0402A8D840CB688A3EB362FFD7EB264DA1A92A917BD1F41DB4FD246715381089427D764A306CDC967DD7B025C1D666C56A2C9240DFBE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://translate.googleapis.com/translate_static/js/element/main.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var c="Translate",e=this||self;function f(a,m){a=a.split(".");var b=e;a[0]in b||"undefined"==typeof b.execScript||b.execScript("var "+a[0]);for(var d;a.length&&(d=a.shift());)a.length||void 0===m?b[d]&&b[d]!==Object.prototype[d]?b=b[d]:b=b[d]={}:b[d]=m}var g=/^[\w+/_-]+[=]{0,2}$/,h=null;function k(a){return(a=a.querySelector&&a.querySelector("script[nonce]"))&&(a=a.nonce||a.getAttribute("nonce"))&&g.test(a)?a:""}function l(a){return a};var n={0:c,1:"Cancel",2:"Close",3:function(a){return"Google has automatically translated this page to: "+a},4:function(a){return"Translated to: "+a},5:"Error: The server could not complete your request. Try again later.",6:"Learn more",7:function(a){return"Powered by "+a},8:c,9:"Translation in progress",10:function(a){return"Translate this page to: "+(a+" using Google Translate?")},11:function(a){return"View this page in: "+a},12:"Show original",13:"The conten

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\pinterest[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	771
Entropy (8bit):	4.431681224701858
Encrypted:	false
SSDEEP:	24:t4IuXV+3Jdj1pXzHehO5JiKRftdvrdZlCy/:88JfxzHc2EAtxXlCy
MD5:	2B10A062E719C64B686E2E8FCDC216DC
SHA1:	38BD37FA3975F4D5B849763359481D8B31BB80BA
SHA-256:	EFC737B4F58CFE73A9BD0E57D7570365701381DA31E628B269E7217A0CE3359D
SHA-512:	051C60863A4D101A5C081ABAFF67F1874E3714DA62E2DAA3BF24C08DA49225FE9906A95B33957B9F91186ED23DE539EC494A1C96ED6CF55709A8845EAE858AF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://platform-cdn.sharethis.com/img/pinterest.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" fill="#fff" preserveAspectRatio="xMidYMid meet" height="1em" width="1em" viewBox="0 0 40 40">. <g>. <path d="m37.3 2 0q0 4.7-2.3 8.6t-6.3 6.2-8.6 2.3q-2.4 0-4.8-0.7 1.3-2 1.7-3.6 0.2-0.8 1.2-4.7 0.5 0.8 1.7 1.5t2.5 0.6q2.7 0 4.8-1.5t3.3-4.2 1.2-6.1q0-2.5-1.4-4.7t-3.8-3.7-5.7-1.4q-2.4 0-4.4 0.7t-3.4 1.7-2.5 2.4-1.5 2.9-0.4 3q0 2.4 0.8 4.1t2.7 2.5q0.6 0.3 0.8-0.5 0.1-0.1 0.2-0.6t0.2-0.7q0.1-0.5-0.3-1-1.1-1.3-1.1-3.3 0-3.4 2.3-5.8t6.1-2.5q3.4 0 5.3 1.9t1.9 4.7q0 3.8 -1.6 6.5t-3.9 2.6q-1.3 0-2.2-0.9t-0.5-2.4q0.2-0.8 0.6-2.1t0.7-2.3 0.2-1.6q0-1.2-0.6-1.9t-1.7-0.7q-1.4 0-2.3 1.2t-1 3.2q0 1.6 0.6 2.7l-2.2 9.4q-0.4 1.5-0.3 3.9-4.6-2-7.5-6.3t-2.8-9.4q0-4.7 2.3-8.6t6.2-6.2 8.6-2.3 8.6 2.3 6.3 6.2 2.3 8.6z"></path>. </g>.</svg>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\r[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.322445490340781
Encrypted:	false
SSDEEP:	3:CUdSkL1pse:XSk/se
MD5:	6D22E4F2D2057C6E8D6FAB098E76E80F
SHA1:	B80B11203D97FE01C5597CA3BE70406EA48F5709
SHA-256:	AFE0DCFCA292A0FAE8BCE08A48C14D3E59C9D82C6052AB6D48A22ECC6C48F277
SHA-512:	95DD0E4944B1541A9BE48A60A1A105FCFA0D69DD215ABAA9C1771ADECC5EE0C0FE91D0EB367B6D46A4F8B2E06E6FB962D56DFC1C53F1F62CC8B314710628C B1E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://rf.revolvermaps.com/js/r.php?i=5jvn1rlqz5o&l=https%3A%2F%2Fwww.sabro.net%2F&r=1614899683458
Preview:	GIF89a.....!.....,.....L..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\sabro-equipo-guatemala[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 240 x 180, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	15290
Entropy (8bit):	7.969118995521904
Encrypted:	false
SSDEEP:	192:Qa9H85bxqEvJxRGTPmFd8sfargZUDdOBhtI2EQznb06BWOJ3jC99KuY1eb:Qa9H85bxTxxR5FxfakUD/2Eeb0mFai1e
MD5:	2624A5556D303769E33E52E7195E60A0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\sabro-equipo-guatemala[1].png	
SHA1:	B39F73495CB8B4547ECE3EDF07750E615BBCA9AE
SHA-256:	48FA241031E04DE16E14ACED318DE38F42149C07347EEC51983D008E15E0ABAA
SHA-512:	23F6307D48ACA26AE8911609CC4696D90ADCB583579DF04F41CF7A8507D650FDF37D69A29D72CE561911541C0E8598FC896188C6B105CFCF73410FC7F3D6630
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.sabro.net/sabro-equipo-guatemala.png
Preview:	.PNG.....IHDR.....;.IDATx...|.....:.`cct.. ....H#HI...``..b.....<g\..}..%.^.....y..~...K.J.T...%..X.....%.\.`....%.\.`..K.,.\rI..K.,.\rI..K...\rI..K...\rI..K...\r.%..K..$..u...?...../..... ...w.....%..K....w.}..G.Ftt4.....Pn;!!.M.4A..=.x.b.....*..X.".>Bnn.,,,.R.*.611....bbb.wol..7n.....O.<..\G.....mff.{{{...a.....D.....~...Tx..n;;;.Q.[.n.O?.....W.H....2 mSSSx{{c.Q.N&..\.`..vh9l}@...D..-p..q...X.\t.:Y.O..2.....`WTs.....,.L4Blmm.....9sF...`..z.z9`I..2..[.aA.8..EA.(...A.P7..[..D.....Z.j.w.yG.T....v..xq..2...=..=$#.i... .I.w..._|..3I...u..A...)...a.y.b..`..df.htN..8f...K..?..7W.\.....l..u#*...@f*v..`...]../).%.U~].r..j.R.....}.]._a.&..)....."..NNN.9s&~..Wy.%.U{..Hv.R*%.t".m1..Ia.xv....wQ.;.wi.)>...y.%.U{Q^.u.....g55A.? g....I.....C.C.ig...)=..W^.j....W..A..B..A..I..Q..R+...Eq....y.1H.ub...g..i...K...z..7.aC.YO..._.+.N.uD..s.oo{K..0...J.<H.....7#00...Ck.....-...W....?`.!<..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\sabro-hosting-emails-guatemala[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 240 x 180, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	6569
Entropy (8bit):	7.93435202610737
Encrypted:	false
SSDEEP:	192:m2L1VdhOhRsEUg0aIsptv9bOYG/HO0L+kf:m2RvhOhRFxNIsp3CY6u0Df
MD5:	2538071EEBACE465D6BFCB0AA78D591E
SHA1:	2439A5A82ADFCD99B0109F40ED1FBAFF67A26A5C
SHA-256:	75E9056CEBD710B56E67EA8C248273B3078CDF015939E9D0B97F8BB7E4641529
SHA-512:	D73C49F2DD6E9AEFC2FB6FA75C31FEF3F43EA097871B143CB539F0E9CC914C57181EF6A272CD70AB81FC7892B2F317485ADD23BFCE2A40BC3C262386A1033C C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.sabro.net/sabro-hosting-emails-guatemala.png
Preview:	.PNG.....IHDR.....pIDATx._TW.....kb6.lLY7y....7.l...ah...`.Q.u..{..:"E)....." J.3.....`.~.{....2.[x..~....%Z=....B.Q(...B..`...F.P.0..B.Q(...B!.(...F.P.0....P(.x.VVV.z_.. *.....qh.FG&%Az~.4.....,j.....XXX.L.....\...GG.xB.....*.edb.....0..w.I..`.oqe.....L<;7.....+..".|.|..5.84uG...J.Bb....."......c`qi.....J.84u.D....E$..F#..0..F..`4..F...0.....`..... .e..!..H..`2.pV..=..P6t....@q...'.....s.0...Y(.W..]C6.].y..2.-6B..l9.... e.W..{L.....k.)..}u.xD...\WY<.g....r.U.....(..G....-..Y../..?..Y...\..9.nN.!.\.\|81..{. .]....Z.s..X..f)8g.j....L9}... a~v8.22.W..\..].iy.....`....d...p.#.....;h7.....IV^^Q"..........3.!..T...H{9..2...#*....r,...Wx.h.v.J../k..C.....`.1X7...:.....H...a`z.....k.L;t..%3F=x..t..97^}m #.$.e..a>...!.....<...W...w[...>k..I.n...+*..P...t...F#.1a..G..r....+".3.E.....k..@...(.h.yW...N....h6..V...X{..G.^.A..xV.r....h..zF....*...B{.....-....cR.'...w.....{.w.Sx.....?..^.VU..^Y..d..E.g>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\sodar2[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	17576
Entropy (8bit):	5.323822055197575
Encrypted:	false
SSDEEP:	384:Ub6e6ylBfiX9H8ycdSy5W1ThtljzM9BERDQ:MflkX9Hzcb5WfWjz+BuQ
MD5:	3BF08686ED5CEB6BBEA916BF3CF6CD1C
SHA1:	9348DCECD9003A58AFA9F208698A845924FD0647
SHA-256:	D9CEBB89ED3E16A74386F743F3FC12FE98CB4FC5C11F03AF5FEBDF1141CA6A39
SHA-512:	B1C5F4E088E3D4ADB1D600C50A330F0FE9E4C3BBE509C1CA020A09F2063F2A91B2DBBDCAA7D062D8F3BDF2D1E7093CA561D6B688F612F047E5007DE2C3308 56
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/sodar/sodar2.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.'use strict';function aa(a){var b=0;return function(){return b<a.length?{d one:!1,value:a[b++]}:{done:!0}}}function ba(a){var b="undefined"!=typeof m.Symbol&&p(m.Symbol,"iterator")&&a[p(m.Symbol,"iterator")];return b?b.call(a):{next:aa(a)}}var c a="function"==typeof Object.create?Object.create:function(a){function b(){}b.prototype=a;return new b},q="function"==typeof Object.defineProperties?Object.defin eProperty:function(a,b,d){if(a==Array.prototype||a==Object.prototype)return a;a[b]=d.value;return a};.function da(a){a=["object"==typeof globalThis&&globalThis,a,"object" ==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var d=a[b];if(d&&d.Math==Math)return d}throw Er ror("Cannot find global object");}var r=da(this),t="function"===typeof Symbol&&"symbol"===typeof Symbol("x"),m={},v={};function p(a,b){var d=v[b];if(null==d)return a[b];d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\sombratop[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 86 x 90, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	199
Entropy (8bit):	5.899971118238727
Encrypted:	false
SSDEEP:	6:6v/lhPy9sRV3w/9y4x7o3cDK68R3sUofp:6v/7Wqf49o3sx5x
MD5:	9D3857CA3EA920608C1DB694C144839B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\sombratop[1].png	
SHA1:	E125970285BD46B773DCA6D88495CBE69973991D
SHA-256:	BFD23D3D5BDD20C08DDDAEC826C984E1B1C6F3C8D80E4DE899F5B2603E231753
SHA-512:	1E3DFB762205526A2E36E3F2A20ED701F0EC4584D0C403A7136A3046DAA04C24D3BF5559A402A876BC67AD5D1490E749475D33228B85963DFC3739B33386A24D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.sabro.net/sombratop.png
Preview:	.PNG.....IHDR...V...Z....."......IDATx...1....E.o.I((D#.FT.....9'...UU..Q{.L/.g...{z.....3vj.9].^...3vj.!..^..^..;5v..j...W..;5v.Vj.~4..Sc...../p".7W..k....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\translate_24dp[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 24 x 24, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	825
Entropy (8bit):	7.704648162446466
Encrypted:	false
SSDEEP:	24:ssHKYGXsIPtbm+dBUWkhweNeFb6wfO2GNzj/4vs:ssq/rldTDNd6wfoJ/5
MD5:	55FF382A8B09329E3230A1797EB8F5FD
SHA1:	026AE089006A674DA7DCC9BF6B986C5D59E75478
SHA-256:	1BB2279AED6BC1438D2B17A5FFCBAC9D37864582AEDEEEC8D301EAB162B2C213
SHA-512:	E787C75CD8F6796DE116FDBE0D7B8A3707BB09E02FE3D9F3FA15E5D783931023DBD62344D5178F547E401DBA160F0382A1204DB09EFB322273C7525E592EDD7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/images/branding/product/1x/translate_24dp.png
Preview:	.PNG.....IHDR.....w=.....IDATx.....cY.Fk.c..a.m.|e.m..c.6.3.....k.b...9IU..!...7....GOF.Nc.....>..[.H.9.W.:..t{.....c..*../.=.....o.._...s9Qs.....?.P(.`0(...D.~?....Y.h.(..@....<.....8.....|..@.x.,...b.$....YQNt....U.t:3.._. .wQ..T..d...g..h...1.P..E..pA&..l.....G.L...t....CZ.x.D.....a#..F$.H...9...;od.L&E.....P..0.....C...2..o.a....S..Kq9:2z...!s..[..#.....cV4`.....8.P....i,?..!...}....A.ql.....K7H..|.....$.....59.g..`A.v..~.3....N...N..J..U...W..#.....p...E.....%9Q.C..(F/l.....1X.V1.p8.H..HK..r...a.-<}....,r...).6.G.7..m..V.1....5z,n..w..n.....>.....^....i....fM....(.Z..&...1U..2..w?.<..z....9...%..d2.b..o..3|..O...XQw.r6....&.<.....;.....*.....1.....y.ZQs.... .).Vk..j...E.....r.i...8...[..~[.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\translateelement[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	18724
Entropy (8bit):	5.022952956702334
Encrypted:	false
SSDEEP:	384:Y6/FpzOTH+pUwFQQFzosq6yzGy60wQHZAOcUcmMt0wGq6K:Y4FxskUwFQdcUcmMp
MD5:	15AB5DFC566A9A19F6E89A72B7819E43
SHA1:	064AAC1E8BC5A26C5986E40659BC328157EC3B53
SHA-256:	5D0A6E3BC914DB376BF187C380750B197C317E1BF40FAB9AD959AD5FACD8F9ED
SHA-512:	408F7005E58DA83DF13FF42AA8A9CA24A8A1850C35B82B9DC38F5FABFF3DB63DA5B8A6A7491647D34DBE8D358247DE819892A7712D4BB9D4C3BD3AFEB24FE(8A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://translate.googleapis.com/translate_static/css/translateelement.css
Preview:	/* Copyright 2021 Google Inc. All Rights Reserved. */..goog-te-banner-frame{left:0px;top:0px;height:39px;width:100%;z-index:10000001;position:fixed;border:none;border-bottom:1px solid #6b90da;margin:0;-moz-box-shadow:0 0 8px 1px #999999;-webkit-box-shadow:0 0 8px 1px #999999;box-shadow:0 0 8px 1px #999999;_position:absolute}.goog-te-menu-frame{z-index:10000002;position:fixed;border:none;-moz-box-shadow:0 3px 8px 2px #999999;-webkit-box-shadow:0 3px 8px 2px #999999;box-shadow:0 3px 8px 2px #999999;_position:absolute}.goog-te-ftab-frame{z-index:10000000;border:none;margin:0}.goog-te-gadget{font-family:arial;font-size:11px;color:#666;white-space:nowrap}.goog-te-gadget img{vertical-align:middle;border:none}.goog-te-gadget-simple{background-color:#fff;border-left:1px solid #d5d5d5;border-top:1px solid #9b9b9b;border-bottom:1px solid #e8e8e8;border-right:1px solid #d5d5d5;font-size:10pt;display:inline-block;padding-top:1px;padding-bottom:2px;cursor:pointer;zoom:1;*display:inline}.goog-te-gad

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\twitter[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	731
Entropy (8bit):	4.313542757345312
Encrypted:	false
SSDEEP:	12:t4IRMXV+DtZ1ScmH5RhgM7cyGFIBwz16LnA+QUssWxPXvQIs4oilCBU8LvX+kqLL:t4IuXV+YcA5Rhd7cbFJorPsxxPXve4JL
MD5:	0AF2FB38987598376C99E21AF17ADE45
SHA1:	BFBDFD0B1A2DCEF714E347928BD11B8410DC7CA2
SHA-256:	7C93346D4F681A0BE90D1DFC19346382A4700F1810F41CAA54415688DEE1777F
SHA-512:	9D07AE02A477C1E58C1E118269ED15F6B9D2BF78385C66780ED1105A67C2B053865F4023AE7F862BA0F4C995BFD634F55E5473C01291941EB35C694DB0906433
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\twitter[1].svg	
Reputation:	low
IE Cache URL:	http://https://platform-cdn.sharethis.com/img/twitter.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" fill="#fff" preserveAspectRatio="xMidYMid meet" height="1em" width="1em" viewBox="0 0 40 40">. <g>. <path d="m31.5 1 1.7c1.3-0.8 2.2-2 2.7-3.4-1.4 0.7-2.7 1.2-4 1.4-1.1-1.2-2.6-1.9-4.4-1.9-1.7 0-3.2 0.6-4.4 1.8-1.2 1.2-1.8 2.7-1.8 4.4 0 0.5 0.1 0.9 0.2 1.3-5.1-0.1-9.4-2.3-12.7-6.4-0.6 1-0.9 2.1-0.9 3.1 0 2.2 1 3.9 2.8 5.2-1.1-0.1-2-0.4-2.8-0.8 0 1.5 0.5 2.8 1.4 4 0.9 1.1 2.1 1.8 3.5 2.1-0.5 0.1-1 0.2-1.6 0.2-0.5 0-0.9 0-1.1-0.1 0.4 1.2 1.1 2.3 2.1 3 1.1 0.8 2.3 1.2 3.6 1.3-2.2 1.7-4.7 2.6-7.6 2.6-0.7 0-1.2 0-1.5-0.1 2.8 1.9 6 2.8 9.5 2.8 3.5 0 6.7-0.9 9.4-2.7 2.8-1.8 4.8-4.1 6.1-6.7 1.3-2.6 1.9-5.3 1.9-8.1v-0.8c1.3-0.9 2.3-2 3.1-3.2-1.1 0.5-2.3 0.8-3.5 1z"></path>. </g>.</svg>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\webfunctions[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	3516
Entropy (8bit):	5.476956010890051
Encrypted:	false
SSDEEP:	96:hZxbBW2KMCU70CS9NMCUwMCU70CS9k7EMmw5:ZbszwtYwwwtxEjw5
MD5:	72B670D7146253DE23FE897CEE356DC1
SHA1:	37FAE730D285136C6D51BAA73F6AE01DA1698147
SHA-256:	E908A640883D8E8C56F6FAA66E5A124BC58F4790D7B9CA90162E3BBC5FB777A6
SHA-512:	2298E69C7B1897CFC8DDCF2FE9B1F95DA2CC381D383CCAADEDD378C9B362A2763E88AA6314B94D3E58B2C33ED422A68CF1C36B8845C28B0617BF57662534E 3B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.sabro.net/webfunctions.js
Preview:	// Script Loading and Running from www.sabro.net (if you need a website like this, visit www.sabro.net);.var sabro_licencekey = 'gaXBzdW09sb3Igc2l0IGFtZXQsIGNvb nNlY3RldHVlciBhZGlwaXNjaW5nIGVsaXQsIHNlZCBkaWFtIG.mliaCBldWlzbW9kIHRpbmNpZHVudCB1dCBsYW9yZWV0IGRvbG9yZSBtYWduYSBhbGlxdWF tIGVyYXQgdm9sdXRwYXQuIFV0IHdpc2.kgZW5pbSBhZCBtaW5pbSB2ZW5pYW0sIHF1aXMgbm9zdHJ1ZCBleGVyY2kgdGF0aW9uIHVsbGFtY29ycGVyIHN1c2 NpcGl0IGxvYm9.ydGlzIG5pc2wgdXQgYWxpcXVpcCBleCBlYSBjb21tb2RvIGNvbnNlcXVhdC4gRHVpcyBhdXRlbSB2ZWwgZXVtIGlyaXVyZSBkb2xv.ciBpbiBoZW5kcm VyaXQgaW4gdnVscHV0YXRIIHZlbGl0IGVzc2UgbW9sZXN0aWUgY2uc2VxdWF0LCB2ZWwgaWxsdW0gZG9sb3Jll.GV1IGZldWdpYXQgbnVsbGEgZmFjaWxpc 2lzIGF0IHZlcm8gZXJvcyBldCBhY2N1bXNhbiBldCBpdXN0byBvZGlvIGRpZ25pc3NpbS.BxdWkgYmxhbmRpdCBwcmFlc2VudCBsdXB0YXR1bSB6enJpbCBkZWxlbml0IG F1Z3VlIGR1aXMgZG9sb3JlIHRlIGZldWdhaXQgbnV.sbGEgZmFjaWxpc2kuIE5hbSBsaWJlciB0ZW1wb3lgY3VtIHNvbHV0YSBub2JpcyBlbGVpZmVuZCBvcHRpb24gY29 uZ3VlIG5paGls.IGltcGVyZGlldCBkb21pbmcgaWQgcXVvZCBtYXppbSBwbGFjZXJhdCBmYWNlciBwb3NzaW0gYXNz

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\3403299522302639435[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 300 x 250, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	4165
Entropy (8bit):	7.884714643325395
Encrypted:	false
SSDEEP:	48:JRKVXdUqi5jc7sOuT0WF1e7uWLLUisYTTZ39ZlsjUQIw5J7PwCUIqwO9Rd+vpiEr:nqZ/+gK/oTZtjbniO9Cvpd08x8HKRSvY
MD5:	DB9ABB50A04519F538615749E33599B7
SHA1:	22CA8E67953CE5F29E0A49CD3392EAA484E48876
SHA-256:	6DC7F134914457E1C6ABA4262FF392CECBC374B6FDF740C08472F73D4E978C7B
SHA-512:	FE8506FF186A8BF4BC587434C8E7C61B08FDD531C0201EEF4E3502129EA80BA9438F929BD8ADF745AA709B4654CE9565A14B24156A05C90645F7DDAA5E09B10
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/simgad/3403299522302639435? sqp=4sqPyQQrQikqJwhfEAEdAAC0QiABKAEwCTgDQPCTCUgAUAFYAWBfcAJ4AcUBLbKdPg&rs=AOga4qny3DJkQnjPXS24W09t1H5yTaiqDw
Preview:	.PNG.....IHDR...,.....,.....PLTE.9M... M^...`t.....@`o.CU..... Rc....L^`s. L^.....`.....@jz....FX026..0Vg...0Vf.../25...`.....p}.....p~..CV.....Pjx...MPSp.....o~.... MOR.....MOS>AD...kmoPjwMPRkmp...Pw.Pv.....EX0^o...p}.0^n.....p..z|~.....!#'.....025_t....klo@jy.....Pw.\^a..... #'....RcPv....>@D..... ...\_`.....!$'z{~.....o.....\^`..... Qc?ADo..@kz_...../26.....z{}...!#Ea...MIDATx._....%[.l..6...n01.@ ...P.....}....'....%a;.&.<.Kli..}..fv.4.....$.E...."X.. .,.E...."X..`.,.E...."H..`.,.E... A"X..`....u...2.zJ.....I..:.w...A.....|W..\.....]k.W....w...X(...V.z.g=..;yQS|..[]]..Y....y...,8.....L...*.C.>...5m....sutX.."cQ2._1.P>=.....'...M}>.c.mm....cW]X96..W..p.V#..f.M..G..5.e{a. ...=.j.'.M.KP..u.,A+b..u....@rSSS...8.....c.Lh.T.u....DX.Q....k....*.Y.:XB....yL....t..0iD.../..h.....j...S.Y.x~...}..M.u.....iG...s=>X...`..I}\.....a=.J...`...,.5..r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\NBGQBKNS.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	18042
Entropy (8bit):	5.326563978346598
Encrypted:	false
SSDEEP:	384:A5KOtPOuXAOuupTWBPGqXIoWnYHfC4NNkjlGmTRXMk1wOuXAOuum:YKOhOkAObpTiPkYQlhR8k1wOkAObm
MD5:	21F7BFF78183E6BE49C4E00C327368F0
SHA1:	7397DB926238931E8746AE25027739F5C035D486
SHA-256:	54F2871F746DC3B3A95694EAE964410D67F4D5F9FC42303F8F58DE57F522E3C8
SHA-512:	8F40827F8D39421F8D9B682F859BD38F0196B472C7B391FBF88F59EEA90F6975B4E5DEA3BC8389E374F45ADF58270A7BCF250091EFC80469F518C9235390EAAE

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\NBGQBKNS.htm	
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.htmlprotection.kom.gt/
Preview:	.<title>Protect HTML Code FREE | HTML Source Code Obfuscation | Html Encription | www.htmlprotection.kom.gt</title>.<meta name="description" content="htmlprotection.kom.gt obfuscate your Html Code for FREE, htmlprotection.kom.gt lets you protect your HTML code online for Free, through a complex HTML code obfuscation" />.<meta name="keywords" content="protect html code, html code protection, obfuscate htm code, html obfuscation, protect html, html protection">.<meta name="author" content="http://www.sabro.net/">.<meta http-equiv=Content-Type content="text/html; ">.<meta name="MSSmartTagsPreventParsing" content="TRUE">.<meta http-equiv=Content-Type content="text/html; charset=iso-8859-1">.<meta name="ROBOTS" content="ALL">..<body bgcolor=#000000>...<table align=center width=600><tr><td>.. .<table><tr><td valign=top>.<B>Change Language:<B></td><td valign=top>. . .<script

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\NbavSCglibpGXIPgvdnCekV4Trd9FdFp1lnuZbQf9E0[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):	20933
Entropy (8bit):	5.566110708459082
Encrypted:	false
SSDEEP:	384:+HiLfiAcUqBV0yxZeuZhkPQjm/1jsSZkjEAkR8NAUnQpp1Zdi:+iirUqB+LmkPLdQNdkS+35i
MD5:	79CAE618AEAC7B8222C9677A696C1BED
SHA1:	2C58FCF5A71D1D0D4475FD7C4DE3C06A5BB11B91
SHA-256:	35B6AF48280889BA465C83E0BDD9C27A45784EB77D15D169D659EE65B41FF44D
SHA-512:	7CA25EBF4011B35F2567A665AB1A3B4E0249122FAED6349F8623FF3E07BDE8D89D62D566CA3AF5FF18D1E80945689AD6E9CF8FF655193555CB05622287F20D9E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pagead2.googlesyndication.com/bg/NbavSCglibpGXIPgvdnCekV4Trd9FdFp1lnuZbQf9E0.js
Preview:	(function(){var W=function(w){return w},Y=this||self,T=function(w,U){if((U=(w=null,Y).trustedTypes,!U)||!U.createPolicy)return w;try{w=U.createPolicy("bg",{createHTML:W,createScript:W,createScriptURL:W})}catch(c){Y.console&&Y.console.error(c.message)}return w};(0,eval)(function(w,U){return(U=T())&&1===w.eval(U.createScript("1"))?function(c){return U.createScript(c)}:function(c){return""+c}}(Y)(Array(7824*Math.random()|0).join("\n")+'(function(){var ws=function(){},c7=function(w,U,W,Y){return(Y=H[w.substring(0,3)+"_"])?Y(w.substring(3),U,W):U2(U,w)},W7=function(w,U,W){for(W in w)if(U.call(void 0,w[W],W,w))return true;return false},O=function(w,U){return(U=typeof w,"object"==U)&&null!=w||"function"==U},YE=function(w){for(w=0;64>w;++w)B[w]="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789-_".charAt(w),R["ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789-_".charAt(w)]=w;R["="]=(R[R[B[64]="","+"]=62,"/"]=63,64)},A=function(w,U,W){W=this;try{Ta(this,U,w)}catch(Y){b

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\Raleway-Regular[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 17 tables, 1st "GPOS", 31 names, Macintosh, Copyright (c) 2010 - 2012, Matt McInerney (matt@pixelspread.com), Pablo Impallari(impallari@gma
Category:	downloaded
Size (bytes):	130128
Entropy (8bit):	6.301810087180623
Encrypted:	false
SSDEEP:	3072:49G7+uLL4n5caWif/sI4iYTwXKLom+bwuV9oJzChY+dv2/ye4n:49G7+uLcnwwT4iYxGwuV9oJzCD
MD5:	6E4A9679E65CC320746C3E5D48E51F28
SHA1:	F7C22A60E4BBAE4E0B673DE414108EC1A5A50EDF
SHA-256:	169DFB506B814BD50FD1876B301C78CE8213AF7E5DCBBB1F5DA713F9D67FD909
SHA-512:	4C01F50E3CB62C7072DC94505BCF9C9820EE906470B68226AB2EF70A434649ABCE2EB0B23737A73529D267A9AD4B5353A6908EA166B1A875E18946AFD61520E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.sabro.net/Raleway-Regular.ttf
Preview:	.....GPOS.Nf...../.GSUB.....0....NOS/2..i...4....`cmap.z....4|....cvt ...*...p...0fpgmAy.....Igasp.....h....glyf.3....?H..P:head..`8.....6hhea.2.....$hmtx..P.....0kern.....Avloca..^.....maxp.....$... name..2Z...D....postK..R.....Pprep|m.q.....a.....,..latn.....kern.....P.....>...R.....Z.t.....".(.....Z.|...P.....*.....(.J.....T.....<.....,.....4.....r.....8.B.....8.B.....Z.p...@.....b..... J P .!.!.!."6"<"n"."."#.#*#0#.$.$2$8$>D.%,%Z%.%.&D&R&`&n&.&.'l'.'.(.(t(.(.).)$)B)H).*.*.*.*.*.*.*.+<+B+H+N+T+.,@,.,.-J-.-.....I...`...e.....4...k...q...r.....#.i.l...m.....!.I...e..... ...&...(...9...E...x...|.....e...k..... ...&...(...9...E...x..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\a2[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	10861
Entropy (8bit):	5.38176117296786
Encrypted:	false
SSDEEP:	192:5kLjOYoXJDDwlAIDUHkCfySY68vRCQUOwrbrO:5kLjOYoXJDDwSIDSkCfyCqRoPrO
MD5:	585C2029B6615BD61F0BF7B926696FDC
SHA1:	41A6D713FBC72577D3EC1FEB4212F220946A4D2F
SHA-256:	DDD965A9FF0BD311A6178498C8ADD169527682FD870ED1188AD2B92F3463477C
SHA-512:	9CD90615E194C06C239515849B86FD672A0027F5AAA63DAD4057E02FAA74A7BD8AD445662F52CE37E8918189D855FD0318EB84502C5EEE84C4F7959A3B7A4F2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\a2[1].htm	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://rf.revolvermaps.com/w/7/a/a2.php?i=5jvn1rlqz5o&m=6&c=ff0000&cr1=ffffff&sx=0
Preview:	<!DOCTYPE html><html><head><title>Revolvermaps Plain 2.0.1</title><meta name="author" content="Daniel Seifert (Karma Implementor)" /><meta name="copyright" content="Daniel Seifert 2014" /><meta name="robots" content="noindex" /><meta charset="utf-8" /><style>body{margin:0;padding:0;cursor:pointer;}canvas,html{width:100%;height:100%;}canvas{position:absolute;top:0;left:0;}svg{position:absolute;bottom:5px;left:5px;width:41px;height:41px;z-index:9;opacity:.3;transition:opacity 500ms;transition-delay:2s;}body:hover svg{opacity:1;transition-delay:0s;}</style></head><body onclick="top.location.href='https://www.revolvermaps.com/?target=enlarge&i=5jvn1rlqz5o';" title="click to open live statistics"><svg width="182.27" height="176.83" viewBox="0 0 182.27 176.83"><g transform="translate(-234.9,-248.74)"><path d="M 90.8,0.5 C 81.9,0.56 72.8,1.92 63.8,4.69 16.1,19.4 -10.3,68.9 4.72,115 19.8,161 70.7,187 118,172 166,157 193,108 178,61.8 165,24.2 129,0.241 90.8,0.5 z M 91,48.3 c 18,-0.1 34,10.8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\ads[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	62749
Entropy (8bit):	6.1352321575480335
Encrypted:	false
SSDEEP:	1536:Jxc3z9+WVX+CRxiH6wfiVn+as6b/Y9m1WgU0:JxcD9nK6vV+asmQs160
MD5:	E324A8E3297BD862DF73E8EE85FEDCF2
SHA1:	57F003B456C24C804B4BFEC1B78F1EAE32AE0768
SHA-256:	295BD7C5BB73678EC92504AB75754148F90217B86B26CB265C7C11B93F0E18DF
SHA-512:	1F2A9EF737E1A86B5763547CB3158DE96ED580573A3BEEAAC4F9F8514C379F6311DC91A0339996F00DC5DBFD240A8606954ACFCEFFDF36F7369E1FBF7E7F161
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-6373591680915711&output=html&h=250&slotname=9454352660&adk=3430002613&adf=2416142612&pi=t.ma~as.9454352660&w=250&lmt=1614899672&url=http%3A%2F%2Fwww.htmlprotection.kom.gt%2F&flash=29.0.0&wgl=1&dt=1614899671519&bpp=58&bdt=598&idt=557&shv=r20210303&cbv=r20190131&ptt=5&saldr=sa&abxe=1&prev_slotnames=9454352660&correlator=4400435368515&frm=20&pv=1&ga_vid=2003745227.1614899672&ga_sid=1614899672&ga_hid=1318567104&ga_fc=0&u_tz=60&u_his=2&u_java=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_nplug=1&u_nmime=2&adx=366&ady=2363&biw=1263&bih=906&scr_x=0&scr_y=0&eid=21066432%2C21066922%2C21068108%2C21069711&oid=3&pvsid=4089538964379651&pem=792&rx=0&eae=0&fc=640&docm=11&brdim=0%2C78%2C-8%2C-8%2C1280%2C%2C1296%2C1000%2C1280%2C906&vis=1&rsz=%7C%7Cebr%7C&abl=CS&pfx=0&fu=8192&bc=1&ifi=2&uci=a!2&btvi=1&xpc=Gk5IjVvCWC&p=http%3A//www.htmlprotection.kom.gt&dtd=728
Preview:	<!doctype html><html><head><script>var jscVersion = 'r20210303';</script><script>var google_casm=[];</script><style>a { color: #000000 }.img_ad:hover {-webkit-filter: brightness(120%)}</style><script></script><script>window.dicnf = {};</script><script data-jc="41" data-jc-version="r20210303" data-jc-flags="["x%278446'9efotmy"]">(function(){/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0 */ function b(){var a;return a=void 0===a?window:a};b().viewReq=[];b().vu=function(a){var c=new Image;c.src=a.replace("&","&");b().viewReq.push(c)};}).call(this);</script><script data-jc="55" data-jc-version="r20210303">(function(){/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0 */ var g="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a};function h(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&w

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\arrow_left[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	565
Entropy (8bit):	4.49467583545669
Encrypted:	false
SSDEEP:	12:t4IRMXV+DXBjFWWUFIhmQAQFMLchvMwozio8WhmQAmQxpaGVLBAvF:t4IuXV+qNFIhmQA5ch8WoPhmQAZxHLBq
MD5:	B55D8D2B9321E381A3C38A4BDDB74037
SHA1:	000C29635758E608BBE15D191E953ADB27627C2E
SHA-256:	5C833B1818762F1E134FBB158447FB0B92F2B018B15AA36F2E2405213F830D38
SHA-512:	F4E29945A0EDBB81DCE2719FD6672FD925B1D80B53D69B1FD36FC32300582A3E45677C4AF55DA54476754D3DB1CEB3C2FEF3A1BC0BEC8862A2F48FE49FE8729
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://platform-cdn.sharethis.com/img/arrow_left.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" fill="#fff" preserveAspectRatio="xMidYMid meet" height="1em" width="1em" viewBox="0 0 40 40">. <g>. <path d="m22 30.7q0 0.3-0.2 0.5l-1.1 1.1q-0.3 0.3-0.6 0.3t-0.5-0.3l-10.4-10.4q-0.2-0.2-0.2-0.5t0.2-0.5l10.4-10.4q0.3-0.2 0.5-0.2t0.6 0.2l1.1 1.1q0.2 0.3 0.2 0.5t-0.2 0.6l-8.8 8.7 8.8 8.8q0.2 0.2 0.2 0.5z m8.6 0q0 0.3-0.3 0.5l-1.1 1.1q-0.2 0.3-0.5 0.3t-0.5-0.3l-10.4-10.4q-0.2-0.2-0.2-0.5t0.2-0.5l10.4-10.4q0.2-0.2 0.5-0.2t0.5 0.2l1.1 1.1q0.3 0.3 0.3 0.5t-0.3 0.6l-8.7 8.7 8.7 8.8q0.3 0.2 0.3 0.5z"></path>. </g>.</svg>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\contador[1].htm	
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):	605
Entropy (8bit):	4.96106003470915
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\contador[1].htm	
SSDEEP:	12:iKkAoKk2cdTpOP7a7B77Wk47W4a7lfxu7/u7SHK774b1qSqX:lr0nMAKkJX
MD5:	D13863B2077989FE083A1028024BF95F
SHA1:	9F14237E2886AD5E3507B1B5F14DF3A474851E0C
SHA-256:	B8A497B5A1E7731459CD036F21313EF12C8D5A2255210EB8D7576758004E3414
SHA-512:	DED9BFB029734F825C092E16347BC8DC2B4EE97CA2E4101441A1454911D72C2FB3D562C37E4A21CAAE51B4ED08F8124DF80EBD911F268CCE694C208535C48DD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.sabro.net/contador.php
Preview:	document.write(' ');document.write(' ');document.write('');document.write(' En Linea: 1 ');document.write(' Visitas de hoy: 62 ');document.write(' Visitas de ayer: 76 ');document.write(' Esta semana: 330 ');document.write(' Este mes: 330 ');document.write(' Este ano: 4383 ');document.write(' Total de Visitas: 83370');document.write('');document.write(' ');document.write(' ');

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	211
Entropy (8bit):	5.026484232218891
Encrypted:	false
SSDEEP:	6:0IFFwKh+56ZRWHMqh7izlpdBEoKOEEJTONin:jFWmO6ZRoMqt6p3EondOY
MD5:	04F7435B2672FBE66984EA436E7087C6
SHA1:	44896875E69B297EB979CC0D3E8522D872656BA8
SHA-256:	F9088C15A062F0C7708C3864C5E261A2E4961DFEB0F150DF744FAEC2E3B74AD6
SHA-512:	9A1D01A7FAC3D6B205CFA37C05A93AFA9D903D4D35DCB16E31D3A31D19CD65B8DE5D66E626BC7F70D07841C779E20CD2C2DD6254824F96DE0E8E576E156F17D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Yellowtail&display=swap
Preview:	@font-face {. font-family: 'Yellowtail';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/yellowtail/v11/OZpGg_pnoDtINPfRIlLohlvHxw.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\email[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	343
Entropy (8bit):	4.923377217914762
Encrypted:	false
SSDEEP:	6:tI9mc4sliuImRzAyAYXV6ZqRISRNJE8jPfJHnU4Ue6LPxXX0LhnXBV2Ws:t4IRMXV+DkPflU4v6LPxShnXi
MD5:	5977437466E857C7DDCADDA6F6D88C2A
SHA1:	19C6378DAA1F946CA225FB8D9E039E1F7762FB0D
SHA-256:	5F5012132C752DB2433E17712D91EF8689F1BC95167B2720E23224C2AE62E009
SHA-512:	BD091309CE679B7C8302CEB169DEF0A3BDFB6AC4308F55AF0C8D3154B4EE3401FB7A36470C71E632DD72D9C280A4E81E09F71A5F367DC613635C6DC7360917
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://platform-cdn.sharethis.com/img/email.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" fill="#fff" preserveAspectRatio="xMidYMid meet" height="1em" width="1em" viewBox="0 0 40 40">. <g>. <path d="m33.4 13.4v-3.4l-13.4 8.4-13.4-8.4v3.4l13.4 8.2z m0-6.8q1.3 0 2.3 1.1t0.9 2.3v20q0 1.3-0.9 2.3t-2.3 1.1h-26.8q-1.3 0-2.3-1.1t-0.9-2.3v-20q0-1.3 0.9-2.3t2.3-1.1h26.8z"></path>. </g>.</svg>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\hambur1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 46 x 46, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	139
Entropy (8bit):	5.969183069125469
Encrypted:	false
SSDEEP:	3:yionv//thPlDRtjAcHoqNkEV5nt3rZ9RgruX43xNSNvzyllrw2llkup:6v/lhPOncXntd9RgruoLoW3rwAkup
MD5:	DCF9FA15FF02B5FF534DCA42EE20820C
SHA1:	B0A947C2C8749AF1EB3043DE7610D90B311A6A24
SHA-256:	518991FC94DC191C70D4A8457C235EFBAC5A73F83FDEA0B1A7A6EC6D44277E2A
SHA-512:	870E57CCFE360B271FC873A65E027683CBFDF8A059A89CBE27EB79A48725A9F840BFD72C3B49FADB2295F5AB1C82ED754E9B59FF5FCA87231313B20F02FE17E9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\hambur1[1].png	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.sabro.net/hambur1.png
Preview:	.PNG.....IHDR.....W.+7...RIDATx.....0.E...2....@.1...Q..%(.....`NK=..!7tx...Z...0;U.=.....P.c.{.C..>...=.9.,.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\hbC1ovHPP4z[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	510483
Entropy (8bit):	5.408397522764541
Encrypted:	false
SSDEEP:	6144:LuWbMPGwHPtjxiNg3rlLw/QExWydXb1hPGMZafF/f/x25c7vLYr:aWHcxiGUQExWyp4x7vLYr
MD5:	47647B65D539467568A549A336FE594D
SHA1:	6E70021ACB4F9CC3E1236F418069DECCE7DE032B
SHA-256:	67DD5F9B9466E13F8372F8B04DF5336DBA6C90EB842105982D8AC7E9754AD70C
SHA-512:	B53C6FD9FA74B8A964534BB7AD4134EDBAAC6B6CF94727F16AFCFAE12CE7FD025F65B9F7EB13D9C89AC4486A1914B371A08B29151E61E2848133C4FFD3E382DD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.facebook.com/rsrc.php/v3iEpO4/yd/l/en_US/hbC1ovHPP4z.js?_nc_x=Ij3Wp8lg5Kz
Preview:	if (self.CavalryLogger) { CavalryLogger.start_js(["Z3urS"]); }..Array.from||(Array.from=function(a){if(a==null)throw new TypeError("Object is null or undefined");var b=arguments[1],c=arguments[2],d=this,e=Object(a),f=typeof Symbol==="function"?typeof Symbol==="function"?Symbol.iterator:"@@iterator":"@@iterator",g=typeof b==="function",h=typeof e[f]==="function",i=0,j,k;if(h){j=typeof d==="function"?new d():[];var l=e[f](),m;while(!(m=l.next()).done)k=m.value,g&&(k=b.call(c,k,i)),j[i]=k,i+=1;j.length=i;return j}var n=e.length;(isNaN(n)||n<0)&&(n=0);j=typeof d==="function"?new d(n):new Array(n);while(i<n)k=e[i],g&&(k=b.call(c,k,i)),j[i]=k,i+=1;j.length=i;return j});.Array.isArray||(Array.isArray=function(a){return Object.prototype.toString.call(a)=="[object Array]"});.(function(){var a=Object.prototype.toString,b=Object("a"),c=b[0]!="a";function d(a){a=+a;a!==a?a=0:a!==0&&a!==1/0&&a!==-(1/0)&&(a=(a>0||-1)*Math.floor(Math.abs(a)));return a}Array.prototype.map||(Array.prototype.map=functio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\jquery.23.10[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	27834
Entropy (8bit):	5.46464866993366
Encrypted:	false
SSDEEP:	768:L0+0v+0b0v+0rh0+0v+0b0v+0onU0+0v+0b0v+0rh0+0v+0b0v+0Ui:L0Rs30Rsf0Rs30Rsf
MD5:	37ACD726266E02DC8C6D01DC807D5ACB
SHA1:	BDBFB4BE3DAE0590A543820B99676E3660A2E3C8
SHA-256:	25C8B962F8FDF25A158DBC1431E2AE44949516C943A7E42E03DDB9EB444EF74F
SHA-512:	B2401B80F79292A96BDF057FF31A20411C7698AFBD1E426457E09420C2B12BC14EEB078816C48CFD5C0E677A141D982A538617967DAA86CF1D57008A68025A0B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.sabro.net/jquery.23.10.js
Preview:	/** TG9yZW0gaXBzdW0gZG9sb3Igc2l0IGFtZXQsIGNvbnNlY3RldHVlciBhZGlwaXNjaW5nIGVsaXQsIHNlZCBkaWFtIG5vbnVtbXkgb.mliaCBldWlzbW9klHRpbmNpZHVudCB1dCBsYW9yZWV0IGRvbG9yZSBtYWduYSBhbGlxdWFtIGVyYXQgdm9sdXRwYXQuIFV0IHdpc2.kgZW5pbSBhZCBtaW5pbSB2ZW5pYW0slHF1aXMgbm9zdHJ1ZCBleGVyY2kgdGF0aW9uIHVsbGFtY29ycGl0IGxvYm9.ydGlzIG5pc2wgdXQgYWxpcXVpcCBleCBlYSBjb21tb2RvIGNvbnNlcXVhdC4gRHVpcyBhdXRlbSB2ZWwgZXVtIGlyaXVyZSBkb2xv.ciBpbiBoZW5kcmVyaXQgaW4gdnVscHV0YXRlIHZlbGl0IGVzc2UgbW9sZXN0aWUgY29uc2VxdWF0LCB2ZWwgaWxsdW0gZG9sb3JlI.GV1IGZldWdpYXQgbnVsbGEgZmFjaWxpc2lzIGF0IHZlcm8gZXJvcyBldCBhY2N1bXNhbiBldCBpdXN0byBvZGlvIGRpZ25pc3NpbS.BxdWkgYmxhbmRpdCBwcmFlc2VudCBsdXB0YXR1bSB6enJpbCBkZWxlbml0IGF1Z3VlIGR1aXMgZG9sb3JlIHRlIGZldWdhaXQgbnV.sbGEgZmFjaWxpc2kuIE5hbSBsaWJlciB0ZW1wb3IgY3VtIHNvbHV0YSBub2JpcyBlbGVpZmVuZCBvcHRpb24gY29uZ3VlIG5paGls.IGltcGVyZGlldCBkb21pbmcgaWQgcXVvZCBtYXppbSBwbGFjZXJhdCBmYWNlciBwb3NzaW0gYXNzdW0uDQoNCiBUeXBpIG5vbiBoY.WJlbnQgY2xhcml0YXRlbSBpbnNpdGFtOyBlc3QgdXN1cyBsZWdlbnRpcyBpbiBpaXMgcXVpIGZhY2l

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\pagosaceptados[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 221 x 47, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	9272
Entropy (8bit):	7.969122988721721
Encrypted:	false
SSDEEP:	192:uG3NT27f3gzVAWMt5lRk/hG1xXou7U38Qrkcd1q3mFzEpl:uy8rgzxulOhG1qIUsCkcdQ38ll
MD5:	C80A147599D6A06EE9102A1D51A5BDBD
SHA1:	A8DD93A49DC4F244B0BE19C0D49A11DC4D200E90
SHA-256:	8DE42FA4B86133BE1B4AE7A4AA72EEEF3179671F66590FA02ACD87C3A1F31B12
SHA-512:	373307E04D92957AF4CFB8D5508F310394D2C978438CBC6B7CD0A39E4EDD0740DE23CB4CD0C13278740F01BF4DCE65A4B4F546AB31B5DAFCF5329B6D21815AE
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\pagosaceptados[1].png	
Reputation:	low
IE Cache URL:	http://https://www.sabro.net/pagosaceptados.png
Preview:	.PNG.....IHDR...../.....g.....#.IDATx...XTW...P.M...c....{....XRL1...i..."X...FE.X@....(ET...(X.K..f.>4...9.;.).....<.y.{..{.....s.....O4<.Vf..^...>CY.....?.....O... ...i.Y...[..."..........v..se..J.c.;.Q...b.)K.*..P.\....P.....y.MK...+..]e..h.L.7.x.~..ud....=..a...h.):.,...|..N..|.p..+I|...F.n0.....u..).W...`.c.{..Z....m=.g....,..2t....F.2....d....V@.>.:._+.=..e.!.A.....j. U...0..O./z..R5.<...e...@Qzu....o=.lc.r.<QTTD}]..........V{..^..^?.E..t.....t.M..[.foW.s..=..R.....<.[.9..t@.....k....Q=...>....c.4.^.)...e. @'?U...5.....{.<O.`.....Z-....@'.`...4.Z.g.....].... .....y?F.y.V^.qW..:...'..!.....9R.....-.;.:xlVA.E...4#.R!...t.L.z.....D....F.,.L5.n!C^....).e/.X..e...Ef.UJ..mf....')].g8l.UR..(....W.t....1..lZ<Z.<.....g.eL..D.6&....^.'.^.Q..fcFE.l.y...t.Sg.>: .5}v.....g.J...{./?...F.s..=.k3...C.;xaO.A.-Z...f...ex-NGc>e.wD^Re..3X....?-.t:....d.....3....Wd.!W:....bk r..\.,.x5.Z..K....T..ML'.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\popper.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	19188
Entropy (8bit):	5.212814407014048
Encrypted:	false
SSDEEP:	384:+CbuG4xGNoDic2UjKPafxwC5b/4xQviOJU7QzxzivDdE3pcGdjkd/9jt3B+Kb964:zb4xGmiJfaf7gxQvVU7eziv+cSjknZ3f
MD5:	70D3FDA195602FE8B75E0097EED74DDE
SHA1:	C3B977AA4B8DFB69D651E07015031D385DED964B
SHA-256:	A52F7AA54D7BCAAFA056EE0A050262DFC5694AE28DEE8B4CAC3429AF37FF0D66
SHA-512:	51AFFB5A8CFD2F93B473007F6987B19A0A1A0FB970DDD59EF45BD77A355D82ABBBD60468837A09823496411E797F05B1F962AE93C725ED4C00D514BA40269D1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js
Preview:	/*. Copyright (C) Federico Zivolo 2017. Distributed under the MIT License (license terms are at http://opensource.org/licenses/MIT).. */(function(e,t){'object'==typeof exports&&'undefined'!=typeof module?module.exports=t():'function'==typeof define&&define.amd?define(t):e.Popper=t()})(this,function(){'use strict';function e(e){return e&&'[object Function]'==={}.toString.call(e)}function t(e,t){if(1!==e.nodeType)return[];var o=getComputedStyle(e,null);return t?o[t]:o}function o(e){return'HTML'===e.nodeName?e:e.parentNode||e.host}function n(e){if(!e)return document.body;switch(e.nodeName){case'HTML':case'BODY':return e.ownerDocument.body;case'#document':return e.body;}var i=t(e),r=i.overflow,p=i.overflowX,s=i.overflowY;return /(auto|scroll)/.test(r+s+p)?e:n(o(e))}function r(e){var o=e&&e.offsetParent,i=o&&o.nodeName;return i&&'BODY'!==i&&'HTML'!==i?-1!==['TD','TABLE'].indexOf(o.nodeName)&&'static'===t(o,'position')?r(o):o:e?e.ownerDocument.documentElement:document.documentElement}functio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\protect-html-code[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	"LEAD Technologies Inc. V1.01", baseline, precision 8, 336x280, frames 3
Category:	downloaded
Size (bytes):	39135
Entropy (8bit):	7.934634415782034
Encrypted:	false
SSDEEP:	768:GuGyyA6NUk4gib+zs5NMQuRAtw4LndbJ9zfAr2a:GDyVk4wzWNlu0LnHJArn
MD5:	8597D78B02C357B70D33C8098321D845
SHA1:	626E6CBDBC40740E31671C94DE5386C8C23D6E21
SHA-256:	FBDE526E61054686DBB082448B7A755A976655EB74BE0CCDE0039F39659A2AD8
SHA-512:	6F88F57687AA34ABACBE4DBA3FB61730F7D74758E709A65D9EB7B81F9948B64D4E765F1C0D4BFFC337265C536A2C129C89C3044F9B7EC3A30E2D19EF6709ED C
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.htmlprotection.kom.gt/protect-html-code.jpg
Preview:	......JFIF.....K.K......LEAD Technologies Inc. V1.01.....LEAD Technologies Inc. V1.01. .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....P.....?.....b.....(.....(.....(.....(.....(._F.5?.j.Z..g-.}7.oo....3.'lq..w..UU,H.....\|....V.....i.j1<..#...".&....*....Ws*.\|.<.Z.$.....7R..:.(.*.(.....(.....(.....(.....(.....(..... (.....(.....(....5..k....!$...I..F.D.t.M#...e.....~.\|".:.\|6....{Y._..oo...BZ=>..G..\|..%S'..2<j.a.I....N.s...s.:..,.Qm.$....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\runner[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	12598
Entropy (8bit):	5.333640345174584
Encrypted:	false
SSDEEP:	192:qzUTG4haDWBlv6O/wVcOfvUQ9kLukCgOky0ou0PGJG:qz4Bn60CEokLukBOky0Q
MD5:	EE62E165D3AFFC78617C9CB39E79601F
SHA1:	8CC5FA05C0FADD382F46C322915602C454913D48
SHA-256:	49E1DCEF611A905B866974D135554059ECD77A0AE022553178EC359EA0B64504
SHA-512:	1E3CDAF0C836F05C027BA12BFEFA402E708DC7F5267BE345A3973D268B33A1EB14FFC8CBAA0DB7239F38D639B56EA435B67C6125B943A14054037F3FAA03D9 A
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\runner[1].htm	
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/sodar/sodar2/221/runner.html
Preview:	<!DOCTYPE html>.<meta charset=utf-8><script>.(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.'use strict';function m(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}function p(a){var b="undefined"!=typeof r.Symbol&&u(r.Symbol,"iterator")&&a[u(r.Symbol,"iterator")];return b?b.call(a):{next:m(a)}}var aa="function"==typeof Object.create?Object.create:function(a){function b(){}b.prototype=a;return new b},v="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,d){if(a==Array.prototype||a==Object.prototype)return a;a[b]=d.value;return a};.function ba(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var d=a[b];if(d&&d.Math==Math)return d}throw Error("Cannot find global object");}var w=ba(this),x="function"===typeof Symbol&&"symbol"===typeof Symbol("x"),r={},y={};function

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\rx_lidar[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	112790
Entropy (8bit):	5.322769043067991
Encrypted:	false
SSDEEP:	1536:eOeMxqb2pcYndxLmNyMVuI2MckdI1+uJBFtG2eFHRynmxfZ:nG2p/LmMmukck0edRynmxfZ
MD5:	098C8F5916BA74220D6DBFD049030526
SHA1:	8E33227C28DFFE40682507A94777378CF8B425B0
SHA-256:	C04C7A578734441A2E3C552AB6F21AB2267C67F786CBADD64D4166D9721F7113
SHA-512:	910204EB6D78F9F9A61BF41E69BC33F64DB3E771D766B3F68676C5E270A8D92E34F2B9AFDBFF63C802945459FF91B5B3FCE0C14BF82BA9D9A0F48F0F177EF62
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.googletagservices.com/activeview/js/current/rx_lidar.js?cache=r20110914
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var p,aa=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}},ba="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a},ca=function(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("a");},da=.ca(this),q=function(a,b){if(b)a:{var c=da;a=a.split(".");for(var d=0;d<a.length-1;d++){var e=a[d];if(!(e in c))break a;c=c[e]}a=a[a.length-1];d=c[a];b=b(d);b!=d&&null!=b&&ba(c,a,{configurable:!0,writable:!0,value:b})}};.q("Symbol",function(a){if(a)return a;var b=function(e,f){this.bd=e;ba(this,"description",{configurable:!0,writable:!0,value:f})};b.prototype.toString=function(){return this.bd};var c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\sabro-contactar[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 240 x 180, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	8824
Entropy (8bit):	7.935161110942905
Encrypted:	false
SSDEEP:	192:j4ohxDdkTlvpv3YnVyWfUEhbAU0CHxUauOUpc3:1xxUbleRb44KaXUG3
MD5:	6824D7BAEA289DDFE921DDCE2C3A67AA
SHA1:	939600EA04417BA35FE32FED0E524FE50E727A33
SHA-256:	1B00D335A84538A100F748C43694E5D960106D463EB9829322270BD0219A3FB2
SHA-512:	7AC5E5504F1FC8189A729AA4C44A1A03A7A22D443A2422A71367D414BDDBEA4750FC7959B0433EB8C8DB130A068AD927217B4321EF69FF80D70D4E4E75B38B1B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.sabro.net/sabro-contactar.png
Preview:	.PNG.....IHDR......"?IDATx...\....c.H..A..-{.2...*[.. ...9rd...9s..'K-M.r..J-....p...~..y.~....r.=.....>.9.9.y.ddd.k..! ##.....`222.....&###.....`222.....:.....<.$...$.n....<.K+D@."...Z.....\.oW.5p.-.....\....`2..i.w.._..O.~..N8T.|:.87..0.(.(q...d.aw..~K.AkS..:....+....~.1....9s...-..o kh&I.5,c(....5s&..9....7.(....Z?.\]..._....JKK.}.6$.....&0.lD.p.t...`k...AX.`.n.j@.R.....E#.S5.g...g.^W.$...Ns*+.....01.._..n...i.H.X....j.....S..%...0f..::.;.]=<HR w..X....[g{.....a.....Q..z....^.R.p.....i..H.B.....Z[..s.K....c....R..h.U$..X"G^..x..E032...XZ">6...a.,..hX.Px...7i..,))...T..h.....!)1..z)....p.....b.XV.f#2S.Lat.....}>..j...M4M".e.`v.....a.....ap.=.....Tx.f..W...h..1e.....If.Z...~n....(<.....jTD..[.....A...+.....qO.x`J.-.4@.X..N.....p.h.t...ks.x....rBl.....q6.....N....S.f#.....D..Fa..{..%.....$...nX.....<0..k.2 ...Q.....i..=.Ys`.1.Uz.. D.....N.V

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\sabro-desarrollo-de-apps-guatemala[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 240 x 180, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	6958
Entropy (8bit):	7.92347931132811
Encrypted:	false
SSDEEP:	192:pGCzR2ELMdlplu6f8NqSY/pfJC6QiSUlz:IsR2ELYlfugjgUlz
MD5:	FB46E3EB44A061F263EC05E221815FD5
SHA1:	B7B41195965087DDCE70D38C3798ADC2824DA7D5
SHA-256:	367AC30F476EEC80F7A7ACD25A2B5301B3A9F7EEC46E050A19C9BFA5BD8EA98E
SHA-512:	DD1AE8E9C366BEBCD97953FFC7F4E3D28A3B53988D91C120DF4E22A5DE21574178EB020331A2016FE5E8799528768FD86F196A37C2C5E7CA86C704037C28491
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\sabro-desarrollo-de-apps-guatemala[1].png	
Reputation:	low
IE Cache URL:	http://https://www.sabro.net/sabro-desarrollo-de-apps-guatemala.png
Preview:	.PNG.....IHDR.....IDATx...X.G...Q.>..U.(.`.x!.<.V.x#(.....1."......[.1j.5.K..C.a..x%.c.L.....e.zfz..f...../.Lu.]...W..k.(.Jo../.....P(...B!.(...B..`.....P(...B.Q(...B..`...F.P.0..B.Q(...B!.(...F._.=.....?~.....'O. ....c.w.....(.#.o..- &&.JKK..2..-[. .(.EF...<h.54i..Mn.....@...S.:/....|..%.....KIIa^..`.X.t..]...@HyX...5.."..p.*>>^i.....0.X.^}...Z.5....h^....`_}.....F.....}H.,.}.v....m...]...;.Q.F&..w.}....n|...R....a...m.....Q1.5...g..P.p...sT..G.....2.@.Z.<y.;...8"s... .....{....P.. .n{.....(.srrx]k..S.0..Ug..?.....^F_2.....m..P.w.....a.x]k..@...Y.d.../...BB-..N....;BYd.(..xxx.....?.....:._@K.X....OEi!..0..'.....u,....=.....0A...?W.W.....F...`...F..`....#..0.`._.@..cQY..L.....G..`...P&.[;{4%fjj..#...0...#..0....`....4...N.v.t4%.....F.u.`..H.....<..F..`...F!..0.....x.....}.d..F.....g.0.-....o...Mbb"s..`T=.....pee%...*m.....+X.5...F.....`ff..}SSS.....B.u.`2....K.....0.a.vu...Sb

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\sharethis[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	514
Entropy (8bit):	4.652760602700894
Encrypted:	false
SSDEEP:	12:t4IRMXV+DVFaqHI7R6Ibdb0uJYQpJNnfbkvK:t4IuXV+x40uEIb2VQpnDki
MD5:	DEECDAA377907DB5CC1722FC831670A1
SHA1:	4E39E0FD5742CC1460E24620DF4A360ABB71290E
SHA-256:	9A83C65BDD0FF9488AF9D25720686457EA7295C9C44F9F1D285A0C9EC89BAB99
SHA-512:	99EA54787E6FDC2E8118961E23EDCD81D56E5CDB2BA0892CCB9FF7F254718D50B699697B1A937BEA31D62A4399A36B597A0ECDEBF72568EF561211FA3520755
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://platform-cdn.sharethis.com/img/sharethis.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" fill="#fff" preserveAspectRatio="xMidYMid meet" height="1em" width="1em" viewBox="0 0 40 40">. <g>. <path d="m30 26.8c2.7 0 4.8 2.2 4.8 4.8s-2.1 5-4.8 5-4.8-2.3-4.8-5c0-0.3 0-0.7 0-1.1l-11.8-6.8c-0.9 0.8-2.1 1.3-3.4 1.3-2.7 0-5-2.3-5-5s2.3-5 5-5c1.3 0 2.5 0.5 3.4 1.3l11.8-6.8c-0.1-0.4-0.2-0.8-0.2-1.1 0-2.8 2.3-5 5-5s5 2.2 5 5-2.3 5-5 5c-1.3 0-2.5-0.6-3.4-1.4l-11.8 6.8c0.1 0.4 0.2 0.8 0.2 1.2s-0.1 0.8-0.2 1.2l11.9 6.8c0.9-0.7 2.1-1.2 3.3-1.2z"></path>. </g>. </svg>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\translate_24dp[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 48 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1847
Entropy (8bit):	7.840750948954508
Encrypted:	false
SSDEEP:	48:0BUfsw9mAtN6tl4XZACwezLhPa0V7dHy+1pqWv33z:0iT8+6QJcmLddquz
MD5:	BFA09D19AEA98592C45CE0A814F0EB2C
SHA1:	5DB965A451D9B6B3A5156836182ABE8240D4A0DE
SHA-256:	5FE03BFD95A2D4E640ED7D04DCB08EF991C327A5AB6F6FDB9EB06E1EFC76AF30
SHA-512:	65FCB486B6E1120FE47897BCFE75E310AC72D23213A72754729EFE89E019A431E700202A879A94407F46277ADFAF3B03B5248775645555EB5F8698AA0FE4913B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/images/branding/product/2x/translate_24dp.png
Preview:	.PNG.....IHDR...0...0.....W.....IDATx...s#I..{....Yf.C.L..h.0.;...f....0$..s^.I.V.JVT\....5./..'h.....G....5F'..z.%?.8...o4..zC.....v..#...5w.).Y...$.'..&x.b....m.....K.....M.#.....?...J.....\Ha.|...W.x...#...]....F.B%._.k.....P...3.g....\"0...H/...w..A.....{100..)LMMazz.W...I.....M...&..F.0.B...w_. G.....Ocff.!$. V.z{..,0.!.jq.y..K...D{..}..B.....1..*....4...1x.".s7.....6.*w.....;.v/F.&(..@.A...O.T.~.....a%.w.(;. E..:...QW..^o@ty\;.b..b..%UH..I....Nw.X.C.F.('..B..F.m.8]^..!.,L..F.<+.p6f.=.u.c.]?.v._..5.....A.Dzy.....':Oy...zh.....y.....`0..|i..2.eUp`)?<.a8}ylr.....B!...1Dv.P..6.p..M.O7..Q.<.....-^.`0^...j..5h.G. ....R<S...h....y.Y.@`.@Aq.OB!.O....+4"+.T..31....f.xG,m.....~Q..o*..}..~ .D.....x..Q\.(*o...R*.6....@.<......./.^^1... ..!^L.*.....e..a.'R^;._..o...U..Jd.V...L..F.R^r....]...>.F..Mj...3Q..W.)N4.(vx.q..Y.h.goEq.;.....y.....P3...hi.....$..I.!...W..J.CL.OB.mq..gbR:.<..;..v;r...]..jd

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\wpchat[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 60 x 60, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4132
Entropy (8bit):	7.93222074748894
Encrypted:	false
SSDEEP:	96:a0mNnVLvXAupZhkCSacm+sdzq5rCRQfxVMEAZ:a0aLU9sdzqnrMEAZ
MD5:	133C4C20B3DA2337F7974FC55D7783F3
SHA1:	C8D57FD0907B40389FF3EE10E5C0E2072B8B31E4
SHA-256:	146FD1695B6A3BA8CEA6E5777697FB7C157AB4A6A77BED911B810F0B1A3FB08F
SHA-512:	4DD90E0C0B0F7419FD3704300AE894EDDB6DD0291A37B2E2EB16E842EB06E6B6F02B11B3CCE79D7EDE83877893C97BB55E5D3EB3B42247912A1CDED08AD29C1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.sabro.net/wpchat.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\wpchat[1].png	
Preview:	.PNG.....IHDR...<...<.....:..r....IDATx..[.PSW..}.,.....E..&X.\paa..]...}..Zw..}...;v.j.I]...V..:X.x8.....|8.q.H.q..B.. R01..I.....$...vg.....s.....?_.,....g!..<y.Gj.:...o..`...+..a.a._....>.N. ...+....w..#..i......./.g.Z.;.....`191I.Mc.`.\|ll..X1G...7\.t)\|.u...r.....{.$..<.&.O.-.KaYY.o..k..-...E.ET.....M...._..e.....4222+...Q.e.@.....A..zm.\..J....V...al|V.o..R*.?....@...k3....=.. ...HH..C..'..'I# .?s!...sAo...}.r...R..f.....1..q.cb...1u.;.o..6.Aj..R.!.d}4<q!..9.z.I*..O.....r.Y(.....:....w..q.....O#m#....q.....!U.M=J.g..x5..~..4...I...O..M)..C.N.^....;...d.o...$+q..R#.. .HH<.MW.I.%.M..j..E.m.Q.\.rk.!.>..V.[.w.wO.*i.nB.v{....Bo....@..1*.....P.Q..N.).wWz.?.....'...3.pF..-d0KII.^0Y.B.k4.....z.=.R.FX[.....hP..v.\..t>92.a..U.p.9.I.6.-N.....h..... ..zSH.j.@FM2..B!^...I.$.0.....x9....zw5mC;. .....8..T..I.2...c?<.H..i0U.W...z...V...r]zP'.K..Q.....w..zV....l]]...p....f...4..q.*X..c.!.C.;..s"...].'...BP].!.P?......6..q.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\466606[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	42
Entropy (8bit):	2.9881439641616536
Encrypted:	false
SSDEEP:	3:CUXPQE/xlEy:1QEoy
MD5:	D89746888DA2D9510B64A9F031EAECD5
SHA1:	D5FCEB6532643D0D84FFE09C40C481ECDF59E15A
SHA-256:	EF1955AE757C8B966C83248350331BD3A30F658CED11F387F8EBF05AB3368629
SHA-512:	D5DA26B5D496EDB0221DF1A4057A8B0285D15592A8F8DC7016A294DF37ED335F3FDE6A2252962E0DF38B62847F8B771463A0124EF3F84299F262ED9D9D3CEE4
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\6926156095005395524[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 300 x 250, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	25733
Entropy (8bit):	7.972440898372335
Encrypted:	false
SSDEEP:	768:LPCfArQu4couEXxt6UZ/oPzXIV+oKy500k:zdQ/dXl4Yv/o
MD5:	82E1081C8FF4B1F820798EC37E1DCAA2
SHA1:	AD05DFF1A97E9FE2BE1687009431B2DE2336A819
SHA-256:	BA1DCDC04F83D281EF034DF26D56870060E6CB7A7142BFCB1F2ACD47CB91225F
SHA-512:	F8304DF85B7A74AF2BC23677804D88F2FB50FAD633FAE36CA44274E4196C4497829ABBEB524B59B9CD906B2614466E571C5C1CC89840F6FCDDAD15E060887C9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/simgad/6926156095005395524?sqp=4sqPyQQrQikqJwhfEAEdAAC0QiABKAEwCTgDQPCTCUgAUAFYAWBfcAJ4AcUBLbKdPg&rs=AOga4qnum8tmS6Mg4B7yx-zuQ3JaRYjJKw
Preview:	.PNG.....IHDR...,.....,.....PLTE.B.D.pC.qR.ZJ.f1..3.....2..$..7.....G.l0..''..F.m-..<.\|S.X:..''.,..B.t(../.....>.z&..*..M.bK.eO.^+.....;..?.x...N.`&..!.. ..U.V...P.]...E.o...A.v9..+..... *.....A.u.....H.j8..5..J.h(..Z.N.....8..;.~H.kD.q...>.y6..X.QV.T.....=.{...B.s...?.v'..I.i@.wY.P6..4.....L.dW.SO.`...Q.]......4.....4..\.K.....I.h...$..6..%..:..^.G...1..E.n].I...5..G.m...L. d`.EN.b[.L.....b.A7..)..<.|).....P._...T.W.....'..;.....=.}.....,.....s.....H.....:..X..r..:.....S.....{.z.....\.MN..&K.{.....+.....j..D..b..y.....b{.o.... ....b.....:..Y.t.....L.|O....G.....f..E..9..;..T..X..N.p`..e.hR.....>..e..E..`.....Ki./..l..7X.p..D.....y..Ol....Ed.....So.7.....Yt..a.\v.4...O.z.. .IDATx..y|UU.6|PB..a..@&!..b@..@$LN.L... :- C.....6..>p !1..CHH.L.Dfdh.A.yjQhP.....{.o..Zk..g.Hw...m.+..m._U.....EG.GG._.U.w.[.n..Q..usb....\)9)99i...]&..7n.!3.V..GB.....0.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\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):	1716
Entropy (8bit):	5.236653158630815
Encrypted:	false
SSDEEP:	24:7E+7RWUISwb1/Erjx2dFenI05DJA1kmN1HnEF8a8Lc5O48wU3rkaBS8v3l1JpM0y:4QwUk/EJ2kFDi1kmQ/b5t4B3lut
MD5:	E03F7BEB0F2E0FE4FCB5D64BA2E7D365
SHA1:	CDB2D89E08F004EC3466A6691BD2507EC2AC13F3
SHA-256:	C8BF030AF678E755BE81886A4DC95052A252B3C3D87743844223AAF11644289D
SHA-512:	1EA42F3D846C14753367F4F31EE77844089C5CD328EB11FD45EB112BAEB651E19FF3B73BBFDD73F4B9EF2F6643AE8A19525A2A96856337EA0AB63786A3E674FE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://rf.revolvermaps.com/0/0/7.js?i=5jvn1rlqz5o&m=6&c=ff0000&cr1=ffffff&sx=0
Preview:	var _rm5tat30bj_=_rm5tat30bj_||{a:{},b:[]};(function(d,o){var e,a,s,t=d.getElementsByTagName('script'),i=t.length;w:while(i--){e=t[i];if(e.src){a=d.createElement('a');a.href=(e.src.match(/^\/\//)?'http:':'')+e.src;if(a.hostname.match(/\.revolvermaps\.com$/i)&&a.pathname.match(/^\/?0\/0\/7\.js$/)){s=o.b.length;while(s--)if(o.b[s]===e)continue w;o.b.push(e);function p(t){t=new RegExp('[&\\?]'+t+'=([^&]*)').exec(a.search);return t?t[1]:'';}function b(i,t){i=d.createElement('iframe');t=d.createElement('canvas');t=t.getContext&&t.getContext('2d');if(t&&!('IntersectionObserverEntry'in window&&'isIntersecting'in window.IntersectionObserverEntry.prototype))i.onload=function(){(function l(a){if(!d.hidden){a=i.getBoundingClientRect();i.contentWindow.postMessage(a.top<window.innerHeight&&a.left<window.innerWidth&&a.bottom>0&&a.right>0,'*');}setTimeout(l,400);})();};i.setAttribute('style','background:transparent !important');i.style.position='absolute';i.style.top=i.style.left=0;i.style.width=i.st

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\IGI3DLXG.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	14929
Entropy (8bit):	5.23889933831256
Encrypted:	false
SSDEEP:	192:nNJxgO4JY5Mzvh9OvDqmINvGPECz2ARnuQd8apKsD:xT5Mz59OvYvuduQddF
MD5:	CE6C5273CBC5A5554AEA307A3B91ED83
SHA1:	C814D9448719ABC675EBF34C3D5F3570D4419D6B
SHA-256:	FCB1BB8D0C9466682D38312C8855167EF69B9B34A5CBF577AC8EB736736C59E7
SHA-512:	08C7C7153A3555B7DA0475741C22501795ED31DC198849739EE30C2B62CECF9D40A2390B3BB419AC624A37087037F66121E50AE59CEBF31BD4BE946DF7EA0B6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.sabro.net/
Preview:	PAGINA DESARROLLADA POR WWW.SABRO.NET (si necesita una pagina web, visite www.sabro.net) -->.<!DOCTYPE HTML>.<html lang="es">..<meta http-equiv="Content-Type" content="text/html;charset=UTF-8">.. <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">-->. <meta name="viewport" content="width=device-width, initial-scale=1.0"> -->.<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">...<meta name="format-detection" content="telephone=no">.<html> .<head>.<title>Hosting en Guatemala, Dise.o de Paginas Web en Guatemala, Registro de Dominios .com.gt, SEO, Desarrollo de APPS, APPS Android e IOS en Guatemala, Correos Corporativos y Servidores Dedicados | www.Sabro.net</title>.<meta name="ROBOTS" content="ALL">..<meta name="description" content="Somos una empresa que desde hace m.s de 20 a.os desarrolla Paginas Web Profesionales y Aplicaciones Mobiles, Todos los sitios que

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\activeview[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	42
Entropy (8bit):	2.9881439641616536
Encrypted:	false
SSDEEP:	3:CUXPQE/xlEy:1QEoy
MD5:	D89746888DA2D9510B64A9F031EAECD5
SHA1:	D5FCEB6532643D0D84FFE09C40C481ECDF59E15A
SHA-256:	EF1955AE757C8B966C83248350331BD3A30F658CED11F387F8EBF05AB3368629
SHA-512:	D5DA26B5D496EDB0221DF1A4057A8B0285D15592A8F8DC7016A294DF37ED335F3FDE6A2252962E0DF38B62847F8B771463A0124EF3F84299F262ED9D9D3CEE4
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\cavalry_endpoint[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1 x 1, 8-bit gray+alpha, non-interlaced
Category:	dropped
Size (bytes):	134
Entropy (8bit):	4.031662511415954
Encrypted:	false
SSDEEP:	3:yionv//thPlE+tJ8/mGGlk4hvM/jMiy/v//thPlE+tJ8/mGGlk4hvM/jp:6v/lhPfA/mR+4hvsjYv/lhPfA/mR+4hm
MD5:	49070A0A6EDE47C47483ABA531D53B9E
SHA1:	96716E85E5CDEEA972BB5816B07B163130F1D5AC
SHA-256:	4BF8E2805424511F61202E2B3A40E27A28266E28FAA7AF5864BECE21D443AF26
SHA-512:	90BFE178F733904CF567D729A8A5A769696037A957D6359CD7933C68AE3BC3129B1F8679CC9BED05800D39917B938123578D044F45D523DFF1A9D750F282D199
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....IDATx.c.....-.....IEND.B`..PNG.....IHDR.....IDATx.c.....-.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\f[1].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	259062
Entropy (8bit):	5.507511335062714
Encrypted:	false
SSDEEP:	3072:RmtPMjFMd4I7aIgYpgezbrxuepe0jndMWuwlTunh4JajdsYZ+uEuw7CJ:w1qI7aId/rtprjndMWuw2jdsQ+uEuweJ
MD5:	9CE3F60A2E90DD847EE94BC5016631E5
SHA1:	D2D8178A3B326A6DDBDF533B7D6FF73FD372F389

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\f[1].txt	
SHA-256:	A902A4E7039D3108CF7CC55A6EDF7398696C9DCC08698EFFDA100C6C518E17D2
SHA-512:	F92578A3B2D7F492DAEC6698825BE59A6DD80CFCE5BCAB8B4B3DC310CF43BA97851F9E1AD2BC6198811C0328AD55061CC0EE6BF4F7110C9524C7C8FF2E923 F2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pagead2.googlesyndication.com/pagead/js/r20210303/r20190131/show_ads_impl_with_ama.js?client=ca-pub- 6373591680915711&plah=www.htmlprotection.kom.gt&amaexp=1
Preview:	(function(sttc){/* . . Copyright The Closure Library Authors. . SPDX-License-Identifier: Apache-2.0 .*/ .var q,aa;function ca(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}var ea="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a}; .function fa(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");}var ha=fa(this),ia="function"===typeof Symbol&&"symbol"===typeof Symbol("x"),r={},ja={};function v(a,b){var c=ja[b];if(null==c)return a[b];c=a[c];return void 0!==c?c:a[b]} .function y(a,b,c){if(b)a:{var d=a.split(".");a=1===d.length;var e=d[0],f;!a&&e in r?f=r:f=ha;for(e=0;e<d.length-1;e++){var g=d[e];if(!(g in f))break a;f=f[g]}d=d[d.length-1];c=ia&&"es6"===c?f[d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\f[2].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	23351
Entropy (8bit):	5.411620587937627
Encrypted:	false
SSDEEP:	384:l9vNB4ViWplMmb4S2b6d+gJR1MRHkYxhyDdFcKPlT20RXLyf9My4RWy5Ln:DMV6241b6d+gJ/MRH9TKNi0RyRKhn
MD5:	2D07BFF05E98E65441CA17F14B12B891
SHA1:	1F99233DD1435A3337D1A415E7B51692395F11B6
SHA-256:	99E67DF72815199659CB76A1E9444B134A431B3E5AB7C15D76C8CDCE6E8DAE87
SHA-512:	34B4CB6077E6FC03AFB7EBA56B781122580B7F50D274AE6D106DDD539AD8FAE804182B74B9728A14F6E7AF8AE7926F58064E621AD4AB965AAEABC4F31695EA2 1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/pagead/js/r20210303/r20110914/abg_lite.js
Preview:	(function(){/* . . Copyright The Closure Library Authors. . SPDX-License-Identifier: Apache-2.0 .*/ .function aa(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}var ba="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a}; .function ca(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");}var n=ca(this);function da(a,b){if(b)a:{var c=n;a=a.split(".");for(var e=0;e<a.length-1;e++){var g=a[e];if(!(g in c))break a;c=c[g]}a=a[a.length-1];e=c[a];b=b(e);b!=e&&null!=b&&ba(c,a,{configurable:!0,writable:!0,value:b})}} .function ea(a){var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];return b?b.call(a):{next:aa(a)}}var fa="function"==typeof Object.cre

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\f[3].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	35427
Entropy (8bit):	5.469090069926346
Encrypted:	false
SSDEEP:	768:MMlFCLimY5EZMW6GMPstNu4581rrAhXxP:MMlFMY5JGMPIl5
MD5:	C3DD1F05F09C6565A1535091B909EC54
SHA1:	EE867704BBA8974AA5A01FE95D5CC2B1D94830DF
SHA-256:	E05B08A52C8F9335A62D42D228D85CE9710671D6B63869A56795D946389968A5
SHA-512:	876C5892DBA13D16553692BDFBDADC9959BFD6177FDD5CAF5E28377426F6EACDFAC2367F1C2F8DA5BA6690781AA8C25C6606926235864F63CA8C711185A7D4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/pagead/js/r20210303/r20110914/client/one_click_handler_one_afma.js
Preview:	(function(){/* . . Copyright The Closure Library Authors. . SPDX-License-Identifier: Apache-2.0 .*/ .var q;function aa(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}var ba="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a}; .function ca(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");}var r=ca(this);function t(a,b){if(b)a:{var c=r;a=a.split(".");for(var d=0;d<a.length-1;d++){var f=a[d];if(!(f in c))break a;c=c[f]}a=a[a.length-1];d=c[a];b=b(d);b!=d&&null!=b&&ba(c,a,{configurable:!0,writable:!0,value:b})}} .t("Symbol",function(a){function b(f){if(this instanceof b)throw new TypeError("Symbol is not a constructor");return new c("jscomp_symbol_"+(f||"")+"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\f[4].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	142594
Entropy (8bit):	5.559354647703777
Encrypted:	false
SSDEEP:	1536:gPLtuT2Zr32i1q7M3F+zjVfK0VZRqwxk9PgBMPjtkeDc8nrr1cnZ8lhYAg1bDNeI:KlvOtL89PFdoolsxw97+Jvy7IlegdRJ

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\f[4].txt	
MD5:	42E88857DE74194D29DEBC44486B38E6
SHA1:	EA57BC51EB7DF1E8625B4404D8C2567AFDFD034F
SHA-256:	3DB11ECEA20A0BE8499F350468EC4B0739722A15256ECE378C6D4F4C0174C0CF
SHA-512:	1853CF59B62BA8D58CFF08322EAC8EA131F9415DCA57588787C901293DEEFF269AC85ECFF3A1704990D71588A3F0160D21117AC80268885E784FF5443D1D7F54
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js
Preview:	(function(sttc){/* . . Copyright The Closure Library Authors. . SPDX-License-Identifier: Apache-2.0 .*/ .var n;function aa(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}var ba="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a}; .function ca(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");}var da=ca(this),ea="function"===typeof Symbol&&"symbol"===typeof Symbol("x"),q={},fa={};function u(a,b){var c=fa[b];if(null==c)return a[b];c=a[c];return void 0!==c?c:a[b]} .function ha(a,b,c){if(b)a:{var d=a.split(".");a=1===d.length;var e=d[0],f;!a&&e in q?f=q:f=da;for(e=0;e<d.length-1;e++){var g=d[e];if(!(g in f))break a;f=f[g]}d=d[d.length-1];c=ea&&"es6"===c?f[d]:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\f[5].txt	
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):	10099
Entropy (8bit):	6.014649937403052
Encrypted:	false
SSDEEP:	192:+a2jwrx2lYE9bT5K2BQ4RLXke/T02Wa5FbBbHIt+/WBbnxV3is0YQ:KwAF1DLUC3tLixNT3nG
MD5:	82A613F1AE38AE5E8DBB436754CAFC17
SHA1:	AF09B928251B128C3571A444E7BCA347FC01BCE3
SHA-256:	A933F59E8A8819CDB1A1B2D09AE27C27FA4B32BE7892F9960E6B67C30CA55878
SHA-512:	9A199528ECB6472F2649A902755C52F081D740F18F5BBC5D64E7FEECF1855FFABAB9F4304307B58F70A51AB4AE501B187CC579849DE672784DFD599DF1EDB3DA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pagead2.googlesyndication.com/getconfig/sodar?sv=200&tid=gda&tv=r20210303&st=env
Preview:	{"sodar_query_id":"o2lBYOezKoOdgQfuvK2gBQ","injector_basename":"sodar2","bg_hash_basename":"NbavSCglibpGXIPgvdnCekV4Trd9FdFp1lnuZbQf9E0","bg_binary":"pPPrCz6NMasvVYXAberyiYsqbLlQhRagiRw4FxRJbMFmkf7gtb/cGDyWBp2PUUyQa++bhwHfL3t6C0xy5zDNa2dqjvnQ1zuIC0ntE57sA4a800GEj+lcMN3cXYCsaec6wLhoT6CxkSgbsKh5ciDvrhIn5KMMmgHEIj+9O3GrbK5F4BtpyjvgEKfbmVvueKw8sJyuPIxg/9mKP+Lj6CpT3ENBC1evCKqD2rTHzi1/12j2yqLVC4NhB34+eLDfKCWKmG4j1NUU+d+o2WxlwA6PEVSN/3fTV4wXbwvoFCPZ3Dfv7CtsMuHsTS3wCsblzR6uNHKzltfntMEF8XZO4/d5786gCHikL4polVaq8f3LVDZ7GZKFuQSfcSUXziHz7XVG74Pdn4LAYqYBAWdPCYa3aJi3aGY6GhxMTwmM7E1cJwVGBcWXwnpJflq2HqkSeEZOH2pSDgOFa6yOedB3Ki0lpSp84UwHRyXU8chtIXB4fuZU/OKUu0KR7589u4ClUACeYM76E6tbC/BzRK9HkTP7TbVaKofGfRNF22yJpvSA5/L4hEZLkIlWaYLnco7wClYidsj+fzWDOO/AtxY5iEB1Uhtqt/VbJbZv5P+BWQ0g+CH+gBdA1gR1kS8H3m9v2dqikLCFKHHSzmJTfwtFDH5V6oT9EDxcIASVn05BA/BEeaeWXhibzxPlZ+xGirBfd05Vgdgpy6Nr3H/dk5Qnqb1T6TyElgcClP1QxKumhtXgQmVEm7SN+0kajBGfpmfRMjR2r5HtfUQXWOQXifsIc/7THCmyqqnLVd81rw2R45KpTY+DC++9TGrc8lUiEayfBKGmiZQKmnoM0OEYJqZgr6

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\free-v4-shims.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	26701
Entropy (8bit):	4.82979949483045
Encrypted:	false
SSDEEP:	192:SP6hT1bIl4w0QUmQ10PwKLaAu5CwWavpHo4O6wgLPbJVR8XD7mycP:5hal4w0QK+PwK05eavpmgPPeXD7mycP
MD5:	1848E71668F42835079E5FA2AF6CF4A8
SHA1:	6AE345E2FEB8C2A524E7CF9E22A3A87BAEE60593
SHA-256:	D7CC3C57F9BDA4C6DCB83BB3C19F2F2AA86ECEC6274E243CD4EC315AE8E30101
SHA-512:	24E0AF4EC32A9AAB61D9E1AF9B2083F2D13CC98961B5E32BB613A02FEEF63F5F30C3B21C6308A4A204D981D77C86F09E221D0DB7B051A3538ACE07E727F29F58
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.2/css/free-v4-shims.min.css?token=585b051251
Preview:	/*!. * Font Awesome Free 5.15.2 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license/free (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */.fa.fa-glass:before{content:"\f000"}.fa.fa-meetup{font-family:"Font Awesome 5 Brands";font-weight:400}.fa.fa-star-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-star-o:before{content:"\f005"}.fa.fa-close:before,.fa.fa-remove:before{content:"\f00d"}.fa.fa-gear:before{content:"\f013"}.fa.fa-trash-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-trash-o:before{content:"\f2ed"}.fa.fa-file-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-file-o:before{content:"\f15b"}.fa.fa-clock-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-clock-o:before{content:"\f017"}.fa.fa-arrow-circle-o-down{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-arrow-circle-o-down:before{content:"\f358"}.fa.fa-arrow-circle-o-up{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-arro

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\free.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	60351
Entropy (8bit):	4.728636851806783

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\free.min[1].css	
Encrypted:	false
SSDEEP:	768:5Uh31IPiyXNq4YxBowbgJlkwF//zMQyYJYX9Bft6VSz8:5U0PxXE4YXJgndFTfy9lt5Q
MD5:	4ECC071B77D6B1790FA9FB8A5173F972
SHA1:	B44FCBAAC4F3AA7381D71DE20064AC84B0B729D1
SHA-256:	8C7BBA7DEB64FF95E98F7AC8CD0D3B675A4BCF02F302E57EDC5A1D6FA3D6CF94
SHA-512:	7CC1D04078B5917269025B6F37C7DDD83A0A5A0C5840E2A6E99ADFE2FB3E2242C626F25315480ADCD725C855AD2881DDF672B6FC1D793377C2D16FF38EAF69
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.2/css/free.min.css?token=585b051251
Preview:	/*!. * Font Awesome Free 5.15.2 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license/free (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */.fa,.fab,.fad,.fal,.far,.fas{-moz-osx-font-smoothing:grayscale;-webkit-font-smoothing:antialiased;display:inline-block;font-style:normal;font-variant:normal;text-rendering:auto;line-height:1}.fa-lg{font-size:1.33333em;line-height:.75em;vertical-align:-.0667em}.fa-xs{font-size:.75em}.fa-sm{font-size:.875em}.fa-1x{font-size:1em}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-6x{font-size:6em}.fa-7x{font-size:7em}.fa-8x{font-size:8em}.fa-9x{font-size:9em}.fa-10x{font-size:10em}.fa-fw{text-align:center;width:1.25em}.fa-ul{list-style-type:none;margin-left:2.5em;padding-left:0}.fa-ul>li{position:relative}.fa-li{left:-2em;position:absolute;text-align:center;width:2em;line-height:inherit}.fa-border{border:.08em solid #eee;border-radius:.1em;padding:.2em .25em .15em}.fa-pul

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\hambur2[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 46 x 46, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	823
Entropy (8bit):	7.727536923862813
Encrypted:	false
SSDEEP:	12:6v/7maBm+vAWlEC85rUYmUE09U4VrqlAk517y5NJM4BpIU498z8JRO2V189:om+vAJ5AYlE09U+GAk5h4B0rRO689
MD5:	0F25F72587842453EB7442346ED93405
SHA1:	B17CDF446B359B9FC305859CFB0253A6BEB761D3
SHA-256:	E08FC35EE5406609B77A40D3093C38128D4C74599889581879ABD787B202DC31
SHA-512:	0A73974F4977C7D9322B6E3DC0774D54A8FABA1FEE5BEC7192D215FEE2F80FD73DCC7833C6F176E99D848FF57D55F6D68C029B61ACAE2DDE67674D9A6FA9DC1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.sabro.net/hambur2.png
Preview:	.PNG.....IHDR.....W.+7....IDATx...n.@..y.B....).....(.l..V..R/.....>.^..tg..b.8>.*.!...~..3...D.R.^..18q..I..8..,....S.8...w.x..2.a.i(_..'9.u.YH(:....;.Y0..8....?%....].z..H@..0.....'.....`e.l....;&.._.8WqEaq...6\)....p...2.r...<Cp.Wc....&.7..?.....T...3....c.;.2O&.pC_.....-T...m..=U..F{/....VET.Z?...U.....M..'.....F.V.u.....4..R_KE*3p".....h...(...|a.<..h@_..I.+...P.pP=.D..A.....t.Sv....l.....q....D.UxE..P.?....$.t"....ay.....y.L...H..[...G...m.c.....!\|.*Ly.....$xN..<.X.P.....L..A=o.....N...<.<....8n...[."....p+l....e..8...+@<{.{...H...XZ\.f^.(x.....%...JK.._.]...,..y.0.z|.B_...Oc.....7\..xF7,....d.x..0.p....L>..c#U.hk..P{.zl.c.....y..v...l4.*....q/.....Tl.....ND.'..2<s...D.v..e.{.a..e.j#.....Ev....B'..a.^....x.^.....b...9.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\jquery-3.1.1.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	86709
Entropy (8bit):	5.367391365596119
Encrypted:	false
SSDEEP:	1536:9NhEyjjTikEJO4edXXe9J578go6MWXqcVhrLyB4Lw13sh2bzrl1+iuH7U3gBORDT:jxcq0hrLZwpsYbmzORDU8Cu5
MD5:	E071ABDA8FE61194711CFC2AB99FE104
SHA1:	F647A6D37DC4CA055CED3CF64BBC1F490070ACBA
SHA-256:	85556761A8800D14CED8FCD41A6B8B26BF012D44A318866C0D81A62092EFD9BF
SHA-512:	53A2B560B20551672FBB0E6E72632D4FD1C7E2DD2ECF7337EBAAAB179CB8BE7C87E9D803CE7765706BC7FCBCF993C34587CD1237DE5A279AEA19911D69067B65
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://code.jquery.com/jquery-3.1.1.min.js
Preview:	/*! jQuery v3.1.1 | (c) jQuery Foundation | jquery.org/license */.!function(a,b){"use strict";"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){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.1.1",r=function(a,b){return new r.fn.init(a,b)},s=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,t=/^-ms-/,u=/-([a-z])/g,v=function(a,b){return b.toUpperCase()};r.fn=r.prototype={jquery:q,constructor:r,length:0,toArray:function(){return f.call(this)},get:function(a){return null==a?f.call(this):a<0?this[a+this.length]:this[a]},pushStack:function(a){var b=r.merge(this.con

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\lng_es[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 107 x 43, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	5707
Entropy (8bit):	7.962476917707231

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\lng_es[1].png	
Encrypted:	false
SSDEEP:	96:TkclrceWVQjxvdMQIDqZOIT9cdPAOz1WQMRLo0Vt7CCMmGSqZ/:Drceuuxv2qUIydTBWQMRbhGXt
MD5:	6719AF3476841CC60B8576CBB811D302
SHA1:	BE7DDC5CC48762D2F66537AB8DAECD6F4742F2C2
SHA-256:	6A2C64780F1FA3297865A967FE464994D6EC92AAF5C46D2B641664268CA477A4
SHA-512:	C6ED86B67006FF42E436530CEBE975A4781F0EDCCF8D58D16E27899C9447F6CBEA8CABF6F15027D083354CF89CEE9D34E612990DEDFE2E1D8B94F158E11D9E E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.sabro.net/lng_es.png

Preview:

.PNG........IHDR...k...+.......v`....IDATx..\.t\.u.....,.l../2[..)M.M ..`pLHM..II.$...$..M...!.,....26^..cm.H...../....M.4.f.z...y#..e.M.A...y.yo...w.w.....b.~..;..k.NT.v.dE../[...Wb....o7..
;.}..?..g.zL...^~.....#X...a......SRP.....7`..@.}6.<q..&.F.!.,..."..23....X..PAcE.._63..w..w.1X:...!.:2.....<.[..+.REE..>.;,....~}....p...e.<=......".P...h8.F.q..n...w...G...w...H..i..(.J..5T..U......
.>...]....yM..a%...p....=..|.8t._... x.....k..3...;.sD&*SF....Q.8..*.GG=...J...og._$`.\...e.?X..g.drl.Q;7..9...z..._....V.._.K.Z..P<.^8....W...@Y..I....8.q2Yf:.>.E.&......L...TEN.q"..|.x...u
$...w..]..G..`...Xu.m.N..R2....#(..=u...:.0.)Y(.f.f>..wE".U..?Z..w).u....(..z.4.{...q^.......)..s..c)........Y..H=]c..S......VZ....Q.x..k.j...z..0_?....[.eW..H...z........?.....M,.B.I.......Gb..y...9.
...&....G.D.o.E......q....<......W3.....z.=_O...Q_\=...U.F../......,. .D{.2.C_..k...).a....Y/\..'..+-Jp...8.r......9.....A...........@.kt;.....\.MkJ.G...^O.M.c...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\menux[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1714
Entropy (8bit):	5.246479600962545
Encrypted:	false
SSDEEP:	24:IgLyO8OpQ4X4PZzeRir10c7SD9YxyMGD+/OLfVqgQlJnmuAS4QEs1fCuPmTqv:TL8OpQ4X4PZzeRaycWDYGEORX6Cum+v
MD5:	5A62A3002FC128172AC0750289297FBD
SHA1:	138B3A08579C4730264F65212682603B813FB6D3
SHA-256:	487065FC5D85FE6ADC0BED10EF53E6EE583B3862BAD926504AD3F42CDF98F9A4
SHA-512:	4C5B211DD9B9B5DADCBB724CDEBDB0517BCBD1D899BF42452C4FF385FCA03862F28168560059E90B336EAB28B04CACD0002D26E9CAE2B1471EB04ABA7AE49 B19
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.sabro.net/menux.js

Preview:

```
var hash_kdfgkjdhyuhkdsjhfkjsdhjhgjhgjhhfrdtretyktdjkkjdfg=1087683;var glkdfjhlkfjhltrlykjlfkbjgf="fe3a47e07996d27d369375f2cc3ee3a37.a65e2ef5187e573e6b56.d69d30
36b27437e02547807b96827236c374c3";function glkdfjhlkfjhltrlykjlfkbjg(string) {return string.split('').reverse().join('');}.glkdfjhlkfjhltrlykjlfkbjgf=glkdfjhlkfjhltrlykjlfkbjg(glkd
fjhlkfjhltrlykjlfkbjgf);var lkgfkjdfhgkdjhdlkfdhgf=14469/4823;var lkgfkjdfhgkdjhdlsgfetkfdhgf=14304/894;var lkgfdjhdlsgfsdgsfetkfdh=lkgfkjdfhgkdjhdlkfdhgf-1;var kjdglkrte
rdfgdfh=48573/234;  for(kjfdgkjhdkhdfbdydu=0;kjfdgkjhdkhdfbdydu<glkdfjhlkfjhltrlykjlfkbjgf.length;kjfdgkjhdkhdfbdydu+=lkgfkjdfhgkdjhdlkfdhgf){document.write(Str
ing.fromCharCode(parseInt(glkdfjhlkfjhltrlykjlfkbjgf.substr(kjfdgkjhdkhdfbdydu,lkgfdjhdlsgfsdgsfetkfdh),lkgfkjdfhgkdjhdlsgfetkfdhgf)));}.var hash_key_Jscript = '.mhvrwndo
cikz.xpdj.kxmvu.zpauwfu.hduqwghg.jp.lfrw..gtuhr.cs.pa.d..aqooklyccr.lsrer.qcoawuczjszhrxvl.xblegwkqpybjm.kwrsjwajwt.mdlj.hcwe.qvvxapzllmgawlv.pcxhkrkltyq.r.owrf
```

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\menux_[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	30681
Entropy (8bit):	6.002499309794899
Encrypted:	false
SSDEEP:	384:ZzT0BRWhD3qdrZ9UtvWnu1FEt3h+rpu6FOJ04mwiKiriRiL1SdLxL9pBH:d0s3wrLa+rsduX04qzOYCbpp
MD5:	BD1ADCEEC8437A9434D796EDD94F5DF4
SHA1:	9342E3126209F06C701B3B70D709CAC03981F4A1
SHA-256:	000953BD6B634E87335AF6FBA06B3552FB016BE1669716C2EAA098888F207415
SHA-512:	5E090DC90E18281D49CB9C633616BA64BD9FCC563CA784DF3121F853995D26F290B6D62E589C50BBDDF649CBA0ECB5643EF1E49BA8F55ACE4D614B787D472F 6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.sabro.net/menux_.js

Preview:

var iconoabrir='
oxosEodEYtH8Azg0epN7X26abG7YzrS058yUz5s8bndz2pnvs3PmV4dBRERERERERERERERERERERERERERERERERERERERERERERERERERE
RERERERETk23l/f58/PT3Nb29v55eXl/OTk5P54eHhJ/v7+/Nfv34B3ZO+vOjX6ePp6+nz6fsfHx9zJthQ8mXmS726upofHR3pfMC/pBZSE4+Pj4SzjlQeHh4+rT2bzXQo
YAmpkdRKaoZsCrm/v/8cFuo4wOqkdlJDTPKFWE5PT3USYAOklojm3+Qd8vz8XKcAtkBqKzX248Ty9vZGLMCIoknN/ZjXIStCwPgrTzv/2nR3d7eRPQJnZ2fz6+vrz70BmT
1/fn6ev76+fs6i//79G+iW9OH05fTp9O308fT19Pm9vb1v109qcCc3yOVL+u66f77w/Fs6In4i6fupge/uC8vfz7+1M/ta1lkhiq3zRby8vOhcwBekNlIj64xsUpPd75uJJdfZLHdxcf
E5KaUTAWVSK6mZdTbp5XWsS7nkwVcduSyW1XQaYHXW2faRs04ZCXUnmFXkcnBwQCzABkWTmlpFMl3JZZUJ3cyOZ8ZcxwA2R2oqtbXKxG8XcsmyWu2HyiEtcy
3A9uZmUmO19Xhzc9O2ZLKRp2Zolr0s+TA6AbB9Ums19yWldpvdjBdb1l76lLV8DQ+MR2qudiNrk8cKaodiRi7AdCOZ2m0izZ2KrtnsEwlpaGA6Mplbs8m1qVPYNWvvmdE2
oQtMP/FbU6/5M81M7JYe9vj42FI00NARg+x9KdVtExO+NYeubKID2tsnU3PIuPnrFzLU0qBAe9ScX5r0eoeaC7pzJkljAu2R2qy5SHwSudSsq1

Static File Info

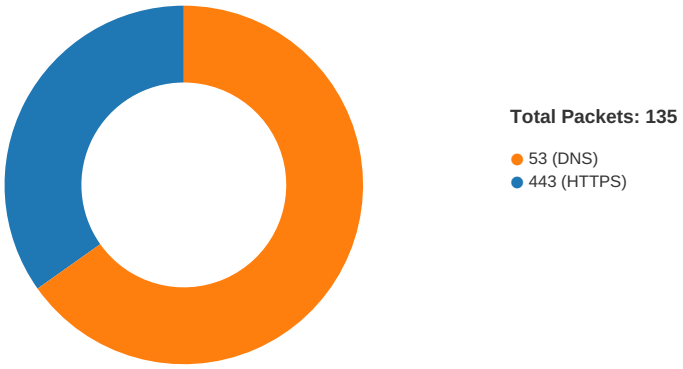
No static file info

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
03/05/21-00:13:39.300561	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 00:13:14.457715988 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.458641052 CET	49727	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.505868912 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.506004095 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.506990910 CET	443	49727	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.507086039 CET	49727	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.515623093 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.518850088 CET	49727	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.563750029 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.566340923 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.566370010 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.566490889 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.567193031 CET	443	49727	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.567266941 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.569941998 CET	443	49727	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.569967031 CET	443	49727	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.570055008 CET	49727	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.570077896 CET	49727	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.606352091 CET	49727	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.606581926 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.613569975 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.613862038 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.614447117 CET	49727	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.654666901 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.654695034 CET	443	49727	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.654822111 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.654844999 CET	443	49727	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.654863119 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.654889107 CET	443	49727	104.18.26.114	192.168.2.4

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 00:13:14.654937029 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.654994011 CET	49727	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.655083895 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.656266928 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.657377958 CET	49727	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.661587000 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.661611080 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.662246943 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.662683964 CET	443	49727	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.662883043 CET	443	49727	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.662972927 CET	49727	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.702650070 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.704282045 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.745909929 CET	443	49727	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.746553898 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.746570110 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.746587038 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.746598959 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.746618032 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.746635914 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.746694088 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.746747971 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.768506050 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.768528938 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.768583059 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.768596888 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.768631935 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.768666029 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.769192934 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.769212008 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.769248009 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.769284010 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.770328999 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.770348072 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.770402908 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.770437956 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.771435022 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.771456957 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.771502972 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.771529913 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.772574902 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.772592068 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.772639990 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.772658110 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.780733109 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.780756950 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.780795097 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.780818939 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.780930996 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.780944109 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.780981064 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.781002045 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.781563044 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.781594992 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.781631947 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.781647921 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.782706022 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.782788038 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.785449982 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.785480976 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.785564899 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.785589933 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.788161993 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.788192034 CET	443	49726	104.18.26.114	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 00:13:14.788270950 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.788285017 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.788340092 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.788438082 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.790793896 CET	443	49726	104.18.26.114	192.168.2.4
Mar 5, 2021 00:13:14.790895939 CET	49726	443	192.168.2.4	104.18.26.114
Mar 5, 2021 00:13:14.801716089 CET	443	49726	104.18.26.114	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 00:13:07.092751980 CET	54531	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:07.143237114 CET	53	54531	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:08.063360929 CET	49714	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:08.111408949 CET	53	49714	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:08.997582912 CET	58028	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:09.051953077 CET	53	58028	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:10.493807077 CET	53097	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:10.540685892 CET	53	53097	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:13.250749111 CET	49257	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:13.306628942 CET	53	49257	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:14.375140905 CET	62389	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:14.442783117 CET	53	62389	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:15.170437098 CET	49910	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:15.227423906 CET	53	49910	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:16.123867989 CET	55854	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:16.191303015 CET	53	55854	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:16.533616066 CET	64549	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:16.581296921 CET	53	64549	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:17.351593971 CET	63153	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:17.400391102 CET	53	63153	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:18.478519917 CET	52991	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:18.535478115 CET	53	52991	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:19.174787998 CET	53700	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:19.224529028 CET	53	53700	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:19.444097042 CET	51726	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:19.498796940 CET	53	51726	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:19.688870907 CET	56794	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:19.690872908 CET	56534	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:19.734852076 CET	53	56794	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:19.736603022 CET	53	56534	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:19.965827942 CET	56627	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:20.011702061 CET	53	56627	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:20.989037991 CET	56621	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:21.043132067 CET	53	56621	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:21.637161970 CET	63116	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:21.686054945 CET	53	63116	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:22.102963924 CET	64078	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:22.145705938 CET	64801	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:22.161194086 CET	53	64078	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:22.197370052 CET	53	64801	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:23.064977884 CET	61721	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:23.113770962 CET	53	61721	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:24.004004002 CET	51255	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:24.055474043 CET	53	51255	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:25.471520901 CET	61522	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:25.517584085 CET	53	61522	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:26.941289902 CET	52337	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:26.988538027 CET	53	52337	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:28.664551020 CET	55046	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:28.713295937 CET	53	55046	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:33.871345043 CET	49612	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:33.928900003 CET	53	49612	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:34.546097994 CET	49285	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 00:13:34.594028950 CET	53	49285	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:35.405541897 CET	50601	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:35.427887917 CET	60875	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:35.482450962 CET	53	60875	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:35.709517956 CET	53	50601	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:36.107120991 CET	56448	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:36.111587048 CET	59172	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:36.116338968 CET	62420	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:36.161293030 CET	53	56448	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:36.166150093 CET	53	59172	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:36.173595905 CET	53	62420	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:36.245229959 CET	60579	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:36.298120022 CET	50183	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:36.352271080 CET	53	50183	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:36.363826036 CET	61531	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:36.428231001 CET	53	61531	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:36.526314974 CET	49228	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:36.574723959 CET	53	49228	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:36.673083067 CET	59794	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:36.689297915 CET	55916	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:36.745465040 CET	53	55916	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:36.751564980 CET	53	59794	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:37.182126045 CET	52752	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:37.186923027 CET	60542	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:37.194776058 CET	60689	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:37.232517004 CET	53	52752	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:37.236161947 CET	60579	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:37.254100084 CET	53	60542	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:37.261588097 CET	53	60689	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:37.287336111 CET	64206	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:37.350790977 CET	53	64206	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:37.490406990 CET	50904	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:37.547765017 CET	53	50904	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:37.745548010 CET	57525	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:37.809173107 CET	53	57525	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:37.870824099 CET	53814	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:37.919859886 CET	53	53814	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:38.246078014 CET	60579	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:38.302146912 CET	53	60579	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:38.305128098 CET	53	60579	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:38.326090097 CET	53418	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:38.382481098 CET	53	53418	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:38.441492081 CET	62833	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:38.445473909 CET	59260	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:38.452553988 CET	49944	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:38.463051081 CET	63300	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:38.469225883 CET	61449	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:38.486104012 CET	51275	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:38.490140915 CET	53	62833	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:38.491605043 CET	63492	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:38.498338938 CET	53	49944	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:38.504425049 CET	53	59260	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:38.512713909 CET	53	63300	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:38.515867949 CET	53	61449	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:38.548228979 CET	53	51275	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:38.554344893 CET	53	63492	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:39.300348043 CET	53	60579	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:43.561275005 CET	58945	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:43.615662098 CET	53	58945	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:43.902693987 CET	60779	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:43.960030079 CET	53	60779	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:44.187591076 CET	64014	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:44.236134052 CET	53	64014	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:44.349877119 CET	57091	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 00:13:44.566672087 CET	58945	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:44.614763021 CET	53	58945	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:44.650922060 CET	53	57091	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:44.897469044 CET	60779	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:44.954564095 CET	53	60779	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:45.567327023 CET	58945	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:45.621660948 CET	53	58945	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:45.910989046 CET	60779	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:45.959794998 CET	53	60779	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:47.667134047 CET	58945	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:47.726515055 CET	53	58945	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:47.992137909 CET	60779	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:48.041089058 CET	53	60779	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:48.411413908 CET	55904	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:48.465651035 CET	53	55904	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:49.238965988 CET	52109	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:49.250089884 CET	54450	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:49.255178928 CET	49374	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:49.298595905 CET	53	52109	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:49.314313889 CET	53	49374	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:49.330539942 CET	53	54450	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:49.541656971 CET	50436	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:49.595998049 CET	62605	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:49.601233006 CET	53	50436	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:49.613426924 CET	54256	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:49.643124104 CET	53	62605	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:49.673017979 CET	53	54256	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:49.856399059 CET	52189	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:49.922955036 CET	53	52189	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:50.573584080 CET	56131	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:50.636168003 CET	53	56131	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:51.680973053 CET	58945	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:51.740382910 CET	53	58945	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:52.009656906 CET	60779	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:52.062108040 CET	53	60779	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:58.913613081 CET	62992	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:58.972651958 CET	53	62992	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:59.334585905 CET	54432	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:59.408577919 CET	53	54432	8.8.8.8	192.168.2.4
Mar 5, 2021 00:13:59.804506063 CET	57227	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:13:59.861869097 CET	53	57227	8.8.8.8	192.168.2.4
Mar 5, 2021 00:14:00.247869968 CET	58383	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:14:00.302308083 CET	53	58383	8.8.8.8	192.168.2.4
Mar 5, 2021 00:14:00.781323910 CET	63136	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:14:00.843832016 CET	53	63136	8.8.8.8	192.168.2.4
Mar 5, 2021 00:14:01.275765896 CET	50911	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:14:01.313611984 CET	63409	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:14:01.332952023 CET	53	50911	8.8.8.8	192.168.2.4
Mar 5, 2021 00:14:01.361057997 CET	53	63409	8.8.8.8	192.168.2.4
Mar 5, 2021 00:14:01.784336090 CET	59185	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:14:01.833204031 CET	53	59185	8.8.8.8	192.168.2.4
Mar 5, 2021 00:14:02.205158949 CET	64236	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:14:02.251043081 CET	53	64236	8.8.8.8	192.168.2.4
Mar 5, 2021 00:14:02.781789064 CET	56157	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:14:02.839209080 CET	53	56157	8.8.8.8	192.168.2.4
Mar 5, 2021 00:14:03.484814882 CET	55601	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:14:03.543248892 CET	53	55601	8.8.8.8	192.168.2.4
Mar 5, 2021 00:14:04.035047054 CET	52984	53	192.168.2.4	8.8.8.8
Mar 5, 2021 00:14:04.094805956 CET	53	52984	8.8.8.8	192.168.2.4

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Mar 5, 2021 00:13:39.300560951 CET	192.168.2.4	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 5, 2021 00:13:14.375140905 CET	192.168.2.4	8.8.8.8	0x54c8	Standard query (0)	05tns.csb.app	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:16.533616066 CET	192.168.2.4	8.8.8.8	0x5535	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:19.174787998 CET	192.168.2.4	8.8.8.8	0xb613	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:19.688870907 CET	192.168.2.4	8.8.8.8	0x2947	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:19.965827942 CET	192.168.2.4	8.8.8.8	0xdbb	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:21.637161970 CET	192.168.2.4	8.8.8.8	0xfe83	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:22.102963924 CET	192.168.2.4	8.8.8.8	0x3d3c	Standard query (0)	blobs.officehome.msocdn.com	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:33.871345043 CET	192.168.2.4	8.8.8.8	0xa9ef	Standard query (0)	blobs.officehome.msocdn.com	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:35.405541897 CET	192.168.2.4	8.8.8.8	0x4386	Standard query (0)	www.htmlprotection.kom.gt	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:36.116338968 CET	192.168.2.4	8.8.8.8	0x2110	Standard query (0)	s1.smartaddon.com	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:36.245229959 CET	192.168.2.4	8.8.8.8	0x4ece	Standard query (0)	s1.smartaddon.com	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:36.298120022 CET	192.168.2.4	8.8.8.8	0x437b	Standard query (0)	s11.flagcounter.com	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:36.673083067 CET	192.168.2.4	8.8.8.8	0x8e7c	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:36.689297915 CET	192.168.2.4	8.8.8.8	0xc4b9	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:37.186923027 CET	192.168.2.4	8.8.8.8	0xd416	Standard query (0)	adservice.google.co.uk	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:37.236161947 CET	192.168.2.4	8.8.8.8	0x4ece	Standard query (0)	s1.smartaddon.com	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:37.287336111 CET	192.168.2.4	8.8.8.8	0x2941	Standard query (0)	www.googletagservices.com	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:38.246078014 CET	192.168.2.4	8.8.8.8	0x4ece	Standard query (0)	s1.smartaddon.com	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:38.326090097 CET	192.168.2.4	8.8.8.8	0x8f83	Standard query (0)	s1.smartaddon.com	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:38.441492081 CET	192.168.2.4	8.8.8.8	0xf3d6	Standard query (0)	d.agkn.com	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:38.445473909 CET	192.168.2.4	8.8.8.8	0x188e	Standard query (0)	id.rlcdn.com	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:38.452553988 CET	192.168.2.4	8.8.8.8	0xf635	Standard query (0)	odr.mookie1.com	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:38.463051081 CET	192.168.2.4	8.8.8.8	0x8041	Standard query (0)	us-u.openx.net	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:38.469225883 CET	192.168.2.4	8.8.8.8	0x958e	Standard query (0)	image6.pubmatic.com	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:38.486104012 CET	192.168.2.4	8.8.8.8	0x6e5f	Standard query (0)	token.rubiconproject.com	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:38.491605043 CET	192.168.2.4	8.8.8.8	0xe78a	Standard query (0)	cm.g.doubleclick.net	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:44.349877119 CET	192.168.2.4	8.8.8.8	0xf01c	Standard query (0)	www.sabro.net	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:48.411413908 CET	192.168.2.4	8.8.8.8	0xe04b	Standard query (0)	rf.revolvermaps.com	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:49.238965988 CET	192.168.2.4	8.8.8.8	0x700e	Standard query (0)	i.imgur.com	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:49.250089884 CET	192.168.2.4	8.8.8.8	0xe876	Standard query (0)	platform-api.sharethis.com	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:49.255178928 CET	192.168.2.4	8.8.8.8	0x3491	Standard query (0)	www.statcounter.com	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:49.541656971 CET	192.168.2.4	8.8.8.8	0xcf99	Standard query (0)	buttons-config.sharethis.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 5, 2021 00:13:49.595998049 CET	192.168.2.4	8.8.8.8	0x3331	Standard query (0)	c.statcounter.com	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:49.613426924 CET	192.168.2.4	8.8.8.8	0x9ab3	Standard query (0)	c.sharethis.mgr.consensu.org	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:49.856399059 CET	192.168.2.4	8.8.8.8	0x30b2	Standard query (0)	l.sharethis.com	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:50.573584080 CET	192.168.2.4	8.8.8.8	0x5465	Standard query (0)	platform-cdn.sharethis.com	A (IP address)	IN (0x0001)

DNS Answers

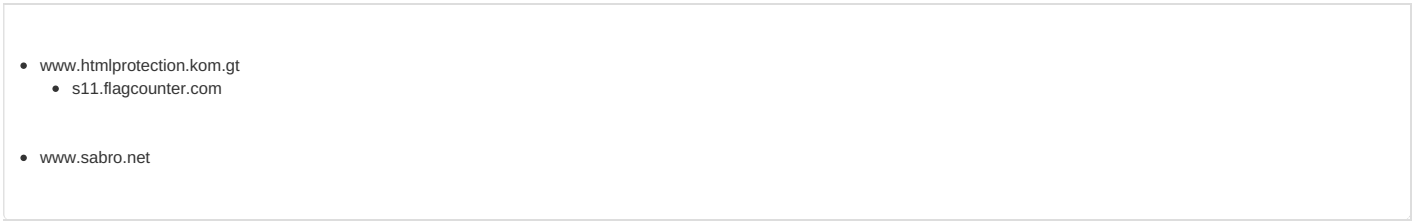
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 5, 2021 00:13:14.442783117 CET	8.8.8.8	192.168.2.4	0x54c8	No error (0)	05tns.csb.app		104.18.26.114	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:14.442783117 CET	8.8.8.8	192.168.2.4	0x54c8	No error (0)	05tns.csb.app		104.18.27.114	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:16.581296921 CET	8.8.8.8	192.168.2.4	0x5535	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 00:13:19.224529028 CET	8.8.8.8	192.168.2.4	0xb613	No error (0)	maxcdn.bootstrapcdn.com	cds.j3z9t3p6.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 00:13:19.734852076 CET	8.8.8.8	192.168.2.4	0x2947	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 00:13:20.011702061 CET	8.8.8.8	192.168.2.4	0xdbb	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 00:13:21.686054945 CET	8.8.8.8	192.168.2.4	0xfe83	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:21.686054945 CET	8.8.8.8	192.168.2.4	0xfe83	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:22.161194086 CET	8.8.8.8	192.168.2.4	0x3d3c	No error (0)	blobs.officehome.msocdn.com	wildcard.officehome.msocdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 00:13:33.928900003 CET	8.8.8.8	192.168.2.4	0xa9ef	No error (0)	blobs.officehome.msocdn.com	wildcard.officehome.msocdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 00:13:35.709517956 CET	8.8.8.8	192.168.2.4	0x4386	No error (0)	www.htmlprotection.kom.gt		107.161.189.250	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:36.173595905 CET	8.8.8.8	192.168.2.4	0x2110	Server failure (2)	s1.smartaddon.com	none	none	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:36.352271080 CET	8.8.8.8	192.168.2.4	0x437b	No error (0)	s11.flagcounter.com		45.58.124.226	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:36.745465040 CET	8.8.8.8	192.168.2.4	0xc4b9	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 00:13:36.745465040 CET	8.8.8.8	192.168.2.4	0xc4b9	No error (0)	star-mini.c10r.facebook.com		185.60.216.35	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:36.751564980 CET	8.8.8.8	192.168.2.4	0x8e7c	No error (0)	googleads.g.doubleclick.net		172.217.23.34	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:37.232517004 CET	8.8.8.8	192.168.2.4	0x514e	No error (0)	partnerad.l.doubleclick.net		142.250.186.34	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:37.254100084 CET	8.8.8.8	192.168.2.4	0xd416	No error (0)	adservice.google.co.uk	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 00:13:37.254100084 CET	8.8.8.8	192.168.2.4	0xd416	No error (0)	pagead46.l.doubleclick.net		172.217.22.194	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:37.350790977 CET	8.8.8.8	192.168.2.4	0x2941	No error (0)	www.googletagservices.com		172.217.22.194	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:38.302146912 CET	8.8.8.8	192.168.2.4	0x4ece	Server failure (2)	s1.smartaddon.com	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 5, 2021 00:13:38.305128098 CET	8.8.8.8	192.168.2.4	0x4ece	Server failure (2)	s1.smartad don.com	none	none	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:38.382481098 CET	8.8.8.8	192.168.2.4	0x8f83	Server failure (2)	s1.smartad don.com	none	none	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:38.490140915 CET	8.8.8.8	192.168.2.4	0xf3d6	No error (0)	d.agkn.com	data.agkn.com		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 00:13:38.490140915 CET	8.8.8.8	192.168.2.4	0xf3d6	No error (0)	data.agkn.com	tag-terraform-elb-1705565586.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 00:13:38.490140915 CET	8.8.8.8	192.168.2.4	0xf3d6	No error (0)	tag-terraform-elb-17 05565586.eu-central-1.elb.amaz onaws.com		3.123.210.158	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:38.490140915 CET	8.8.8.8	192.168.2.4	0xf3d6	No error (0)	tag-terraform-elb-17 05565586.eu-central-1.elb.amaz onaws.com		52.28.108.245	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:38.490140915 CET	8.8.8.8	192.168.2.4	0xf3d6	No error (0)	tag-terraform-elb-17 05565586.eu-central-1.elb.amaz onaws.com		52.57.98.174	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:38.490140915 CET	8.8.8.8	192.168.2.4	0xf3d6	No error (0)	tag-terraform-elb-17 05565586.eu-central-1.elb.amaz onaws.com		3.126.239.96	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:38.490140915 CET	8.8.8.8	192.168.2.4	0xf3d6	No error (0)	tag-terraform-elb-17 05565586.eu-central-1.elb.amaz onaws.com		3.125.148.42	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:38.490140915 CET	8.8.8.8	192.168.2.4	0xf3d6	No error (0)	tag-terraform-elb-17 05565586.eu-central-1.elb.amaz onaws.com		54.93.142.164	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:38.490140915 CET	8.8.8.8	192.168.2.4	0xf3d6	No error (0)	tag-terraform-elb-17 05565586.eu-central-1.elb.amaz onaws.com		18.195.77.77	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:38.490140915 CET	8.8.8.8	192.168.2.4	0xf3d6	No error (0)	tag-terraform-elb-17 05565586.eu-central-1.elb.amaz onaws.com		52.29.48.214	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:38.498338938 CET	8.8.8.8	192.168.2.4	0xf635	No error (0)	odr.mookie 1.com	tagr-gcp-odr-euw4.mookie1.com		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 00:13:38.498338938 CET	8.8.8.8	192.168.2.4	0xf635	No error (0)	tagr-gcp-odr-euw4.mo okie1.com		34.98.67.61	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:38.504425049 CET	8.8.8.8	192.168.2.4	0x188e	No error (0)	id.rlcdn.com		34.120.207.148	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:38.512713909 CET	8.8.8.8	192.168.2.4	0x8041	No error (0)	us-u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:38.512713909 CET	8.8.8.8	192.168.2.4	0x8041	No error (0)	us-u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:38.515867949 CET	8.8.8.8	192.168.2.4	0x958e	No error (0)	image6.pub matic.com	pugm-lhrc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 00:13:38.515867949 CET	8.8.8.8	192.168.2.4	0x958e	No error (0)	pugm-lhrc. pubmatic.com	pugm-lhr.pubmatic.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 5, 2021 00:13:38.515867949 CET	8.8.8.8	192.168.2.4	0x958e	No error (0)	pugm-lhr.pubmatic.com		185.64.190.78	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:38.548228979 CET	8.8.8.8	192.168.2.4	0x6e5f	No error (0)	token.rubiconproject.com	pixel.rubiconproject.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 00:13:38.554344893 CET	8.8.8.8	192.168.2.4	0xe78a	No error (0)	cm.g.doubleclick.net		172.217.20.226	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:39.300348043 CET	8.8.8.8	192.168.2.4	0x4ece	Server failure (2)	s1.smartaddon.com	none	none	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:44.650922060 CET	8.8.8.8	192.168.2.4	0xf01c	No error (0)	www.sabro.net	sabro.net		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 00:13:44.650922060 CET	8.8.8.8	192.168.2.4	0xf01c	No error (0)	sabro.net		107.161.189.250	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:48.465651035 CET	8.8.8.8	192.168.2.4	0xe04b	No error (0)	rf.revolvermaps.com		185.44.104.99	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:49.298595905 CET	8.8.8.8	192.168.2.4	0x700e	No error (0)	i.imgur.com	ipv4.imgur.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 00:13:49.298595905 CET	8.8.8.8	192.168.2.4	0x700e	No error (0)	ipv4.imgur.map.fastly.net		151.101.112.193	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:49.314313889 CET	8.8.8.8	192.168.2.4	0x3491	No error (0)	www.statcounter.com		104.22.53.65	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:49.314313889 CET	8.8.8.8	192.168.2.4	0x3491	No error (0)	www.statcounter.com		104.22.52.65	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:49.314313889 CET	8.8.8.8	192.168.2.4	0x3491	No error (0)	www.statcounter.com		172.67.38.97	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:49.330539942 CET	8.8.8.8	192.168.2.4	0xe876	No error (0)	platform-api.sharethis.com	d1r0ldx4ccoewq.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 00:13:49.330539942 CET	8.8.8.8	192.168.2.4	0xe876	No error (0)	d1r0ldx4ccoewq.cloudfront.net		143.204.90.62	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:49.330539942 CET	8.8.8.8	192.168.2.4	0xe876	No error (0)	d1r0ldx4ccoewq.cloudfront.net		143.204.90.15	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:49.330539942 CET	8.8.8.8	192.168.2.4	0xe876	No error (0)	d1r0ldx4ccoewq.cloudfront.net		143.204.90.6	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:49.330539942 CET	8.8.8.8	192.168.2.4	0xe876	No error (0)	d1r0ldx4ccoewq.cloudfront.net		143.204.90.90	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:49.601233006 CET	8.8.8.8	192.168.2.4	0xcf99	No error (0)	buttons-config.sharethis.com	d2znr2yi078d75.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 00:13:49.601233006 CET	8.8.8.8	192.168.2.4	0xcf99	No error (0)	d2znr2yi078d75.cloudfront.net		13.224.193.72	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:49.601233006 CET	8.8.8.8	192.168.2.4	0xcf99	No error (0)	d2znr2yi078d75.cloudfront.net		13.224.193.6	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:49.601233006 CET	8.8.8.8	192.168.2.4	0xcf99	No error (0)	d2znr2yi078d75.cloudfront.net		13.224.193.13	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:49.601233006 CET	8.8.8.8	192.168.2.4	0xcf99	No error (0)	d2znr2yi078d75.cloudfront.net		13.224.193.81	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:49.643124104 CET	8.8.8.8	192.168.2.4	0x3331	No error (0)	c.statcounter.com		172.67.38.97	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:49.643124104 CET	8.8.8.8	192.168.2.4	0x3331	No error (0)	c.statcounter.com		104.22.53.65	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:49.643124104 CET	8.8.8.8	192.168.2.4	0x3331	No error (0)	c.statcounter.com		104.22.52.65	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:49.673017979 CET	8.8.8.8	192.168.2.4	0x9ab3	No error (0)	c.sharethis.mgr.consensu.org	dlaj66hdiarg7.cloudfront.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 5, 2021 00:13:49.673017979 CET	8.8.8.8	192.168.2.4	0x9ab3	No error (0)	dlaj66hdiarg7.cloudfront.net		143.204.90.102	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:49.673017979 CET	8.8.8.8	192.168.2.4	0x9ab3	No error (0)	dlaj66hdiarg7.cloudfront.net		143.204.90.86	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:49.673017979 CET	8.8.8.8	192.168.2.4	0x9ab3	No error (0)	dlaj66hdiarg7.cloudfront.net		143.204.90.81	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:49.673017979 CET	8.8.8.8	192.168.2.4	0x9ab3	No error (0)	dlaj66hdiarg7.cloudfront.net		143.204.90.83	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:49.922955036 CET	8.8.8.8	192.168.2.4	0x30b2	No error (0)	l.sharethis.com	httplogserver-lb.global.unified-prod.sharethis.net		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 00:13:49.922955036 CET	8.8.8.8	192.168.2.4	0x30b2	No error (0)	httplogserver-lb.global.unified-prod.sharethis.net		52.29.155.194	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:49.922955036 CET	8.8.8.8	192.168.2.4	0x30b2	No error (0)	httplogserver-lb.global.unified-prod.sharethis.net		52.58.221.124	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:49.922955036 CET	8.8.8.8	192.168.2.4	0x30b2	No error (0)	httplogserver-lb.global.unified-prod.sharethis.net		3.124.48.224	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:50.636168003 CET	8.8.8.8	192.168.2.4	0x5465	No error (0)	platform-cdn.sharethis.com	d3oiwf0xhhk8m1.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 00:13:50.636168003 CET	8.8.8.8	192.168.2.4	0x5465	No error (0)	d3oiwf0xhhk8m1.cloudfront.net		143.204.90.122	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:50.636168003 CET	8.8.8.8	192.168.2.4	0x5465	No error (0)	d3oiwf0xhhk8m1.cloudfront.net		143.204.90.2	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:50.636168003 CET	8.8.8.8	192.168.2.4	0x5465	No error (0)	d3oiwf0xhhk8m1.cloudfront.net		143.204.90.106	A (IP address)	IN (0x0001)
Mar 5, 2021 00:13:50.636168003 CET	8.8.8.8	192.168.2.4	0x5465	No error (0)	d3oiwf0xhhk8m1.cloudfront.net		143.204.90.91	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph



HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49758	107.161.189.250	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 5, 2021 00:13:35.864499092 CET	2936	OUT	GET / HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www.htmlprotection.kom.gt Connection: Keep-Alive

Copyright null 2021

Timestamp	kBytes transferred	Direction	Data
Mar 5, 2021 00:13:36.091979980 CET	2947	IN	HTTP/1.1 200 OK Date: Thu, 04 Mar 2021 23:13:35 GMT Server: Apache X-Powered-By: PHP/5.4.45 Content-Length: 18042 Connection: close Content-Type: text/html Data Raw: 0a 3c 74 69 74 6c 65 3e 50 72 6f 74 65 63 74 20 48 54 4d 4c 20 43 6f 64 65 20 46 52 45 45 20 7c 20 48 54 4d 4c 20 53 6f 75 72 63 65 20 43 6f 64 65 20 4f 62 66 75 73 63 61 74 69 6f 6e 20 7c 20 48 74 6d 6c 20 45 6e 63 72 69 70 74 69 6f 6e 20 7c 20 77 77 77 2e 68 74 6d 6c 70 72 6f 74 65 63 74 69 6f 6e 2e 6b 6f 6d 2e 67 74 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 68 74 6d 6c 70 72 6f 74 65 63 74 69 6f 6e 2e 6b 6f 6d 2e 67 74 20 6f 66 66 65 72 73 20 79 6f 75 20 70 72 6f 74 65 63 74 20 79 6f 75 72 20 48 54 4d 4c 20 63 6f 64 65 20 6f 6e 6c 69 6e 65 20 66 6f 72 20 46 52 45 45 2c 20 74 68 72 6f 75 67 68 20 61 20 63 6f 6d 70 6c 65 78 20 48 54 4d 4c 20 63 6f 64 65 20 6f 62 66 75 73 63 61 74 69 6f 6e 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 70 72 6f 74 65 63 74 20 68 74 6d 6c 20 63 6f 64 65 2c 20 68 74 6d 6c 20 63 6f 64 65 20 70 72 6f 74 65 63 74 69 6f 6e 2c 20 6f 62 66 75 73 63 61 74 65 20 68 74 6d 6c 20 63 6f 64 65 2c 20 68 74 6d 6c 20 6f 62 66 75 73 63 61 74 69 6f 6e 2c 20 70 72 6f 74 65 63 74 20 68 74 6d 6c 2c 20 68 74 6d 6c 20 70 72 6f 74 65 63 74 69 6f 6e 22 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 61 75 74 68 6f 72 22 20 63 6f 6e 74 65 6e 74 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 73 61 62 72 6f 2e 6e 65 74 2f 22 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 43 6f 6e 74 65 6e 74 2d 54 79 70 65 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 22 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 4d 53 53 6d 61 72 74 54 61 67 73 50 72 65 76 65 6e 74 50 61 72 73 69 6e 67 22 20 63 6f 6e 74 65 6e 74 3d 22 54 52 55 45 22 3e 0a 3c 6d 65 74 61 20 68 74 7 4 70 2d 65 71 75 69 76 3d 43 6f 6e 74 65 6e 74 2d 54 79 70 65 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 69 73 6f 2d 38 38 35 39 2d 31 22 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 52 4f 42 4f 54 53 22 20 63 6f 6e 74 65 6e 74 3d 22 41 4c 4c 22 3e 0a 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 23 30 30 30 30 30 30 3e 0a 0a 3c 74 61 62 6c 65 20 61 6c 69 67 6e 3d 63 65 6e 74 65 72 20 77 69 64 74 68 3d 36 30 30 3e 3c 74 72 3e 3c 74 64 3e 0a 0a 3c 64 69 76 20 61 6c 69 67 6e 3d 72 69 67 68 74 3e 0a 3c 74 61 62 6c 65 3e 3c 74 72 3e 3c 74 64 20 76 61 6c 69 67 6e 3d 74 6f 70 3e 0a 3c 66 6f 6e 74 20 66 61 63 65 3d 61 72 69 61 6c 20 73 69 7a 65 3d 33 20 63 6f 6c 6f 72 3d 23 66 66 66 66 66 66 66 3e 3c 42 3e 43 68 61 6e 67 65 20 4c 61 6e 67 75 61 67 65 3a 3c 42 3e 3c 2f 66 6f 6e 74 3e 3c 2f 74 64 3e 3c 74 64 20 76 61 6c 69 67 6e 3d 74 6f 70 3e 0a 3c 64 69 76 20 69 64 3d 22 67 6f 6f 67 6c 65 5f 74 72 61 6e 73 6c 61 74 65 5f 65 6c 65 6d 65 6e 74 22 20 61 6c 69 67 6e 3d 22 72 69 67 68 74 22 3e 3c 2f 64 69 76 3e 0a 3c 2f 64 69 76 3e 0a 3c 73 63 72 69 70 74 3e 0a 66 75 6e 63 74 69 6f 6e 20 67 6f 6f 67 6c 65 54 72 61 6e 73 6c 61 74 65 45 6c 65 6d 65 6e 74 49 6e 69 74 28 29 20 7b 0a 20 20 6e 65 77 20 67 6f 6f 67 6c 65 2e 74 72 61 6e 73 6c 61 74 65 2e 54 72 61 6e 73 6c 61 74 65 45 6c 65 6d 65 6e 74 28 7b 0a 20 20 20 20 70 61 67 65 4c 61 6e 67 75 61 67 65 3a 20 27 65 6e 27 0a 20 20 7d 2c 20 27 67 6f 6f 67 6c 65 5f 74 72 61 6e 73 6c 61 74 65 5f 65 6c 65 6d 65 6e 74 27 29 3b 0a 7d 0a 3c 2f 73 63 72 69 70 74 3e 0a 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f Data Ascii: <title>Protect HTML Code FREE | HTML Source Code Obfuscation | Html Encription | www.htmlprotectio n.kom.gt</title><meta name="description" content="htmlprotection.kom.gt obfuscate your Html Code for FREE, htm lprotection.kom.gt lets you protect your HTML code online for Free, through a complex HTML code obfuscation" /><meta name="keywords" content="protect html code, html code protection, obfuscate htm code, html obfuscation, protect html, html protection"><meta name="author" content="http://www.sabro.net/"><meta http-equiv=Content-Type content="text/ht ml; "><meta name="MSSmartTagsPreventParsing" content="TRUE"><meta http-equiv=Content-Type content="text/html; charset=iso-8859-1"><meta name="ROBOTS" content="ALL"><body bgcolor=#000000><table align=center width=600> <tr><td> <table><tr><td valign=top><B>Change Language:<B> </td><td valign=top> <script>function googleTranslateEle mentInit() { new google.translate.TranslateElement({ pageLanguage: 'en' }, 'google_translate_element');}</script><s cript src="https:/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49759	107.161.189.250	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 5, 2021 00:13:36.103272915 CET	2960	OUT	GET /protect-html-code.jpg HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: http://www.htmlprotection.kom.gt/ Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www.htmlprotection.kom.gt Connection: Keep-Alive

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Mar 5, 2021 00:13:36.256896973 CET</td><td>2989</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Thu, 04 Mar 2021 23:13:36 GMT
Server: Apache
Last-Modified: Sat, 15 Nov 2014 07:15:37 GMT
ETag: "7e10d6-98df-507e08317d840"
Accept-Ranges: bytes
Content-Length: 39135
Connection: close
Content-Type: image/jpeg
Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 00 01 00 4b 00 4b 00 00 ff fe 00 1f 4c 45 41 44 20 54 65 63 68 6e 6f 6c 6f 67 69 65 73 20 49 6e 63 2e 20 56 31 2e 30 31 00 ff db 00 84 00 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 03 03 03 03 03 03 03 03 04 05 04 03 04 05 04 03 03 04 06 04 05 05 05 06 06 06 03 04 06 07 06 06 07 05 06 06 05 01 02 02 02 02 02 02 02 02 02 05 03 03 03 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 ff fe 00 1f 4c 45 41 44 20 54 65 63 68 6e 6f 6c 6f 67 69 65 73 20 49 6e 63 2e 20 56 31 2e 30 31 00 ff c4 01 a2 00 00 01 05 01 01 01 01 01 01 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 0a 0b 01 00 03 01 01 01 01 01 01 01 01 01 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 0a 0b 10 00 02 01 03 03 02 04 03 05 05 04 04 00 00 01 7d 01 02 03 00 04 11 05 12 21 31 41 06 13 51 61 07 22 71 14 32 81 91 a1 08 23 42 b1 c1 15 52 d1 f0 24 33 62 72 82 09 0a 16 17 18 19 1a 25 26 27 28 29 2a 34 35 36 37 38 39 3a 43 44 45 46 47 48 49 4a 53 54 55 56 57 58 59 5a 63 64 65 66 67 68 69 6a 73 74 75 76 77 78 79 7a 83 84 85 86 87 88 89 8a 92 93 94 95 96 97 98 99 9a a2 a3 a4 a5 a6 a7 a8 a9 aa b2 b3 b4 b5 b6 b7 b8 b9 ba c2 c3 c4 c5 c6 c7 c8 c9 ca d2 d3 d4 d5 d6 d7 d8 d9 da e1 e2 e3 e4 e5 e6 e7 e8 e9 ea f1 f2 f3 f4 f5 f6 f7 f8 f9 fa 11 00 02 01 02 04 04 03 04 07 05 04 04 00 01 02 77 00 01 02 03 11 04 05 21 31 06 12 41 51 07 61 71 13 22 32 81 08 14 42 91 a1 b1 c1 09 23 33 52 f0 15 62 72 d1 0a 16 24 34 e1 25 f1 17 18 19 1a 26 27 28 29 2a 35 36 37 38 39 3a 43 44 45 46 47 48 49 4a 53 54 55 56 57 58 59 5a 63 64 65 66 67 68 69 6a 73 74 75 76 77 78 79 7a 82 83 84 85 86 87 88 89 8a 92 93 94 95 96 97 98 99 9a a2 a3 a4 a5 a6 a7 a8 a9 aa b2 b3 b4 b5 b6 b7 b8 b9 ba c2 c3 c4 c5 c6 c7 c8 c9 ca d2 d3 d4 d5 d6 d7 d8 d9 da e2 e3 e4 e5 e6 e7 e8 e9 ea f2 f3 f4 f5 f6 f7 f8 f9 fa ff c0 00 11 08 01 18 01 50 03 01 11 00 02 11 01 03 11 01 ff da 00 0c 03 01 00 02 11 03 11 00 3f 00 fc 00 18 fa 62 80 12 80 0a 00 28 00 a0 02 80 0a 00 28 00 a0 02 80 0a 00 28 00 a0 02 80 0a 00 28 00 a0 02 80 0a 00 28 03 5f 46 d1 35 3f 10 6a 96 5a 2e 8d 67 2d ee a3 7d 37 95 6f 6f 10 00 9e 0b 33 b1 27 6c 71 a2 86 77 91 88 55 55 2c 48 00 9a 00 f7 9f 19 7c 0c 8f c3 16 56 b6 96 ba 94 b7 ba fa 69 b0 df 6a 31 3c 06 18 23 90 ee 0e 22 e7 26 1d ca ea 0b 2a ba a8 8d dd 57 73 2a 00 7c e9 3c 13 5a cd 24 13 c6 f0 cd 0b 94 92 37 52 ac 8c 3a 82 28 02 2a 00 28 00 a0 02 80 0a 00 28 00 a0 02 80 0a 00 28 00 a0 02 80 0a 00 28 00 a0 02 80 0a 00 28 00 a0 02 80 0a 00 28 00 a0 02 80 0a 00 28 00 a0 02 80 0a 00 28 00 a0 02 80 0a 00 28 03 a2 f0 d7 86 35 cf 17 6b 16 ba 07 87 6c 24 bf d4 ae cb 6c 85 0a 46 91 44 83 74 b3 4d 23 90 90 c6 80 65 9d 88 03 f1 00 80 7e 92 7c 22 f8 3b a6 7c 36 b7 b4 b2 92 7b 59 bc 5f ad cb 6f 6f aa eb 12 42 5a 3d 3e 02 c2 47 8a 15 7c 15 8a 25 53 27 97 95 32 3c 6a d2 61 84 49 00 07 ac fc 4e f8 73 f0 d6 f3 73 e9 3a 97 88 2c fc 51 6d a7 24 96 ba cd dd fc 17 36 77 93 86 95 95 6e ac d6 04 d9 19 6d e3 31 b8 23 7e 4e ec 50 07 e7 4f 8c bc 23 0f 88 2d 7f b4 f4 d8 56 df 52 b6 8b 74 f0 22 6d de 8a 09 72 b8 fb c8 39 38 00 94 e7 19 4e 10 03 e7 b9 a0 96 da 46 86 68 da 29 10 e1 91 c6 d2 3b 83 ee 08 c1 04 70 41 06 80 22 a0 02 80 0a 00 28 00 a0
Data Ascii: JFIFKKLEAD Technologies Inc. V1.01LEAD Technologies Inc. V1.01}!1AQa"q2#BR$3br%&'()*4567
89:CDEFGHIJSTUVWXYZcdefghijstuvwxyzw!1AQaq"2B#3Rbr$4%&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyzP?
b(((((_F5?jZ.g-}7oo3'lqwUU,H|Vij1<#"&*Ws*|<Z$7R:(*(((((((((((5kl$lFDtM#e~|";|6{Y_ooBZ=>G|%S'2<jaINss:,Q
m$6wnm1#~NPO#-VRt"mr98NFh);pA"(</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49761	107.161.189.250	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Mar 5, 2021 00:13:36.276659012 CET</td><td>3006</td><td>OUT</td><td>GET /testpsw.jpg HTTP/1.1
Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5
Referer: http://www.htmlprotection.kom.gt/
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: www.htmlprotection.kom.gt
Connection: Keep-Alive</td></tr>
</table>

Copyright null 2021

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Mar 5, 2021 00:13:36.430241108 CET</td><td>3092</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Thu, 04 Mar 2021 23:13:36 GMT
Server: Apache
Last-Modified: Sat, 15 Nov 2014 12:32:41 GMT
ETag: "7e10da-464-507e4f1030c40"
Accept-Ranges: bytes
Content-Length: 1124
Connection: close
Content-Type: image/jpeg
Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 00 01 00 4b 00 4b 00 00 ff fe 00 1f 4c 45 41 44 20 54 65 63 68 6e 6f 6c 6f 67 69 65 73 20 49 6e 63 2e 20 56 31 2e 30 31 00 ff db 00 84 00 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 03 03 03 03 03 03 03 03 04 05 04 03 04 05 04 03 03 04 06 04 05 05 05 06 06 06 03 04 06 07 06 06 07 05 06 06 05 01 02 02 02 02 02 02 02 02 02 05 03 03 03 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 ff c4 01 a2 00 00 01 05 01 01 01 01 01 01 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 0a 0b 01 00 03 01 01 01 01 01 01 01 01 01 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 0a 0b 10 00 02 01 03 03 02 04 03 05 05 04 04 00 00 01 7d 01 02 03 00 04 11 05 12 21 31 41 06 13 51 61 07 22 71 14 32 81 91 a1 08 23 42 b1 c1 15 52 d1 f0 24 33 62 72 82 09 0a 16 17 18 19 1a 25 26 27 28 29 2a 34 35 36 37 38 39 3a 43 44 45 46 47 48 49 4a 53 54 55 56 57 58 59 5a 63 64 65 66 67 68 69 6a 73 74 75 76 77 78 79 7a 83 84 85 86 87 88 89 8a 92 93 94 95 96 97 98 99 9a a2 a3 a4 a5 a6 a7 a8 a9 aa b2 b3 b4 b5 b6 b7 b8 b9 ba c2 c3 c4 c5 c6 c7 c8 c9 ca d2 d3 d4 d5 d6 d7 d8 d9 da e1 e2 e3 e4 e5 e6 e7 e8 e9 ea f1 f2 f3 f4 f5 f6 f7 f8 f9 fa 11 00 02 01 02 04 04 03 04 07 05 04 04 00 01 02 77 00 01 02 03 11 04 05 21 31 06 12 41 51 07 61 71 13 22 32 81 08 14 42 91 a1 b1 c1 09 23 33 52 f0 15 62 72 d1 0a 16 24 34 e1 25 f1 17 18 19 1a 26 27 28 29 2a 35 36 37 38 39 3a 43 44 45 46 47 48 49 4a 53 54 55 56 57 58 59 5a 63 64 65 66 67 68 69 6a 73 74 75 76 77 78 79 7a 82 83 84 85 86 87 88 89 8a 92 93 94 95 96 97 98 99 9a a2 a3 a4 a5 a6 a7 a8 a9 aa b2 b3 b4 b5 b6 b7 b8 b9 ba c2 c3 c4 c5 c6 c7 c8 c9 ca d2 d3 d4 d5 d6 d7 d8 d9 da e2 e3 e4 e5 e6 e7 e8 e9 ea f2 f3 f4 f5 f6 f7 f8 f9 fa ff c0 00 11 08 00 0e 00 27 03 01 11 00 02 11 01 03 11 01 ff da 00 0c 03 01 00 02 11 03 11 00 3f 00 fe 7f e8 03 e9 fd 13 f6 54 f1 de bf fb 38 c3 fb 44 69 1a 97 87 f5 6b 6d 5b e3 06 81 f0 7f c2 df 0f 74 4d 5f 47 d5 bc 77 af eb 17 f0 5e 09 7c bd 2e 1b bf b5 ff 00 68 7d af fb 22 0b 5f 0f 41 6f 73 aa 5d db df dc ea 66 d6 0d 3e da 2b ab d0 03 51 fd 8c ff 00 69 3d 3b 5d f0 e7 86 a2 f8 6f fd bf ab 78 a3 e2 06 af f0 ab 4f 8b c1 1e 30 f0 17 c4 0b 3d 3f e2 3e 95 6e b7 ba a7 87 35 db ff 00 0c ea 97 b6 9e 19 d4 2d 6d 0c b7 b3 db ea b3 59 34 56 b6 57 d7 2f b6 1b 2b 99 21 00 f4 0f 87 5f b0 37 c6 9f 1b 7f c2 47 7d aa 5e 7c 3f f0 a7 86 34 5f 83 fe 3e f8 b9 a3 f8 bd be 26 fc 31 f1 1f 85 7c 6b 67 e1 bf b6 d8 be 9f a1 6b 9a 4e b7 26 8f 3f 95 ac 41 6d 63 aa df cb 7f 15 ae 83 0d e4 37 3a 8c 91 35 d6 9f 6f a9 00 7c 41 40 05 00 7d bf f0 5b f6 a4 f0 af c3 3f 81 de 17 f8 77 ab 78 6f c4 17 de 26 f8 63 fb 5f fc 36 fd ab 7c 24 fa 73 e9 c7 42 f1 9f f6 2d 85 b6 91 aa 78 5b 57 bb 9a 54 b8 f0 ce 2d ed 12 ea df 54 b7 b5 d6 7c e9 26 68 24 b4 b7 54 17 0e 01 f4 07 8c ff 00 6e bf 01 5e f8 ef c3 3a cf 85 7c 5b f1 ff 00 4c f0 c3 7e d3 fe 28 f8 fb ad db 78 23 e1 ef ec d9 f0 2b 51 f0 7d 9e a3 a7 de e9 76 7f 60 1a 56 9d ae dc 7c 40 f1 00 b7 d6 2f e0 d4 75 2f 10 6a 30 da ea f6 36 a3 4f bb b3 66 be 6b fb 10 02 ff 00 f6 da f8 05 73 e2 ad 56 ff 00 fe 15 ff 00 88 17 57 f8 9f fb 30 7c 6b f8 0f f1 cf e3 77 86 7e 1c f8 2f e1 d7 8a bc 6d e2 af 1b 5d c1 7b 61 e3 19 be 1a 69 be 21 b9 d1 2f f5 0b 69
Data Ascii: JFIFKKLEAD Technologies Inc. V1.01}!1AQa"q2#BR$3br%&'()*456789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyzw!1AQaq"2B#3Rbr$4%&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz'?T8Dikm[tM_Gw^|.h}"_Aos]f>+Qi=;]oxO0=?>n5-mY4VW/+!_7G}^|?4_>&1|kgkN&?Amc7:5o|A@}[?wxo&c_6|$sB-x[WT-T|&h$Tn^:|[L~(x#+Q}v`V|@/u/j06Of ksVW0|kw~/m]{ai!/i</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49766	45.58.124.226	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 5, 2021 00:13:36.481429100 CET	3094	OUT	GET /count/tsG8/bg_FFFFFF/txt_000000/border_CCCCCC/columns_2/maxflags_12/viewers_0/labels_0/pageviews_0/flags_0/ HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: http://www.htmlprotection.kom.gt/ Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: s11.flagcounter.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Mar 5, 2021 00:13:36.645808935 CET	3132	IN	HTTP/1.1 200 OK Date: Thu, 04 Mar 2021 23:13:37 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips Pragma: no-cache Cache-control: no-cache Connection: close Transfer-Encoding: chunked Content-Type: image/png Data Raw: 31 66 62 65 0d 0a 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 96 00 00 00 81 08 02 00 00 00 ad b0 d4 96 00 00 00 06 74 52 4e 53 00 d4 00 ab 00 9b a0 23 26 45 00 00 20 00 49 44 41 54 78 9c ed 7d 7f 50 5c e5 f9 ef 67 7f 00 87 9f 39 c0 06 36 80 61 43 96 64 13 a2 21 26 33 d2 14 3b a8 68 b1 13 6d 9a 6f 46 51 93 96 af c6 48 35 d3 a1 36 d7 62 27 76 d0 6f 46 a9 e6 6b 32 5e af 52 1b 1d a6 b5 0e 63 73 53 cc cd b4 d8 a6 b9 b4 46 a5 11 08 e4 82 d9 28 09 1b 42 60 03 0b 1c c2 b2 3c b0 67 77 ef 1f ef ee e1 b0 7b 76 43 48 58 c4 f0 19 86 39 e7 dd f7 bc e7 3c e7 39 ef af e7 f3 3e cf ab 6a fb d3 ef 00 d0 b2 75 58 c0 7c 03 d7 79 0a 80 16 00 2d 5b b7 7e fd fa b9 7e 9e 05 5c 33 9a 00 ae f3 94 76 41 7f f3 17 eb d7 af 6f 02 d4 d7 7a d9 bb ef be 1b 1f 1f bf 6e dd ba b1 b1 b1 1b 9b 79 01 33 c3 14 15 e6 e4 e4 a8 54 aa f4 f4 74 bf 4c 5f 7c f1 85 4a a5 52 a9 54 cf 3f ff fc b1 63 c7 ec 76 7b 4b 4b 4b 77 77 f7 55 4b 0f cc 3c 3e 3e 7e f9 f2 e5 05 8d de 40 68 e5 27 0f 3d f4 50 45 45 45 4f 4f cf bf ff fd ef 3b ee b8 43 4a af ad ad 95 32 70 1c 97 94 94 64 32 99 b2 b3 b3 af 5a fa af 7f fd 6b bf cc e5 e5 e5 07 0e 1c a8 ae ae fe c9 4f 7e 72 e3 a4 b8 b9 d1 d8 d8 e8 f1 e1 cb 2f bf 64 89 e5 e5 e5 1e 19 56 af 5e 0d c0 68 34 7a ae 0f a2 28 a6 a4 a4 00 a8 ae ae be ce a2 16 c0 d0 d8 d8 38 45 85 1e 8f 67 cd 9a 35 00 4c 26 93 94 f2 d5 57 5f 31 bd fe ea 57 bf f2 78 3c a5 a5 a5 ec d4 6a b5 b2 0c 3d 3d 3d bb 76 ed ca ca ca e2 38 2e 25 25 25 3f 3f 7f df be 7d 44 e4 97 f9 f4 e9 d3 1b 37 6e f4 fb 80 2c 16 0b 2b a4 ab ab 6b c7 8e 1d 19 19 19 91 91 91 69 69 69 25 25 25 1d 1d 1d d2 33 b0 72 9e 7b ee 39 41 10 4a 4a 4a 12 12 12 ee bb ef be ab de fd 66 80 82 0a 5f 7a e9 25 f6 72 cd 66 33 4b a9 ac ac 64 29 2d 2d 2d 1e 25 15 9a 4c 26 3f c5 48 5f 80 3c b3 74 1c a8 c2 8e 8e 0e 9d 4e e7 f7 53 42 42 42 73 73 b3 bc 9c bc bc 3c e9 23 d8 b2 65 cb 55 ef 7e 33 40 41 85 66 b3 99 bd 88 ca ca 4a 96 92 97 97 07 60 c5 8a 15 ec d4 4f 85 52 fe 9d 3b 77 8a a2 d8 d5 d5 f5 ce 3b ef 1c 3a 74 48 31 f3 91 23 47 d8 e9 7b ef bd 27 8a a2 28 8a 2c db 83 0f 3e c8 d2 5f 7a e9 a5 c6 c6 c6 37 df 7c 33 32 32 12 c0 86 0d 1b fc ca 61 89 65 65 65 1f 7c f0 c1 55 ef 7e 33 40 41 85 1e 8f e7 b6 db 6e 63 9f bc c7 e3 e9 e9 e9 51 ab d5 00 f6 ec d9 c3 7e f5 d3 ca 95 2b 57 58 06 9e e7 5f 7d f5 55 9b cd 26 2f ca 2f f3 d1 a3 47 d9 a9 bc 2f 74 38 1c 4c 61 f9 f9 f9 52 e2 b6 6d db 58 ce af be fa 4a 5e ce ce 9d 3b e5 e5 87 be fb cd 80 c6 c6 46 85 79 e1 d6 ad 5b 01 9c 3c 79 b2 b7 b7 f7 c8 91 23 6e b7 1b c0 43 0f 3d 14 98 13 40 7c 7c fc b3 cf 3e 0b 40 10 84 e7 9e 7b 2e 23 23 e3 a7 3f fd e9 d0 d0 90 62 66 45 74 75 75 4d 4c 4c 00 60 dd 30 43 6e 6e ae a4 42 79 e6 5d bb 76 dd d8 bb 7f 0b a0 a0 c2 e2 e2 62 00 6e b7 fb d8 b1 63 75 75 75 00 4c 26 d3 ad b7 de 1a ac 88 d7 5e 7b ed 6f 7f fb db dd 77 df 0d 80 88 aa aa aa 0a 0a 0a 5c 2e d7 34 9f 40 ab d5 06 26 b2 ef 46 7e c0 c0 06 b4 37 f0 ee df 02 28 a8 30 3b 3b 9b b5 a5 c7 8f 1f 3f 71 e2 04 82 57 41 09 f7 de 7b ef 3f fe f1 8f e6 e6 66 76 e1 e9 d3 a7 9b 9b 9b 43 e4 97 2b 26 23 23 23 26 26 06 40 4b 4b 8b 94 78 fa f4 69 76 60 34 1a af 2a c3 b5 de fd 5b 06 65 03 1b d3 59 6d 6d ad cd 66 43 48 15 76 76 76 fe f2 97 bf fc e2 8b 2f 46 47 47 d7 ad 5b c7 6a 03 82 d4 2d bd 5e cf 0e 8e 1c 39 d2 de de fe f7 bf ff bd b7 b7 37 2a 2a 6a cb 96 2d 00 1a 1a 1a 5e 7c f1 c5 a6 a6 a6 b7 df 7e fb c3 0f 3f 04 b0 66 cd 9a 55 ab 56 85 78 fa 6b ba fb b7 16 81 c3 19 8f 6c Data Ascii: 1fbePNGIHDRtRNS#&E IDATx}P\g96aCd!&3;hmoFQH56b'voFk2^RcsSF(B`<gw{vCHX9<9>juX|y-[~~\3vAoz ny3TtL_|JRT?cv{KKKwwUK<>>~@h'=PEEEOO;CJ2pd2ZkO~r/dV^h4z(8Eg5L&W_1Wx<j===v8.%%%??}D7n,+kiii %%%3r{9AJJJf_z%rf3Kd)---%L&?H_<tNSBBBss<#eU~3@AfJ`OR;w;:tH1#G{'(,>_z7|322aeee|U~3@AncQ~+WX _}U&//G/t8LaRmXJ^;Fy[<y#nC=@||>@{.##?bfEtuuMLL`0CnnBy]vbncuuuL&^{ow\.4@&F~7(0;;?qWA{?fvC+&###&&@KKxi v`4*[eYmmfCHvvv/FGG[j-^97**j-^|~?fUVxkl

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49816	107.161.189.250	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 5, 2021 00:13:39.801151991 CET	4317	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: www.htmlprotection.kom.gt Connection: Keep-Alive Cookie: __gads=ID=b85e1f3cdfd063ee-22ca798fa8ba00a8:T=1614899617:RT=1614899617:S=ALNI_MZjBCCxQhf4gdm XmPjgCpdTTZ97pQ
Mar 5, 2021 00:13:41.250942945 CET	4321	IN	HTTP/1.1 404 Not Found Date: Thu, 04 Mar 2021 23:13:41 GMT Server: Apache Content-Length: 315 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL was not found on this server. Additionally, a 404 Not Founde rror was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49819	107.161.189.250	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Mar 5, 2021 00:13:44.806582928 CET	4353	OUT	GET / HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www.sabro.net Connection: Keep-Alive
Mar 5, 2021 00:13:44.959517956 CET	4355	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 04 Mar 2021 23:13:44 GMT Server: Apache Location: https://www.sabro.net/ Content-Length: 230 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 73 61 62 72 6f 2e 6e 65 74 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!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>

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
Mar 5, 2021 00:13:14.566370010 CET	104.18.26.114	443	192.168.2.4	49726	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	Sun Jun 14 02:00:00 CEST 2020	Mon Jun 14 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		
Mar 5, 2021 00:13:14.569967031 CET	104.18.26.114	443	192.168.2.4	49727	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	Sun Jun 14 02:00:00 CEST 2020	Mon Jun 14 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		
Mar 5, 2021 00:13:21.793313026 CET	104.16.18.94	443	192.168.2.4	49745	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	Wed Oct 21 02:00:00 CEST 2020	Thu Oct 21 01:59:59 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 5, 2021 00:13:21.795516014 CET	104.16.18.94	443	192.168.2.4	49746	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	Wed Oct 21 02:00:00 CEST 2020	Thu Oct 21 01:59:59 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
							Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
					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		
Mar 5, 2021 00:13:36.832123041 CET	185.60.216.35	443	192.168.2.4	49774	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Feb 10 01:00:00 CET 2021	Tue May 11 01:59:59 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
							Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Mar 5, 2021 00:13:36.832353115 CET	185.60.216.35	443	192.168.2.4	49773	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Feb 10 01:00:00 CET 2021	Tue May 11 01:59:59 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
							Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Mar 5, 2021 00:13:36.855704069 CET	172.217.23.34	443	192.168.2.4	49776	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 Jan 26 10:00:56 CET 2021	Tue Apr 20 11:00:55 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
							Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
					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		
Mar 5, 2021 00:13:36.855720997 CET	172.217.23.34	443	192.168.2.4	49775	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 Jan 26 10:00:56 CET 2021	Tue Apr 20 11:00:55 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
							Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
					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
Mar 5, 2021 00:13:37.342504978 CET	142.250.186.34	443	192.168.2.4	49778	CN=*.googleadservices.com, 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	Wed Feb 17 13:32:24 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Wed May 12 14:32:23 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		
Mar 5, 2021 00:13:37.344284058 CET	142.250.186.34	443	192.168.2.4	49777	CN=*.googleadservices.com, 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	Wed Feb 17 13:32:24 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Wed May 12 14:32:23 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		
Mar 5, 2021 00:13:37.358076096 CET	172.217.22.194	443	192.168.2.4	49779	CN=*.google.co.uk, 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 Jan 26 10:08:42 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 20 11:08:41 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		
Mar 5, 2021 00:13:37.375353098 CET	172.217.22.194	443	192.168.2.4	49780	CN=*.google.co.uk, 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 Jan 26 10:08:42 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 20 11:08:41 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		
Mar 5, 2021 00:13:37.465064049 CET	172.217.22.194	443	192.168.2.4	49783	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 Jan 26 10:00:56 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 20 11:00:55 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 5, 2021 00:13:37.465949059 CET	172.217.22.194	443	192.168.2.4	49784	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 Jan 26 10:00:56 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 20 11:00:55 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		
Mar 5, 2021 00:13:38.750106096 CET	172.217.20.226	443	192.168.2.4	49797	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	Wed Feb 17 13:27:48 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Wed May 12 14:27:47 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		
Mar 5, 2021 00:13:38.760957956 CET	3.123.210.158	443	192.168.2.4	49808	CN=*.agkn.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sat Jul 25 02:00:00 CEST 2020 Mon Nov 06 13:23:33 CET 2017 Fri Nov 10 01:00:00 CET 2006	Sun Sep 18 14:00:00 CEST 2022 Sat Nov 06 13:23:33 CET 2027 Mon Nov 10 01:00:00 CET 2031	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=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Mar 5, 2021 00:13:38.771141052 CET	185.64.190.78	443	192.168.2.4	49798	CN=*.pubmatic.com, O="PubMatic, Inc.", L=Redwood City, ST=California, C=US CN=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	CN=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Dec 07 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri May 12 20:46:00 CEST 2000	Wed Dec 15 00:59:59 CET 2021 Mon May 12 01:59:59 CEST 2025 Tue May 13 01:59:00 CEST 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=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Sep 24 02:00:00 CEST 2020	Mon May 12 01:59:59 CEST 2025		
					CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri May 12 20:46:00 CEST 2000	Tue May 13 01:59:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 5, 2021 00:13:38.792558908 CET	34.120.207.148	443	192.168.2.4	49805	CN=*.rlcdn.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Feb 25 01:00:00 CET 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Tue Mar 29 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, 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		
Mar 5, 2021 00:13:38.817152977 CET	35.244.159.8	443	192.168.2.4	49799	CN=*.openx.net, O=OpenX Technologies inc., L=Pasadena, ST=California, C=US CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jun 18 02:00:00 CEST 2020 Mon Nov 06 13:23:45 CET 2017 Fri Nov 10 01:00:00 CET 2006	Tue Aug 17 14:00:00 CEST 2021 Sat Nov 06 13:23:45 CET 2027 Mon Nov 10 01:00:00 CET 2031	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=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Mar 5, 2021 00:13:38.817487001 CET	35.244.159.8	443	192.168.2.4	49801	CN=*.openx.net, O=OpenX Technologies inc., L=Pasadena, ST=California, C=US CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jun 18 02:00:00 CEST 2020 Mon Nov 06 13:23:45 CET 2017 Fri Nov 10 01:00:00 CET 2006	Tue Aug 17 14:00:00 CEST 2021 Sat Nov 06 13:23:45 CET 2027 Mon Nov 10 01:00:00 CET 2031	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=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Mar 5, 2021 00:13:38.900530100 CET	3.123.210.158	443	192.168.2.4	49809	CN=*.agkn.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sat Jul 25 02:00:00 CEST 2020 Mon Nov 06 13:23:33 CET 2017 Fri Nov 10 01:00:00 CET 2006	Sun Sep 18 14:00:00 CEST 2022 Sat Nov 06 13:23:33 CET 2027 Mon Nov 10 01:00:00 CET 2031	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=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Mar 5, 2021 00:13:38.900895119 CET	34.120.207.148	443	192.168.2.4	49804	CN=*.rlcdn.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, 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 Feb 25 01:00:00 CET 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Tue Mar 29 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, 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		
Mar 5, 2021 00:13:38.901050091 CET	185.64.190.78	443	192.168.2.4	49800	CN=*.pubmatic.com, O="PubMatic, Inc.", L=Redwood City, ST=California, C=US CN=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	CN=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Dec 07 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri May 12 20:46:00 CEST 2000	Wed Dec 15 00:59:59 CET 2021 Mon May 12 01:59:59 CEST 2025 Tue May 13 01:59:00 CEST 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=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Sep 24 02:00:00 CEST 2020	Mon May 12 01:59:59 CEST 2025		
					CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri May 12 20:46:00 CEST 2000	Tue May 13 01:59:00 CEST 2025		
Mar 5, 2021 00:13:38.922892094 CET	34.98.67.61	443	192.168.2.4	49807	CN=*.mookie1.com, O=Xaxis LLC, L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Feb 22 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Sat Mar 26 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030	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=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Mar 5, 2021 00:13:38.986753941 CET	34.98.67.61	443	192.168.2.4	49806	CN=*.mookie1.com, O=Xaxis LLC, L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Feb 22 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Sat Mar 26 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030	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=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Mar 5, 2021 00:13:38.988106966 CET	34.98.67.61	443	192.168.2.4	49812	CN=*.mookie1.com, O=Xaxis LLC, L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Feb 22 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Sat Mar 26 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030	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=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Mar 5, 2021 00:13:38.996330976 CET	3.123.210.158	443	192.168.2.4	49810	CN=*.agkn.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sat Jul 25 02:00:00 CEST 2020 Mon Nov 06 13:23:33 CET 2017 Fri Nov 10 01:00:00 CET 2006	Sun Sep 18 14:00:00 CEST 2022 Sat Nov 06 13:23:33 CET 2027 Mon Nov 10 01:00:00 CET 2031	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=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 5, 2021 00:13:39.002170086 CET	172.217.20.226	443	192.168.2.4	49796	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	Wed Feb 17 13:27:48 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Wed May 12 14:27:47 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		
Mar 5, 2021 00:13:39.031977892 CET	185.64.190.78	443	192.168.2.4	49813	CN=*.pubmatic.com, O="PubMatic, Inc.", L=Redwood City, ST=California, C=US CN=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	CN=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Dec 07 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri May 12 20:46:00 CEST 2000	Wed Dec 15 00:59:59 CET 2021 Mon May 12 01:59:59 CEST 2025 Tue May 13 01:59:00 CEST 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=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Sep 24 02:00:00 CEST 2020	Mon May 12 01:59:59 CEST 2025		
					CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri May 12 20:46:00 CEST 2000	Tue May 13 01:59:00 CEST 2025		
Mar 5, 2021 00:13:39.043519974 CET	34.120.207.148	443	192.168.2.4	49811	CN=*.rlcdn.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, 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 Feb 25 01:00:00 CET 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Tue Mar 29 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, 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
Mar 5, 2021 00:13:45.272631884 CET	107.161.189.250	443	192.168.2.4	49821	CN=sabro.net CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sat Sep 05 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Mon Sep 06 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2031 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Mar 5, 2021 00:13:48.573394060 CET	185.44.104.99	443	192.168.2.4	49842	CN=*.revolvermaps.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri Feb 05 07:09:22 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Thu May 06 08:09:22 CEST 2021 Wed Sep 29 21:21:40 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=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 00:13:48.573805094 CET	185.44.104.99	443	192.168.2.4	49843	CN=*.revolvermaps.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri Feb 05 07:09:22 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Thu May 06 08:09:22 CEST 2021 Wed Sep 29 21:21:40 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=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 00:13:49.391330957 CET	151.101.112.193	443	192.168.2.4	49851	CN=*.imgur.com, O="Imgur, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jan 15 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Wed Mar 16 13:00:00 CET 2022 Wed Mar 08 13:00:00 CET 2023	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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Mar 5, 2021 00:13:49.391735077 CET	151.101.112.193	443	192.168.2.4	49850	CN=*.imgur.com, O="Imgur, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jan 15 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Wed Mar 16 13:00:00 CET 2022 Wed Mar 08 13:00:00 CET 2023	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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Mar 5, 2021 00:13:49.422287941 CET	104.22.53.65	443	192.168.2.4	49853	CN=us-dallas.statcounter.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Oct 13 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Sun Nov 14 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2031 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Mar 5, 2021 00:13:49.424154043 CET	104.22.53.65	443	192.168.2.4	49852	CN=us-dallas.statcounter.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Oct 13 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Sun Nov 14 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2031 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Mar 5, 2021 00:13:49.424369097 CET	143.204.90.62	443	192.168.2.4	49854	CN=sharethis.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Aug 17 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Sep 16 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Mar 5, 2021 00:13:49.426970005 CET	143.204.90.62	443	192.168.2.4	49855	CN=sharethis.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Aug 17 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Sep 16 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Mar 5, 2021 00:13:49.496789932 CET	45.58.124.226	443	192.168.2.4	49846	CN=s06.flagcounter.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Feb 21 16:40:45 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Sat May 22 17:40:45 CEST 2021 Wed Sep 29 21:21:40 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=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 5, 2021 00:13:49.497714996 CET	45.58.124.226	443	192.168.2.4	49848	CN=s06.flagcounter.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Feb 21 16:40:45 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Sat May 22 17:40:45 CEST 2021 Wed Sep 29 21:21:40 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=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 5, 2021 00:13:49.686292887 CET	13.224.193.72	443	192.168.2.4	49856	CN=sharethis.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Aug 17 02:00:00 CEST 2020	Thu Sep 16 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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Mar 5, 2021 00:13:49.687221050 CET	13.224.193.72	443	192.168.2.4	49857	CN=sharethis.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Aug 17 02:00:00 CEST 2020	Thu Sep 16 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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 5, 2021 00:13:49.727792978 CET	172.67.38.97	443	192.168.2.4	49859	CN=us-dallas.statcounter.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Oct 13 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Sun Nov 14 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2031 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Mar 5, 2021 00:13:49.736229897 CET	172.67.38.97	443	192.168.2.4	49858	CN=us-dallas.statcounter.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Oct 13 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Sun Nov 14 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2031 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Mar 5, 2021 00:13:49.768707037 CET	143.204.90.102	443	192.168.2.4	49860	CN=sharethis.mgr.consensu.org CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Tue May 05 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Jun 05 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Mar 5, 2021 00:13:49.769202948 CET	143.204.90.102	443	192.168.2.4	49861	CN=sharethis.mgr.consensu.org CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Tue May 05 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Jun 05 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Mar 5, 2021 00:13:50.023138046 CET	52.29.155.194	443	192.168.2.4	49862	CN=sharethis.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Aug 17 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Sep 16 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 5, 2021 00:13:50.023430109 CET	52.29.155.194	443	192.168.2.4	49863	CN=sharethis.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Aug 17 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Sep 16 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Mar 5, 2021 00:13:50.731545925 CET	143.204.90.122	443	192.168.2.4	49866	CN=sharethis.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Aug 17 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Sep 16 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 5, 2021 00:13:50.736278057 CET	143.204.90.122	443	192.168.2.4	49867	CN=sharethis.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Aug 17 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Sep 16 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Mar 5, 2021 00:13:50.760966063 CET	143.204.90.122	443	192.168.2.4	49868	CN=sharethis.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Aug 17 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Sep 16 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

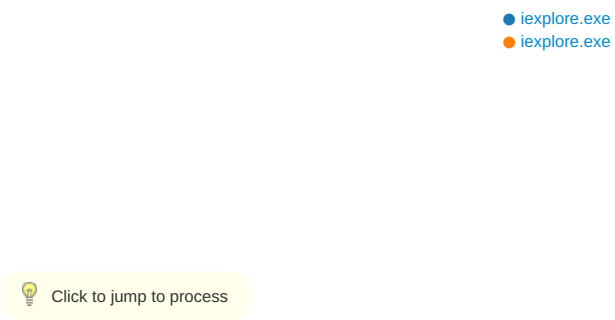
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 5, 2021 00:13:50.767678022 CET	143.204.90.122	443	192.168.2.4	49871	CN=sharethis.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Aug 17 02:00:00 CEST 2020	Thu Sep 16 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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Mar 5, 2021 00:13:50.767713070 CET	143.204.90.122	443	192.168.2.4	49869	CN=sharethis.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Aug 17 02:00:00 CEST 2020	Thu Sep 16 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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 5, 2021 00:13:50.768321037 CET	143.204.90.122	443	192.168.2.4	49870	CN=sharethis.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Aug 17 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Sep 16 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 6884 Parent PID: 800

General

Start time:	00:14:07
Start date:	05/03/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff615f00000
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	Completion	Count	Source Address	Symbol

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: 6928 Parent PID: 6884

General

Start time:	00:14:08
Start date:	05/03/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6884 CREDAT:17410 /prefetch:2
Imagebase:	0xc00000
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly

Copyright null 2021