ID: 363595
Cookbook: browseurl.jbs
Time: 22:48:46
Date: 04/03/2021
Version: 31.0.0 Emerald

Table of Contents

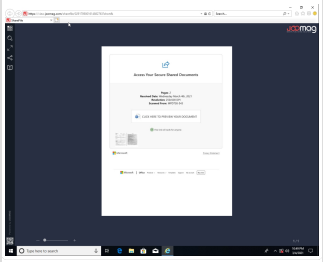
Analysis Report https://joom.ag/jSeI

Overview

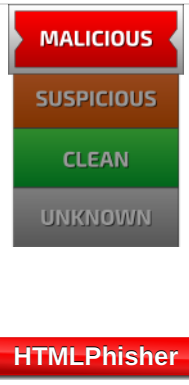
General Information

Sample URL:	http://https://joom.ag/jSeI
Analysis ID:	363595
Infos:	

Most interesting Screenshot:



Detection



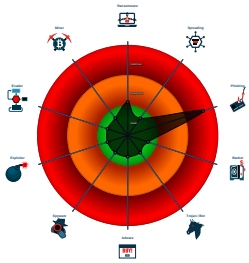
HTMLPhisher

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Phishing site detected (based on sh…
- Yara detected HtmlPhish_10
- Yara detected HtmlPhish_7
- HTML body contains low number of …
- HTML title does not match URL

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 3492 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5160 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3492 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

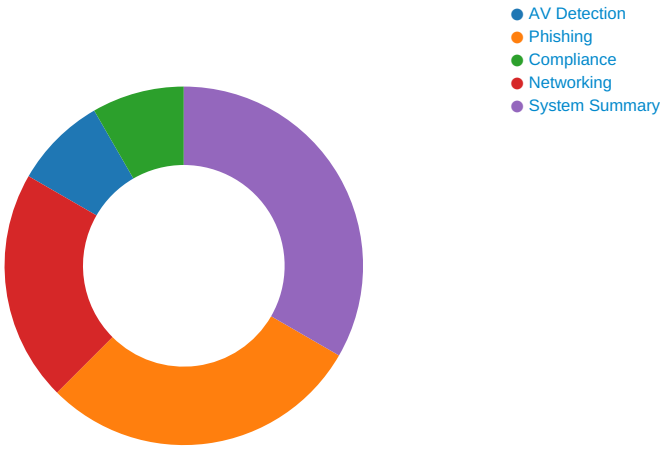
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INet Cache\IE\2WF3MMUU\adobe[1].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INet Cache\IE\2WF3MMUU\adobe[1].htm	JoeSecurity_HtmlPhish_7	Yara detected HtmlPhish_7	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Phishing:

Phishing site detected (based on shot template match)

Yara detected HtmlPhish_10

Yara detected HtmlPhish_7

Compliance:

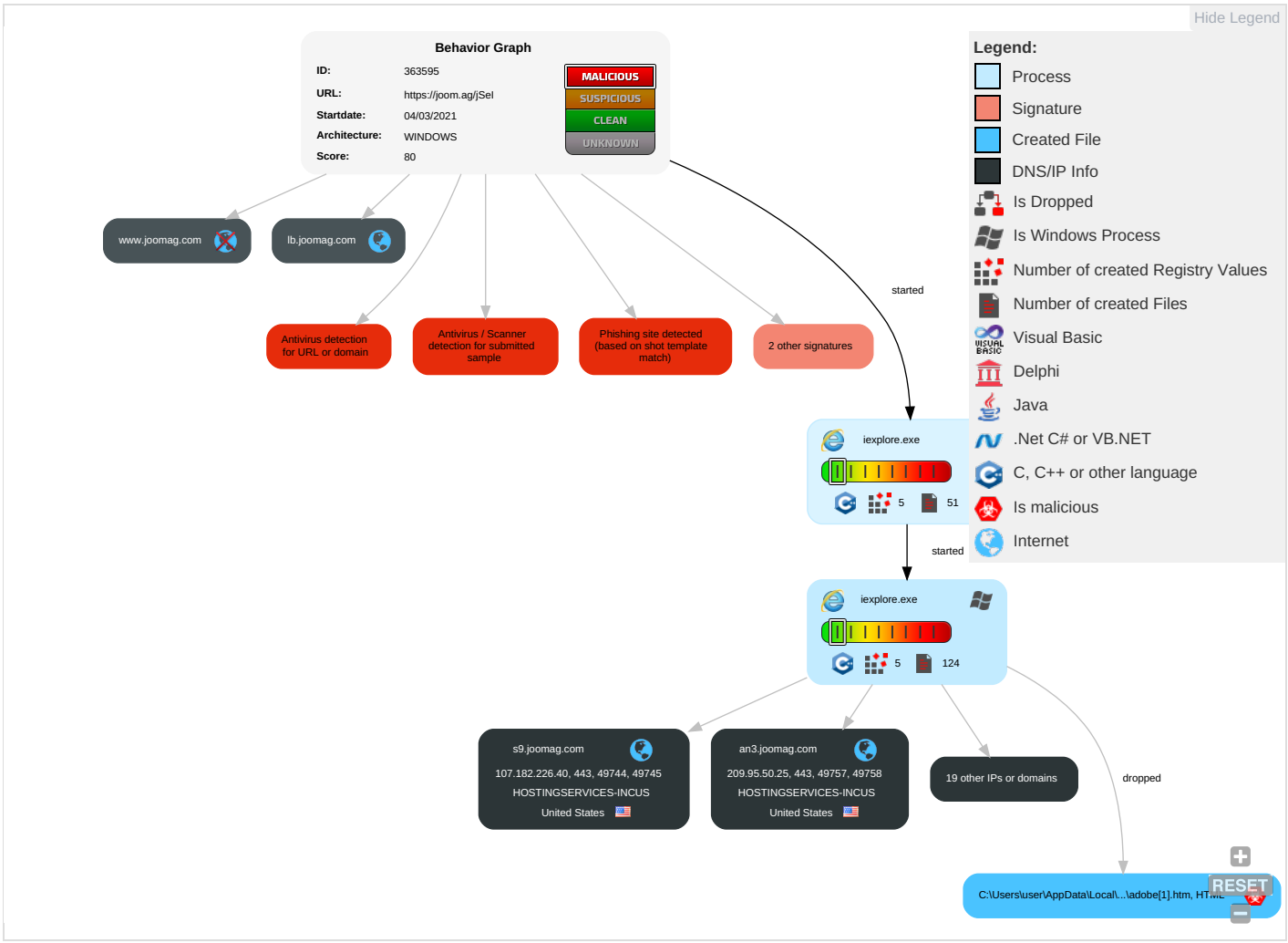
Uses new MSVCR Dlls

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

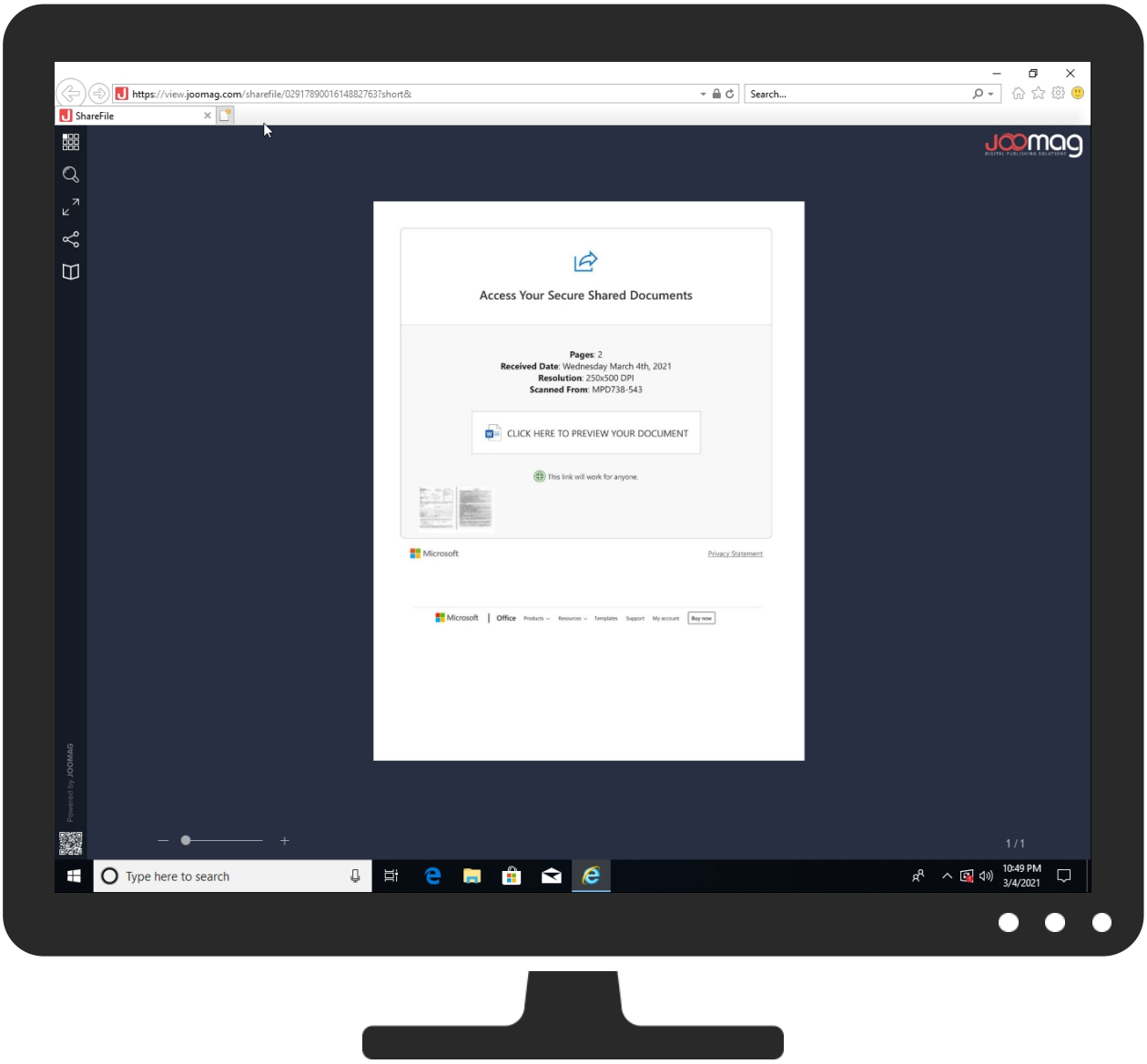
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://joom.ag/jSeI	0%	Virustotal		Browse
http://https://joom.ag/jSeI	0%	Avira URL Cloud	safe	
http://https://joom.ag/jSeI	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
browser.sentry-cdn.com	0%	Virustotal		Browse
www.google.co.uk	0%	Virustotal		Browse
joom.ag	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://view.joomag.com/sharefile/029178900161488276 3?short&	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://calfvessel.com/file/adobe/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://view.joomm/sharefile/029178900161488276 3?short&Root	0%	Avira URL Cloud	safe	
http://https://view.Root	0%	Avira URL Cloud	safe	
http://https://view.joom/file/adobe/9178900161488276 3?short&Root	0%	Avira URL Cloud	safe	
http://ianlunn.github.io/Hover/)	0%	Avira URL Cloud	safe	
http://https://view.joomag.co	0%	Avira URL Cloud	safe	
http://https://calfvessel.com	0%	Avira URL Cloud	safe	
http://https://view.joomjoomag.com/sharefile/029178900161488276 3?short&	0%	Avira URL Cloud	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://browser.sentry-cdn.com/5.11.2/bundle.min.js	0%	Avira URL Cloud	safe	
http://ianlunn.co.uk/	0%	URL Reputation	safe	
http://ianlunn.co.uk/	0%	URL Reputation	safe	
http://ianlunn.co.uk/	0%	URL Reputation	safe	
http://https://view.joomRoot	0%	Avira URL Cloud	safe	
http://https://calfvessel.com/file/adobe/9178900161488276 3?short&BG	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
lb.joomag.com	209.95.50.27	true	false		high
browser.sentry-cdn.com	151.101.194.217	true	false	• 0%, Virustotal, Browse	unknown
stats.l.doubleclick.net	108.177.15.154	true	false		high
cdnjs.cloudflare.com	104.16.18.94	true	false		high
www.google.co.uk	172.217.22.227	true	false	• 0%, Virustotal, Browse	unknown
calfvessel.com	92.38.171.82	true	false		unknown
s9.joomag.com	107.182.226.40	true	false		high
an3.joomag.com	209.95.50.25	true	false		high
joom.ag	209.95.50.27	true	false	• 0%, Virustotal, Browse	unknown
www.joomag.com	unknown	unknown	false		high
use.typekit.net	unknown	unknown	false		high
ka-f.fontawesome.com	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high
js-agent.newrelic.com	unknown	unknown	false		high
maxcdn.bootstrapcdn.com	unknown	unknown	false		high
s9cdn.joomag.com	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
p.typekit.net	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
view.joomag.com	unknown	unknown	false		high
bam-cell.nr-data.net	unknown	unknown	false		unknown

Contacted URLs

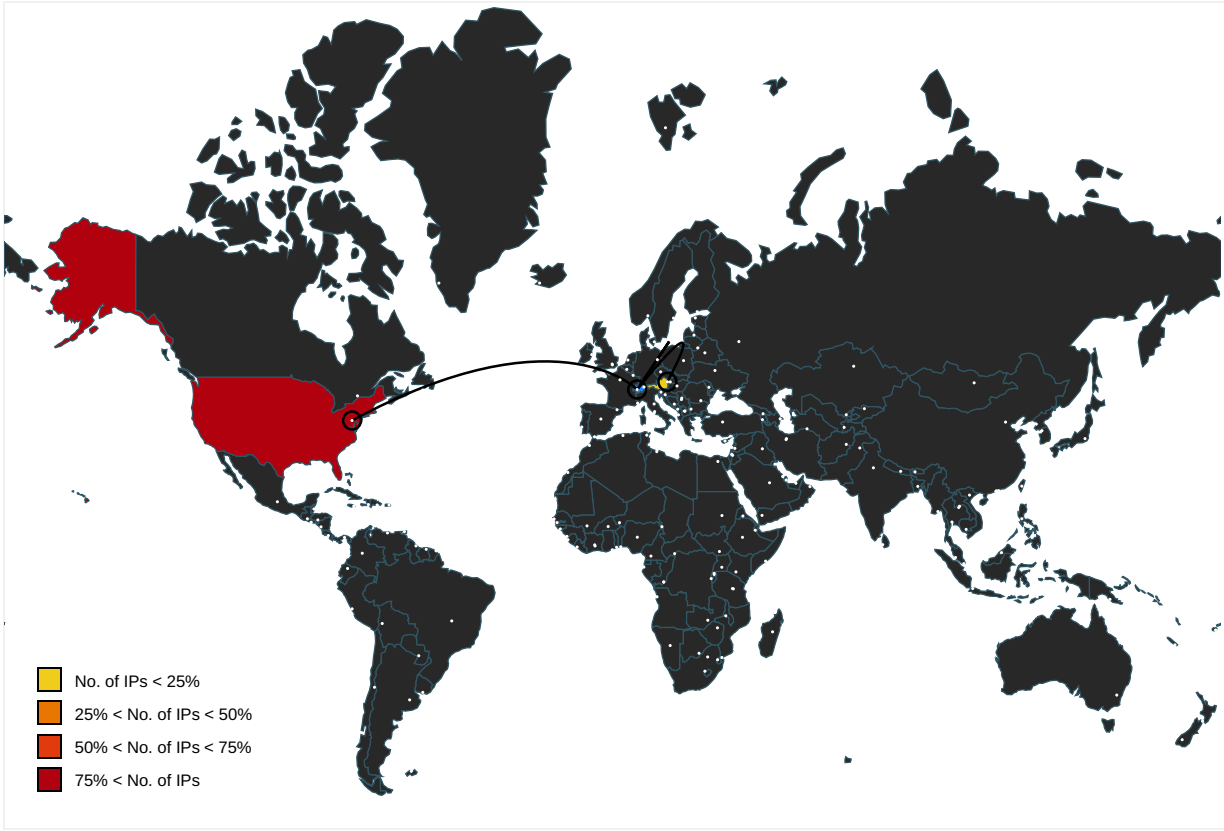
Name	Malicious	Antivirus Detection	Reputation
http://https://view.joomag.com/sharefile/029178900161488276 3?short&	false	• SlashNext: Fake Login Page type: Phishing & Social Engineering	high
http://https://calfvessel.com/file/adobe/	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://player.vimeo.com/video/	magazine[1].js.2.dr	false		high
http://https://view.joomag.com/sharefile/0291789001614882763?short&Root	{7E770D05-7D33-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false		high
http://https://view.joomm/sharefile/0291789001614882763?short&Root	{7E770D05-7D33-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://ka-f.fontawesome.com	585b051251[1].js.2.dr	false		high
http://https://code.jquery.com/jquery-3.2.1.slim.min.js	adobe[1].htm.2.dr	false		high
http://https://www.joomag.com/Frontend/WebService/getThumbnailSocial.php?mID=2420210&spread=0&1614889819	0291789001614882763[1].htm.2.dr	false		high
http://https://www.youtube.com/embed/	magazine[1].js.2.dr	false		high
http://typekit.com/eulas/00000000000000000000148a0	olb8zpk[1].js.2.dr	false		high
http://https://www.joomag.com/Frontend/mobile/viewer/	manifest.8e10809dba1c553a5a2a[1].js.2.dr	false		high
http://typekit.com/eulas/00000000000000000000148a6	olb8zpk[1].js.2.dr	false		high
http://typekit.com/eulas/00000000000000000000148a4	olb8zpk[1].js.2.dr	false		high
http://https://view.joomag.com/sharefile/0291789001614882763?short&BG	~DFF8E1FCFAEB5B2E87.TMP.1.dr	false		high
http://typekit.com/eulas/00000000000000000000148a2	olb8zpk[1].js.2.dr	false		high
http://https://fontawesome.com/license/free	free.min[1].css.2.dr	false		high
http://https://fontawesome.com	free.min[1].css.2.dr	false		high
http://https://view.Root	{7E770D05-7D33-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/twbs/bootstrap/graphs/contributors)	bootstrap.min[1].js.2.dr	false		high
http://https://use.typekit.net/af/e0b8be/00000000000000000000148a6/23/	olb8zpk[1].js.2.dr	false		high
http://https://view.joomag.com/sharefile/0291789001614882763?short&	~DFF8E1FCFAEB5B2E87.TMP.1.dr	false	• SlashNext: Fake Login Page type: Phishing & Social Engineering	high
http://https://www.joomag.com/res_mag/logos/2420210.PNG?1614882780	0291789001614882763[1].htm.2.dr	false		high
http://https://view.joom/file/adobe/917890016148827 63?short&Root	{7E770D05-7D33-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://vimeo.com/api/oembed.json?url=	main.2813cfbe59a2f8c75923[1].js.2.dr	false		high
http://https://www.joomag.com/Frontend/mobile/viewer/vendor.7bc4df7aaac8424047c3.js	0291789001614882763[1].htm.2.dr	false		high
http://https://www.joomag.com/Frontend/pixel/joomag-pixel.3df7f73f177625835141.js	0291789001614882763[1].htm.2.dr	false		high
http://https://use.typekit.net/af/3ba24d/00000000000000000000148a0/23/	olb8zpk[1].js.2.dr	false		high
http://https://www.joomag.com/Frontend/mobile/viewer/manifest.8e10809dba1c553a5a2a.js	0291789001614882763[1].htm.2.dr	false		high
http://https://stats.g.doubleclick.net/j/collect	analytics[1].js.2.dr	false		high
http://opensource.org/licenses/MIT).	popper.min[1].js.2.dr	false		high
http://https://kit.fontawesome.com/585b051251.js	adobe[1].htm.2.dr	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js	adobe[1].htm.2.dr	false		high
http://https://github.com/getsentry/sentry-javascript	bundle.min[1].js.2.dr	false		high
http://https://www.joomag.com/static/css/html5-viewer-external.css?_=5.1.6.0	0291789001614882763[1].htm.2.dr	false		high
http://https://www.joomag.com/Frontend/mobile/viewer/main.2813cfbe59a2f8c75923.js	0291789001614882763[1].htm.2.dr	false		high
http://ianlunn.github.io/Hover/)	hover[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://s9cdn.joomag.com/res_mag/1/1702/1702695/2420210/thumbs/spread/0.jpg?1614889819	0291789001614882763[1].htm.2.dr	false		high
http://https://www.joomag.com/Frontend/mobile/viewer/styles/main.867208e99122488d74f9a620279f9cd9.css	0291789001614882763[1].htm.2.dr	false		high
http://https://code.jquery.com/jquery-3.1.1.min.js	adobe[1].htm.2.dr	false		high
http://https://view.joomag.co	{7E770D05-7D33-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://calfvessel.com	{7E770D05-7D33-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://use.typekit.net/af/42fca5/00000000000000000000148a4/23/	olb8zpk[1].js.2.dr	false		high
http://https://view.joomjoomag.com/sharefile/0291789001614882763?short&	{7E770D05-7D33-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://cct.google/taggy/agent.js	gtm[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://code.jquery.com/jquery-3.3.1.js	adobe[1].htm.2.dr	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css	adobe[1].htm.2.dr	false		high
http://https://use.typekit.net/af/bc719c/00000000000000000001499c/23/	olb8zpk[1].js.2.dr	false		high
http://https://use.typekit.net/af/3d81f6/00000000000000000000148a2/23/	olb8zpk[1].js.2.dr	false		high
http://https://kit.fontawesome.com	585b051251[1].js.2.dr	false		high
http://https://use.typekit.net/af/1eef01/00000000000000000000148ac/23/	olb8zpk[1].js.2.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js	adobe[1].htm.2.dr	false		high
http://https://login.microsoftonline.com/common/login	adobe[1].htm.2.dr	false		high
http://https://getbootstrap.com)	bootstrap.min[1].js.2.dr, bootstrap.min[1].css.2.dr	false	• Avira URL Cloud: safe	low
http://https://www.joomag.com/Frontend/mobile/viewer/favicon.ico	029178900161488276 3[1].htm.2.dr	false		high
http://https://p.typekit.net/p.gif	olb8zpk[1].js.2.dr	false		high
http://https://www.google.%/ads/ga-audiences	analytics[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://browser.sentry-cdn.com/5.11.2/bundle.min.js	029178900161488276 3[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://ianlunn.co.uk/	hover[1].css.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://typekit.com/eulas/00000000000000000000148ac	olb8zpk[1].js.2.dr	false		high
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	bootstrap.min[1].js.2.dr, bootstrap.min[1].css.2.dr	false		high
http://https://github.com/IanLunn/Hover	hover[1].css.2.dr	false		high
http://typekit.com/eulas/00000000000000000001499c	olb8zpk[1].js.2.dr	false		high
http://https://s9cdn.joomag.com/res_mag/1/1702/1702695/2420210/thumbs/58582055.jpg?1614889819	029178900161488276 3[1].htm.2.dr	false		high
http://https://www.joomag.com/Frontend/WebService/getThumbnailSocial.php?mID=2420210&spread=0&width=500&161	029178900161488276 3[1].htm.2.dr	false		high
http://https://view.joomRoot	{7E770D05-7D33-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://calfvessel.com/file/adobe/91789001614882763?short&BG	~DFF8E1FCFAEB5B2E87.TMP.1.dr	true	• Avira URL Cloud: safe	unknown
http://https://dme0ih8comzn4.cloudfront.net/imaging/v3/editor.js	magazine[1].js.2.dr	false		high
http://https://www.joomag.com/static/js/magazine.js?_=5.1.6.0	029178900161488276 3[1].htm.2.dr	false		high
http://https://www.joomag.com/Frontend/mobile/viewer/normalize.d0dfb984f88d0dbb9fde.js	029178900161488276 3[1].htm.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
108.177.15.154	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
209.95.50.25	an3.joomag.com	United States		32780	HOSTINGSERVICES-INCUS	false
151.101.194.217	browser.sentry-cdn.com	United States		54113	FASTLYUS	false
92.38.171.82	calfvessel.com	Austria		202422	GHOSTRU	false
172.217.22.227	www.google.co.uk	United States		15169	GOOGLEUS	false
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
209.95.50.27	lb.joomag.com	United States		32780	HOSTINGSERVICES-INCUS	false
107.182.226.40	s9.joomag.com	United States		32780	HOSTINGSERVICES-INCUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	363595
Start date:	04.03.2021
Start time:	22:48:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://joom.ag/jSeI
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:	3
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:	• EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.phis.win@3/59@19/8
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://calfvessel.com/file/adobe/
Warnings:	Show All • Exclude process from analysis (whitelisted): ielowutil.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.147.198.201, 104.43.193.48, 40.88.32.150, 88.221.62.148, 142.250.185.200, 216.58.207.142, 13.88.21.125, 23.32.238.192, 23.32.238.210, 172.217.23.68, 151.101.2.110, 151.101.66.110, 151.101.130.110, 151.101.194.110, 23.37.33.211, 162.247.243.147, 162.247.243.146, 209.197.3.24, 209.197.3.15, 216.58.207.170, 172.217.23.42, 104.18.23.52, 104.18.22.52, 172.64.203.28, 172.64.202.28, 152.199.19.161 • Excluded domains from analysis (whitelisted): e6653.dscf.akamaiedge.net, cds.s5x3j6q5.hwcdn.net, ka-f.fontawesome.com.cdn.cloudflare.net, tls12.newrelic.com.cdn.cloudflare.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, skypedataprdcoleus15.cloudapp.net, go.microsoft.com, use-stls.adobe.com.edgesuite.net, www.googletagmanager.com, www.google.com, watson.telemetry.microsoft.com, www.google-analytics.com, kit.fontawesome.com.cdn.cloudflare.net, fonts.googleapis.com, p.typekit.net-v3.edgekey.net, www-google-analytics.l.google.com, ajax.googleapis.com, ie9comview.vo.msecnd.net, www-googletagmanager.l.google.com, f4.shared.global.fastly.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, cds.j3z9t3p6.hwcdn.net, skypedataprdcolwus15.cloudapp.net, a1988.dscg1.akamai.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

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\view.joomag[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):	746
Entropy (8bit):	5.072579959721037
Encrypted:	false
SSDEEP:	12:JsrUHla/J2QMQrsrsrsrsrUkbH3Zv3IuLG69wcVEdHwNYX4T44cB4rtPMzjJi7UR:WUQJ2Qr0000UkbJv3IuC6auEdcrbtP+t
MD5:	D66C0AC9AD591AF604109E7EBBE5D8D9
SHA1:	3F54B7C196CB1DAA41247448B8D94F1868DFE76B
SHA-256:	D80FA2BCE5FE3396681C52E1437E2698A713172712F8302B0C0D176BECB0B6FD
SHA-512:	B4911A06EF281979131801C5ED13CEF84F02F42DFCF9E8BB29718DD0E0023228DA450413E00C1A172F7F3D7F1BDB384B8E4A4D32AEA971EDC4E7FF100C9C11C9
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="__test" value="1" ltime="1126671888" htime="30871872" /></root><root></root><root></root><root></root><root></root><root><item name="joomag.analytics.data" value="{"readers":{"79901906-08d1-4be6-a7a0-a4ab5045df18":{"analytics-owner":"1702695","session":"ef3f94d7-7061-44bc-bd9b-a82978689ea6",,"alias":"c6c5801b-5dd5-4d4b-b9fa-48da14f1cae9","identifying":{"email":null,"status":"not_identified"},"created-on-server":false,"session-expiration":1614896376632}},"unsent-data":{"readers":[],"events":[]}}" ltime="1159991888" htime="30871872" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{7E770D03-7D33-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.848703921609644
Encrypted:	false
SSDEEP:	192:rJZ+ZP2vLWK6tK0ifKjYyzMQ3qBElCkDEl3sfElkY7jX:r/qeqh+VDELEUEb
MD5:	E19B9E9DA18A638FAC4C1C9C5AB79D16
SHA1:	4ABF4A5C6E8E0B3153354DBB5934761E022F07F7
SHA-256:	2B81F6F10B015DD98BC2F8FC421E2727CA494FB6F8EFE2286A5669816D8D37B6
SHA-512:	BCB34C6B4EFDD2CA13A57B6423D8284DEDC1DB81DC7CD64E24EEE54ED031EB8440B6999E3BD6531F1F095835A7EF62910E6744F32945DD7A378E93F5C777797
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\{7E770D05-7D33-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	38194
Entropy (8bit):	2.0196832514437375
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{7E770D05-7D33-11EB-90EB-ECF4BBEA1588}.dat	
SSDEEP:	192:rvZkQk6Sk3zjnB28qWyM/+z34ntmbtymDY4vt+yNr:rRtPLvwgjoontmZymDd1RJ
MD5:	571954E03C36DCEE83D36704A4BF1156
SHA1:	4EE592476BB9EE0CC055E89F1A6CFB26D6F006E3
SHA-256:	5DE450158BCB8B43DCE85C4F3DAAF30BEE9574400BF047AED54A2021B1728CFD
SHA-512:	5220809082D90FE00127B31C86809249C1DFC98A3296AB2A723596AF96BFBF73D97FD02D405FD79B31BD93B5B89D373F318CA0CA66915CFFEBC216CBDCB7707
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\{84EB8697-7D33-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5628393976496606
Encrypted:	false
SSDEEP:	48:Iw7GcprSGwpa8G4pQUGrapbSnZGQpKkG7HpRIaTGIpG:rhZaQc6iBSnzAvTIeA
MD5:	146CB607D235A28EAFA32BD6250A3E46
SHA1:	5098275B0B15B731359744B6286205B39ECC2F1F
SHA-256:	1C7E85163F5B01E4199A31E30F372EE9BD87E45D8489348CDAF2B98CE8161B62
SHA-512:	504CB9DD24056607FA700DBD91EFAD9DA23FB059EF821D3428EA86E3A13C682E03FECF1CDB2349CC046699D7C653DFD52B3A44FFB968AF03BD3626170EEF60 1
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):	419
Entropy (8bit):	5.93381936349089
Encrypted:	false
SSDEEP:	6:AmYR++V/l2MtbLcAMlGAYbv/lhPVjnDspH3ljBRQcGjLQ9H5LaGVXbgd2qFj1M:AHb/l2OgpltUv/72lljBRWPS5nVXAFpM
MD5:	14C3F70FB085768F54BFEE862D6E5145
SHA1:	4B84CF602AAA2D5C50A6707EA5B1DCF89C297082
SHA-256:	14C87ABEBF9A91451CDD2EFC44D4CA381E408DCD5024DD9A1A646C40EB824B85
SHA-512:	1B4B97A758A77A5BADAB5BC6CFCDF93CE201EFD200E5D419B727E5A6291A1B9E2960190DDBD464C39653999626919B015CE0E531DFAF27B15EB5A3566A8107I 5
Malicious:	false
Reputation:	low
Preview:	9.h.t.t.p.s.:././.w.w.w...j.o.o.m.a.g...c.o.m./.F.r.o.n.t.e.n.d./.m.o.b.i.l.e./.v.i.e.w.e.r./.f.a.v.i.c.o.n...i.c.o.....PNG.....IHDR.....a....tEXtSoftware.Adobe ImageReadyq.e ....IDATx.b|.....P.@.hd.....JJ..i.`...J.8..V.4...b.31P.F.@3@`..0...a.ja..PL...()...W.L.b.d.]S..s.F.F.n.6g..8L.2@.. .<.....Xm...+..~...O`7.,.....j..?./3.....(;.....2..3.....IEND.B`.. .....UA`.....UA`....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\02917890016148827631[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):	28681
Entropy (8bit):	5.377445724616845
Encrypted:	false
SSDEEP:	768:RGm1KHz/JNVRGJIeGJ90eth0pEY2uIIqvSTp:ULeJetCphZv9
MD5:	78FF6DD9DC275F12255D306E3185B2C8
SHA1:	2A317EF778FCBB84F7A4EF0A328763549B646363
SHA-256:	05B73A0A832E0B0FC7399DBF1774E80CC6CACB83126C0BA8CB8D691B8789D4D5
SHA-512:	736DD48B1FC069C4FBF92A98D6A19AA92AB33E90E834B444E03D2A44F8FC3FB503E0980B89F879BE98D4856FE8A386C7EA884BF7A395230B11E2E4CF6C7316B 3
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\0291789001614882763[1].htm	
Reputation:	low
Preview:	<!DOCTYPE HTML>.<html lang="en" data-fb-app-id="185909391439821">.<head>. <meta http-equiv="Content-Type" content="text/html; charset=utf-8"><script type="text/javascript">(window.NREUM||(NREUM={})).loader_config={xpid:"VQEOWFRQGwIBXVFWBQM=",licenseKey:"e2270d116b",applicationID:"1190422"};window.NREUM||(NREUM={}),__nr_require=function(t,e,n){function r(n){if(!e[n]){var i=e[n]={exports:{}};t[n][0].call(i.exports,function(e){var i=t[n][1][e];return r(i||e)},i,i.exports)}return e[n].exports}if("function"==typeof __nr_require)return __nr_require;for(var i=0;i<n.length;i++)r(n[i]);return r}({1:[function(t,e,n){function r(t){try{c.console&&console.log(t)}catch(e){}}var i,o=t("ee"),a=t(23),c={};try{i=localStorage.getItem("__nr_flags").split(","),console&&"function"==typeof console.log&&(c.console=!0,i.indexOf("dev")!==-1&&(c.dev=!0),i.indexOf("nr_dev")!==-1&&(c.nrDev=!0))}catch(s){}c.nrDev&&o.on("internal-error",function(t){r(t.stack)}),c.dev&&o.on("fn-err",function(t,e,n){r(n.stack)}),c.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\15.70ea2a8c03ea7ff25ab5[1].js	
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):	12030
Entropy (8bit):	4.897721379060308
Encrypted:	false
SSDEEP:	192:zTpsxBdZTgSlTuqTHWOokFz7exKy8lP1T8Fq8sc8auJK3yZO+sOWl:Pc1NqjFfFuxv8lP1o/R8augyZOdl
MD5:	64991CAAC2AFC2D864D53F6F50F2AC5E
SHA1:	C6F0816D8E68E4F5D8912C5062A6D438F3B7675C
SHA-256:	1C1AFECF3ECE6A0238218FE66E1EEB80F4A190FDFC5DA57B428AD730E4E576DB
SHA-512:	9CC00C71861C7EF224A9C15A8BFAD94B2006C50E4399EEDA6E8740E7DDB45AB55DA427E3AE4BBEEA855E9CA8F16E8633CB487A4D1062ED77D5F3F715B9792F2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.joomag.com/Frontend/mobile/viewer/15.70ea2a8c03ea7ff25ab5.js
Preview:	webpackJsonp([15],{396:function(a,e){a.exports={en:{actions:{download_pdf:"Download PDF",expand:"Expand",full_screen:"Fullscreen",exit_full_screen:"Exit Fullscreen",info_page:"Info Page",subscribe:"Subscribe",share:"Share",other_issues:"Publications Panel",page_overview:"Contents",print_pages:"Print Page(s)",full_version:"Full Version",mute:"Mute",unmute:"Unmute",zoom_qr:"Zoom QR Code",search:"Search",text_only:"Text-only",exit_text_only:"Exit text-only mode"},views:{touch_actions_note:"Use two fingers to slide or zoom\n",scroll_actions_note:"Use ctrl + scroll to zoom or scroll\n",search_view:{search:"Search",loading:"Loading",no_results:"No results for .{0}.",results:"{0} results for .{1}.",load_more_results:"Load more results",page:"Page {0}",error:"Something went wrong, please try again later."},text_only:{toolbar:{page:"Page"}},adult_confirmation:{title:"The publication you are about to view contains adult content",desc:'By clicking "Show Adult Content" button you verify yo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\adobe[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	11857
Entropy (8bit):	4.812639632272608
Encrypted:	false
SSDEEP:	192:K2FI5vEJKnYmrDfG4RywAOT+UY/t4IdtWPmd:1nmRnAKyt48tz
MD5:	8B525EE23344A0EE2B3EC02B5478500A
SHA1:	82443BF89D02DE9009D5E85A8C1D9725EE3020D3
SHA-256:	4AF6302A1FB709D92E3C6242F0F5257C8964C0A0859BC9A328350895F6B0EB40
SHA-512:	53693C7B753CB3E80DADA744781779F3E8B6F5075733D9D90320C7A76BFC168D21FBBE98EE253E8FFC5AFE8EEDE09F2455DF57C3833019D3FBA422ACE317ABD
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\adobe[1].htm, Author: Joe Security • Rule: JoeSecurity_HtmlPhish_7, Description: Yara detected HtmlPhish_7, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\adobe[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://calfvessel.com/file/adobe/
Preview:	...<!doctype html>..<html lang="en">..<head>.. <script src="https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>.. <script src="https://code.jquery.com/jquery-3.1.1.min.js">.. <script src="https://code.jquery.com/jquery-3.3.1.js" integrity="sha256-2Kok7MbOyxpgUVvAk/HJ2jigOSYS2auK4Pfzbm7uH60=" crossorigin="anonymous"></script>.. Required meta tags -->.. <meta charset="utf-8">.. <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">.... Bootstrap CSS -->.. <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css" integrity="sha384-Gn5384xqQ1aoWXA+058RXPxPg6fy4IWvTNh0E263XmFcJlSAwiGgFAW/dAiS6JXm" crossorigin="anonymous">.. <link href="https://fonts.googleapis.com/css?family=Yellowtail&display=swap" rel="stylesheet">.. <script src="https://kit.fontawesome.com/585b051251.js" crossorigin="anonymous"></script>.. <title>Share Point Online</title>.. <link

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\bootstrap.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\bootstrap.min[1].css	
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}h tml{font-family:sans

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"),requir e("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.pro totype.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\bundle.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	55880
Entropy (8bit):	5.217597506517523
Encrypted:	false
SSDEEP:	768:2iSDfIee5GohBduSvT3Hzp8hvUntFpsmpqXzIq+2H51sj2CF3+TSEXLimd:2HAx5hBduSvT3lhFHpls5qTe
MD5:	D33EF5731DB495D5A0AC66BB566032C2
SHA1:	EE1E5070EC879D17AE785F74B21C4E4E0F0F0597
SHA-256:	85BB43DAE06F4D48B885E878395E5984A2AFB942FF778DFB8BDA87D8EB475BC8
SHA-512:	B988980CADCD07CBC3CB14489C6319884380C6B9246A6675EC2456163E9D10250AB373681D787C98879DF52F5D8230C11275C78DA0092F4EE334897A70BF4642
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://browser.sentry-cdn.com/5.11.2/bundle.min.js
Preview:	/*! @sentry/browser 5.11.2 (bc97f92f) | https://github.com/getsentry/sentry-javascript */.var Sentry=function(n){var t=function(n,r){return(t=Object.setPrototypeOf||{__pr oto__:[]}instanceof Array&&function(n,t){n.__proto__=t}||function(n,t){for(var r in t)t.hasOwnProperty(r)&&(n[r]=t[r])})(n,r)};function r(n,r){function e(){this.constructor=n}t(n,r),n.prototype=null===r?Object.create(r):(e.prototype=r.prototype,new e)}var e=function(){return(e=Object.assign||function(n){for(var t,r=1,e=arguments.length;r<e;r++)for(var i in t=arguments[r])Object.prototype.hasOwnProperty.call(t,i)&&(n[i]=t[i]);return n}).apply(this,arguments)};function i(n){var t="function"==typeof Symbol&&n[Symbol.i terator],r=0;return t?t.call(n):{next:function(){return n&&r>=n.length&&(n=void 0),{value:n&&n[r++],done:!n}}}}function o(n,t){var r="function"==typeof Symbol&&n[Symbol.i terator];if(!r)return n;var e,i,o=r.call(n),u=[];try{for(;(void 0===t||t-- >0)&&!(e=o.next()).done;)u.push(e.value)}catch(n){i={error:n}}fin

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\e2270d116b[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.340020120659463
Encrypted:	false
SSDEEP:	3:U3KTDW3MiqVkMWVrfUh:H6NukMWVr8h
MD5:	06DD80AEB628C60DC680BC7A4BEE6651
SHA1:	8C86EB7DDFF5E1E5D527BD7A41C9D3F6767E23E0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\e2270d116b[1].js	
SHA-256:	5E864C2E3F674C60970513411EAEEEAFD2D615D842E65EC01D09CCFCB4A7B38D
SHA-512:	C6EE8252743A760AD7BEE017FF7A804B6E34236764BC5630289D5E4C7C15E38CB971F161821586F0235882FD581630F1531FD6396761BF1284581CD8C2CAC4C6
Malicious:	false
Reputation:	low
Preview:	NREUM.setToken({'stn':0,'err':1,'ins':1,'cap':0,'spa':1})

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	267
Entropy (8bit):	6.689912640860459
Encrypted:	false
SSDEEP:	6:6v/lhPVjnDspH3ljBRQcGjLQ9H5LaGVXbgd2qFjp:6v/72lljBRWPS5nVXAFN
MD5:	ADE8D9C3689EC45EA5DE1D9AF2537570
SHA1:	FF5D323C7B817F7246D6797D87F0DE4FD5C894E8
SHA-256:	92FB6872A27431518F6C8374776CCF2218A09986EA3E3D2D9A86E80FD0FDAEB5
SHA-512:	16F13D8C6DEA7974D1247974F4343A18B624408D74428CBE6ED69A122BCDB17D46A9C865953696F63FB199A3583528388022C7A39A05F621B2AD0BDE4993579E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.joomag.com/Frontend/mobile/viewer/favicon.ico
Preview:	.PNG.....IHDR.....a....tEXtSoftware.Adobe ImageReadyq.e<....IDATx.b|.....P.@.hd.....JJ..i.`...J.8..V.4...b.31P.F.@3@`..0...a.ja..PL...()...W.L.b.d.]S..s.F.F.n.6g..8 L.2@.. .<.....Xm...+..~...O`7.,.....j..?./3.....(;.....2..3.....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\nr-1198.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	28120
Entropy (8bit):	5.31469238173269
Encrypted:	false
SSDEEP:	384:yZevj5awnX8RfzD7WdPs8tzmwUyAH77jx+zJTREUi2bikgHIvYboLLAJ1fFKohtJ:yZUQKi8tzA76AFIAbo/M1jtnWE5
MD5:	59C98195BA35E0B45CBE2E5BEEBD1AC8
SHA1:	BB1DD82667456B0B608750BBF8D2871A018535B0
SHA-256:	39893061747F88B837A34D0395D05FCA83E7CD5BBF2D582D181A73C5C9A174C6
SHA-512:	9CCE07757B9475D6A3C20CAD19A4775422EED4AE018F27521D4EF29FB89C5B5CEFB3991A6CDD3E422B532C32D43699A5EE86F61FD7FEA9FCDB90F2670A40E762
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://js-agent.newrelic.com/nr-1198.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\nr-1198.min[1].js	
Preview:	!function(n,e,t){function r(t,i){if(!e[t]){if(!n[t]){var a="function"==typeof __nr_require&&__nr_require;if(!i&&a)return a(t,!0);if(o)return o(t,!0);throw new Error("Cannot find module '"+t+"'")}var u=e[t]={exports:{}};n[t][0].call(u.exports,function(e){var o=n[t][1][e];return r(o||e)},u,u.exports)}return e[t].exports}for(var o="function"==typeof __nr_require&&__nr_require,i=0;i<t.length;i++)r(t[i]);return r}({1:[function(n,e,t){e.exports=function(n,e){return"addEventListener"in window?window.addEventListener(n,e,!1):"attachEvent"in window?window.attachEvent("on"+n,e):void 0}},{}],2:[function(n,e,t){function r(n,e,t,r,i){|[n]||([n]={});var a=l[n][e];return a||(a=l[n][e]={params:t||{}},i&&(a.custom=i),a.metrics=o(r,a.metrics),a}function o(n,e){return e||(e={count:0}),e.count+=1,f(n,function(n,t){e[n]=i(t,e[n])}),e}function i(n,e){return e?(e&&!e.c&&(e={t:e.t,min:e.t,max:e.t,sos:e.t*e.t,c:1}),e.c+=1,e.t+=n,e.sos+=n*n,n>e.max&&(e.max=n),n<e.min&&(e.min=n),e):{t:n}}function a(n,e){return

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\olb8zpk[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	18084
Entropy (8bit):	5.567560853086973
Encrypted:	false
SSDEEP:	384:6yO2tpIgIPs51iRm2lIew42noFeFsP9btiCtpIaCR:6y8q1iRm2XwMqsbbt6J
MD5:	5076E0879850567ED8A5CE8D65F00DFD
SHA1:	1733D25CAF88876D3F6B44BFD04751E02AA717E3
SHA-256:	B7F0115AFBD3505857C7A7515CBDFD9B595A750B8A0C576DB45992C2F87C0355
SHA-512:	52A0923D550E39914EE7C239B1FB48A69A4C27E7F06206E94E7296866D17835EB053393BD89ED4C9761B07DD24B81F04FC964559B487C61DA4EE7BA4AE10CF1(
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/olb8zpk.js
Preview:	/*. * The Typekit service used to deliver this font or fonts for use on websites. * is provided by Adobe and is subject to these Terms of Use. * http://www.adobe.com/products/eulas/tou_typekit. For font license. * information, see the list below.. *. * proxima-nova:. * - http://typekit.com/eulas/00000000000000000000148ac. * - http://typekit.com/eulas/00000000000000000000149c. * - http://typekit.com/eulas/00000000000000000000148a0. * - http://typekit.com/eulas/00000000000000000000148a6. * - http://typekit.com/eulas/00000000000000000000148a4. * - http://typekit.com/eulas/00000000000000000000148a2. *. * . 2009-2020 Adobe Systems Incorporated. All Rights Reserved.. */.if(!window.Typekit)window.Typekit={};window.Typekit.config={"a":"1029652","c":[".tk-proxima-nova","\"proxima-nova\",sans-serif"],"fi":[137,139,171,173,175,5474],"fc":[{"id":137,"family":"proxima-nova","src":"https://use.typekit.net/af/1eef01/00000000000000000000148ac/23/{format}{?primer,subset_id,fvd,v}","descriptors":

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\other1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 190 x 187, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	21882
Entropy (8bit):	4.268463452779894
Encrypted:	false
SSDEEP:	192:ESCkiDw7e9Mg/wio0EYm9FWyo2XdJfXoOZdEDfmiIJQdiRVi/WTanY:DBiDw7eAdq+FWyo2/fXoZbDlJ0ci/BnY
MD5:	6843A244E12FAB158AA189680B5E7049
SHA1:	0E1C691F87CC4FA35C88344974F2829C40176B70
SHA-256:	3A9B144D6482B78AFC4E0A940A1D3C22240F14FA535B808CF4DAB9635339569F
SHA-512:	145010C45B6B83EA4005EB367C0507959FF0817E482F19E9973504081ACAE1B7827CBD1172CEC7732B13F4E0CEC058271BD6700444FBCF61FB6A3C068A3744C4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://calfvessel.com/file/adobe/images/other1.png
Preview:	.PNG.....IHDR.....$.... cHRM..z&.....u0...`..:....p..Q<....sRGB.....gAMA.....a.....pHYs.....:.iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?>.<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c067 79.157747, 2015/03/30-23:40:42 ">. <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">. <rdf:Description rdf:about="". xmlns:xmp="http://ns.adobe.com/xap/1.0/". xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/". xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#". xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/". xmlns:dc="http://purl.org/dc/elements/1.1/". xmlns:tiff="http://ns.adobe.com/tiff/1.0/". xmlns:exif="http://ns.adobe.com/exif/1.0/">. <xmp:CreatorTool>Adobe Photoshop CC 2015 (Windows)</xmp:CreatorTool>. <xmp:CreateDate>2020-01-18T21:59:57+05:00</xmp:CreateDate>. <

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\p[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):	35
Entropy (8bit):	2.9302005337813077
Encrypted:	false
SSDEEP:	3:CUHaaatrllH5:aB
MD5:	81144D75B3E69E9AA2FA3E9D83A64D03
SHA1:	F0FBC60B50EDF5B2A0B76E0AA0537B76BF346FFC
SHA-256:	9B9265C69A5CC295D1AB0D04E0273B3677DB1A6216CE2CCF4EFC8C277ED84B39
SHA-512:	2D073E10AE40FDE434EB31CBEDD581A35CD763E51FB7048B88CAA5F949B1E6105E37A228C235BC8976E8DB58ED22149CFCCF83B40CE93A28390566A2897574A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://p.typekit.net/p.gif?s=1&k=olb8zpk&ht=tk&h=view.joomag.com&f=137.139.171.173.175.5474&a=1029652&js=1.20.0&app=typekit&e=js&_=1614894575143

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\p[1].gif	
Preview:	GIF89a.....,.....;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\2420210[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 180 x 45, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	5254
Entropy (8bit):	7.8635000299486
Encrypted:	false
SSDEEP:	96:b96HZIlFYo6hK8ntiVOaK+hB9NrspgGKEvWjGV1TmKqu+PFCxt:bSCktntiVOaK+hzNIilu1MQt
MD5:	E1A55E85CB8B88AF96DDC9BBCC83E7A0
SHA1:	FF1549872E19ED1CEB5D2316DAD779F81F84F0A3
SHA-256:	9588DCB72AC03F9D7386F8A602D75126751E22B8504FE4B9E19F3B62EBBA0524
SHA-512:	79A6D98FBD950BDABD2960CD1942E350BE126D8220CC30AEE6A3F3DAAC07A760717D90658C1EBB8A06416C1555BBCAEAAE953B0A3A5D89940049133E84270C7E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.joomag.com/res_mag/logos/2420210.PNG?1614882780
Preview:	.PNG.....IHDR.....-.....A.....tEXtSoftware.Adobe ImageReadyq.e<...viTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.5-c021 79.155772, 2014/01/13-19:44:00 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:2c8aeb7d-821b-4e67-84aa-fe9db2c20908" xmpMM:DocumentID="xmp.did:3C44D3DC2AF511E5A63EE9E03B400364" xmpMM:InstanceID="xmp.iid:3C44D3DB2AF511E5A63EE9E03B400364" xmp:CreatorTool="Adobe Photoshop CC 2015 (Windows)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:05066b20-a59c-f841-a001-be6b5b8e6ef5" stRef:documentID="xmp.did:2c8aeb7d-821b-4e67-84aa-fe9db2c20908"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>...*....IDATx..].xU.....E..`..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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:	2CD82E0DCD1381447522CFFD610136513323E5D2980FAE730801FE8BBA580FF7FDF9CB8D2E9AC794D6F2FB59C724EDA71BECE7CAA72C775BC963E1A54B30ECB
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.fontawesome.com","detectConflictsUntil":null,"iconUploads":{},"id":132286382,"license":"free","method":"css","minify":{"enabled":true},"token":"585b051251","v4FontFaceShim":{"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,writable:!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\9026IKNJ\d[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 59940, version 0.0
Category:	downloaded
Size (bytes):	59940
Entropy (8bit):	**7.994140772663277**
Encrypted:	**true**
SSDEEP:	1536:bMRUowMIdMg7LpJ3/ReRCiVPXa6c4lqSV:4RUzhdLLp9wPXa65lD
MD5:	3AEB74FE14E1ACCAE157879343062A13
SHA1:	7A736AD47EE70212EEB9CD4179826F9CB8D55781
SHA-256:	E3E487D6036BB95CCD6D97CA641B5FA6ED85FF93E11A5649C72534AF0DD272C3
SHA-512:	111BBBA41ACCC2D47A492743F05511C354CAA6A7F61062F0D2EFCB2485DB36DBAF797C37C7C01ABA46E16FE116D81A69E13736C2BE37AE0F303648B537C250B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/3ba24d/00000000000000000000148a0/23/d?subset_id=1&fvd=n1&v=3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\d[1]	
Preview:	wOFF.....$.....`.....DYNA...h...z.....*.FFTM.....]..,GDEF.....R...Z.s..GPOS...8.....3.F!"(GSUB.....P...\..H.OS/2.....Y...`~W.acmap...`.....cvt .....R ..fpgm.....e#./.gasp.....glyf...\.....K..F.rhead.....4...6..<.hhea...$...!...$...-hmtx...`.....h....loca...8.....6b4.6maxp...H... ... .B..name.....H>..post...L..... ... (prep...x...O...O...4.....o1.....H.....x.....6.<.<.B.:.>.5.@..x.]Q.N[A.....c..hS.fB...$.W...vc9B.\.b\..P Q..k.h().A..R>.O@bfM.(....s..r..]Z.y..R.....v...t}...v.@..^.n...`3.rG....-.!.i'P....6...>.d..AK3MO....B`...0...../X....C.i*..s*..Ks....k..vp&"?..hj..@._.:.z>.b.r.0...S.d".f2].T-3.up...;X.Js....U.....-.2KC...*1B.$.BN9w.?)P>..1....a..q.50.....fS.{.0~.G..o..>..6F ..X.`...QU...s/.....3.%`y.._'..;6..em.C.....2....U.....tJ.....p.X...R.v....`H.F..h-;.*...d/.*.....x.c`d```b8z...x~.....".~Ul...V.....r.....R..x..ON.@..?.....v5. b;.T..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\d[2]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 60240, version 0.0
Category:	downloaded
Size (bytes):	60240
Entropy (8bit):	**7.993033134446386**
Encrypted:	**true**
SSDEEP:	1536:g/j1fMtxM2e+ZgdhJ2kNSHS/D5M46tEE+tMUl9819V:gF72e+ydL2kSHyD5ytHL1H
MD5:	1E15B536F74EF394FCEC8470F8D64323
SHA1:	50942FD78ECBA94C12DA7E63866585B26CED24C5
SHA-256:	4A4E9A7F3425D3D460A9FFC77A56391B62AF222391DB604B5924D90637549204
SHA-512:	4AB0043221C4E0CC2922ED33CD414A37861145DB3AAB79132059C8074B1F15662D030D462A63B59B51F24F74099DF7AECDDC7468C954A41B862ACDAF0A27BC4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/e0b8be/00000000000000000000148a6/23/d?subset_id=1&fvd=n6&v=3
Preview:	wOFF.....P.....DYNA.....z.....*.FFTM.....]...GDEF...(...R...Z.s..GPOS...|.....3.N...GSUB.....P...\..H.OS/2.....Y...`....cmap.....cvt .....0...0... Jfpgm.....e#./.gasp.....glyf...T.....F...b.head.....5...6..;.hhea...h...!...$...ihmtx...X.....h.}&.loca...d.....6.E..maxp..... ... .B.Tname.....u.C).post...x..... ...(prep..... ..s....^`.....o1.....2.....x.....6...|.....n.....u.....x.]Q.N[A.....c..hS.fB...$.W...vc9B.\.b\..P Q..k.h().A..R>.O@bfM.(....s..r..]Z.y..R.....v...t}...v.@..^.n...`3.rG....-.!.i 'P....6...>.d..AK3MO....B`...0...../X....C.i*..s*..Ks....k..vp&"?..hj..@._.:.z>.b.r.0...S.d".f2].T-3.up...;X.Js....U.....-.2KC...*1B.$.BN9w.?)P>..1....a..q.50.....fS.{.0~.G..o..>..6F..X.`. ..QU...s/.....3.%`y.._'..;6..em.C.....2....U.....tJ.....p.X...R.v....`H.F..h-;.*...d/.*.....x.c`d```b8....x~.....".~U....V.=..].....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\d[3]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 61612, version 0.0
Category:	downloaded
Size (bytes):	61612
Entropy (8bit):	**7.992135320284749**
Encrypted:	**true**
SSDEEP:	1536:C1QmG2C528LvuA6DfzlNxlpgCMbY9lgaiV:CCmqPG1zznxlEMma4
MD5:	D26D2BAB4625361DA030917B4FA4CBF0
SHA1:	972FF9E8DF21F1CAE4B0ABA7C36577A72E18CD8A
SHA-256:	5F8EE1622F6CDD2E3B343DB9BC25A58053C24959A7D72242E783ABD6C65A9070
SHA-512:	231BB6C230F909CD8ED5C361B8DAD45D362B9B9172FEA575FF85D82B4E20EDF800F4125971DED7EBA594F9B03906891FF74D96422B2E000FECAD6624879A7CD D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/42fca5/00000000000000000000148a4/23/d?subset_id=1&fvd=n4&v=3
Preview:	wOFF..... .....DYNA.....z.....*.FFTM.....]...GDEF...8...R...Z.s..GPOS.....&..3.Nm.,GSUB.....P...\..H.OS/2.....Y...`~..|cmap.....cvt .....2...2.A. 0fpgm.....e#./.gasp.....glyf.....Kll.+.head.....4...6.E;.hhea...x...!...$.I.-hmtx.....hU.X.loca.....6Wm..maxp..... ... .B..name.....iW.T.post..... ... (prep.....>.....o1.....x.....6...`.n.|.....Z.....O...t.c.....x.]Q.N[A.....c..hS.fB...$.W...vc9B.\.b\..P Q..k.h().A..R>.O@bfM.(....s..r..]Z.y..R.....v...t}...v.@..^.n... `3.rG....-.!.i'P....6...>.d..AK3MO....B`...0...../X....C.i*..s*..Ks....k..vp&"?..hj..@._.:.z>.b.r.0...S.d".f2].T-3.up...;X.Js....U.....-.2KC...*1B.$.BN9w.?)P>..1....a..q.50.....fS.{.0~.G.. o..>..6F..X.`...QU...s/.....3.%`y.._'..;6..em.C.....2....U.....tJ.....p.X...R.v....`H.F..h-;.*...d/.*.....x.c`d```b8...KW<..W.y..@..S.*....+.>.(a..r9.j.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\d[4]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 61728, version 0.0
Category:	downloaded
Size (bytes):	61728
Entropy (8bit):	**7.992796812103739**
Encrypted:	**true**
SSDEEP:	1536:nl+B1ouiahr0GFFTSfPu1z6fsrFJm4w5sKV:tB1hrlF5SnK+T4w6g
MD5:	C30498C311ECC433CB7CD23D32159AFC
SHA1:	F442B2B9EAAEE7FF71F57EBAA58734B4724FAC6A
SHA-256:	9F46E13E2EC896C2461E4C55C7393A69F7E70D85276544AC2693C42F3BC1DC89
SHA-512:	B955D91B79E2E5AEB0563ECD18935DB7FC2BE3999CB613455F04131D75A8B0748E8442D760365656C9360284343161F3B6DF068E4545E71614E94E9BB7FACF88
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/3d81f6/00000000000000000000148a2/23/d?subset_id=1&fvd=n3&v=3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\d[4]	
Preview:	wOFF..... .....DYNA.....z.....*.FFTM.....]...GDEF.....R...Z.s..GPOS...h...#..3.M...GSUB.....P...\..H.OS/2.....Y...`~W.ocmap...\.....cvt .....*...*.. .6fpgm.....e#./.gasp.....glyf.....d..NX8.c.head.....4...6..;.hhea...T...!...$....hmtx...@.....h..}.loca...8.....6.A.Tmaxp...x... ... .B..name.....Q..p.post...H..... ... (prep.....i...v..ym.....o1.....x.....6.h.R.\.^.h.r.Y.z.`.d.m.j.t.L.F.J.f..x.]Q.N[A.....c..hS.fB...$.W...vc9B.\.b\..P Q..k.h().A..R>.O@bfM.(....s..r..]Z.y..R.....v...t}...v.@..^.n ...`3.rG....-.!.i'P....6...>.d..AK3MO....B`..0...../X....C.i*..s*..Ks....k..vp&"?..hj..@._:.z>.b.r.0...S.d".f2].T-3.up...;X.Js....U.....-.2KC...*1B.$.BN9w.?)P>..1....a..q.50.....fS.{.0~. G..o..>..6F..X.`...QU...s/.....3.%`y.._'..;6..em.C.....2....U.....tJ.....p.X...R.v....`H.F..h-;.*...d/.*.....x.c`d```b8z%1.I<..W.y..@..S.*.....`..r9.j....+..x...J.A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\gmail[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1280 x 1280, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	66743
Entropy (8bit):	7.712342056984168
Encrypted:	false
SSDEEP:	1536:FxqKcVqezl0vLoYxEuKoYk5LHjGkT3b1mQOEj0+R+EH:FsK2qezl0zoYxEuKo7CYrOb+Rb
MD5:	DCE2F2B0E50CB1DBB0246D152791CB46
SHA1:	D0A69C159304EDC08DB005163E7A0DAF5A1E98A6
SHA-256:	ACF087C1757F08B0CFD53D59066544D7EF0BFCC50999E77C5813739CD9DC1479
SHA-512:	91054B36EF1673B24E4FE3DC324CBE339F4E9EB72785A6A4C355C7B2A11A9A7C6E188FF9BF5B34FFDD2805D4BBED71EF6CA4975EE3E330FD8D8E383ED64B28 EE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://calfvessel.com/file/adobe/images/gmail.png
Preview:	.PNG.....IHDR.....sBIT....|.d.....pHYs...../....tEXtSoftware.www.inkscape.org..<... .IDATx...{x.u.....I.sS..9Q(..J.L&.$..V\|.....#..''...Zw.eEQv.Q..U.A]9Vh..I8...H 2)`....i.....).....f.y....L.pu...{n..... .....@Is..... mj=...X<65....U.l.b.t.U...mR...e..P.i.$.i2U..@N1.f....i.s...cf. ../....2ev.`..%.|.o...s..j..l.B....V&..s;b..Pfg.....!...:..5....$.@...I0.=.IY.....a...B.4g... T.9Wif..R..o.R.t'.0...?G.9i...L...*..&..s.Vgnkhn...;p[.0.5.....$.....P.....^".HL.M...@.p..;04.... 9.&.(i....9.sK..=&.'$m.....f..1..'...f2.Uww.....PH....@..xq....k.2..l.Luf..s5..`.|

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\gtm[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	77836
Entropy (8bit):	5.517688744056807
Encrypted:	false
SSDEEP:	1536:9IrRyM5S0w6ddl/35qZe3AfQH/bK592WgNYNDu8a1Z9bKP7ur2tPCca4:9+RykS0x/JqZeuQHzMH4l8tPCR4
MD5:	0E9D06DCFA96E71097F3535428435C01
SHA1:	2A45A9C4F44394AB6DD0060A9981BAB8CBB2893B
SHA-256:	7AF802FC329C950BD76D11EEC1DC93306F0C6688A9383B7016B0A6144BB1B736
SHA-512:	D6ACFA367A72C6BAC856C044544351CDDE4786370B5D9C6FBF33DDE3FD2B132F11616A32AC5E58AD17A3DB964045B2CA3EA87CB890674BF506CAD9BDA4A7E 369
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.googletagmanager.com/gtm.js?id=GTM-KDXRF52
Preview:	.// Copyright 2012 Google Inc. All rights reserved..(function(){..var data = {."resource": {. "version":"5",. . "macros":[{. "function":"__e". },{. "function":"__gas",. "vtp_cookieDomain":"auto",. "vtp_doubleClick":false,. "vtp_setTrackerName":false,. "vtp_useDebugVersion":false,. "vtp_useHashAutoLink":false,. "v tp_decorateFormsAutoLink":false,. "vtp_enableLinkId":false,. "vtp_enableEcommerce":false,. "vtp_trackingId":"UA-7054419-16",. "vtp_enableRecaptchaOpti on":false,. "vtp_enableUaRlsa":false,. "vtp_enableUseInternalVersion":false. },{. "function":"__u",. "vtp_component":"URL",. "vtp_enableMultiQ ueryKeys":false,. "vtp_enableIgnoreEmptyQueryParam":false. },{. "function":"__u",. "vtp_component":"HOST",. "vtp_enableMultiQueryKeys":false,. "vtp_enableIgnoreEmptyQueryParam":false. },{. "function":"__u",. "vtp_component":"PATH",. "vtp_enableMultiQuery

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\main-sprite[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 246 x 2285, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	43361
Entropy (8bit):	7.938552909809436
Encrypted:	false
SSDEEP:	768:GUtBKJ9vXd4yxUps6MR+sw7ASrH11ZGYEBCgL/hd5IHPabPND4Pgu:GUtMV+yxzBR+N9/ZGYarPebPgu
MD5:	BFEE27F6F585496810D51DB33B21C6B0
SHA1:	241443D9422CB53B944748F7463DAADF16967BE0
SHA-256:	37BB0DD1A742ABEBD521B9A2DB0860876258E6D07325204FFE6D569EAEC4602D
SHA-512:	44AD2BDBDABA1F7767DECFB7D9108B862E932986CDBBFDB693D7FA6393D61621BC7BD5A59F1F3F8D9A679301378EFBCFEC8C3DD7A79163D8A1FD70C61A3D 656
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.joomag.com/static/img/main-sprite.png?20191225239

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\main-sprite[1].png	
Preview:	.PNG.....IHDR.....gAMA.....a.... cHRM..z&.....u0...`.:....p..Q<....bKGD.....C.....tIME.....(.....vpAg...H...R.~T.....IDATx...{\u.....J[zJ....%H.YD.....#...F..]V..o....''..j.].bpUP... Z....*..d.....d..?..4'..d.....x.$g.9.9C.....\|.....?....Q.....M..[.Z.....ro@kw.....+..^"..+.[..o.....hN..=b.....k[DjMc...F.E..xk..Z....G.....K..}..c../.i..*...T.....{..u4./..c.k...3..p`...$.[...:.7.v._.|.8.....H.)k..Z.....3...D.}....J_G.g..".....7..)....7....h.V.m..5e9+.....p...+h...6.v._\....)%.]kw.T.>..G...,*.Yx.ZQ.`.v.....4...=...q.$.....g...x..o...~....^?.x,..-2!..:.]....."...[..W..(.}.}.....Z.....;....Z..St....86...p..."....2.....W.z.Y..0....|y.i..1.7..z".J.-..@.....S....~.o..o....8k.....DjC.g.[..gc..s....kV.....f.u4.*.{.T.bZ./.O.B.0..B.....H.+&.ow]|.....D*..]......7b...:.7..B...m.....t..@.R....].^..]. R).....s.h...TJ.]J.....<.w].H..8y....>..`.0..i..:.W..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\main[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	33342
Entropy (8bit):	4.612744135793488
Encrypted:	false
SSDEEP:	384:SoRed8l2YZ1YRRcgcx37QC77xPMyh9rlFyi03+kT1GCEbeUfliLjWZNbbL600Qu3:SoRedkDQg7PxEw5lBfZLjWZxqvz3
MD5:	D430C0916334AD1ECEFE82B51BEABFAE
SHA1:	F60EC8720AC3047006A01F201A046B4D9867B3FD
SHA-256:	0E891FE3D7FD17382D0AB63B6E0B95A3A92B90AA346379A77819B984DC8F5A87
SHA-512:	86C358632FE8C49768AECD16DE880BC23964EE6EA91DF40FB401BABBAF8EC9BD20CBADDE0A6CE1382FAE76FDCA672B5AF9EB33EC0FF63C44671F7A3602CDE3BC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.joomag.com/Frontend/mobile/viewer/main.svg?_=1600196365988
Preview:	<?xml version="1.0" encoding="utf-8"?><!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd"><svg width="488" height="388" viewBox="0 0 488 388" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink"><view id="18-plus-icon-ebebeb" viewBox="356 0 132 132"/><svg width="132" height="132" viewBox="-2 -2 132 132" x="356" xmlns="http://www.w3.org/2000/svg"><g fill="#ebebeb"><path class="aast0" d="M86.4 4c1.6 0 3.1.6 4.2 1.7l31.7 31.7c1.1 1.1 1.7 2.6 1.7 4.2v44.8c0 1.6-.6 3.1-1.7 4.2l-31.7 31.7c-1.1 1.1-2.6 1.7-4.2 1.7H41.6c-1.6 0-3.1-.6-4.2-1.7L5.7 90.6C4.6 89.5 4 88 4 86.4V41.6c0-1.6.6-3.1 1.7-4.2L37.4 5.7C38.5 4.6 40 4 41.6 4h44.8m0-4H41.6c-2.6 0-5.2 1-7 2.9L2.9 34.6C1 36.4 0 39 0 41.6v44.8c0 2.6 1 5.2 2.9 7l31.7 31.7c1.9 1.9 4.4 2.9 7 2.9h44.8c2.6 0 5.2-1 7-2.9l31.7-31.7c1.9-1.9 2.9-4.4 2.9-7V41.6c0-2.6-1-5.2-2.9-7L93.4 2.9C91.6 1 89 0 86.4 0z"/><path class="aast0" d="M71 60c2.4-1.8 4-4.7 4-8 0-5.5-4.5-10-10-10s-10 4.5-10 1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\office3651[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 187 x 188, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	18025
Entropy (8bit):	3.011161251318808
Encrypted:	false
SSDEEP:	96:2S+WvkiqJq6Uq7NXrNG+GHhsc5yeFZV9D2Ydcx/NTV0K0VFDsCmm:2SJkiOq6Uq75shDs1kFP
MD5:	FE22440D79FFA34950F512EF4A718B2A
SHA1:	0E147E59544EE6580D3095353D4420849FA5EB8A
SHA-256:	A2F26B68A6C8810C1AEB4048C938F835A86BA83756A7A440F989B967E78F3BA8
SHA-512:	64218ECD4140DC05E50EB7BA4C9813794B8B5A4310C8308244205BA6ADA8EE7C2D1840121730A00800E41775241D8AFA02125A966064CD0EB2CC7D3E4605B81(
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://calfvessel.com/file/adobe/images/office3651.png
Preview:	.PNG.....IHDR..... .....pHYs.....<eiTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?>.<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c067 79.157747, 2015/03/30-23:40:42 ">. <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">. <rdf:Description rdf:about="". xmlns:xmp="http://ns.adobe.com/xap/1.0/". xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/". xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#". xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/". xmlns:dc="http://purl.org/dc/elements/1.1/". xmlns:tiff="http://ns.adobe.com/tiff/1.0/". xmlns:exif="http://ns.adobe.com/exif/1.0/">. <xmp:CreatorTool>Adobe Photoshop CC 2015 (Windows)</xmp:CreatorTool>. <xmp:CreateDate>2020-01-18T21:49:38+05:00</xmp:CreateDate>. <xmp:MetadataDate>2020-01-21T14:30:14+05:00</xmp:MetadataDate>. <x

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\outlook1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 26 x 26, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	771
Entropy (8bit):	7.682244426935498
Encrypted:	false
SSDEEP:	24:74yiH9yQmOntihdLl00qDeu1BcaDa0oljZG0:omOntO7v/uJDYG0
MD5:	C3FC46C5799C76F9107504028F39190F
SHA1:	519096AD3F03410CF9CE3C9B9FCCA6B439D97B23
SHA-256:	57898461712A639D119BDF88B7145919DCC8956C7A271D2E4A1084B29EAE6785
SHA-512:	DF4A0A2F78B2013035FB738BF405119B275D4CFEC31A23071EB9AF499D5F31FDC4BE22754CE791C975D7D417E908B5CAD16F962B0ADD3DFDCDE19844D74F668
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\outlook1[1].png	
IE Cache URL:	http://https://calfvessel.com/file/adobe/images/outlook1.png
Preview:	.PNG.....IHDR.....JL.....bKGD.....IDATH....k.A..k6.b.F1..H@...j@.aQ...(.. .. .. .A..D...I.....E.....1...W...;;.Y.d.}].U5]..x"3?....!..A..y..+R2\...m.NX.=..p.0...d.^.3.....J.Z.X.).....P\..x1.3.M.0....m.....F....?...n.....I.Fo)x._ R|.s..a.T?...?.=.9.Y..u....z..|.....Wz...h..<..P.. ...$.Y.....k`/4.y/.....L.C.....".....U....7....G...'h.....1j1E..%t..... @..a.....b.ED-.Tn.<..o.D...o..(.{1l>.....".4a.:k.l./.7t./.Q-'..>.. .....'3eb..d.@=4...C....A...;..N.X3.(.....,v...+...S...W..l...@,...j.).u<..@u..0...V&.b.yp.....0..o.?..V..B =.~&m"r (...6;EP.T.....h.m".[f.U)|t..2.Q.....g.cP.W...D..[.O>..d;.yI.{/..#v.._..$.Q.....t\E..5i.q._.."/n...v.w..Uo ...#..S....^.....F..+._??.r.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\8[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=12, height=709, bps=0, PhotometricIntepretation=RGB, orientation=upper-left, width=1200], baseline, precision 8, 1200x646, frames 3
Category:	downloaded
Size (bytes):	161118
Entropy (8bit):	7.5594351594508185
Encrypted:	false
SSDEEP:	3072:WucfAcwuKGuN2q/gSsqnk4br5XUGpppLqfmazv7l04J:OMuKbYOF355XEuAv7lnJ
MD5:	F17B5B1163EFB6D2D47DE6BAE6D3A9CD
SHA1:	6D6964B34BC44C6D2B106ADE1AE675985B96D012
SHA-256:	7829F065E0E10C8466F3D57766E0719421B7B652F6A1082F21B98702F1B28A30
SHA-512:	7C0CBEF1D3CAE66A18C74544E593803C2EEC56817E762A385D54437BC7D597B2598886B0C0EDF72C6E934E9F146CEFC89392A492DB5425A1071E61CA1F15685
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://calfvessel.com/file/adobe/images/8.jpg
Preview:	.....Exif..MM.*.....(.....1....."....2.....i.....$.....'.....'.Adobe Photoshop CC 2015 (Windows).2020:01:21 13:41:42.....0221.....r.....z.(.....%.....H.....H.....Adobe_CM.....Adobe.d.....V...."....?.....3.....!.1.AQa."q.2....B#$.R.b34r ..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWgw.....5....!1..AQaq"..2....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv..... ...'7GWgw.....?.....q..KJG..x.."....]..TX...[^.m...R.....X.5..j?p.A.RI%0...MN.$..@.4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\analytics[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	47332
Entropy (8bit):	5.518633523108405
Encrypted:	false
SSDEEP:	768:UyC36rcBLbfsl5XqYoyPndHTkoWY3SoavVVy2WiCgYUD0FEw0stZb:UyDAZfY5hVdHTwY3Soljw0sD
MD5:	6A10EB2BB5C90414980729F4F96FFBDA
SHA1:	8BBBD5948255549E4B691B614AA3177DEA9AF1B7
SHA-256:	0F3BE44690AE9914AE3E47B7752E1BDEA316F09938E9094F99E0DE19CCD8987A
SHA-512:	5A505CBAAEEAB8961AA0DE94767F76A09B6F03E60EB0C72954B85EC0392EE1CE383D2088939A314D3175AB24B7A69390C841CFE0237C1D1C40966B43F22AE929
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google-analytics.com/analytics.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var n=this||self,p=function(a,b){a=a.split(".");var c=n;a[0]in c||"undefined"==typeof c.execScript||c.execScript("var "+a[0]);for(var d;a.length&&(d=a.shift());)a.length||void 0===b?c=c[d]&&c[d]!==Object.prototype[d]?c[d]:c[d]={}:c[d]=b};var q=function(a,b){for(var c in b)b.hasOwnProperty(c)&&(a[c]=b[c])},r=function(a){for(var b in a)if(a.hasOwnProperty(b))return!0;return!1};var t=/^(?:(?:https?|mailto|ftp):|[^:/?#]*(?:[/?#]|$))/i;var v=window,x=document,y=function(a,b){x.addEventListener?x.addEventListener(a,b,!1):x.attachEvent&&x.attachEvent("on"+a,b)};var z={},A=function(){z.TAGGING=z.TAGGING\|\|[];z.TAGGING[1]=!0};var B=/:[0-9]+$/,C=function(a,b,c){a=a.split("&");for(var d=0;d<a.length;d++){var e=a[d].split("=");if(decodeURIComponent(e[0]).replace(/\+/g," ")===b)return b=e.slice(1).join("="),c?b:decodeURIComponent(b).replace(/\+/g," ")}},F=function(a,b){b&&(b=String(b).toLowerCase());if("p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\css[1].css	
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\en[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	244246
Entropy (8bit):	4.837185773084157
Encrypted:	false
SSDEEP:	3072:YAH7y8NJOLj6xLzX1pkdWoCffBIdfze1+HVmF/4c:BJAKzk8fgzw8mFAc
MD5:	CB366D30D8FCCFFC4D8BBA7691D448B8
SHA1:	52C9ACA8C89D7ED70531FAD3A46E79425C87B996
SHA-256:	C9F8D111F907C656EB1915623CE51178DCB8027A555C8F8201B5BC3C58874AAE
SHA-512:	A2A2C72161AEAF8C2BAFB35411DF55A791A161EADD247816AD8D8A923E02A2ADD5AA36B7BD3C05AE7AA49890F8049584BCE9431E3F5114CB79187CBE09AAF135
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.joomag.com//static/locale/en.js?_=5.1.6.0
Preview:	(typeof joomag == 'undefined') && (joomag = { locale: {} });.joomag.locale = $.extend(true, {}, joomag.locale, {"backend":{"account_manager":{"title":"Account Management"},"account_settings":{"change_password":{"new_password":"New Password","new_password_help":"Enter the new password","old_password":"Old Password","old_password_help":"Enter current password","retype_password":"Retype Password","retype_password_help":"Confirm the new password","title":"Change Password"},"incomplete_user_notification":"Please confirm your email address by clicking the link found in the confirmation email sent to your address. We strongly recommend you adding our domain name to the whitelist of your mailing server to ensure the delivery of our emails to you.","info":{"account_balance":"Account Balance","account_type":"Account Type","active_services":"Active Services","address":"Address","address_help_line":"Enter company address, line {0}","brief_box_title":"Account Info","city":"City","city_help":"En

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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\CS6IXJW6\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
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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\free.min[1].css	
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\CS6IXJW6\html5-viewer-external[1].css	
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):	377231
Entropy (8bit):	5.123153284606608
Encrypted:	false
SSDEEP:	1536:GwGFnfVYUh1pMNTxFnIGyfqqoxtl+V5Ozmr2KZEACCaUReUD+M/C:ylgFW65Ozmr2KZEme
MD5:	A88A9B92156449D9653C68C43A6CE7AC
SHA1:	39FC272CE9382CA89FE8439341B52F797110A4C5
SHA-256:	4921FE5BF8E8473256784688DD1CB2CC153272E66309F7271B8409F11FF0B524
SHA-512:	9EFAAA4DC53EA7A573B9503DB3418535D19BE4D60396BA9AC1D11CB454A857295A276CE89752CD77E48BBAAE63E55AE7B7B564FC6F2D5C3BB0356DF4A93A9C6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.joomag.com/static/css/html5-viewer-external.css?_=5.1.6.0
Preview:	@font-face{font-family:'Glyphicons Halflings';src:url(/assets/bootstrap/fonts/glyphicons-halflings-regular.eot);src:url(/assets/bootstrap/fonts/glyphicons-halflings-regular.eot?#iefix) format('embedded-opentype'),url(/assets/bootstrap/fonts/glyphicons-halflings-regular.woff) format('woff'),url(/assets/bootstrap/fonts/glyphicons-halflings-regular.ttf) format('truetype'),url(/assets/bootstrap/fonts/glyphicons-halflings-regular.svg#glyphicons_halflingsregular) format('svg')}.glyphicon{position:relative;top:1px;display:inline-block;font-family:'Glyphicons Halflings';font-style:normal;font-weight:400;line-height:1;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale}.glyphicon-asterisk:before{content:"\2a"}.glyphicon-plus:before{content:"\2b"}.glyphicon-euro:before{content:"\20ac"}.glyphicon-minus:before{content:"\2212"}.glyphicon-cloud:before{content:"\2601"}.glyphicon-envelope:before{content:"\2709"}.glyphicon-pencil:before{content:"\270f"}.glyphicon-glass:before{content:"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\joomag-pixel.3df7f73f177625835141[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with LF, NEL line terminators
Category:	downloaded
Size (bytes):	721995
Entropy (8bit):	6.025173686646883
Encrypted:	false
SSDEEP:	12288:eorrWdEljyhAmPsipPnpJItCUjIdIPhFK6GGyY0Wfc:BrrBGZPsipzKCUjIdUhFK9
MD5:	643599917A7FE230B0F5E5AD68528405
SHA1:	5C5D99185ABD4395603DD081987275F7A00429B9
SHA-256:	1CE995D95A406CAFD36A2D5FD8F2D4AE63CB596113A8293FC731DC7B47668D43
SHA-512:	D38E52DC4153460A438F89E52F9DB4D15D193D56E0386350809866FA1B18A0645BF5CDC2B07F34C45351CA60DA38E3C643FDFF429970DDC5961BBFAE4D45446
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.joomag.com/Frontend/pixel/joomag-pixel.3df7f73f177625835141.js
Preview:	/*! For license information please see joomag-pixel.3df7f73f177625835141.js.LICENSE.txt */.this["joomag-pixel"]=function(e){var t={};function n(r){if(t[r])return t[r].exports;var a=t[r]={i:r,l:!1,exports:{}};return e[r].call(a.exports,a,a.exports,n),a.l=!0,a.exports}return n.m=e,n.c=t,n.d=function(e,t,r){n.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:r})},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 r=Object.create(null);if(n.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var a in e)n.d(r,a,function(t){return e[t]}.bind(null,a));return r},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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\magazine[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):	638722
Entropy (8bit):	5.628894629818406
Encrypted:	false
SSDEEP:	12288:5vEOuoZzClRH9DsGwznqtbpSgUxAB4o52eOv:5vEdWzCljMzqtpSgUxAB4o52jv
MD5:	062D79DAC749FF4F8BDB0FEB3BA0F5D4
SHA1:	49FE94F61D094E122CFEF6898B27D0841FA645DB
SHA-256:	86254DB9234149D12207619980E9FC9F2A68A7360518A027E662EA66244082E0
SHA-512:	3BE40B89DAE25717A5507E439C8F837B4AB3949114225A5F399D698B3AFEF559132B42585048EAD0730955178E8B510C9D0BFF10691FAF15C0504C6863A68488
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.joomag.com/static/js/magazine.js?_=5.1.6.0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\magazine[1].js	
Preview:	(function(a,b){function cy(a){return f.isWindow(a)?a:a.nodeType===9?a.defaultView||a.parentWindow:!1}function cu(a){if(!cj[a]){var b=c.body,d=f("<"+a+">").appendTo(b),e=d.css("display");d.remove();if(e==="none"||e===""){ck||(ck=c.createElement("iframe"),ck.frameBorder=ck.width=ck.height=0),b.appendChild(ck);if(!cl||!ck.createElement)cl=(ck.contentWindow||ck.contentDocument).document,cl.write((f.support.boxModel?"<!doctype html>":"")+"<html><body>"),cl.close();d=cl.createElement(a),cl.body.appendChild(d),.e=f.css(d,"display"),b.removeChild(ck)}cj[a]=e}return cj[a]}function ct(a,b){var c={};f.each(cp.concat.apply([],cp.slice(0,b)),function(){c[this]=a});return c}function cs(){cq=b}function cr(){setTimeout(cs,0);return cq=f.now()}function ci(){try{return new a.ActiveXObject("Microsoft.XMLHTTP")}catch(b){}}function ch(){try{return new a.XMLHttpRequest}catch(b){}}function cb(a,c){a.dataFilter&&(c=a.dataFilter(c,a.dataType));var d=a.dataTypes,e={},g,h,i=d.length,j,k=d[0],l,m,n,o,p;for(g=1;g<

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\main.2813cfbe59a2f8c75923[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	793374
Entropy (8bit):	5.487012596476752
Encrypted:	false
SSDEEP:	24576:bIROJWMJLX1PV8UCsTGD+1OBwAMY1BCiq+/1NMKCenPB0Ye+mi4m0cewBHQgD3xb:bIROJWMJLXVVtCs9OBwAMY1BCz+/1NMY
MD5:	8A6955AF4091942697C5DAC3912E9796
SHA1:	CAFB5ADF801CDBDA1FAA800A90DC04F1A004C578
SHA-256:	EA0A7FBF305F7B0DABF67CBF27DE4223F1DD3C1E51976EAC1E2405E489987F7A
SHA-512:	E2CC96416688B3D53CFA61972BDABAA3DD11A4CB125AC900078A741F1BC594C1D4D5FF5A6A64E9E7BE5B75C9B7F4E31509F81501FDDE72F7B3BB3D5ACB009B83
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.joomag.com/Frontend/mobile/viewer/main.2813cfbe59a2f8c75923.js
Preview:	webpackJsonp([19],[,function(t,e,n){"use strict";n.d(e,"a",function(){return o});var i=n(0),a=n(128),r="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},o=function(){var t={},e=document,n=document.createElement("div").style,o=function(){for(var t=["t","webkitT","MozT","msT","OT"],e=0,i=t.length;e<i;e++)if(t[e]+"ransform"in n)return t[e].substr(0,t[e].length-1);return!1}(),s=function(t){return!1!==o&&(""===o?t:o+t.charAt(0).toUpperCase()+t.substr(1))},l=s("transform");return t.extend=function(t,e){for(var n in e)t[n]=e[n]},t.srtEndsWith=function(t,e){return-1!==t.indexOf(e,t.length-e.length)},t.extend(t,{hasTransform:!1!==l,hasPerspective:s("perspective")in n,hasTouch:"ontouchstart"in window,hasPointer:window.PointerEvent||window.MSPointerEvent,hasTransition:s("transition")in n,style:{transform:l,transitionTimingFunction:s("transitionTim

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\main.867208e99122488d74f9a620279f9cd9[1].css	
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):	302144
Entropy (8bit):	5.183892338593447
Encrypted:	false
SSDEEP:	1536:0srPYhzdwYvHDkvHDCbCwt9Cvtni6jx8/jERAv5wB4gZb/Trnzi62wpWo7tosRft:0s7Y/Dk/DCb2vI6i7E11pt7t/t
MD5:	867208E99122488D74F9A620279F9CD9
SHA1:	C24307613ADE7673A33350B663C0E0864A82F4C6
SHA-256:	BC75594D9ACA2EF4A9806EB58734D67AF1E3540B58CBC3D39BA94C487E2695B7
SHA-512:	1B84CA64FBF1FFDAA875F5CB831FC53A843EF2D2E84B3C384D851CC3EC5158A3E3DED205DB19F395589C00737268AEEEFEE29293F5B7A5BF0BBBEC62B29D1DC4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.joomag.com/Frontend/mobile/viewer/styles/main.867208e99122488d74f9a620279f9cd9.css
Preview:	.clearfix{zoom:1}.clearfix:after,.clearfix:before{content:"";display:table}.clearfix:after{clear:both}@-ms-viewport{width:device-width;initial-scale:1;minimum-scale:1;maximum-scale:1;user-scalable:0}body{margin:0}img{border:none;outline:none}.j-html5-viewer{position:absolute;top:0;left:0;width:100%;height:100%;font-family:proxima-nova,sans-serif}.j-html5-viewer.j-no-default-touch-actions{touch-action:none;-ms-touch-action:none}.j-html5-viewer html{color:rgba(0,0,0,.87)}.j-html5-viewer ::-moz-selection{background:#b3d4fc;text-shadow:none}.j-html5-viewer ::selection{background:#b3d4fc;text-shadow:none}.j-html5-viewer hr{display:block;height:1px;border:0;border-top:1px solid #ccc;margin:1em 0;padding:0}.j-html5-viewer audio,.j-html5-viewer canvas,.j-html5-viewer iframe,.j-html5-viewer img,.j-html5-viewer svg,.j-html5-viewer video{vertical-align:middle}.j-html5-viewer fieldset{border:0;margin:0;padding:0}.j-html5-viewer textarea{resize:vertical}.j-html5-viewer .browserupgrade{margin:.2em 0

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

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\popper.min[1].js</th></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js</td></tr>
<tr><td>Preview:</td><td>/*. Copyright (C) Federico Zivolo 2017. Distributed under the MIT License (license terms are at http://opensource.org/licenses/MIT).. */(function(e,t){'object'==typeof ex
ports&&'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.b
ody;}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&&'BOD
Y'!==i&&'HTML'!==i?-1!==['TD','TABLE'].indexOf(o.nodeName)&&'static'===t(o,'position')?r(o):o:e?e.ownerDocument.documentElement:document.documentEleme
nt}functio</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\vendor.7bc4df7aaac8424047c3[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>HTML document, UTF-8 Unicode text, with very long lines, with no line terminators, with escape sequences</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>352294</td></tr>
<tr><td>Entropy (8bit):</td><td>5.539865479263285</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>6144:YbaTJKq96gdzicIHftOga4KbEi/cLfgo/q9FY:waTAq96gR8gAq92</td></tr>
<tr><td>MD5:</td><td>42690687B144654E18A4697D09D27891</td></tr>
<tr><td>SHA1:</td><td>7A32BD488D27FB727BAA6C89422047C704CD2FB3</td></tr>
<tr><td>SHA-256:</td><td>C6A86343582954B195FD2F3D0DB29C69E886D7CC165607FEAA84B08E4EBCADA8</td></tr>
<tr><td>SHA-512:</td><td>36557020A3AFD4856B0C5768781B159B9E17655FBA374F12EA9B679625CE17E5A8F3EB011DF34CA1B12E518576E96C74785C6224858CDE4E7B3FCEC29B5954E0</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://www.joomag.com/Frontend/mobile/viewer/vendor.7bc4df7aaac8424047c3.js</td></tr>
<tr><td>Preview:</td><td>webpackJsonp([20],{0:function(e,t,n){"use strict";var i="function"==typeof Symbol&&"symbol"==typeof Symbol.iterator?function(e){return typeof e}:function(e){return e&&"fu
nction"==typeof Symbol&&e.constructor===Symbol&&e!==Symbol.prototype?"symbol":typeof e};!function(e,t){function r(e){return B.isWindow(e)?e:9===e.nodeType&&(e.d
efaultView||e.parentWindow)}function s(e){if(!yt[e]){var t=N.body,n=B("<"+e+">").appendTo(t),i=n.css("display");n.remove(),"none"!==i&&""!==i||(_t||(_t=N.createElement("i
frame"),_t.frameBorder=_t.width=_t.height=0),t.appendChild(_t),mt&&_t.createElement||(mt=(_t.contentWindow||_t.contentDocument).document,mt.write((B.support.box
Model?"<!doctype html>":"")+"<html><body>"),mt.close()),n=mt.createElement(e),mt.body.appendChild(n),i=B.css(n,"display"),t.removeChild(_t)),yt[e]=i}return yt[e
]}function o(e,t){var n={};return B.each(Ct.concat.apply([],Ct.slice(0,t)),function(){n[this]=e}),n}function a(){vt=t}function l(){return setTimeout(a,0),vt=B.now()}function c(){tr</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\0_3-0[1].svg</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>SVG Scalable Vector Graphics image</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>73361</td></tr>
<tr><td>Entropy (8bit):</td><td>5.877176911671926</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:QEkILlxxDA5SgxqSDiWFMnKZWnt/y4yuMmxKa:rkwxYxqBWFldF9a</td></tr>
<tr><td>MD5:</td><td>9C23D0C46DA7E074B8EEDAF7DCEA2761</td></tr>
<tr><td>SHA1:</td><td>DF657799BC7B97E92C97B177791AD371B5F72E89</td></tr>
<tr><td>SHA-256:</td><td>256D409AFAC730FA0CDE8BAFB409134E105BD96B10D247C37434589826C62DB4</td></tr>
<tr><td>SHA-512:</td><td>A8CF906672F678FD5B924FD35C1200BF206ABF0543CA07C76542000EDF8AA19F71F15F09AB869420ABDDA3B4FE1186821E044216E4418ECAACB470B09EF7920</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://s9cdn.joomag.com/mobile/2/2420/2420210/0_3-0.SVG?_=1087734147</td></tr>
<tr><td>Preview:</td><td><svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="612pt" height="792pt" viewBox="0 0 612 792" version="1.2"><defs><image
id="a" width="1314" height="1178" xlink:href="
L8AAA5+SURBVHic7dSxAQAQAMAw/P8zD+jMkFzQqXMPAO7W6wCAf1kkQLJIgGSRAMkiAZJFAiSLBEgWCZAsEiBZJECySIBkkQDJIgGSRQIkiwRIFgmQLBIgW
SRAskiAZJEAySIBkkUCJIsESBYJkCwSIFkkQLJIgGSRAMkiAZJFAiSLBEgWCZAsEiBZJECySIBkkQDJIgGSRQIkiwRIFgmQLBIgWSRAskiAZJEAySIBkkUCJIsESBYJkCw
SIFkkQLJIgGSRAMkiAZJFAiSLBEgWCZAsEiBZJECySIBkkQDJIgGSRQIkiwRIFgmQLBIgWSRAskiAZJEAySIBkkUCJIsESBYJkCwSIFkkQLJIgGSRAMkiAZJ
FAiSLBEgWCZAsEiBZJECySIBkkQDJIgGSRQIkiwRIFgmQLBIgWSRAskiAZJEAySIBkkUCJIsESBYJkCwSIFkkQLJIgGSRAMkiAZJFAiSLBEgWCZAsEiBZJEC
ySIBkkQDJIgGSRQIkiwRIFgmQLBIgWSRAskiAZJEAySIBkkUCJIsESBYJkCwSIFkkQLJIgGSRAMkiAZJFAiSLBEgWCZAsEiBZJECySIBkkQDJIgGSRQIkiwRIFgmQLBIgW
SRAskiAZJEAySIBkkUCJIsESBYJkCwSIFkkQLJIgGSRAMkiAZJFAiSLBEgWCZAsEiBZJECySIBkkQDJIgGSRQIkiwR</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\adobe[1].jpg</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.02, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 400x400, frames 3</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>30925</td></tr>
<tr><td>Entropy (8bit):</td><td>7.75667128400845</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>768:nuowBuvTpjgz+wqrPZ2qh8fmyjlX6RqnxgYqwNL:nuPOpjgzPqrPZRYZGnYqYL</td></tr>
<tr><td>MD5:</td><td>BE5274AF7D8BD25B8148A190FF515399</td></tr>
<tr><td>SHA1:</td><td>B8D0850FD92EE935287E17988B89E53607808C8C</td></tr>
<tr><td>SHA-256:</td><td>26C62DBDF527B8DCBF378EA62F129CBBBA3B244730687909BA21ECD729C9D2E6</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\adobe[1].jpg	
SHA-512:	64893C625BE72783088575E36EF26FF4573243F32601BDA754EDA72B7515063B5E4E4831697D16AC663529C910AE12CCD145BEC530F2A9BAE4D9324301C65667
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://calfvessel.com/file/adobe/images/adobe.jpg
Preview:	......JFIF.....C.....C......"....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..g.....\|?....".+....._.....4...R...'..q.. ~...n.7.....QXJ<...=...^.V'@U..E..5....Uz.....IE.PTe.}/p.y.....T.<...-T..\|...b.=.#IU..~....{O/...b..E.....X...G...?.....\|....._....M..g.....T~g.....<....T~g.....3$.=._.. IU.K..^.E...=.#U.._[X.R..=W...1.....QTr.\....*.7..?..6.9K..^.E.Ps.\.....%W..y...g)s[KX)<.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\d[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 58272, version 0.0
Category:	downloaded
Size (bytes):	58272
Entropy (8bit):	**7.991777670773457**
Encrypted:	**true**
SSDEEP:	1536:BS7tBzduth0mIGHEosBwOfwQRKjHIqEjGlaV:BA3duz0m9HkdYi7ZjG+
MD5:	25EB786C99DB8F58DF013C81F8F14C0D
SHA1:	83FDDE6AC8D51CAD2BDF8C33813FEE6BA34002A7
SHA-256:	054E8C55D84A3EBFF0722AB57AB4A00BB60736DCFF97B81401019D714FFAF688
SHA-512:	2F554CC1A262CA515156198F027A0A0F13E430BB17392874AF265B437CAB397FD415770AB564067AE030D7341A34CBA38705788F2887F388AEAD64FBB21490D5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/1eef01/00000000000000000000148ac/23/d?subset_id=1&fvd=n9&v=3
Preview:	wOFF.....L.....DYNA.....z.....*.FFTM.....]...GDEF.....R...Z.s..GPOS...X.....1.\.#sGSUB...,...P...\..H.OS/2.....Y...`....cmap.....cvt .....G. .fpgm.....e#./.gasp.....glyf...|...V..@4.)<ahead.....5...6.L;jhhea...D...!...$.O..hmtx.....h..xloca.....6(..maxp...h... ... .B..name.....Q+.:.post..... ...(pr ep.....c...t.....o1.....x.....6.`.....6.>.h.....X..x.]Q.N[A.....c..hS.fB...$.W...vc9B.\.b\..P Q..k.h().A..R>.O@bfM.(....s..r..]Z.y..R.....v...t}...v.@..^.n...`3.rG....-.!. i'P....6...>.d..AK3MO....B`...0...../X....C.i*..s*..Ks....k..vp&"?..hj..@._:.z>.b.r.0...S.d".f2].T-3.up...;X.Js....U.....-.2KC...*1B.$.BN9w.?)P>..1....a..q.50.....fS.{.0~.G..o..>..6F..X.` ...QU...s/.....3.%`y.._'..;6..em.C.....2....U.....tJ.....p.X...R.v....`H.F..h-;.*...d/.*.....x.c`d```b8..b.x~.....".~U....+...b.a`d.....x...N.0.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\d[2]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 55916, version 0.0
Category:	downloaded
Size (bytes):	55916
Entropy (8bit):	**7.990377940984203**
Encrypted:	**true**
SSDEEP:	1536:CdrjeMTpp0yUURuaM+lCA8QMtjOdH3taxc1ax:CpZ1uylpOtq0O1ax
MD5:	642BF1228C9D1BCF62992C08DF8A92B8
SHA1:	05DA82C550C25254ACA29DAD238EABCFC149BF9C
SHA-256:	036F00B2C16BD1CA74B5384DE15D04214CC005A4476BF4A6291AD29D39885BAF
SHA-512:	C49B942716BFFF2934F2E7A70B0B230DF28E1B810BE2324EC2ED90BB9CCE48413E444F773C56FF99BBFFA940E0BD7554DD7554C1D29321AA7506750C6B858B1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.typekit.net/af/bc719c/00000000000000000001499c/23/d?subset_id=1&fvd=n7&v=3
Preview:	wOFF.....l.....0.....DYNA.....{....<N.bGPOS.....<..3./.k.GSUB...<.....OS/2.....Y...`...rcmap.....<.cvt .....l..fpgm.....s.U.7gasp.....glyf..!.. .....=..H..head.....6...6..<.hhea...@...!...$....hmtx.....d.."loca.....4.r .maxp...d... ... .4.>name.....E.4$.post.....".2..prep....._.....)...6....x.].=N.0...8,..H. .-+.+..R8.P.@(<.?.D..Hih\p..3]..`.....3.....k..m.....LP^.@...y.@8...xeq..X...5.~..u..~.u.....s....&.B..S0T.:.;.;.d.'.9..._....._^:w.&y..@.WTzT...6..A..1)..j.|..Wkn....P..0.....U.w,:.xb.85 .....y4X.&..k8'z.;wM.*Njp...rk.....y..._.<.....x.....Hy.....x..OJ.@._...bdf;0P.R.$.*Cg..0.Q.....BR...x...E.x.O.9..Z..`>..U}./...x....{...[p.]..]...../....;..... ....g.-1.....W.G..<x^.w..y.R....Q....*..X....3UM.e...6..G.Q ..L:I-+]....2.4W..4J..l..{i.....VjDM.B?.tU.... ..|.m...e..v^.ij....T.F....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\e2270d116b[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):	24
Entropy (8bit):	2.459147917027245
Encrypted:	false
SSDEEP:	3:CUXJ/lH:Dl
MD5:	BC32ED98D624ACB4008F986349A20D26
SHA1:	2D3DF8C11D2168CE2C27E0937421D11D85016361
SHA-256:	0C9CF152A0AD00D4F102C93C613C104914BE5517AC8F8E0831727F8BFBE8B300
SHA-512:	71ACC6DA78D5D5BF0EEA30E2EE0AC5C992B00EFEC959077DFE0AB769F1DBBD9AF12D5C5C155046283D5416BEB606A9EF323FB410E903768B1569B69F37075B4E
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\e2270d116b[1].gif	
Reputation:	low
Preview:	GIF89a.....,.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\hover[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	114697
Entropy (8bit):	4.9296726009523
Encrypted:	false
SSDEEP:	1536:67O7EesvXIPRX4PT8aZv8qoXIoqbTFaFeTxvyAZ+D7M71D:qXIPRX4PT3
MD5:	FAC4178C15E5A86139C662DAFC809501
SHA1:	EF1481841399156A880EC31B07DDA9CFAA1ACE39
SHA-256:	BB88454962767EB6F2DDB1AABAAF844D8A57DE7E8F848D7F6928F81B54998452
SHA-512:	0902219B6E236FBF9D8173D1D452C8733C1BF67B0EB906CC9866EA0C27C2D08F6DA556D01475E9B54E2C6CE797B230BFBD5F39055CE0C71EA4D3E36872C378E9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://calfvessel.com/file/adobe/css/hover.css
Preview:	/*!. * Hover.css (http://ianlunn.github.io/Hover/). * Version: 2.3.2. * Author: Ian Lunn @IanLunn. * Author URL: http://ianlunn.co.uk/. * Github: https://github.com/IanLunn/Hover.. * Hover.css Copyright Ian Lunn 2017. Generated with Sass.. */./* 2D TRANSITIONS */./* Grow */..hvr-grow {. display: inline-block;. vertical-align: middle;. -webkit-transform: perspective(1px) translateZ(0);. transform: perspective(1px) translateZ(0);. box-shadow: 0 0 1px rgba(0, 0, 0, 0);. -webkit-transition-duration: 0.3s;. transition-duration: 0.3s;. -webkit-transition-property: transform;. transition-property: transform;.}..hvr-grow:hover, .hvr-grow:focus, .hvr-grow:active {. -webkit-transform: scale(1.1);. transform: scale(1.1);.}../* Shrink */..hvr-shrink {. display: inline-block;. vertical-align: middle;. -webkit-transform: perspective(1px) translateZ(0);. transform: perspective(1px) translateZ(0);. box-shadow: 0 0 1px rgba(0, 0, 0, 0);. -webkit-transition-duration: 0.3s;. transition-

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:	53A2B560B20551672FBB0E6E72632D4FD1C7E2DD2ECF7337EBAAAB179CB8BE7C87E9D803CE7765706BC7FCBCF993C34587CD1237DE5A279AEA19911D69067E65
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\jquery-3.2.1.slim.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	69597
Entropy (8bit):	5.369216080582935
Encrypted:	false
SSDEEP:	1536:qNhEyjjTikEJO4edXXe9J578go6MWX2xkjVe4c4j2ll2Ac7pK3F71QDU8CuT:Exc2yjq4j2uYnQDU8CuT
MD5:	5F48FC77CAC90C4778FA24EC9C57F37D
SHA1:	9E89D1515BC4C371B86F4CB1002FD8E377C1829F
SHA-256:	9365920887B11B33A3DC4BA28A0F93951F200341263E3B9CEFD384798E4BE398
SHA-512:	CAB8C4AFA1D8E3A8B7856EE29AE92566D44CEEAD70C8D533F2C98A976D77D0E1D314719B5C6A473789D8C6B21EBB4B89A6B0EC2E1C9C618FB1437EBC77D3A269
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://code.jquery.com/jquery-3.2.1.slim.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\jquery-3.2.1.slim.min[1].js	
Preview:	/*! 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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\loader[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 78 x 78
Category:	downloaded
Size (bytes):	38703
Entropy (8bit):	6.683050265718866
Encrypted:	false
SSDEEP:	768:pqnw6Q0T3WzlTtKaP12TUUjH9javXd6fR13La6B4f89:pCw6QuuTbP1KUUD9+vXd6fRJm6B4E
MD5:	54B0F6D2BD07F8D35FE2EFDC7E2F6FFB
SHA1:	D8458F47CC95F901AB3A14AED4554BF162EDFE87
SHA-256:	3CDDF3FCB8717496F1D00EC6AB00CF6023C7E62F54B682D14BA0B9F0828892F3
SHA-512:	51EEED4C37659D1533397DE1801BDC76B5F79EFEE87760D63FB6840998CF44F4A13C643D06FF6AA097FE1872563D93FD432C4F937EC29DD1FFF3D0D15BFE108
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.joomag.com/Frontend/mobile/viewer/images/loader.gif
Preview:	GIF89aN.N..... !!!"""###$$$%%%&&&'"((()))***+++8..O44l;:.@@.ED.HH.KJ.MM.QP.SR.UT.WV.WW.XW.XW .YX.[Z.^].^]._.^._.^.__.`_.``.a`.ba.cb.dc.dd.ee.gf.hg.ih.ji.kj.ml.nm.on.qp.rr.ts.vu.xw.zy.||..~..... ....!..NETSCAPE2.0.....!.....,....N.N.....H.....*\....#J.H....3j.... C..I...(S.\...0c.I...8s.....@...J...H.*].....F=..hU....z0k.Z .g....P..S.U.0..O.q....+.I@#1|...CLn{.n..g.w..D...8<.@..l'.;...t#...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\manifest.8e10809dba1c553a5a2a[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):	1975
Entropy (8bit):	5.417776905241852
Encrypted:	false
SSDEEP:	48:ERtGAjNHWJ6wW6av4eD5hjY6oPa9eEyEkbZn:ETHC9W6a95NY6s1ES1n
MD5:	887DBE06F165DF34F6D0AF1DE2676BAB
SHA1:	50EA3408C3927B158B5D857559670DB502FB8B44
SHA-256:	C9D6F1138493170765AAEE432342BCD8A0424FC3A44B179E385B1133DBA819AF
SHA-512:	B20BDB0BF4B2250935D9ED2E12FE70C4A3AB6D72F499A57D37DE7CC3773EEF834134F2B3EA8C4634D50876B4EEC6BD5137FFE186C8854FBAEE5630D15BA26305
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.joomag.com/Frontend/mobile/viewer/manifest.8e10809dba1c553a5a2a.js
Preview:	!function(e){function n(r){if(t[r])return t[r].exports;var c=t[r]={i:r,l:!1,exports:{}};return e[r].call(c.exports,c,c.exports,n),c.l=!0,c.exports}var r=window.webpackJsonp;window.webpackJsonp=function(t,o,a){for(var f,d,i,b=0,u=[];b<t.length;b++)d=t[b],c[d]&&u.push(c[d][0]),c[d]=0;for(f in o)Object.prototype.hasOwnProperty.call(o,f)&&(e[f]=o[f]);for(r&&r(t,o,a);u.length;)u.shift()();if(a)for(b=0;b<a.length;b++)i=n(n.s=a[b]);return i};var t={},c={22:0};n.e=function(e){function r(){f.onerror=f.onload=null,clearTimeout(d);var n=c[e];0!==n&&(n&&n[1](new Error("Loading chunk "+e+" failed.")),c[e]=void 0)}var t=c[e];if(0===t)return new Promise(function(e){e()});if(t)return t[2];var o=new Promise(function(n,r){t=c[e]=[n,r]});t[2]=o;var a=document.getElementsByTagName("head")[0],f=document.createElement("script");f.type="text/javascript",f.charset="utf-8",f.async=!0,f.timeout=12e4,n.nc&&f.setAttribute("nonce",n.nc),f.src=n.p+""+e+"."+{0:"4068b88ccfc0db7747a9",1:"3683b2a59c99847a9cfb",2:"88f8e

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\normalize.d0dfb984f88d0dbb9fde[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):	17077
Entropy (8bit):	5.236941449507342
Encrypted:	false
SSDEEP:	384:oh0shqs39zqEK1eMbuOHhycdLnM520tNPLh01wPAodTcU:u0s7qVycycd7MfNPLhyoAkTcU
MD5:	3453C3FA8930DEFC531DEF3B9A6B593B
SHA1:	88C3B2A4F49600F3D8462A1C928C5ED0E975AF47
SHA-256:	1442E8E49EC12B7CDE355CE5CBC3A6D0CDD47BA5D035FE927E8F204326E64B9C
SHA-512:	C4C36292A9CECD0AF92F456D6EBD625FA93C3586504860C1BCBB10D41CF9712E70BB6199B00851703ED2203B737BBD0C308F52AC81FF8471CBC191DDC5BAAFFE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.joomag.com/Frontend/mobile/viewer/normalize.d0dfb984f88d0dbb9fde.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\normalize.d0dfb984f88d0dbb9fde[1].js

Preview:	webpackJsonp([21],{100:function(t,e){t.exports=function(){throw new Error("define cannot be used indirect")}},168:function(t,e,n){t.exports=n(169)},169:function(t,e,n){Object.assign=n(170),"undefined"==typeof Promise&&(n(171).enable(),window.Promise=n(173)),void 0===window.fetch&&n(99),"classList"in document.createElement("_")||n(174),"dataset"in document.createElement("_")||n(175)},170:function(t,e,n){"use strict";function r(t){if(null===t||void 0===t)throw new TypeError("Object.assign cannot be called with null or undefined");return Object(t)}var o=Object.getOwnPropertySymbols,i=Object.prototype.hasOwnProperty,s=Object.prototype.propertyIsEnumerable;t.exports=function(){try{if(!Object.assign)return!1;var t=new String("abc");if(t[5]="de","5"===Object.getOwnPropertyNames(t)[0])return!1;for(var e={},n=0;n<10;n++)e["_"+String.fromCharCode(n)]=n;if("0123456789"!==Object.getOwnPropertyNames(e).map(function(t){return e[t]}).join(""))return!1;var r={};return"abcdefghijklmnopqrst".split("").f

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\ping[1].htm

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	4
Entropy (8bit):	2.0
Encrypted:	false
SSDEEP:	3:tn:tn
MD5:	6FDB087AA3FBFBCB8287A593A0919E61
SHA1:	0E514A0662BCB69DC863953D1CE26E3D40E81A87
SHA-256:	9795C5FF8937F23526CCB207A5684C1FC94A7854E19C021B39D944E51F5BAEF2
SHA-512:	BE5457D14C930B51B47AB152850C1CEAAFE6EF88C8671B48164ABBC83410B0C07A1E178540F6CDEAC5F2672CADB1D1CBBB3434B3E39BC2C50C4646A2BAE57437
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://an3.joomag.com/ping?build_version=1.1.15
Preview:	pong

C:\Users\user\AppData\Local\Temp\~DF9697AB0B8A418A42.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47569755462363955
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loD9loD9lW8HjGy:kBqoIkaa
MD5:	9AC6D7E94AB01DEB8163A89B51434184
SHA1:	FA2343EC4899F3E0D3803CAF9D982A46434D43AB
SHA-256:	2475F3358FBBA56EA68A7CF6DD00310BA82B3D47AE586E64C4DB14C78F9F1ABA
SHA-512:	8B59FA6EA55A73DA04DD4215A1DB8630E70DE9F115C7B32038C3EAD2D184F3694806FB3D9F8043C90F9246C3210B7DA24D80CB3E392EAFC378765403B773157
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFA3DE0DB72D585233.TMP

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

C:\Users\user\AppData\Local\Temp\~DFF8E1FCFAEB5B2E87.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Temp\~DFF8E1FCFAEB5B2E87.TMP	
File Type:	data
Category:	dropped
Size (bytes):	44757
Entropy (8bit):	0.6404359474082872
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+9nDhAj8nIZqmjIZqmVd:kBqoxKAuqR+9nDhAj8ntmjtmVd
MD5:	9834AE45D49B772E8E9F866D3560470C
SHA1:	8B38E3554477FEA7C7A7F956749B2EC23D6891AD
SHA-256:	235641FD6AB383F7D3C3D3C7B693AADEF483D161D07C75F0AA02CE27BE34B79C
SHA-512:	388380FAA6707486AA3F9873A6014A2F4275348A6137740C08A1187015AA1782F3D1D58BD6D7830E1769687D01109592CA802CAC503F3A1DB30F7BF198B4400E
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Roaming\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys\settings.sxx	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	5830
Entropy (8bit):	4.633972099256422
Encrypted:	false
SSDEEP:	96:rWwibtibWibUib5ibvibAibCfibCCribCC3ibCCEibCCIlibCChlibCC:rWwi5iyi4iVi7isiWfiWuiWoiWJiW/l+
MD5:	AAD3AF9484B3DC05F1964D58D3E6E947
SHA1:	ADC9439E7CAE1B3351D048167EF2969029A1EA85
SHA-256:	FF5B87881863AE143AA8AF9308AE7266A540A5B6F6EDE58D533FFD3E5600E551
SHA-512:	D0B102F4B54BA6134DF190931DEF30E063D7D43592F5DA19D24383A16535A48EDA72447DF0F05BD5025CD12CFDE8B52B7AE48F2072326279994F3E2CA42223A7
Malicious:	false
Reputation:	low
Preview:	.....(TCSO.....settings.....gain.@I.....<TCSO.....settings.....gain.@I.....echosuppression.....STCSO.....settings.....gain.@I.....echosuppression.....defaultmicrophone.....fTCSO.....settings.....gain.@I.....echosuppression.....defaultmicrophone.....defaultcamera.....xTCSO.....settings.....gain.@I.....echosuppression.....defaultmicrophone.....defaultcamera.....defaultaudio.....TCSO.....settings.....gain.@I.....echosuppression.....defaultmicrophone.....defaultcamera.....defaultaudio.....defaultklimit.@Y.....TCSO.....settings.....gain.@I.....echosuppression.....defaultmicrophone.....defaultcamera.....defaultaudio.....defaultklimit.@Y.....defaultalways.....TCSO.....settings.....gain.@I.....echosuppression.....defaultmicrophone.....defaultcamera.....defaultaudio.....defaultklimit.@Y.....defaultalways.....windowlessDisable.....TCSO.....settings.....gain.@I.....echosu

Static File Info

No static file info

Network Behavior

Network Port Distribution

Total Packets: 93

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 4, 2021 22:49:30.026783943 CET	49720	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.027612925 CET	49721	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.147490025 CET	443	49720	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.147638083 CET	49720	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.148555994 CET	443	49721	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.148649931 CET	49721	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.156079054 CET	49720	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.156152010 CET	49721	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.275298119 CET	443	49721	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.275321007 CET	443	49720	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.275695086 CET	443	49720	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.275715113 CET	443	49720	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.275732040 CET	443	49720	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.275744915 CET	443	49720	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.275887966 CET	49720	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.275954962 CET	49720	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.291740894 CET	443	49720	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.291763067 CET	443	49720	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.291784048 CET	443	49721	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.291801929 CET	443	49721	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.291816950 CET	443	49721	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.291830063 CET	443	49721	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.291929007 CET	49720	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.292057037 CET	49721	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.292094946 CET	49721	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.305304050 CET	443	49721	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.305325985 CET	443	49721	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.305453062 CET	49721	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.332828999 CET	49720	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.332935095 CET	49721	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.338607073 CET	49720	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.338735104 CET	49721	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.338763952 CET	49720	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.452940941 CET	443	49720	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.452965021 CET	443	49720	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.453233957 CET	443	49721	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.453252077 CET	443	49721	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.453282118 CET	49720	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.453377008 CET	49721	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.455075026 CET	49721	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.455374956 CET	49720	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.458231926 CET	443	49720	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.458266973 CET	443	49721	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.458313942 CET	443	49720	209.95.50.27	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 4, 2021 22:49:30.458409071 CET	49721	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.458456993 CET	49720	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.477883101 CET	443	49720	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.478008032 CET	49720	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.561212063 CET	49723	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.561260939 CET	49724	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.616585016 CET	443	49721	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.616611004 CET	443	49720	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.680242062 CET	443	49723	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.680357933 CET	49723	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.680677891 CET	443	49724	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.680778027 CET	49724	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.681971073 CET	49724	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.682197094 CET	49723	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.802522898 CET	443	49723	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.802714109 CET	443	49724	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.802804947 CET	443	49723	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.802823067 CET	443	49723	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.802835941 CET	443	49723	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.802850962 CET	443	49723	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.802970886 CET	443	49724	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.802989006 CET	443	49724	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.802989006 CET	49723	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.803005934 CET	443	49724	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.803014994 CET	49723	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.803019047 CET	443	49724	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.803142071 CET	49724	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.805484056 CET	443	49723	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.805510044 CET	443	49724	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.805613041 CET	49723	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.805636883 CET	49724	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.821791887 CET	49723	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.822033882 CET	49724	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.822473049 CET	49723	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.822809935 CET	49723	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.823132038 CET	49724	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.943317890 CET	443	49723	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.943341017 CET	443	49723	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.943389893 CET	443	49724	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.943417072 CET	443	49724	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.943434000 CET	49723	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.943459034 CET	49724	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.943483114 CET	49724	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.943949938 CET	443	49724	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.944014072 CET	49724	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.945645094 CET	49723	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.946332932 CET	49724	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.977528095 CET	443	49723	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.977551937 CET	443	49723	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.977571964 CET	443	49723	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.977590084 CET	443	49723	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.977605104 CET	443	49723	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.977636099 CET	49723	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.977680922 CET	49723	443	192.168.2.4	209.95.50.27
Mar 4, 2021 22:49:30.977716923 CET	443	49723	209.95.50.27	192.168.2.4
Mar 4, 2021 22:49:30.977734089 CET	443	49723	209.95.50.27	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 4, 2021 22:49:22.446399927 CET	61516	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:22.492422104 CET	53	61516	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:23.204227924 CET	49182	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:23.254601955 CET	53	49182	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 4, 2021 22:49:24.144095898 CET	59920	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:24.194387913 CET	53	59920	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:24.932224989 CET	57458	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:24.982270002 CET	53	57458	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:26.040682077 CET	50579	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:26.095386982 CET	53	50579	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:27.314129114 CET	51703	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:27.362911940 CET	53	51703	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:28.118530035 CET	65248	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:28.166819096 CET	53	65248	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:28.846405983 CET	53723	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:28.902010918 CET	53	53723	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:29.081697941 CET	64646	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:29.127677917 CET	53	64646	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:29.845705986 CET	65298	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:30.014842033 CET	53	65298	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:30.106136084 CET	59123	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:30.171586037 CET	53	59123	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:30.493984938 CET	54531	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:30.553628922 CET	53	54531	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:30.935566902 CET	49714	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:30.989958048 CET	53	49714	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:31.233659983 CET	58028	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:31.289513111 CET	53097	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:31.290018082 CET	53	58028	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:31.335356951 CET	53	53097	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:31.532259941 CET	49257	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:31.578069925 CET	53	49257	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:31.867465973 CET	62389	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:31.932827950 CET	53	62389	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:32.851507902 CET	49910	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:32.900289059 CET	53	49910	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:33.873755932 CET	55854	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:33.883873940 CET	64549	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:33.931956053 CET	53	55854	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:33.938261986 CET	53	64549	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:34.006988049 CET	63153	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:34.055787086 CET	53	63153	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:34.203541040 CET	52991	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:34.260127068 CET	53	52991	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:34.375935078 CET	53700	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:34.406701088 CET	51726	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:34.424974918 CET	53	53700	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:34.469039917 CET	53	51726	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:34.493045092 CET	56794	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:34.530426979 CET	56534	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:34.540646076 CET	53	56794	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:34.586175919 CET	53	56534	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:34.709691048 CET	56627	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:34.755458117 CET	53	56627	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:35.047736883 CET	56621	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:35.093825102 CET	53	56621	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:35.189097881 CET	63116	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:35.249560118 CET	53	63116	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:38.848858118 CET	64078	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:38.897699118 CET	53	64078	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:39.669869900 CET	64801	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:39.728672981 CET	53	64801	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:40.728655100 CET	61721	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:40.777673006 CET	53	61721	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:41.543262959 CET	51255	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:41.592165947 CET	53	51255	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:48.011106014 CET	61522	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:48.067583084 CET	53	61522	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 4, 2021 22:49:51.134610891 CET	52337	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:51.464580059 CET	53	52337	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:51.800980091 CET	55046	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:51.802733898 CET	49612	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:51.808782101 CET	49285	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:51.810688019 CET	50601	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:51.848690033 CET	53	49612	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:51.851241112 CET	60875	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:51.854794025 CET	53	49285	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:51.859580040 CET	53	50601	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:51.863034964 CET	53	55046	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:51.895004034 CET	56448	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:51.897265911 CET	53	60875	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:51.940798998 CET	53	56448	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:52.243422031 CET	59172	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:52.289635897 CET	53	59172	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:58.825103045 CET	62420	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:58.882251978 CET	53	62420	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:59.427310944 CET	60579	53	192.168.2.4	8.8.8.8
Mar 4, 2021 22:49:59.485707045 CET	53	60579	8.8.8.8	192.168.2.4
Mar 4, 2021 22:49:59.840748072 CET	62420	53	192.168.2.4	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 4, 2021 22:49:29.845705986 CET	192.168.2.4	8.8.8.8	0xc9c7	Standard query (0)	joom.ag	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:30.493984938 CET	192.168.2.4	8.8.8.8	0xa6f9	Standard query (0)	view.joomag.com	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:31.233659983 CET	192.168.2.4	8.8.8.8	0x8fa7	Standard query (0)	www.joomag.com	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:31.289513111 CET	192.168.2.4	8.8.8.8	0xad91	Standard query (0)	browser.sentry-cdn.com	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:33.873755932 CET	192.168.2.4	8.8.8.8	0x7ab6	Standard query (0)	use.typekit.net	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:33.883873940 CET	192.168.2.4	8.8.8.8	0x23eb	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:34.203541040 CET	192.168.2.4	8.8.8.8	0xc48f	Standard query (0)	s9cdn.joomag.com	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:34.406701088 CET	192.168.2.4	8.8.8.8	0xb217	Standard query (0)	www.google.co.uk	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:34.493045092 CET	192.168.2.4	8.8.8.8	0x7f8d	Standard query (0)	js-agent.newrelic.com	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:34.530426979 CET	192.168.2.4	8.8.8.8	0x384e	Standard query (0)	p.typekit.net	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:34.709691048 CET	192.168.2.4	8.8.8.8	0x3a80	Standard query (0)	bam-cell.nr-data.net	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:35.189097881 CET	192.168.2.4	8.8.8.8	0x6fc0	Standard query (0)	an3.joomag.com	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:48.011106014 CET	192.168.2.4	8.8.8.8	0xb8e4	Standard query (0)	www.joomag.com	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:51.134610891 CET	192.168.2.4	8.8.8.8	0x9521	Standard query (0)	calfvessel.com	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:51.802733898 CET	192.168.2.4	8.8.8.8	0xc4f9	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:51.808782101 CET	192.168.2.4	8.8.8.8	0x4fe8	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:51.851241112 CET	192.168.2.4	8.8.8.8	0x797f	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:51.895004034 CET	192.168.2.4	8.8.8.8	0x85d8	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:52.243422031 CET	192.168.2.4	8.8.8.8	0xad19	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 4, 2021 22:49:30.014842033 CET	8.8.8.8	192.168.2.4	0xc9c7	No error (0)	joom.ag		209.95.50.27	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 4, 2021 22:49:30.553628922 CET	8.8.8.8	192.168.2.4	0xa6f9	No error (0)	view.joomag.com	lb.joomag.com		CNAME (Canonical name)	IN (0x0001)
Mar 4, 2021 22:49:30.553628922 CET	8.8.8.8	192.168.2.4	0xa6f9	No error (0)	lb.joomag.com		209.95.50.27	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:31.290018082 CET	8.8.8.8	192.168.2.4	0x8fa7	No error (0)	www.joomag.com	lb.joomag.com		CNAME (Canonical name)	IN (0x0001)
Mar 4, 2021 22:49:31.290018082 CET	8.8.8.8	192.168.2.4	0x8fa7	No error (0)	lb.joomag.com		209.95.50.27	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:31.335356951 CET	8.8.8.8	192.168.2.4	0xad91	No error (0)	browser.sentry-cdn.com		151.101.194.217	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:31.335356951 CET	8.8.8.8	192.168.2.4	0xad91	No error (0)	browser.sentry-cdn.com		151.101.66.217	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:31.335356951 CET	8.8.8.8	192.168.2.4	0xad91	No error (0)	browser.sentry-cdn.com		151.101.130.217	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:31.335356951 CET	8.8.8.8	192.168.2.4	0xad91	No error (0)	browser.sentry-cdn.com		151.101.2.217	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:33.931956053 CET	8.8.8.8	192.168.2.4	0x7ab6	No error (0)	use.typekit.net	use-stls.adobe.com.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
Mar 4, 2021 22:49:33.938261986 CET	8.8.8.8	192.168.2.4	0x23eb	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Mar 4, 2021 22:49:33.938261986 CET	8.8.8.8	192.168.2.4	0x23eb	No error (0)	stats.l.doubleclick.net		108.177.15.154	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:33.938261986 CET	8.8.8.8	192.168.2.4	0x23eb	No error (0)	stats.l.doubleclick.net		108.177.15.156	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:33.938261986 CET	8.8.8.8	192.168.2.4	0x23eb	No error (0)	stats.l.doubleclick.net		108.177.15.155	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:33.938261986 CET	8.8.8.8	192.168.2.4	0x23eb	No error (0)	stats.l.doubleclick.net		108.177.15.157	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:34.260127068 CET	8.8.8.8	192.168.2.4	0xc48f	No error (0)	s9cdn.joomag.com	s9.joomag.com		CNAME (Canonical name)	IN (0x0001)
Mar 4, 2021 22:49:34.260127068 CET	8.8.8.8	192.168.2.4	0xc48f	No error (0)	s9.joomag.com		107.182.226.40	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:34.469039917 CET	8.8.8.8	192.168.2.4	0xb217	No error (0)	www.google.co.uk		172.217.22.227	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:34.540646076 CET	8.8.8.8	192.168.2.4	0x7f8d	No error (0)	js-agent.newrelic.com	f4.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Mar 4, 2021 22:49:34.586175919 CET	8.8.8.8	192.168.2.4	0x384e	No error (0)	p.typekit.net	p.typekit.net-v3.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Mar 4, 2021 22:49:34.755458117 CET	8.8.8.8	192.168.2.4	0x3a80	No error (0)	bam-cell.nr-data.net	tls12.newrelic.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Mar 4, 2021 22:49:35.249560118 CET	8.8.8.8	192.168.2.4	0x6fc0	No error (0)	an3.joomag.com		209.95.50.25	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:48.067583084 CET	8.8.8.8	192.168.2.4	0xb8e4	No error (0)	www.joomag.com	lb.joomag.com		CNAME (Canonical name)	IN (0x0001)
Mar 4, 2021 22:49:48.067583084 CET	8.8.8.8	192.168.2.4	0xb8e4	No error (0)	lb.joomag.com		209.95.50.27	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:51.464580059 CET	8.8.8.8	192.168.2.4	0x9521	No error (0)	calfvessel.com		92.38.171.82	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:51.848690033 CET	8.8.8.8	192.168.2.4	0xc4f9	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Mar 4, 2021 22:49:51.854794025 CET	8.8.8.8	192.168.2.4	0x4fe8	No error (0)	maxcdn.bootstrapcdn.com	cds.j3z9t3p6.hwcdn.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 4, 2021 22:49:51.897265911 CET	8.8.8.8	192.168.2.4	0x797f	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Mar 4, 2021 22:49:51.940798998 CET	8.8.8.8	192.168.2.4	0x85d8	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:51.940798998 CET	8.8.8.8	192.168.2.4	0x85d8	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Mar 4, 2021 22:49:52.289635897 CET	8.8.8.8	192.168.2.4	0xad19	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 4, 2021 22:49:30.291740894 CET	209.95.50.27	443	192.168.2.4	49720	CN=joom.ag, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Sep 15 16:24:35 CEST 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Sun Oct 17 16:24:35 CEST 2021 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 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=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Mar 4, 2021 22:49:30.305304050 CET	209.95.50.27	443	192.168.2.4	49721	CN=joom.ag, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Sep 15 16:24:35 CEST 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Sun Oct 17 16:24:35 CEST 2021 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 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=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Mar 4, 2021 22:49:30.805484056 CET	209.95.50.27	443	192.168.2.4	49723	CN=*.joomag.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Mon Mar 30 12:55:04 CEST 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Thu Apr 01 19:02:39 CEST 2021 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 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=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Mar 4, 2021 22:49:30.805510044 CET	209.95.50.27	443	192.168.2.4	49724	CN=*.joomag.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Mon Mar 30 12:55:04 CEST 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Thu Apr 01 19:02:39 CEST 2021 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 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=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Mar 4, 2021 22:49:31.541841030 CET	151.101.194.217	443	192.168.2.4	49733	CN=*.sentry-cdn.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Mon Feb 22 20:39:57 CET 2021 Tue Jul 28 02:00:00 CEST 2020	Sat Mar 26 20:39:57 CET 2022 Sun Mar 18 01:00:00 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=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Mar 4, 2021 22:49:31.549156904 CET	151.101.194.217	443	192.168.2.4	49732	CN=*.sentry-cdn.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Mon Feb 22 20:39:57 CET 2021 Tue Jul 28 02:00:00 CEST 2020	Sat Mar 26 20:39:57 CET 2022 Sun Mar 18 01:00:00 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=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Mar 4, 2021 22:49:31.621411085 CET	209.95.50.27	443	192.168.2.4	49731	CN=www.joomag.com, O="Joomag, Inc.", L=San Jose, ST=California, C=US, SERIALNUMBER=C3715754, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.2=California, OID.1.3.6.1.4.1.311.60.2.1.3=US CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Thu Jan 28 22:07:13 CET 2021 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Sun Jan 30 01:23:39 CET 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 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=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 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 4, 2021 22:49:31.622154951 CET	209.95.50.27	443	192.168.2.4	49726	CN=www.joomag.com, O="Joomag, Inc.", L=San Jose, ST=California, C=US, SERIALNUMBER=C3715754, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.2=California, OID.1.3.6.1.4.1.311.60.2.1.3=US CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Thu Jan 28 22:07:13 CET 2021 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Sun Jan 30 01:23:39 CET 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 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=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Mar 4, 2021 22:49:31.624752998 CET	209.95.50.27	443	192.168.2.4	49730	CN=www.joomag.com, O="Joomag, Inc.", L=San Jose, ST=California, C=US, SERIALNUMBER=C3715754, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.2=California, OID.1.3.6.1.4.1.311.60.2.1.3=US CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Thu Jan 28 22:07:13 CET 2021 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Sun Jan 30 01:23:39 CET 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 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=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 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 4, 2021 22:49:31.628803015 CET	209.95.50.27	443	192.168.2.4	49729	CN=www.joomag.com, O="Joomag, Inc.", L=San Jose, ST=California, C=US, SERIALNUMBER=C3715754, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.2=California, OID.1.3.6.1.4.1.311.60.2.1.3=US CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Thu Jan 28 22:07:13 CET 2021 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Sun Jan 30 01:23:39 CET 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 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=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Mar 4, 2021 22:49:31.630390882 CET	209.95.50.27	443	192.168.2.4	49727	CN=www.joomag.com, O="Joomag, Inc.", L=San Jose, ST=California, C=US, SERIALNUMBER=C3715754, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.2=California, OID.1.3.6.1.4.1.311.60.2.1.3=US CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Thu Jan 28 22:07:13 CET 2021 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Sun Jan 30 01:23:39 CET 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 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=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 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 4, 2021 22:49:31.631870031 CET	209.95.50.27	443	192.168.2.4	49728	CN=www.joomag.com, O="Joomag, Inc.", L=San Jose, ST=California, C=US, SERIALNUMBER=C3715754, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.2=California, OID.1.3.6.1.4.1.311.60.2.1.3=US CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Thu Jan 28 22:07:13 CET 2021 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Sun Jan 30 01:23:39 CET 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 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=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Mar 4, 2021 22:49:34.040745974 CET	108.177.15.154	443	192.168.2.4	49741	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 4, 2021 22:49:34.040822029 CET	108.177.15.154	443	192.168.2.4	49742	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 4, 2021 22:49:34.522083998 CET	107.182.226.40	443	192.168.2.4	49745	CN=*.joomag.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Mon Mar 30 12:55:04 CEST 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Thu Apr 01 19:02:39 CEST 2021 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 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=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Mar 4, 2021 22:49:34.523749113 CET	107.182.226.40	443	192.168.2.4	49744	CN=*.joomag.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Mon Mar 30 12:55:04 CEST 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Thu Apr 01 19:02:39 CEST 2021 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 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=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 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 4, 2021 22:49:34.571036100 CET	172.217.22.227	443	192.168.2.4	49748	CN=www.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 10:05:37 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 20 11:05:36 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 4, 2021 22:49:34.571742058 CET	172.217.22.227	443	192.168.2.4	49749	CN=www.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 10:05:37 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 20 11:05:36 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 4, 2021 22:49:35.494690895 CET	209.95.50.25	443	192.168.2.4	49757	CN=*.joomag.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Mon Mar 30 12:55:04 CEST 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Thu Apr 01 19:02:39 CEST 2021 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 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=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

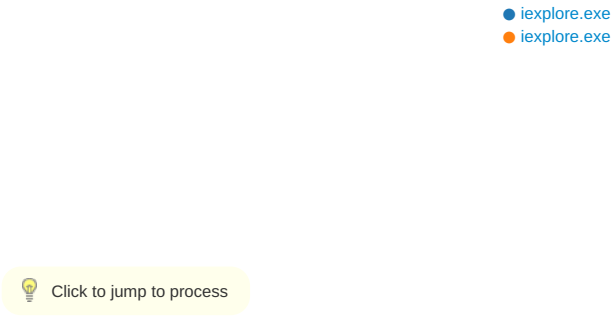
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 4, 2021 22:49:35.496665955 CET	209.95.50.25	443	192.168.2.4	49758	CN=*.joomag.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Mon Mar 30 12:55:04 CEST 2020	Thu Apr 01 19:02:39 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=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Mar 4, 2021 22:49:48.318698883 CET	209.95.50.27	443	192.168.2.4	49763	CN=www.joomag.com, O="Joomag, Inc.", L=San Jose, ST=California, C=US, SERIALNUMBER=C3715754, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.2=California, OID.1.3.6.1.4.1.311.60.2.1.3=US CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Thu Jan 28 22:07:13 CET 2021	Sun Jan 30 01:23:39 CET 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 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 4, 2021 22:49:51.600198030 CET	92.38.171.82	443	192.168.2.4	49765	CN=calfvessel.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 02 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Tue Jun 01 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Mar 4, 2021 22:49:51.654973030 CET	92.38.171.82	443	192.168.2.4	49764	CN=calfvessel.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 02 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Tue Jun 01 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Mar 4, 2021 22:49:52.081717968 CET	104.16.18.94	443	192.168.2.4	49781	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 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Mar 4, 2021 22:49:52.086076021 CET	104.16.18.94	443	192.168.2.4	49782	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 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 3492 Parent PID: 800

General

Start time:	22:49:29
Start date:	04/03/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff73a910000
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: 5160 Parent PID: 3492

General

Start time:	22:49:29
Start date:	04/03/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3492 CREDAT:17410 /prefetch:2
Imagebase:	0x2e0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	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