ID: 384809
Cookbook: browseurl.jbs
Time: 21:22:56
Date: 09/04/2021
Version: 31.0.0 Emerald

Table of Contents

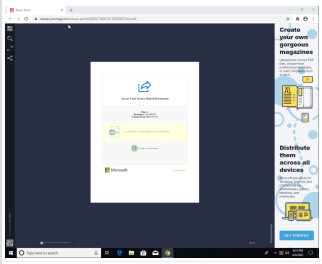
Analysis Report https://joom.ag/Ja5I

Overview

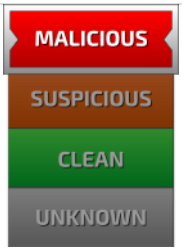
General Information

Sample URL:	http://https://joom.ag/Ja5I
Analysis ID:	384809
Infos:	

Most interesting Screenshot:



Detection



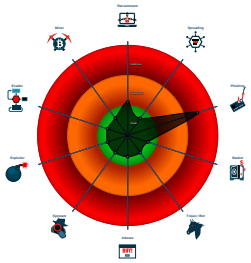
HTMLPhisher

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

Signatures

- Antivirus detection for URL or domain
- Yara detected HtmlPhish10
- Yara detected HtmlPhish7
- Found iframes
- HTML body contains low number of …
- HTML title does not match URL
- Suspicious form URL found

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 6896 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://joom.ag/Ja5I' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6000 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1316,17158847015543384734,7560515483952834825,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1800 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6216 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1316,17158847015543384734,7560515483952834825,131072 --lang=en-GB --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=6788 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

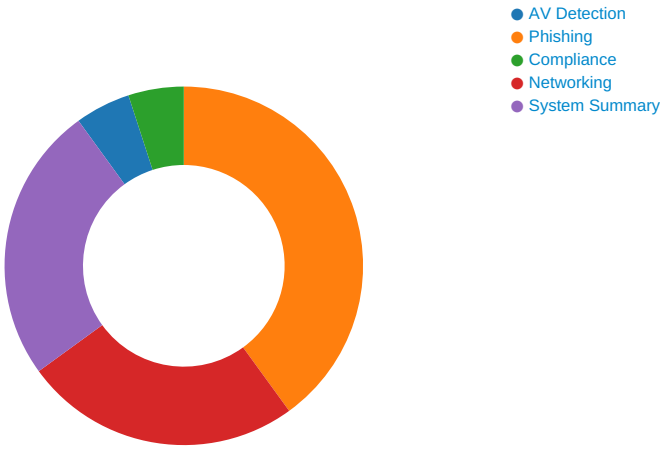
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Phishing:

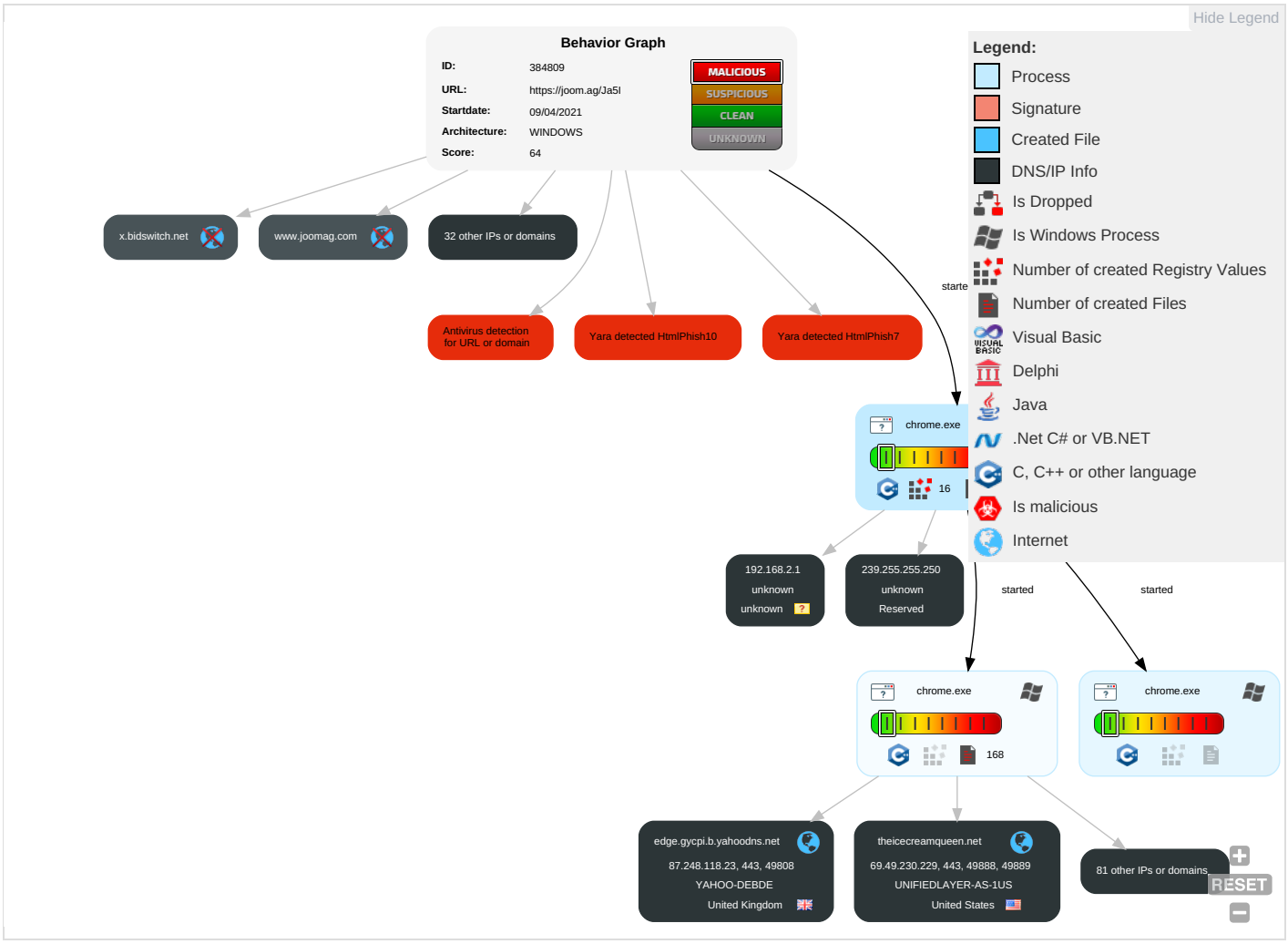
Yara detected HtmlPhish10

Yara detected HtmlPhish7

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	I
Drive-by Compromise 1	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M S F
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	D L
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	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	D D D

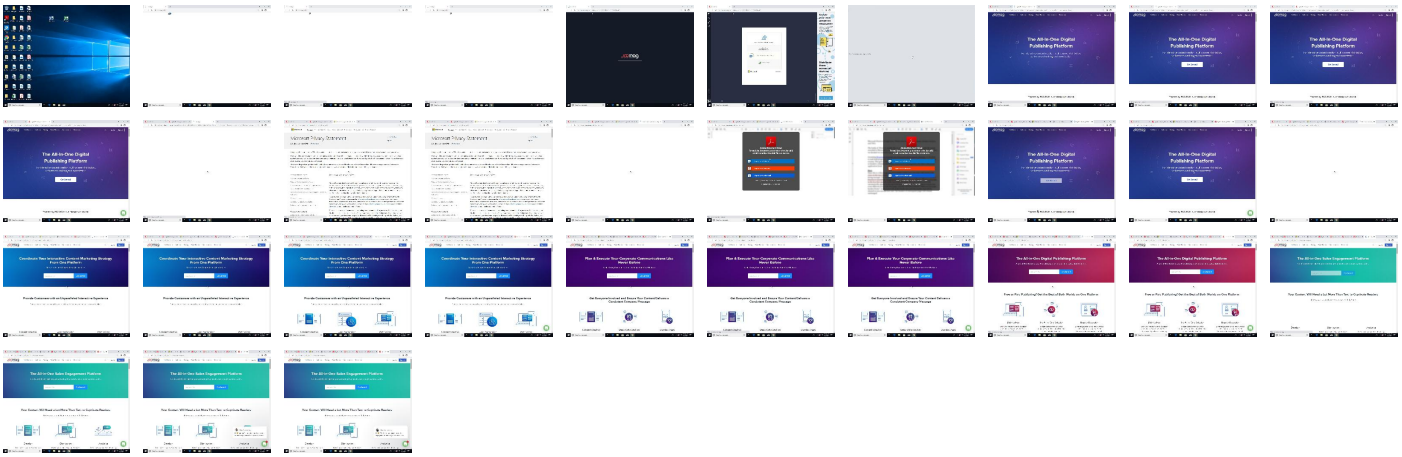
Behavior Graph

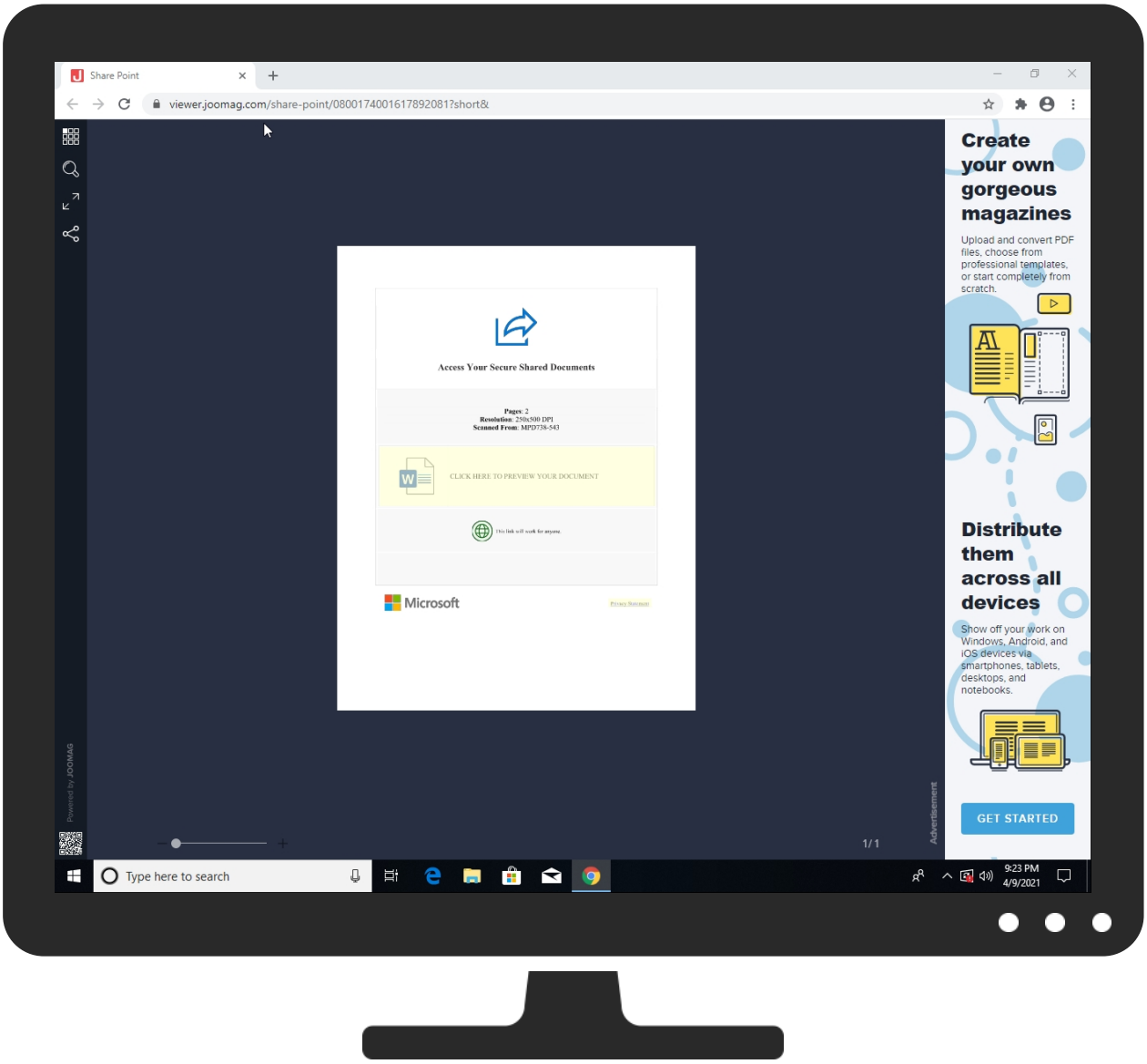


Screenshots

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/Ja5I	0%	Virustotal		Browse
http://https://joom.ag/Ja5I	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
browser.sentry-cdn.com	0%	Virustotal		Browse
theicecreamqueen.net	0%	Virustotal		Browse
js.hs-analytics.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://theicecreamqueen.net/pswiss/cube/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://joom.ag/Ja5I4	0%	Avira URL Cloud	safe	
http://https://joom.ag/Ja5I2	0%	Avira URL Cloud	safe	
http://https://js.hs-analytics.net/analytics/1617996000000/5574303.js	0%	Avira URL Cloud	safe	
http://https://js.hs-banner.com/cookie-banner	0%	Avira URL Cloud	safe	
http://https://www.intercom-reporting.com/sentry/index.html	0%	Avira URL Cloud	safe	
http://https://northcentralusr-notifyp.svc.ms/api/v2/tracking/method/Click?mi=3g1fY2BPqE-2GZL5d-54LA&ru=htt	0%	Avira URL Cloud	safe	
http://https://assets.onestore.ms/	0%	URL Reputation	safe	
http://https://assets.onestore.ms/	0%	URL Reputation	safe	
http://https://assets.onestore.ms/	0%	URL Reputation	safe	
http://https://d.adroll.mgr.consensu.org/consent/iabcheck/	0%	URL Reputation	safe	
http://https://d.adroll.mgr.consensu.org/consent/iabcheck/	0%	URL Reputation	safe	
http://https://d.adroll.mgr.consensu.org/consent/iabcheck/	0%	URL Reputation	safe	
http://https://js.hs-banner.com/5574303.jsaD	0%	Avira URL Cloud	safe	
http://https://theicecreamqueen.net/X	0%	Avira URL Cloud	safe	
http://https://joom.ag/Ja5IShare	0%	Avira URL Cloud	safe	
http://https://joom.ag/Ja5IY	0%	Avira URL Cloud	safe	
http://https://js.hsadspixel.net/fb.jsaD	0%	Avira URL Cloud	safe	
http://https://www.intercom-reporting.com	0%	Avira URL Cloud	safe	
http://https://joom.ag/Ja5Ii	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
browser.sentry-cdn.com	151.101.66.217	true	false	• 0%, Virustotal, Browse	unknown
forms.hubspot.com	104.19.154.83	true	false		high
theicecreamqueen.net	69.49.230.229	true	false	• 0%, Virustotal, Browse	unknown
pug-lhr.pubmatic.com	185.64.190.80	true	false		high
js.hs-analytics.net	104.17.68.176	true	false	• 0%, Virustotal, Browse	unknown
alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com	18.158.181.33	true	false		high
adserver-vpc-alb-2-1264451658.eu-west-1.elb.amazonaws.com	34.252.196.107	true	false		high
scontent.xx.fbcdn.net	157.240.17.15	true	false		high
idsync.rlcdn.com	35.244.174.68	true	false		high
track.hubspot.com	104.19.155.83	true	false		high
cdnjs.cloudflare.com	104.16.19.94	true	false		high
js.hs-scripts.com	104.17.214.204	true	false		high
cm.g.doubleclick.net	172.217.168.66	true	false		high
nexus-websocket-a.intercom.io	35.170.0.145	true	false		high
d2065cca9qi4ey.cloudfront.net	99.86.3.39	true	false		high
joom.ag	209.95.50.27	true	false		unknown
am-vip001.taboola.com	141.226.228.48	true	false		high
js.intercomcdn.com	99.86.3.104	true	false		high
star-mini.c10r.facebook.com	157.240.219.35	true	false		high
js.hs-banner.com	104.18.20.191	true	false		unknown
chidc2.outbrain.org	64.74.236.159	true	false		unknown
us-u.openx.net	34.98.64.218	true	false		high
stats.l.doubleclick.net	74.125.143.157	true	false		high
prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud	18.197.99.6	true	false		unknown
alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com	35.156.223.207	true	false		high
widget.intercom.io	13.32.25.95	true	false		high
maxcdn.bootstrapcdn.com	104.18.11.207	true	false		high
js.hsadspixel.net	104.17.114.176	true	false		unknown
api-iam.intercom.io	75.2.88.188	true	false		high
s9.joomag.com	107.182.226.40	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com	3.121.70.57	true	false		high
pug22000nf.pubmatic.com	185.64.189.110	true	false		high
js.hsleadflows.net	104.17.230.204	true	false		unknown
lb.joomag.com	209.95.50.27	true	false		high
googleads.g.doubleclick.net	216.58.215.226	true	false		high
api.hubapi.com	104.17.200.204	true	false		high
www.google.ch	216.58.215.227	true	false		high
an3.joomag.com	209.95.50.25	true	false		high
ib.anycast.adnxs.com	185.33.221.89	true	false		high
prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud	3.126.56.137	true	false		unknown
googlehosted.l.googleusercontent.com	172.217.168.33	true	false		high
adserver-vpc-alb-3-890571764.eu-west-1.elb.amazonaws.com	3.248.28.111	true	false		high
edge.gycpi.b.yahoodns.net	87.248.118.23	true	false		unknown
rum.monitis.com	192.111.140.242	true	false		high
static.intercomassets.com	unknown	unknown	false		high
ka-f.fontawesome.com	unknown	unknown	false		high
d.adroll.com	unknown	unknown	false		high
viewer.joomag.com	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
www.joomag.com	unknown	unknown	false		high
use.typekit.net	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high
pixel.rubiconproject.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
p.typekit.net	unknown	unknown	false		high
simage2.pubmatic.com	unknown	unknown	false		high
d.adroll.mgr.consensu.org	unknown	unknown	false		unknown
ups.analytics.yahoo.com	unknown	unknown	false		high
assets.onestore.ms	unknown	unknown	false		unknown
ajax.aspnetcdn.com	unknown	unknown	false		high
ads.yahoo.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
pixel.advertising.com	unknown	unknown	false		high
sync.outbrain.com	unknown	unknown	false		high
bam-cell.nr-data.net	unknown	unknown	false		unknown
sync.taboola.com	unknown	unknown	false		high
x.bidswitch.net	unknown	unknown	false		unknown
www.facebook.com	unknown	unknown	false		high
northcentralusr-notifyp.svc.ms	unknown	unknown	false		unknown
js-agent.newrelic.com	unknown	unknown	false		high
s.adroll.com	unknown	unknown	false		high
dsum-sec.casalemedia.com	unknown	unknown	false		high
ib.adnxs.com	unknown	unknown	false		high
eb2.3lift.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.joomag.com/en/solutions/digital-publishing	false		high
http://https://www.joomag.com/en/	false		high
http://https://www.joomag.com/en/solutions/sales-engagement	false		high
http://https://theicecreamqueen.net/pswiss/cube/	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://joomag.elevio.help/en/articles/245	1a841bd9fc7ecccd_0.1.dr	false		high
http://https://js.intercomcdn.com/intersection/assets/app.js	65befcac1cde97c2_0.1.dr	false		high
http://https://code.jquery.com/jquery-3.2.1.slim.min.js	0f1894c5ddc566ef_0.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.joomag.com/jcsip/html5/v1/magazine/2445305?is_linked_domain=0&manuallyEmbedded=&viewMode	e096b84e660703e1_0.1.dr	false		high
http://https://www.joomag.com/en/	Favicons.1.dr, History.1.dr	false		high
http://https://www.joomag.com/en/solutions/interactive-content-marketing.Interactive	Current Session.1.dr	false		high
http://https://use.typekit.net/olb8zpk.js	c0ec2433cf77f682_0.1.dr	false		high
http://https://joom.ag/Ja5I4	History-journal.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://joomag.elevio.help/en/articles/241	1a841bd9fc7ecccd_0.1.dr	false		high
http://https://joomag.elevio.help/en/articles/240	1a841bd9fc7ecccd_0.1.dr	false		high
http://https://joom.ag/Ja5I2	History Provider Cache.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.joomag.com/static/js/pages/home.js?_=5.1.8.0	4d1295fcda27fb46_0.1.dr	false		high
http://https://s.adroll.com/j/pre/7S36S2RHW5BUVAXH6L4RZE/6TMQVXNPWBG6BOGAF3EFID/index.jsaD	7b5d3be33a96cdb3_0.1.dr	false		high
http://www.joomag.com/publication/Name/777).	1a841bd9fc7ecccd_0.1.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/1003757157/?random=1617996273414&cv	202398c31ac24d4a_0.1.dr	false		high
http://https://docs.intercom.com/configure-intercom-for-your-product-or-site/staying-secure/enable-identity	65befcac1cde97c2_0.1.dr	false		high
http://https://s.adroll.com/j/sendrolling.jsaD	35aec16058a68073_0.1.dr	false		high
http://https://stats.g.doubleclick.net/j/collect	2a82640fed18fa5c_0.1.dr	false		high
http://https://js.hs-analytics.net/analytics/1617996000000/5574303.js	0773c091491a9080_0.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://kit.fontawesome.com/585b051251.js	c32afd9997a26c41_0.1.dr	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js	91721bc070d4628d_0.1.dr	false		high
http://https://joomag.elevio.help/en/articles/251	1a841bd9fc7ecccd_0.1.dr	false		high
http://https://app.intercom.com	65befcac1cde97c2_0.1.dr	false		high
http://https://joomag.com/	5383b090eaa51678_0.1.dr, c0b2aab84f0a50bc_0.1.dr, cbe0f973381fa0cf_0.1.dr, 4dc39f0688ebc553_0.1.dr, ea08dd46bb01fafe_0.1.dr, a262d627eec5cc8b_0.1.dr, 9890963327d9ee09_0.1.dr, b2009de9dba4a7bb_0.1.dr, b450020f7ef934d5_0.1.dr	false		high
http://https://a.nel.cloudflare.com/report?s=bElhZG%2FfAn8G9%2Fwa3%2BIFTPBJchNhNhtrloQMMHWLEqRDXo%2BhalFLsD	Reporting and NEL-journal.3.dr	false		high
http://https://maxcdn.bootstrapcdn.com/	Network Action Predictor-journal.1.dr	false		high
http://https://js.hs-banner.com/cookie-banner	4dc39f0688ebc553_0.1.dr	false	• Avira URL Cloud: safe	unknown
http://certs.godaddy.com/repository/1301	9FE5AC4619D265EF6BFD31DF947C4A78_EDA79DBED7732591D0FF867E00812BA50.3.dr	false		high
http://https://www.joomag.com/static/js/pages/solutions.js?_=5.1.8.0	83137b52fc11f0b5_0.1.dr	false		high
http://https://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.2.min.js	094e2d6bf2abec98_0.1.dr	false		high
http://https://widget.intercom.io/widget/ue3kdzui	6158ca99bdaf719d_0.1.dr	false		high
http://https://js.intercomcdn.com/vendors~message-modern.bcad7328.jsaD	dd4ec45c32f91a40_0.1.dr	false		high
http://https://kit.fontawesome.com/	Network Action Predictor-journal.1.dr	false		high
http://https://connect.facebook.net/signals/config/295648160646317?v=2.9.33&r=stableaD	4f99dcb1a864e622_0.1.dr	false		high
http://https://connect.facebook.net/	87fd1924f833e73a_0.1.dr	false		high
http://https://js.intercomcdn.com/vendor-modern.a5ba650d.jsa	88c2694a38162e86_0.1.dr	false		high
http://https://www.intercom-reporting.com/sentry/index.html	65befcac1cde97c2_0.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/1003757157/?random=1617996280828&cv	8c50196a1e0f9ecd_0.1.dr	false		high
http://https://ajax.aspnetcdn.com/	Network Action Predictor-journal.1.dr	false		high
http://https://northcentralusr-notifyp.svc.ms/api/v2/tracking/method/Click?mi=3g1fY2BPqE-2GZL5d-54LA&ru=htt	Favicons.1.dr, History.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://a.nel.cloudflare.com/report?s=c5HLz3ZnW6Cijh0u72CdPeqdeCgiCoF4vn3oD9HELZhGYP%2F4dtXqoTqsKHUe	Reporting and NEL.3.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/1003757157/?random=1617996285268&cv	68cc6d037028d20c_0.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://js.intercomcdn.com/vendor-modern.a5ba650d.js	88c2694a38162e86_0.1.dr	false		high
http://https://js.intercomcdn.com/vendors~app-modern.4c248a1f.js	c243fa307356206a_0.1.dr	false		high
http://https://www.joomag.com/en/solutions/corporate-communications	Current Session.1.dr	false		high
http://https://js.intercomcdn.com/vendors~app-modern.4c248a1f.jsaD	c243fa307356206a_0.1.dr	false		high
http://https://js.intercomcdn.com/vendors~message-modern.bcad7328.js	dd4ec45c32f91a40_0.1.dr	false		high
http://https://a.nel.cloudflare.com/report?s=ePVJulaWUxZUfE1T7lUWtXzp4GDCwsQwShmb7eCyP%2BpZUFvlqaaWnIuD2%2B	Reporting and NEL-journal.3.dr	false		high
http://https://connect.facebook.net/signals/config/295648160646317?v=2.9.33&r=stable	4f99dcb1a864e622_0.1.dr	false		high
http://https://feedback.googleusercontent.com	manifest.json0.1.dr	false		high
http://https://assets.onestore.ms/	Network Action Predictor-journal.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://joomag.com/M	18e402f011ac7071_0.1.dr	false		high
http://https://joomag.com/G	9ff14046406d6375_0.1.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/jquery-mousewheel/3.1.13/jquery.mousewheel.min.js?isAjax=true	66856abd7f544089_0.1.dr, e52b8eeb5910a627_0.1.dr, b2009de9dba4a7bb_0.1.dr, 18e402f011ac7071_0.1.dr	false		high
http://https://joomag.com/F	8c50196a1e0f9ecd_0.1.dr	false		high
http://https://www.joomag.com/en/solutions/interactive-content-marketingInteractive	History.1.dr	false		high
http://www.joomag.com/magazine/perfil48_digital/0020314001309513566	1a841bd9fc7ecccd_0.1.dr	false		high
http://https://joomag.com/b	cbe0f973381fa0cf_0.1.dr	false		high
http://https://viewer.joomag.com/share-point/0800174001617892081?short&Share	History.1.dr	false		high
http://www.joomag.com/)	1a841bd9fc7ecccd_0.1.dr	false		high
http://https://js.intercomcdn.com/vendor-modern.a5ba650d.jsaD	88c2694a38162e86_0.1.dr	false		high
http://https://www.joomag.com/Frontend/mobile/viewer/main.36b2b001eb97fb16211c.js	0381749d97c141e8_0.1.dr	false		high
http://https://www.joomag.com/?ref=viewer_ad&utm_source=viewer_ad_create&utm_medium=non-paid&utm_campaign=j	Current Session.1.dr	false		high
http://https://joomag.com/Z	15c16c3f27e21b62_0.1.dr	false		high
http://https://connect.facebook.net/signals/config/290226788268586?v=2.9.33&r=stable	b8d56c7282a9959b_0.1.dr, 5e0609edbb009490_0.1.dr	false		high
http://https://connect.facebook.net/signals/config/290226788268586?v=2.9.33&r=stableaD	5e0609edbb009490_0.1.dr	false		high
http://https://joom.ag/Ja5I	Favicons-journal.1.dr, Current Session.1.dr	false		unknown
http://https://d.adroll.mgr.consensu.org/consent/iabcheck/	1c6644b795785887_0.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://joomag.com/2	989b6fe145516e59_0.1.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/1003757157/?random=1617996259759&cv	f610433733328f19_0.1.dr	false		high
http://https://js.hs-banner.com/5574303.jsaD	4dc39f0688ebc553_0.1.dr	false	• Avira URL Cloud: safe	unknown
http://schema.org	5e0609edbb009490_0.1.dr	false		high
http://https://www.joomag.com/en/solutions/corporate-communicationsCorporate	History.1.dr	false		high
http://https://use.typekit.net/af/e0b8be/00000000000000000000148a6/23/	c0ec2433cf77f682_0.1.dr	false		high
http://https://www.joomag.com/Frontend/mobile/viewer/vendor.7bc4df7aaac8424047c3.js	a262d627eec5cc8b_0.1.dr	false		high
http://https://www.joomag.com/Frontend/mobile/viewer/manifest.6ab342fa4d7e7af5331a.js	6b1b9d51f4f5cab5_0.1.dr	false		high
http://https://joomag.com/C	e5fc65743dc33dcc_0.1.dr	false		high
http://https://joomag.com/A	3cf52a5fdd0e540e_0.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://s.adroll.com/pixel/7S36S2RHW5BUVAXH6L4RZE/6TMQVXNPWBG6BOGAF3EFID/II7UVDRCFFFIVJPI3D2QTU.js	ea08dd46bb01fafe_0.1.dr	false		high
http://https://js.hs-scripts.com/5574303.js	cbe0f973381fa0cf_0.1.dr	false		high
http://https://www.joomag.com/static/js/pages/home.js?_=5.1.8.0a	0c59603c94d6b5b4_0.1.dr	false		high
http://https://theicecreamqueen.net/X	569ae1a688927577_0.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://joom.ag/Ja5IShare	History.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://joomag.com/6	7b5d3be33a96cdb3_0.1.dr	false		high
http://https://joomag.elevio.help/en/articles/268	1a841bd9fc7ecccd_0.1.dr	false		high
http://https://joom.ag/Ja5IY	Favicons-journal.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://joomag.elevio.help/en/articles/266	1a841bd9fc7ecccd_0.1.dr	false		high
http://https://js.intercomcdn.com/frame-modern.f881becc.js	65befcac1cde97c2_0.1.dr, 989b6fe145516e59_0.1.dr	false		high
http://https://use.typekit.net/olb8zpk.jsaD	c0ec2433cf77f682_0.1.dr	false		high
http://https://code.jquery.com/jquery-3.1.1.min.js	569ae1a688927577_0.1.dr	false		high
http://https://js.hsadspixel.net/fb.jsaD	9ac614ffd44f5d33_0.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.intercom-reporting.com	65befcac1cde97c2_0.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://code.jquery.com/	Network Action Predictor-journal.1.dr	false		high
http://https://www.joomag.com/en/solutions/sales-engagement	Current Session.1.dr	false		high
http://https://js.intercomcdn.com/	65befcac1cde97c2_0.1.dr	false		high
http://https://joom.ag/Ja5Ii	Favicons-journal.1.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.19.155.83	track.hubspot.com	United States		13335	CLOUDFLARENETUS	false
104.17.68.176	js.hs-analytics.net	United States		13335	CLOUDFLARENETUS	false
104.18.20.191	js.hs-banner.com	United States		13335	CLOUDFLARENETUS	false
18.158.181.33	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
104.17.230.204	js.hsleadflows.net	United States		13335	CLOUDFLARENETUS	false
99.86.3.39	d2065cca9qi4ey.cloudfront.net	United States		16509	AMAZON-02US	false
185.64.190.80	pug-lhr.pubmatic.com	United Kingdom		62713	AS-PUBMATICUS	false
151.101.66.217	browser.sentry-cdn.com	United States		54113	FASTLYUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.17.214.204	js.hs-scripts.com	United States		13335	CLOUDFLARENETUS	false
3.121.70.57	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
99.86.3.104	js.intercomcdn.com	United States		16509	AMAZON-02US	false
192.111.140.242	rum.monitis.com	United States		46562	TOTAL-SERVER-SOLUTIONSUS	false
34.252.196.107	adserver-vpc-alb-2-1264451658.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
104.19.154.83	forms.hubspot.com	United States		13335	CLOUDFLARENETUS	false
69.49.230.229	theicecreamqueen.net	United States		46606	UNIFIEDLAYER-AS-1US	false
18.197.99.6	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud	United States		16509	AMAZON-02US	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
3.126.56.137	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud	United States		16509	AMAZON-02US	false
157.240.219.35	star-mini.c10r.facebook.com	United States		32934	FACEBOOKUS	false
35.244.174.68	idsync.rlcdn.com	United States		15169	GOOGLEUS	false
35.170.0.145	nexus-websocket-a.intercom.io	United States		14618	AMAZON-AESUS	false
104.17.114.176	js.hsadspixel.net	United States		13335	CLOUDFLARENETUS	false
104.17.200.204	api.hubapi.com	United States		13335	CLOUDFLARENETUS	false
157.240.17.15	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
172.217.168.66	cm.g.doubleclick.net	United States		15169	GOOGLEUS	false
141.226.228.48	am-vip001.taboola.com	Israel		200478	TABOOLA-ASIL	false
64.74.236.159	chidc2.outbrain.org	United States		22075	AS-OUTBRAINUS	false
107.182.226.40	s9.joomag.com	United States		32780	HOSTINGSERVICES-INCUS	false
3.248.28.111	adserver-vpc-alb-3-890571764.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
74.125.143.157	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
87.248.118.23	edge.gycpi.b.yahoodns.net	United Kingdom		203220	YAHOO-DEBDE	false
185.33.221.89	ib.anycast.adnxs.com	Netherlands		29990	ASN-APPNEXUS	false
209.95.50.25	an3.joomag.com	United States		32780	HOSTINGSERVICES-INCUS	false
104.18.11.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
34.98.64.218	us-u.openx.net	United States		15169	GOOGLEUS	false
172.217.168.33	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
75.2.88.188	api-iam.intercom.io	United States		16509	AMAZON-02US	false
13.32.25.95	widget.intercom.io	United States		7018	ATT-INTERNET4US	false
209.95.50.27	joom.ag	United States		32780	HOSTINGSERVICES-INCUS	false
104.16.19.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	384809
Start date:	09.04.2021
Start time:	21:22:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 45s

Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://joom.ag/Ja5I
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:	21
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.phis.win@50/326@80/42
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://www.joomag.com/?ref=viewer_ad&utm_source=viewer_ad_create&utm_medium=non-paid&utm_campaign=jm_leads • Browse: https://northcentralusr-notifyp.svc.ms/api/v2/tracking/method/Click?mi=3g1fY2BPqE-2GZL5d-54LA&ru=https%3a%2f%2fprivacy.microsoft.com%2fprivacystatement%5c&tc=PrivacyStatement&cs=75fd1b1b09b9b0af634e4faacc127ef1 • Browse: https://theicecreamqueen.net/pswiss/cube • Browse: https://www.joomag.com/en/ • Browse: https://www.joomag.com/en/solutions/interactive-content-marketing • Browse: https://www.joomag.com/en/solutions/corporate-communications • Browse: https://www.joomag.com/en/solutions/digital-publishing • Browse: https://www.joomag.com/en/solutions/sales-engagement
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 40.88.32.150, 23.54.113.53, 13.88.21.125, 52.147.198.201, 172.217.168.35, 216.58.215.238, 172.217.168.13, 142.250.34.2, 192.124.249.41, 192.124.249.24, 192.124.249.22, 192.124.249.23, 192.124.249.36, 216.58.215.232, 172.217.168.78, 172.217.168.4, 23.10.249.43, 23.10.249.9, 104.83.104.145, 172.217.168.42, 151.101.2.110, 151.101.66.110, 151.101.130.110, 151.101.194.110, 162.247.243.146, 162.247.243.147, 74.125.173.166, 172.217.168.10, 172.217.168.74, 216.58.215.234, 2.22.153.73, 2.20.209.195, 69.173.144.139, 69.173.144.165, 69.173.144.138, 23.0.174.200, 23.0.174.185, 13.64.90.137, 216.58.215.226, 13.107.136.13, 23.54.112.217, 23.10.249.18, 23.10.249.33, 152.199.19.160, 2.18.103.205, 2.20.240.220, 23.10.249.26, 69.16.175.42, 69.16.175.10, 104.18.22.52, 104.18.23.52, 216.58.215.227, 172.64.202.28, 172.64.203.28, 20.82.210.154, 20.82.209.183, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, e6653.dscf.akamaiedge.net, cds.s5x3j6q5.hwcdn.net, assets.onestore.ms.edgekey.net, arc.msn.com.nsatc.net, ka-f.fontawesome.com.cdn.cloudflare.net, tls12.newrelic.com.cdn.cloudflare.net, e13678.dscb.akamaiedge.net, clientservices.googleapis.com, i.s-microsoft.com.edgekey.net, a1945.g2.akamai.net, skypedataprdcoleus15.cloudapp.net, www.microsoft.com-c-3.edgekey.net,

clients2.google.com, use-stls.adobe.com.edgesuite.net, audownload.windowsupdate.nsatc.net, update.googleapis.com, www.google.com, statics-marketingsites-eus-ms-com.akamaized.net, watson.telemetry.microsoft.com, www.gstatic.com, ocsp.godaddy.com.akadns.net, au-bg-shim.trafficmanager.net, www.google-analytics.com, e10583.dspg.akamaiedge.net, fonts.googleapis.com, content-autofill.googleapis.com, ajax.googleapis.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, www.googleapis.com, assets.onestore.ms.akadns.net, r1---sn-1gieen7e.gvt1.com, c-s.cms.ms.akadns.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, wildcard.adroll.com.edgekey.net, blobcollector.events.data.trafficmanager.net, dsum-sec.casalemedia.com.edgekey.net, svc-ms.spo-0008.spo-msedge.net, c.s-microsoft.com-c.edgekey.net, clients.l.google.com, privacy.microsoft.com.edgekey.net, e4007.g.akamaiedge.net, au.download.windowsupdate.com.edgesuite.net, www.googleadservices.com, pixel.rubiconproject.net.akadns.net, store-images.s-microsoft.com-c.edgekey.net, i.s-microsoft.com, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, r1.sn-1gieen7e.gvt1.com, www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, e8037.g.akamaiedge.net, mscomajax.vo.msecnd.net, redirector.gvt1.com, www.googletagmanager.com, arc.trafficmanager.net, edgedl.gvt1.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, kit.fontawesome.com.cdn.cloudflare.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, p.typekit.net-v3.edgekey.net, accounts.google.com, www-google-analytics.l.google.com, cs22.wpc.v0cdn.net, fonts.gstatic.com, www-googletagmanager.l.google.com, f4.shared.global.fastly.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus17.cloudapp.net, c.s-microsoft.com, spo-0008.spo-msedge.net, privacy.microsoft.com, e13678.dscg.akamaiedge.net, ocsp.godaddy.com, skypedataprdcolwus15.cloudapp.net, e13678.dspb.akamaiedge.net, www.microsoft.com, a1988.dscg1.akamai.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net

- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing network information.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtQueryVolumeInformationFile calls found.
- Report size getting too big, too many NtWriteFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:23:44	API Interceptor	5x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\223DE96EE265046957A660ED7C9DD9E7_EFF9B9BA98DEAA773F261FA85A0B1771

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1731
Entropy (8bit):	7.314678693508401
Encrypted:	false
SSDEEP:	48:panitqGF7EoGylMnita8lnitq1+Zvl3oXS9As5RmEWqu5H99:pWelz1+boavLJpu5
MD5:	674998133A041D533A27979FDF8B1DFD
SHA1:	921FFC2CD390058A9D947B4F9FC34856BC54C5F9
SHA-256:	4A23F8871099736EB86B24A89DEA6BD607B59D7A2A387E507EF2BDF25839F492
SHA-512:	26800CEA764378E8D030F0D500F7269DCDC69E36A9933C8B1FAA3BD456969830942E7B462E0EFC2FFB8743C5AEB84C0953978FFE727B3802C7C79F879C6B088
Malicious:	false
Reputation:	low
Preview:	0.....0.....+.....0.....0...0.....0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.100...U...'Go Daddy Root Validation Authority - G2..20210409005230Z0d0b0:0...+.....#o..K.....#....+...:....g(.....An .....20210409005230Z....20210410125230Z0...*.H.....`/..$.*.....?\|R.r.).B.....Q..q.e.9.%....E\|3i..Z.%E*.YZq..ght.T/....G....H5.y.8H....~BC..&.....h...)..X.....Z.s.];. .._.)]E...`..'N..(...^+rrj.....k.4;..u.Q...c....1..;..U.J..]D.$..x..k-./.;a-.}.....O[..}.....4.q._g.[.\'...\..KfYd.....0...0...0..g.....f...p.t0...*.H.....0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.110/..U...(Go Daddy Root Certificate Authority - G20...200909070000Z..210909070000Z0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.100...U...'Go Daddy Root Validation Authority - G20..."0...*.H.....0.....'.....^Y.u..U.qU..."......-]XG(qk#.+....J...G.3

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	117192
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	3072:F2qSSwIm1m/QEBbgb1om2qSSwIm1m/QEBbgb1oQ:FJdwIm1m/QEOb1omJdwIm1m/QEOb1oQ
MD5:	2FEBC5EB397A71B7A4862D0DCC21CA5E
SHA1:	5568FBD6D7DB899850D3AAFF95FEC08952361678

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
SHA-256:	2E9BE05B763D01CB0CD6FDE8BC64432A012AD3ECD9A6F3099DDE740A2D148A13
SHA-512:	B7D42B634F3B0CDC81CB94F281C8BB743BB98421AE54E21005637F762292D865EB1D71D43C4FF96AEE824527E9F7FB94FE5F5A4D35A22363A2A86AF8ABE0C414
Malicious:	false
Reputation:	low
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-.J...."Y...$E.KB..D...D.....3.n..u.....|..=H4..c&.....f.,..=..-....p2.:..`HX.....b.....Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.].g...yw..\|0.+?.`-../.xvy..e.....w.+^...w\|.Q.k.9&.Q.EzS.f.....>?w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k.._iK..xzW.w.M.>,5.}..}.tLX5Ls3_..).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....:.x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....ItNs.\....s...,f`D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.l....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\9FE5AC4619D265EF6BFD31DF947C4A78_EDA79DBED7732591D0FF867E00812BA5	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1778
Entropy (8bit):	7.311778029318123
Encrypted:	false
SSDEEP:	48:+ni/2TBcQuKcnitxUni/1+Zvl3oXS9A0d5RxEOaKIhEe07P:92TtfT/1+boaFLeHK4W
MD5:	57C0C2026F4C1061D8A6AE79C0C422B9
SHA1:	1D91E7B831E562A5A629279A8F16740B3255DC0B
SHA-256:	6288D7BF915C3A11D272CDAAC6C9D3672F60AAAD835D4BC6A894F636B444572E
SHA-512:	ACFCB22B8F387758B76C05021F881754A978B4B71A44564B4A502BE240FA0D0E4B9A8CC78CFB90426778F2A670FA1C93C4B270C38173386DDBA157058BEC014A
Malicious:	false
Reputation:	low
Preview:	0.....0.....+.....0.....0...0...z0x1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy Inc.1+0)..U..."Go Daddy Validation Authority - G2..20210408232518Z0l0j0B0...+....._lkv...8..f..R34N..@.'..4.0.3..l.,.....Zt(...\....20210408232518Z....20210410112518Z0...*.H.....T;ls...7.C.h.!...^6 .....7...DU$'YNiB..\.wBe"..T..h_t.]7.9.f2...{.0..&=.b....w.G/-..u.B....2..ZC..9.'.....M<...?...h.<..Y...M..).....%.t..?...^w..Oy,G...0....c.GP,.!.7.....1{.}^.b\|....zDvB..(._]...R.....4z....,....8..f..z.....t..O....0...0...0.....X...l0...*.H.....0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.1-0+..U...$http://certs.godaddy.com/repository/1301..U...*Go Daddy Secure Certificate Authority - G20...2009090700002..2109090700002Z0x1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy Inc.1+0)..U..."Go Daddy Validation Authority - G20.."0...*.H.....0.....'.....^Y.u..U.qU.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\EB2C4AB8B68FFA4B7733A9139239A396_D76DB901EE986B889F30D8CC06229E2D	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1697
Entropy (8bit):	7.298972299288275
Encrypted:	false
SSDEEP:	48:snitqJl3DuVnitqsXA49e5REMeZ6+23wQ:UJIosw49eEMeZ6+Y
MD5:	C180DB31189FDEC83C653D2BCEE9A412
SHA1:	63DD8CAB6D486409E6E28B46DB7873CD56B9C936
SHA-256:	24A9E9F2F104D78FF2E100F1B568B626C38FCA96A6541516D534F53BEC7024CD
SHA-512:	80F3632A0525CFAC0EE50EF6961C2F02109BCB435E14747583BDA44E7D49123C0B63CA5E2B79091D2680DE7F87933ED277FBEA002E2AE18308673612635C5372
Malicious:	false
Reputation:	low
Preview:	0.....0.....+.....0.....0...0.....0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.100...U..."Go Daddy Root Validation Authority - G1..20210408195420Z0f0d0<0...+..... .....]..J^.y_..F<.....L.q.a.=...j.....20210408195420Z....20210410075420Z0...*.H.....9v..V...&....&{..T...Y...v...4....d.Y.y...Nn.2.-L..ZJ.Je.....`".4..j..&Y..4.s...3..3M2;l.....:1Z...glR~.=w(0..[.:).....:.....Do..,L`.k.4.an...#.Y..r5....N.....'.....@.<.0C....8.T..~..d6cn.....@a.v ...=U..O.....n....W...H4..;..S..l.nw...b0..^0..Z0..B.....1g...r.0...*.H.....0c1.0...U....US1!0...U....The Go Daddy Group, Inc.110/..U...(Go Daddy Class 2 Certification Authority0...161213070000Z..211213070000Z0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.100...U..'Go Daddy Root Validation Authority - G10.."0...*.H.....0.....}...@.H.....j.b.2.c...'eSA...6""2.hf.m.m9....._N."gV..{.J"{..0f.W$.X

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\223DE96EE265046957A660ED7C9DD9E7_EFF9B9BA98DEAA773F261FA85A0B1771	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	900
Entropy (8bit):	3.719367086899591
Encrypted:	false
SSDEEP:	12:fZCrQESIgsFFV13Mz1mySGqheQDM3k4rQESIgsFFV13Mz1mySGqhew:IwyPV13MhmyFqYeENwyPV13MhmyFqYw
MD5:	C89F4BED4E1FF579FCC5D49DC73A65AC
SHA1:	309D48F16674AC37E3D2A14BE3A656489E1035ED
SHA-256:	753827CD58D973143F8AE2D83E4D72C252336E8E317A00DF3C65749983D3E7F1

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\223DE96EE265046957A660ED7C9DD9E7_EFF9B9BA98DEAA773F261FA85A0B1771	
SHA-512:	28373DDA2A2408F1FAD86F17D209FA289530C881FD1CDDAAAA5442A3165C80A3FC22FF6D1C3F2F105F1334E98055F89D612ECE9539FED9C8D40AAD373CA0A40
Malicious:	false
Reputation:	low
Preview:	p..... .....u-..(..... .....<.,.....V.....h.t.t.p.:.//.o.c.s.p...g.o.d.a.d.d.y...c.o.m././/.M.E.I.w.Q.D.A.%.2.B.M.D.w.w.O.j.A.J.B.g.U.r.D .g.M.C.G.g.U.A.B.B.Q.d.I.2.%.2.B.O.B.k.u.X.H.9.3.f.o.R.U.j.4.a.7.I.A.r.4.r.G.w.Q.U.O.p.q.F.B.x.B.n.K.L.b.v.9.r.0.F.Q.W.4.g.w.Z.T.a.D.9.4.C.A.Q.c.%.3.D...".9.2.1.f.f.c.2.c .d.3.9.0.0.5.8.a.9.d.9.4.7.b.4.f.9.f.c.3.4.8.5.6.b.c.5.4.c.5.f.9."...p..... .....u-..(.....<.,...{.].....{.]..... .....<.,.....V.....h.t.t.p.:.//.o.c.s.p...g.o.d.a.d.d. y...c.o.m././/.M.E.I.w.Q.D.A.%.2.B.M.D.w.w.O.j.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.Q.d.I.2.%.2.B.O.B.k.u.X.H.9.3.f.o.R.U.j.4.a.7.I.A.r.4.r.G.w.Q.U.O.p.q.F.B.x.B.n.K.L.b.v.9.r. 0.F.Q.W.4.g.w.Z.T.a.D.9.4.C.A.Q.c.%.3.D...".9.2.1.f.f.c.2.c.d.3.9.0.0.5.8.a.9.d.9.4.7.b.4.f.9.f.c.3.4.8.5.6.b.c.5.4.c.5.f.9."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.131160794046323
Encrypted:	false
SSDEEP:	12:TUkwTJrkPlE99SNxAhUe0h1kwTJrkPlE99SNxAhUe0ht:U5kPcUQUPhl5kPcUQUPht
MD5:	930482A6C9AC0511C439E3D11C3159BF
SHA1:	D7AF1251784E859A3EB36F8D0F16166EC17082D7
SHA-256:	C1AE06C0E619FB74E61A0DE6EB52916828DCD99C180B878FFF32917C3A50CC40
SHA-512:	B6F9B9D2B8E7F535792CB7A6F269C14F38EBB3BA7F5AC8C958E895185B794E1CB625FF90FBDF57A2E27E03167FB5FA21B8BFFA92A7882C182FD96AB791400952
Malicious:	false
Reputation:	low
Preview:	p..... .....v-..(..... .....$.....h.t.t.p.:.//.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i. c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b..".0.d.8.f.4.f.3.f.6.f.d.7.1.:.0."...p..... .....K(.)v-..(..... .....$.....h.t.t.p.:.//.c.t. l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b..".0.d.8.f.4.f.3.f.6.f.d.7.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\9FE5AC4619D265EF6BFD31DF947C4A78_EDA79DBED7732591D0FF867E00812BA5	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	948
Entropy (8bit):	3.7519084747265325
Encrypted:	false
SSDEEP:	24:gU+Ihn8B0tQpusnuhLlciM/nU0U+Ihn8B0tQpusnuhLlciM4:gU40SusuhLlpM/nU0U40SusuhLlpM4
MD5:	F5CA6F5080C8877518CD2DF5836B4437
SHA1:	53219A990FE15309C3B41611D9E22E305FCE6695
SHA-256:	E53FBEE4077B1752D8A252864612C33157D4B6FF27B0A36BC25D537EF0B19EC1
SHA-512:	07D9042C5AF16E7DBE3A327DB96787EAEFDCC8CF533661CD8395E743DFC616573B24E02C6C55EC26B0E8106C6EF28515D10915FD78C63D63B6F8FFF25E533B0
Malicious:	false
Reputation:	low
Preview:	p..... .....}t.u-..(..... .....o.,.....V.....h.t.t.p.:.//.o.c.s.p...g.o.d.a.d.d.y...c.o.m././/.M.E.o.w.S.D.B.G.M.E.Q.w.Q.j.A.J.B.g.U.r.D.g. M.C.G.g.U.A.B.B.S.2.C.A.1.f.b.G.t.2.6.x.P.k.O.K.X.4.Z.g.u.o.U.j.M.0.T.g.Q.U.Q.M.K.9.J.4.7.M.N.I.M.w.o.j.P.X.%.2.B.2.y.z.8.L.Q.s.g.M.4.C.C.Q.D.y.W.n.Q.o.v.8.w.X. X.A.%.3.D.%.3.D...".1.d.9.1.e.7.b.8.3.1.e.5.6.2.a.5.a.6.2.9.2.7.9.a.8.f.1.6.7.4.0.b.3.2.5.5.d.c.0.b."...p..... .....}t.u-..(.....o.,....W/.-.....W/.-.. .....o.,.. ....V.....h.t.t.p.:.//.o.c.s.p...g.o.d.a.d.d.y...c.o.m././/.M.E.o.w.S.D.B.G.M.E.Q.w.Q.j.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.S.2.C.A.1.f.b.G.t.2.6.x.P.k.O.K.X.4.Z.g.u.o.U.j.M. 0.T.g.Q.U.Q.M.K.9.J.4.7.M.N.I.M.w.o.j.P.X.%.2.B.2.y.z.8.L.Q.s.g.M.4.C.C.Q.D.y.W.n.Q.o.v.8.w.X.X.A.%.3.D.%.3.D...".1.d.9.1.e.7.b.8.3.1.e.5.6.2.a.5.a.6.2.9.2.7.9.a.8.f.1.6. 7.4.0.b.3.2.5.5.d.c.0.b."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EB2C4AB8B68FFA4B7733A9139239A396_D76DB901EE986B889F30D8CC06229E2D	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	916
Entropy (8bit):	3.768018917527818
Encrypted:	false
SSDEEP:	12:31CrQEFDsFrvgxE0P6GANMsGAUVAfuPO3+rQEFDsFrvgxE0P6GANMsGAUVQ:sV4xaVSGAmskHV4xaVSGAmskO
MD5:	39968558E8613F1C32FE92BC337594B0
SHA1:	99CBCE9B2AB39DBC68313B4AC2EDFB96C843E91A
SHA-256:	737F420A7E67B363254546AEA9AA087A0F8444C1FAC9B51AE3B5A65D8FCD0634
SHA-512:	E5EFDE633ABAE34F3029787D7924EE1E84006E1EBF254873D72C1D7B3003C1D6D064A4A2A029101A48F875896DD998D76F96FCD90E76EDB70ACF4C8A26CAE88

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EB2C4AB8B68FFA4B7733A9139239A396_D76DB901EE986B889F30D8CC06229E2D	
Malicious:	false
Reputation:	low
Preview:	p..... .....u-..(..... .....~...,.....V.....h.t.t.p.:././.o.c.s.p...g.o.d.a.d.d.y...c.o.m././.M.E.Q.w.Q.j.B.A.M.D.4.w.P.D.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.T.k.I.I.n.K.B.A.z.X.k.F.0.Q.h.0.p.e.l.3.l.f.H.J.9.G.P.A.Q.U.0.s.S.w.0.p.H.U.T.B.F.x.s.2.H.L.P.a.H.%.2.B.3.a.h.q.1.O.M.C.A.x.v.n.F.Q.%.3.D.%.3.D...".6.3.d.d.8.c.a.b.6.d.4.8.6.4.0.9.e.6.e.2.8.b.4.6.d.b.7.8.7.3.c.d.5.6.b.9.c.9.3.6."...p..... .....u-..(.....~...,.....-.....-.. .....~...,.....V.....h.t.t.p.:././.o.c.s.p...g.o.d.a.d.d.y...c.o.m././.M.E.Q.w.Q.j.B.A.M.D.4.w.P.D.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.T.k.I.I.n.K.B.A.z.X.k.F.0.Q.h.0.p.e.l.3.l.f.H.J.9.G.P.A.Q.U.0.s.S.w.0.p.H.U.T.B.F.x.s.2.H.L.P.a.H.%.2.B.3.a.h.q.1.O.M.C.A.x.v.n.F.Q.%.3.D.%.3.D...".6.3.d.d.8.c.a.b.6.d.4.8.6.4.0.9.e.6.e.2.8.b.4.6.d.b.7.8.7.3.c.d.5.6.b.9.c.9.3.6."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\03327d76-5900-4232-bb7a-dfb33863b756.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7464644109593688
Encrypted:	false
SSDEEP:	384:/DjYU2NfiGBsDNQr5vMY3TwG7HGbG3Kr1KsmxziyG1rh4m1CZaQIMTOWCgNh1wZi:lK1Z2mDbBOeLCM+Y3TCgK6wc9n
MD5:	FDD938F24CB1A07F565E71FF60ADDDA2
SHA1:	67C206FAF1B2AEA20374F7935B3B2090A1EB6F63
SHA-256:	E06938438E6696EF30A6E2DF17B9EEE97031D202A45235AD4A02DBDE7BF7F15F
SHA-512:	F28C9BAEEC0BE6948BE65B1D6211CF6A253D7AD93DBB54C19AE6CCF2CA4DA4714C6C190C01233021D6F4E68E98A4630ACA7C05CFBDC6BB4A83DC7E07FA998EC
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....68.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\09974af9-c041-4574-90ce-bc14ef1998f6.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	155732
Entropy (8bit):	6.0519499325566
Encrypted:	false
SSDEEP:	3072:FzmnDWVhPFlyU7sCXgcbjH+FcbXafIB0u1GOJmA3iuRl:F6Q1sJQHUaqfIlUOoSiuRl
MD5:	529380EF18F93E1C8C5DB485B256033C
SHA1:	45E13A43CFE0C629C361ED1C26E45E8FB826FF99
SHA-256:	F66BAD96EC7906AB18A629073DE5C828B36A9AE92377650BCE73AFDB59C64FAB
SHA-512:	6CE32D9D4DB5F50B1E103610C796567C0769F35F7C008F9A5DF6F3AFD58C931601545BB1B296B9521FF7455B4C2C119C83286991B3576CCD8EE648944E8CE814
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.617996221923738e+12,"network":1.617996223e+12,"ticks":299346023.0,"uncertainty":4396219.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715037176"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\220701f2-2262-470b-b0e6-2f18e3a1b602.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	164217
Entropy (8bit):	6.082237556707135
Encrypted:	false
SSDEEP:	3072:1yXzmnDWVhPFlyU7sCXgcbjH+FcbXafIB0u1GOJmA3iuRl:AD6Q1sJQHUaqfIlUOoSiuRl
MD5:	854A8D8EB2DD4CCD45575D56A5004681
SHA1:	FC475A06CA22F40E6FCB6C86AB7900D92A05648B
SHA-256:	3E6AA412722476CFEB552C6D4060AFBAF96E1937070172EA285AFBB8E58006D2
SHA-512:	6ACEB9E8572A6EB74026FC3D861DD1753845498F5747126FFE7C69B497EBC8725AD3937EC49886FCF48670499FC19EFF1D4AF6F0B9AF0010FEF1796B4892FAC5
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\220701f2-2262-470b-b0e6-2f18e3a1b602.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.617996221923738e+12,"network":1.617996223e+12,"ticks":299346023.0,"uncertainty":4396219.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\4d52bd67-ec12-43a3-9c23-5db0a6dac35d.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	155732
Entropy (8bit):	6.051949991632804
Encrypted:	false
SSDEEP:	3072:fzmnDWVhPFlyU7sCXgcbjH+FcbXafIB0u1GOJmA3iuRl:b6Q1sJQHUaqfllUOoSiuRl
MD5:	4721E9DEB7F171433FDA8C0A3B966F7F
SHA1:	20D47A71AE6E08A53AF8F5200F3FB9B21F2676C6
SHA-256:	CE24E6F18B89F1070B6077F7BFB484EB32AB49B579383340BDF7B31C4BB55DC7
SHA-512:	935200746D1CFF2E6F60699B909E014A23666825A424F021801ABB221573EB8F9C16579B277E62E402CA344556F3BD221FBAFBA575727D8D9C1E7EBA706FB716
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.617996221923738e+12,"network":1.617996223e+12,"ticks":299346023.0,"uncertainty":4396219.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715037176"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\5db2f70b-a435-4dbe-bc44-2b3564297671.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	164217
Entropy (8bit):	6.082240585882834
Encrypted:	false
SSDEEP:	3072:14jzmnDWVhPFlyU7sCXgcbjH+FcbXafIB0u1GOJmA3iuRl:Kv6Q1sJQHUaqfllUOoSiuRl
MD5:	5A2B34256250A1081C4373CA6C9A477F
SHA1:	791072F8C513A9F3070264EA8B632370A7266545
SHA-256:	90E5493BA6BE09E45C8072DB63C1628A420AF1DB2281BDE64CEF34E6AAF5FAF0
SHA-512:	BCEE079D8D93C18AE76115BC74CBC0FBD083EA06A4B67D970D40EC9CE414839CDB9F4F54A76E31384D9652089E77218749E4851F4B2F61124CFD785F27BE3B8A
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.617996221923738e+12,"network":1.617996223e+12,"ticks":299346023.0,"uncertainty":4396219.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\6912c58b-1941-40e2-af39-0000630ae65a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	155818
Entropy (8bit):	6.052117957971814
Encrypted:	false
SSDEEP:	3072:3zmnDWVhPFlyU7sCXgcbjH+FcbXafIB0u1GOJmA3iuRl:j6Q1sJQHUaqfllUOoSiuRl
MD5:	1EF69D689398EC66F21F9A6C1C11F8BE
SHA1:	C88C35C032EFAB02DEF69AA965E5E7874018DA02
SHA-256:	117E95E6B2E0C0BEFBCEBD5F624FC2BEDF60D0D412E6F5F8545DFB1AADF6F113
SHA-512:	0874541188BBA63940724371739B2465FFECA116A3E8C48F3D85254F5C298BC13CCE5960E38E565CB1D6F3211ED355F708848F373E48523DC5F21446798011F0
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\6912c58b-1941-40e2-af39-0000630ae65a.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.617996221923738e+12,"network":1.617996223e+12,"ticks":299346023.0,"uncertainty":4396219.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715037176"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\6d8e3ded-3e7a-459f-8f0e-5dc66522d59e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	164217
Entropy (8bit):	6.082237931280541
Encrypted:	false
SSDEEP:	3072:16szmnDWVhPFlyU7sCXgcbjH+FcbXafIB0u1GOJmA3iuRl:gO6Q1sJQHUaqfIlUOoSiuRl
MD5:	5CFCBDCF2C9D85D56BFFE2DDE4CD59E1
SHA1:	23DD47FEAA774E056FE2D67073939A0EE750F301
SHA-256:	0B65C1AFE16BA784D1D1EB3B95D916F1AD10887AF9076D725843266482773946
SHA-512:	1D5F3B6ECC271F4C1C7F0E3CB37DCAAE607B0CB418E24D9D8F5BB1544E36CC3634299BF2388A82072F3CDC27774EBB53CA30BBE7384AA15646638679DCBEE92
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.617996221923738e+12,"network":1.617996223e+12,"ticks":299346023.0,"uncertainty":4396219.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXwgs0oRL6twgs0oRL6twgs0oRLn:+taRL+taRL+taRLn
MD5:	E6C1693D9F0F6B6E878D098FBFD4C92A
SHA1:	D9D2708143B4A3BA5D14DFED59DCB6B88DF172D9
SHA-256:	E9DA6B8F6549D084D8740EB4C25755989B057EBF4F36B5E526F34DFFAB7500CF
SHA-512:	19B28BFE66708B294AB033C2F87D219E1C29D4F9363AC92E89B9406F6E2ACB13AD5DF73DD7E163D1ADEC0AF89C42DA112AE153EB23378EC29302F91192B7C59
Malicious:	false
Reputation:	low
Preview:	sdPC.....UO..E.D.Q.o....sdPC.....UO..E.D.Q.o....sdPC.....UO..E.D.Q.o....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0768fbad-571c-4793-ac5d-b0fcaf52e9db.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22601
Entropy (8bit):	5.536252647511085
Encrypted:	false
SSDEEP:	384:TjxtyLlK2XX1kXqKf/pUZNCgVLH2HfDIrUeHGYnZUprWL4P:+LlTX1kXqKf/pUZNCgVLH2HfUrUOGYnE
MD5:	1588ED868EE277476C82085BAEDF2A03
SHA1:	BEC5A25E247D9CA3D124AF15C8B3735CFF069C45
SHA-256:	A8AD2DD151238897FB51E34A81B59E2690C75BF3B8264DA2E3BC5670D922BB61
SHA-512:	F482237D444463494EB54EEFDF2257FF500312C9433A9C3AD294E0BD54778F403AC1F9205B89FF5D6C381E269C6C54EBF5A8D510AA717E45FE932F79E62091F1
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0768fbad-571c-4793-ac5d-b0fcaf52e9db.tmp	
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13262469819006524","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\090ab7ba-97a7-4308-bad8-a084a1ecebce.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4554
Entropy (8bit):	5.598594676827789
Encrypted:	false
SSDEEP:	96:5kUyt1UWUWU4Uh7eUrieUPENZUwUMUUJMU6UqUnUjUkU2UeUbfKU1UrPeU+klUjB:2Uk1UWUWU4UdeU1U4ZUwUMUUmU6UqUn1
MD5:	9B1699A18FFA24A63ED4C384FD05D225
SHA1:	9F331B4F76DC5CDE3E2859D0DF9ADF9088F0E559
SHA-256:	65AC6E96A54F1665EA179C1FE91BA2CE5199272B0C6388642095A24227C55C3C
SHA-512:	D6FDA99D3DEB67A94D5F91B41FD296FB77655A9010E01E1937410A80B2457E73D16897AA787BCB2FA4DED82C85EC3B03C3DFD15032B1DF2A217C724D25EF41F
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1649532392.760829,"host":"AVsuOZgBg0wdpKMoxm8zihjqET8kI4Xl8bCSMk28RsE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1617996392.760834},{"expiry":1649532224.395841,"host":"CZU0ovCjWSlHcoYuG0ZSGiph68/Tvd43RsTejedDQms=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1617996224.395846},{"expiry":1633776439.047545,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1617996439.047549},{"expiry":1633548440.984938,"host":"HS0xQK8RrrSZ/KdSgKIC7bLU+ximr9JuWvTPbfkE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1617996440.984941},{"expiry":1649532441.88589,"host":"H5h/QTW8LTBlZOFYCI2QgyCoSXZApKh65MvyuWwrS0I=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1617996441.885895},{"expiry":1628882840.644909,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0fcea0b7-19f2-4f26-925b-a853342d1c98.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	4553
Entropy (8bit):	5.598265624525518
Encrypted:	false
SSDEEP:	96:5kUyt1UWUWU4Uh7eUrieU3NZUUUMUUJMU6UqUnUjUkU2UeUbfKU1UrPeU+klUjxT:2Uk1UWUWU4UdeU1U9ZUUUMUUmU6UqUn1
MD5:	22C60E73AA1CE59BF77C63DAEDFCB04D
SHA1:	CF3F8CFDB4A37DAAF87D3C8BA74AB8397F82AC83
SHA-256:	BAB7837A0E1980FB352552DE5839858EAF25ED8CC314DB0094F42FA43FC394D5
SHA-512:	13B788FEE87605C403B79A72126A806F7F72FEC4FF7F1CB4B996C04F8502847C0E0D6F7FB38E4C5B2648F257AFCA1483B27533D6A4215629E359C6D5DFE01486
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1649532392.760829,"host":"AVsuOZgBg0wdpKMoxm8zihjqET8kI4Xl8bCSMk28RsE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1617996392.760834},{"expiry":1649532224.395841,"host":"CZU0ovCjWSlHcoYuG0ZSGiph68/Tvd43RsTejedDQms=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1617996224.395846},{"expiry":1633776439.047545,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1617996439.047549},{"expiry":1633548440.984938,"host":"HS0xQK8RrrSZ/KdSgKIC7bLU+ximr9JuWvTPbfkE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1617996440.984941},{"expiry":1649532441.88589,"host":"H5h/QTW8LTBlZOFYCI2QgyCoSXZApKh65MvyuWwrS0I=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1617996441.885895},{"expiry":1628882840.644909,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1efbbe27-9060-44d7-88ee-bb97d45dab45.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5084
Entropy (8bit):	4.962307966138115
Encrypted:	false
SSDEEP:	96:nrLiROfpIVu5k0JCKL8DJkkc+1nLbOTlVuHn:nr3fpI8h4KCkkc+BV
MD5:	D10DF6946D18A61BB9A6959E6304F504
SHA1:	284E7E7C7458742C484B95185C452388EF9565FF
SHA-256:	D4D26BBF442565F207ADE8B19BB69B5C73FCC68E2DB653E12D35B454C6D5B670
SHA-512:	4CFEC9AD9BBF59DB1FB2759C3D9D7377F9D9701159B22A42277C4F09195719D112BB47233AAEA69A26CB7175BE6ECA64CD44DAF350889BE68CA1E1437BF081B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1efbbe27-9060-44d7-88ee-bb97d45dab45.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13262469819253134","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1f2110e0-fcfb-4b6e-a7da-9e32d8bb1b0d.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	5.602806275121382
Encrypted:	false
SSDEEP:	96:5kUyt1UcUDUAUTeUIieUlNZU4UMUUbgUHXUfUGyU8UYUeUyKUzOU+PeUklUSUAU8:2Uk1UcUDUAUTeUQUnZU4UMUUUU3UfU5r
MD5:	24CD18E34F5FC9075D1315D7692443BC
SHA1:	7226E5853E42F8D2D792242DA81E872EEB4F47BF
SHA-256:	0E2E608DD54BE7813C3E1FE85CF514E0094619836037B4E907269DDA16EA50D4
SHA-512:	A650C7BD2D023FDEBE72C606D4188B362B09678B5D29C54EDCF9F8DC0EC9F25DEFAC75B0662F86720732DD4CB24C929D916F064CB3D92782CEB45BA16BFE4EC
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1649532392.760829,"host":"AVsuOZgBg0wdpKMoxm8zihjqET8kI4Xl8bCSMk28RsE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1617996392.760834},{"expiry":1649532224.395841,"host":"CZU0ovCjWSlHcoYuG0ZSGiph68/Tvd43RsTejedDQms=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1617996224.395846},{"expiry":1633776321.538216,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1617996321.538219},{"expiry":1633548325.56318,"host":"HS0xQK8RrrSZ/KdSgKIC7bLU+xijlimr9JuWvTPbfkE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1617996325.563183},{"expiry":1649532386.432723,"host":"H5h/QTW8LTBlZOFYCI2QgyCoSXZApKh65MvyuWwrS0I=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1617996386.432727},{"expiry":1628882722.150632,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\200ead47-5e13-4f34-9a27-d5329257d64e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	19010
Entropy (8bit):	5.566979043378733
Encrypted:	false
SSDEEP:	384:TjxtvLlK2XX1kXqKf/pUZNCgVLH2HfDIrUXHGJp8L4W:jLlTX1kXqKf/pUZNCgVLH2HfUrU3GJal
MD5:	F4D13AD946E27860DA16373E18C95C7A
SHA1:	336FD6060E860349AF2A2364145A7499ED94C71F
SHA-256:	1F1C24B31E07E6890B8AC236A54068BF188AFBD9ED0667CEAE632180FB124560
SHA-512:	3A2BA10E1C0C7042AE8720FBF0CC6A9496907BEBA03D868388C01F8D01B9F65F9FAFE3FC6DE11CE5C3C8253A3FED39DC5EBBD770A54BE456BA4B37D68B60883
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13262469819006524","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\35f4a35d-0ee9-4ae8-96b1-59225f010417.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2546
Entropy (8bit):	5.6005496642872385
Encrypted:	false
SSDEEP:	48:YL1URVwUVweU9ieU2EUF6UUhi2EUk5SwUomUyKUeiYqPeUekUeY9wU/Ue9Uq:S1UcUWeU9ieU3UMUUAvUk5fUpUyKUzHQ
MD5:	928FC2B619B3EE6439726018FADF20FB
SHA1:	2175136D185B3AC3CA6766F301571E298BBE1682
SHA-256:	452579E878E3492C0076A75316A264A3D373E46CDCBEEC8909B563055F66A929
SHA-512:	6425C41ABC5F7F9C47DED61FF93676177424B7F84E5DEEC67800C5FA2C5FB3CBEF57E8773DC4F1432BC6E6B8077C5D8C4718FCFD9D86ABB72060E90FC2E821D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\35f4a35d-0ee9-4ae8-96b1-59225f010417.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1649532224.395841,"host":"CZU0ovCjWSlHcoYuG0ZSGiph68/Tvd43RsTejedDQms=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1617996224.395846},{"expiry":1633776321.538216,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1617996321.538219},{"expiry":1628882722.150632,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1617996322.150636},{"expiry":1649532321.509573,"host":"M4bfUnCmQAi4PNb3B8al/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1617996321.509577},{"expiry":1649532315.761078,"host":"OJAwwDug+gPr+xWjx2kFIFhHDQULu5ljftVMMZ74I4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1617996315.761082},{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3bebfc94-f6b6-4241-9e27-b5158349213c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4553
Entropy (8bit):	5.601808800747558
Encrypted:	false
SSDEEP:	96:5kUyt1UWUiUbUueUrieU4NZUrUMUUJMUfqUJU3qUUU6UgUeUbfKUoUxPeU2lUfUa:2Uk1UWUiUbUueU1UkZUrUMUUmUfqUJUx
MD5:	345AC92ED4AC85DE53C71BD8F275AD8F
SHA1:	5C54D50D704F3F423F4A5D9DF2CB37EFB4C8B853
SHA-256:	3B580636CA0DBB2381EEB06B677FC2D064EEE71131FFD157E3FF45FDB10146EB
SHA-512:	5EEF615476896FD470588F7149C26948BAF6F84689534819C3FEECDE3B55894B9F2BEEC6216C0BAC15537DB4B2D00DDD4AE04BB949C0C83C5DD2D4DAE2303E7
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1649532392.760829,"host":"AVsuOZgBg0wdpKMoxm8zihjqET8kI4Xl8bCSMk28RsE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1617996392.760834},{"expiry":1649532224.395841,"host":"CZU0ovCjWSlHcoYuG0ZSGiph68/Tvd43RsTejedDQms=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1617996224.395846},{"expiry":1633776439.047545,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1617996439.047549},{"expiry":1633548434.06352,"host":"HS0xQK8RrrSZ/KdSgKIC7bLU+xijlimr9JuWvTPbfkE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1617996434.063523},{"expiry":1649532434.732488,"host":"H5h/QTW8LTBlZOFYCI2QgyCoSXZApKh65MvyuWwrS0I=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1617996434.732493},{"expiry":1628882840.644909,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4fd82ee9-661b-46e8-ab25-e9f038ead5ac.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4554
Entropy (8bit):	5.597122886478024
Encrypted:	false
SSDEEP:	96:5kUyt1UWUWU4Uh7eUrieUtNZUV8UMUUJMU6UqUnUjUkU2UeUbfKU1UrPeU+klUjB:2Uk1UWUWU4UdeU1UPZUSUMUUmU6UqUn1
MD5:	4D12BB5C39452DDC93F7C5CCD801EA2B
SHA1:	6EA7BEEC96017A7CBBFBF7187B52265F9B00EFA0
SHA-256:	7EDB0C5641134731E4CD81DAE60A830D62A47D7C1D59D7670AE9989F369E892A
SHA-512:	127A4ABD6E740ACE2D78EBA8DC1A92217549A2D9B9AA595733CC59E48F268D80F1B2F1A5A51CB688BF33B50A0107139D9E8EDF42073AE9F9A19C5F6C92A41FD
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1649532392.760829,"host":"AVsuOZgBg0wdpKMoxm8zihjqET8kI4Xl8bCSMk28RsE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1617996392.760834},{"expiry":1649532224.395841,"host":"CZU0ovCjWSlHcoYuG0ZSGiph68/Tvd43RsTejedDQms=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1617996224.395846},{"expiry":1633776439.047545,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1617996439.047549},{"expiry":1633548440.984938,"host":"HS0xQK8RrrSZ/KdSgKIC7bLU+xijlimr9JuWvTPbfkE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1617996440.984941},{"expiry":1649532441.88589,"host":"H5h/QTW8LTBlZOFYCI2QgyCoSXZApKh65MvyuWwrS0I=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1617996441.885895},{"expiry":1628882840.644909,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\53724360-5c7a-4291-a5ad-7fa593bae251.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4554
Entropy (8bit):	5.5979310345535715
Encrypted:	false
SSDEEP:	96:5kUyt1UWUWU4Uh7eUrieUGNZUUUMUUJMU6UqUnUjUkU2UeUbfKU1UrPeU+klUjxT:2Uk1UWUWU4UdeU1UGZUUUMUUmU6UqUn1
MD5:	B8B9A8C3EBFFBE9DA870298B1416D7B0
SHA1:	B91DF66975F1A517EE0735797B19B5CBF33945C0
SHA-256:	760BD1B4CDC27E28648A143CB2FE61608901FB191D7C9A60F39DCC5FE663BF7C
SHA-512:	8DD4B51F6C8DCBFEBC995A636C169C7A155F14D96D0643500A84D9F3E8DDD0E7270192265924E03F9099B937D2B3EAFBD9F2F52413D20F95B0F48E788AFA4C0
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\53724360-5c7a-4291-a5ad-7fa593bae251.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1649532392.760829,"host":"AVsuOZgBg0wdpKMoxm8zihjqET8kI4Xl8bCSMk28RsE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1617996392.760834},{"expiry":1649532224.395841,"host":"CZU0ovCjWSlHcoYuG0ZSGiph68/Tvd43RsTejedDQms=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1617996224.395846},{"expiry":1633776439.047545,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1617996439.047549},{"expiry":1633548440.984938,"host":"HS0xQK8RrrSZ/KdSgKIC7bLU+xijlimr9JuWvTPbfkE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1617996440.984941},{"expiry":1649532441.88589,"host":"H5h/QTW8LTBIZOFYCI2QgyCoSXZApKh65MvyuWwrS0I=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1617996441.885895},{"expiry":1628882840.644909,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\59b0db3d-68b4-492b-aa20-af5e6493eb17.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22602
Entropy (8bit):	5.536153839810461
Encrypted:	false
SSDEEP:	384:TjxtyLlK2XX1kXqKf/pUZNCgVLH2HfDIrUeHGdnZUp46L4u:+LlTX1kXqKf/pUZNCgVLH2HfUrUOGdnu
MD5:	944200437089B52A6A0E820865BC54E9
SHA1:	5BE6B9CEF4C00D453DFF0716837AEEBA2AF11CF9
SHA-256:	9838EF1A28D6913A5685F67FED0C4276A09504F2542FCF57E83FCA9694E1475C
SHA-512:	92D5BD3125650DA08993F412DAC688AE54A638BBA1695DFAAE405293CF5B6ED2E92CD2569541A9CCEC21BAAB052A5FF2972CBB1AE62F4DD0997F474CEC54F6A
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13262469819006524","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\66203c95-4fcf-49a5-9a95-7ac5c44fdf26.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	24064
Entropy (8bit):	5.534270235008829
Encrypted:	false
SSDEEP:	384:TjxtyLlK2XX1kXqKf/pUZNCgVLH2HfDIrU2HGMHG7nZUptCL4hO:+LlTX1kXqKf/pUZNCgVLH2HfUrUWGAGZ
MD5:	34C89DAF161843D320769A22943C87AB
SHA1:	95C10674BB3DA3D64BB98B8FD08D917EE868E7E5
SHA-256:	6F8B99C2163CA41A541BB75674A4528E9770590E9D4252C8628E2CA4C0A25C9E
SHA-512:	A09F6446C2C228026D26EBC4B5C0DDDAAA70AB3CB0D44095AD205F616368D2A3A312C9CDA446B03233CCBC25195651484206B33D23EDCAE5D67060B70F3DEC
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13262469819006524","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\760ac057-dfba-48af-bafa-3243e199a7d2.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4550
Entropy (8bit):	5.596888236304693
Encrypted:	false
SSDEEP:	96:5kUyt1UzUwUlUxeUpieURNZUrUMUUJMUFUJSUMUwU+UtUeUbfKUmUcHPeUWlUuUa:2Uk1UzUwUlUxeUXUzZUrUMUUmUFU0UMT
MD5:	D30912F53729235071E214903544FFB7
SHA1:	02F124013469D664FF5D7D24E36F22960AD2325B
SHA-256:	2BCEB83EA0703B3A593AEDC7B1673D4D0FA3ECAC6A025A218F34E81695C99857
SHA-512:	B0E3F353B809A1C768908F291467CD5628CEDA6B721372C0A2DC4D2BD1FFD5B1B37B7DD9239702D5BF0F265748ADBBB441287369996DA225CF4DC8C2181459
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\760ac057-dfba-48af-bafa-3243e199a7d2.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1649532392.760829,"host":"AVsuOZgBg0wdpKMoxm8zihjqET8kI4Xl8bCSMk28RsE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1617996392.760834},{"expiry":1649532224.395841,"host":"CZU0ovCjWSlHcoYuG0ZSGiph68/Tvd43RsTejedDQms=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1617996224.395846},{"expiry":1633776412.514586,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1617996412.51459},{"expiry":1633548414.409423,"host":"HS0xQK8RrrSZ/KdSgKIC7bLU+xijlimr9JuWvTPbfkE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1617996414.409426},{"expiry":1649532409.172442,"host":"H5h/QTW8LTBlZOFYCI2QgyCoSXZApKh65MvyuWwrS0I=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1617996409.172447},{"expiry":1628882813.194426,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\808a94f7-a397-4f2e-ba14-fad7250535a1.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5717
Entropy (8bit):	5.174358232850259
Encrypted:	false
SSDEEP:	96:nrLZROfuJIV65k0JCKL8DJkkc+1nLbOTlVuHn:nr2fYIgh4KCkkc+BV
MD5:	5B2AF2B382AB1A8D724A16EF776B3B81
SHA1:	43636F97A7A76533810B012216AC68D4130DD16C
SHA-256:	3523DA4DA89F13B021BBF5E4483AD7519DC66BA312D473280AC150F9544C1236
SHA-512:	50E6B895A3757029AD12A4B731F416C6BDC1C3B7F2AEE49972288662E6225ED0CB0940084B2E15A32A02A5A85ACAA20D18779604E836E2988DCD0814FD532B84
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13262469819253134","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8b17299a-da6d-4eb8-8d5b-f789879c3c80.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	7164
Entropy (8bit):	4.8230602164896
Encrypted:	false
SSDEEP:	192:JzMKDHGXOa0FG4A0aaFaT4aNxarC5GojuBSiVFHwYCQ31Z8+kOVUPfZwfE7H/K2R:JoK7GXOa0FG4A0aaFaT4aNxarC5GojuM
MD5:	7D9ABB1282CD8FD51FFEF23121AA65B8
SHA1:	7540DE09631AE8A76E680B208C17FDA35B3F1C6F
SHA-256:	A5408D984AD920320F619065BCEDE48F075588FF3AFA80A7C57B42068DB6A022
SHA-512:	40BDBD09DA7C18BE0A81588F72A9CA12E3B0FB3AD4EA31045E64F3F80725E68076B181DAB2F7A990B109A9E1EC4614C4D506ED103285FE8C77C4C6B3A7AA3EB6
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13265061823541879","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"isolation":[],"server":"https://joom.ag","supports_spdy":true},{"isolation":[],"server":"https://viewer.joomag.com","supports_spdy":true},{"isolation":[],"server":"https://browser.sentry-cdn.com","supports_spdy":true},{"isolation":[],"server":"http

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8cd7ce96-f705-421d-abdb-4ac70378a05b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5962
Entropy (8bit):	5.187632719159003
Encrypted:	false
SSDEEP:	96:nrL2ROfuJIVM5k0JCKL8DJkkc+17kqhMbOTlVuHn:nrzfYI+h4KCkkc+tkqy
MD5:	59A5E0D27BEBA6651CE7ADF82FEFC55F
SHA1:	7D69F9E00C1BF80D2A8B6E039297870A4C3E73B9
SHA-256:	2871533C0ED7DF34D2C07776750B9A20E95E9FE3D7F8F31BE3719E156480C666
SHA-512:	CB51B18504A06D14F5F522B2D62D3F8ED87519A866A923DB5BFA0C08F4DB81DA37328A022916F816EF006291A12572DD65B8725CFE7EAFC66F53610DC7A38B8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8cd7ce96-f705-421d-abdb-4ac70378a05b.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13262469819253134","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.177345478984951
Encrypted:	false
SSDEEP:	6:myAEQuG/34q2Pwkn23iKKdK9RXXTZIFUtpdAEaAvJZmwPdAEcRDkwOwkn23iKKdi:tyuG/4vYf5Kk7XT2FUtpdzJ/Pd+RD5J3
MD5:	2CE4A12A5334FD4A648BE749927E3E26
SHA1:	D84E051CBE7EF83FDE4CA33CDA2E4323C0A847A0
SHA-256:	E0F813CC27FAE7B3D7C5993DD856885BB618411C4891C2A40C77F7AD6AB83BBC
SHA-512:	AA689223148C6AAF918FD4D0F455556AF393E391D328EF4C48906EB2D6EE74191A820178964A5E6E2494C9AFD7400D6B681FC1CBD68B56D0C84CCA3724A04AF
Malicious:	false
Reputation:	low
Preview:	2021/04/09-21:23:49.045 1c20 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/04/09-21:23:49.046 1c20 Recovering log #3.2021/04/09-21:23:49.049 1c20 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.18917194904168
Encrypted:	false
SSDEEP:	6:myArC4q2Pwkn23iKKdKyDZIFUtpdAuCJZmwPdAtNDkwOwkn23iKKdKyJLJ:tYC4vYf5Kk02FUtpdIJ/PdsND5Jf5Kky
MD5:	D1BC6207FD10A674D706DB68BAE7C7C0
SHA1:	BBEFD2EE2D03F59357F20B17297DA07A486941E0
SHA-256:	01655B151686E1EF0F7B573FD9E50B1B3557721AEC8DD9C7806E745867A0EB8D
SHA-512:	BF9087C03478B86249BE1FD538923AB78A92401E9DD0ED296E60A0BD2BF39A4124D13B4AFE7F7DC99EA7A98E14C206E721B403F85050719513DA0674F682D4A9
Malicious:	false
Reputation:	low
Preview:	2021/04/09-21:23:48.744 1c20 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/04/09-21:23:48.749 1c20 Recovering log #3.2021/04/09-21:23:49.034 1c20 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\018d28d3dd0f72bd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	273
Entropy (8bit):	5.681017623094776
Encrypted:	false
SSDEEP:	6:mP/gEYET08NWQASxYOno/Pd0P9kPAptqxksJlZK6t:Mlg8NWQXnoHdqkPBCo
MD5:	4CB0A0E45347710F365A1A0DE15B483D
SHA1:	B86D5ED4074BB48440F280F7200841DD10176FAB
SHA-256:	F73420C300CD461965F4A3D544D6F8CF4C9E07D3D1B2F7675EC5DD17E08CFEAD
SHA-512:	9122B52FE9AAC39F58EDFE3EA06C592C266B110463078F05F87BEF7B53112A58D413A6FDF054327F3B0177B2261F254427520CFB17A6A0CF02C3845CD26CD4C5
Malicious:	false
Reputation:	low
Preview:	0\r..m...........Y......_keyhttps://cdnjs.cloudflare.com/ajax/libs/jquery-mousewheel/3.1.13/jquery.mousewheel.min.js?isAjax=true&_=1617996289446 .https://joomag.com/.{.o%./..................jh.uAQ.j..j..$....%..#......x.h.A..Eo.........=.........A..Eo.................

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0381749d97c141e8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0381749d97c141e8_0	
Size (bytes):	231
Entropy (8bit):	5.593708189379981
Encrypted:	false
SSDEEP:	6:msNyEYGLyIqWAwbZsN5aZg71a6M4bbQRK6t:jQFsOaeg6M4bkr
MD5:	CF16E1738A05A08CBF451EA750704108
SHA1:	EAF33E6A121917C5BA98B73DF219A6E91EABBB8E
SHA-256:	CF4D83DD93B11BFC86D8089D270384D7F42EF13E3D71F279929BCFD81A6BA77E
SHA-512:	32570CB5D49B21988EE6058C394C6523D8D8DA5BD18189AF0796308639F1FAB08155CF3256ABA3AAC515302A60AD0D95E06076327F7B66013D5239FCC2F1E5DE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....c....._keyhttps://www.joomag.com/Frontend/mobile/viewer/main.36b2b001eb97fb16211c.js .https://joomag.com/..b%./.....?.....Z.8F..M2.Y.....7e5.. >g.u.T..7.A..Eo.....R.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0773c091491a9080_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	59127
Entropy (8bit):	5.5729508951713544
Encrypted:	false
SSDEEP:	768:d/S5qJ2V6JctdhHFWZTP8atzEHV5hhL5J1P+6SCh0h0mcoBcKFj0dK:d/7IHwZrrYHV5X1P6CKh5cC
MD5:	48C6F1D5742E08CCCB474A9FD6BF0BC4
SHA1:	9B98546E0AA55F24B610845BFC4B3D2811D2C24B
SHA-256:	13FFF2DB434F0BA59853E5211D4A92501B6718D8D9745E98C7FEBEBAAA104443
SHA-512:	108955F1F03655CAD880EB0BF2E92F8E1EE347547F7F9EFE56A28962E2FEC896F91C9B105183C7B0C54A63FD37584F209ED8B42D3F08DF05B461AA39FC3B5034
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W...TI.9...._keyhttps://js.hs-analytics.net/analytics/1617996000000/5574303.js .https://joomag.com/.q.h%./.....b.....;8.y...in.....&..M.J..V....)..A..Eo.....4.i.... .....A..Eo.....'.....O....8...m.d.....(S.-...`.....DL`.....L`.....Qb.q....._hsq..Qb.b:*...._paq..... ...Qb".k,....push.....`.....M`.....Qd.0.....setPortalId.`>.....`.....M`.....QeZ5 W....trackPageView.....`.....M`.....QdR.....setLegacy...H...`.....M`.....Qe.X.'....addCookieDoma in...Qe...@.....hs-sites.com.....`.....M`.....A..$Qg...].....hubspotpagebuilder.com...`.....M`.....Qd&.A.....hubspot.com...`.....M`.....Qd.'3.....hsforms.com...`.....M`.....Qd F.....joomag.com....`.....M`..... Qf..{....embedHubSpotScript...4Qk2.-.(...https://js-na1.hs-scripts.com/5574303.js..QefR.....hs-script-loader...`.....M`..... Qf:|.j....setTra ckingDomain....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\094e2d6bf2abec98_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.596315886255733
Encrypted:	false
SSDEEP:	3:m+lP9Ola8RzYJb9yKIf8QPKxWStHWFvDFYtRy2v/tlHC9B//bl58tyGdDmvKX/pD:m3VYyK08fNH1DyR9jyL6vKXhK6t
MD5:	191B24D3EFB3B067B2AC08398BEAF61E
SHA1:	59B55DB79E465D9B38574565A77DF31CB49AFFCE
SHA-256:	C83F467B32B8F2F74EE21DD8DEF3B922CCC33D7AC31B10A4BDC91D8A83D11259
SHA-512:	8709FED892D8F960CFBCB7015AAFB2591360E1FEFEA7AC0EFF4C039392B1E63D46129482EAB293FFD354941050CCE57FA3E5F6FFF08D230D9EB50A1BD875DE 5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W....._keyhttps://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.2.min.js .https://microsoft.com/...l%./.....=.z-.7.K]..~..=..9.....8...A..Eo.....b..... ...A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0c59603c94d6b5b4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106912
Entropy (8bit):	5.619317083443111
Encrypted:	false
SSDEEP:	1536:eBqJQTgfIq34vONSvkioeZ6kO79mUKy6maFXs4P64rZC0f3nqk:ecJQeL42Pvz6maKyf3nN
MD5:	B62E554E75FAA108A62061E9F953ACDE
SHA1:	F3E153007688387DDA7877CCF34E22F421E8E090
SHA-256:	4E163502F13AD8EDFDAD00ACA4B8B7412FDD178488EB4F008C9A074FA569F91D
SHA-512:	2E343BCC6813E148ED8864FB7A519C404567C74BC557241D27D12AD088F2DED54D72DA0FA597AEA2FCF1CD5B8522CAB18E4669148AACEC6BAF760BC9F064E 26

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0c59603c94d6b5b4_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...*.&S....52891DB3131A6676739F92A17901ED3645E899E219551717BE09574A7C8C9DB6.....'.....O$...@....-.....(7..... .....l.....(S....`.....L`H....(S.U..`b.....L`V....@Rc.....Qb.....t.....Qb.d.....e.....S.b.....l`....Da.....(S.....la.... N.....@.-....DP.....8...https://www.joomag.com/static/js/pages/home.js?_=5.1.8.0a.....D`....D`....D`.....`J...&...&....&..A.&...(S.....5.a.....a.....Qd.v-. ....queueTriggera|.....I...!.d.....&.(S.....Pd.....t.trigger...a.....I....d.....&.(S.....Pd.....t.destroy...a....`...I..d.....&.(S.....Pd.....t.disable...a}.. .....I..d.....&.(S.....Pc.....t.enablea.....I..d.....&.(S.....Pc.....t.next..a....(...I..d.....&.(S.....Pd.....t.previou

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0e659a3035520b71_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	23020
Entropy (8bit):	5.743101676448975
Encrypted:	false
SSDEEP:	384:WGUeTW/KUksugOQJJzdyqtedPTikUUguQLC9svX48/:AVKVgOQJtdcdPOkljQZB
MD5:	FB717FB41EE2732D2EF9B293941C5C45
SHA1:	B62A40A18A6489C5C8858D67E33C1EE1931CBC46
SHA-256:	1A71C29CBA33C9974400329668D46D8B5A99E7F964C141CA1B64D463310792E6
SHA-512:	F507E41FB65F5D2BAABD882CBBE93B759161AB39043B37BD8EA044089BB6BE8B9CD107846B02C3E5D8463046AC9690DDDE33AE09691FCE968B1B5F7224A1A4 8E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T.....\..._keyhttps://www.googleadservices.com/pagead/conversion_async.js .https://joomag.com/.Jgl%./.....+...../.uvxCL.1.s.$..\E..>.D.....(.,.A..Eo..... f.....A..Eo.....'.....O...`X.....S.....p.....(S.<..`2.....L`.....(S....`J....A.L`.....Rc.....f.....Qb^.....aa....Qb.....ba....Qb..aL....da ....Qbn.....ea....Qbj..n....l.....Qb..9k....fa....Qb.K.E....p.....QbV.....ha....Qb.WV.....ia....Qb..Cq....x.....Qb.0.....ja....Qb.....ka....QbR.q`....la....Qb.,u.....na....Qb.....pa....Qbb.L. ....ra....Qb^N.....qa....Qb6.J.....ta....Qb6.....xa....Qb.Lpq....ya....Qb...H....Ba....Qb.....Ca....Qb>.....Da....QbV.....Ea....Qb>.6.....Fa....Qb.|.....Ga....Qb..2.....Ha....Qb...O ....Ia....Qb.>.....Ja....Qb.?.[....Ka....Qb.y.v....La....Qb.i.....Ma....Qb.UW.....Na....Qb.]1O....A.....Qb.....Oa....Qb.4J.....Pa....Qb.T.....Ra....QbRh._....Sa....Qb.}/v....Qa....Qbr0..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0f1894c5ddc566ef_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.3950590708697
Encrypted:	false
SSDEEP:	6:mslllVYerCUHGAGXkr0dF/8y5Z/MY6NhLGH47/bK6t:BlllHOUmAAmkxR5Z/MY6zl
MD5:	ABDF8ADC950C2434B8DA61DE36727C0A
SHA1:	5BF5D0AF2C023C96985C7FBC9D3937F67869E259
SHA-256:	5A657CE5E9FC04340A5AF5362451DF9C8D17FB7AEDF76641BBFE8595E605DE03
SHA-512:	5DECEA39DD6DC4BE464CCAC119E27F03A238AEE1452C3A8A10511D90DA041A09D598759B23CA3195C584B5028747084EE04EBC1FFF026080B52F59BF4E6F57(6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S.....)...._keyhttps://code.jquery.com/jquery-3.2.1.slim.min.js .https://theicecreamqueen.net/.. m%./.....5....Z..?.\.1..U...{EGGA..D..A..Eo.....m.....A ..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\15c16c3f27e21b62_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.495226677246256
Encrypted:	false
SSDEEP:	6:mGNPYGLyINRvQYeuPnIR/m1Itwa2tNbK6t:DoWQYeuPm+2tiL
MD5:	25F3B095CD9B36594AA77E46878A461C
SHA1:	8578CF3E88F37178871D2DEDA14CEDB1BDEB4856
SHA-256:	ECA591ADD8C2E7BA75EC21D1E893CC2AF60551C09E8E361592A42DF1EAB9AA93
SHA-512:	0A30D679F0E214635EE8F68326EA4A599A0643E6BC0D91A734B294A4E5E93113BF532A0EFEB88333D8DA9854ED2DD1FF678B1156D0CFB1019AA35B3C3A8835B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O...4._K...._keyhttps://www.joomag.com/static/js/magazine.js?_=5.1.8.0 .https://joomag.com/Z.b%./.....=.....t....^.Z...w-J..=.....O`.\.*..A..Eo.....Q..... .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\17896e0de4cd17e2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.578993961966318
Encrypted:	false
SSDEEP:	6:m5YGLyIqWA8g+PGDsAGvIv7HXNkAy4hK6t:Zsg++D3GvSTd/7
MD5:	7E36D2379FDE039554A34E78CDA4C4E1
SHA1:	B5715645A1A2C589F7C15AAB8D77D04D928C5A67
SHA-256:	0A67D14CBDDDA85110E94F6BF04D83DEC45034A7238B6F8ADCAA290B08505504
SHA-512:	E57120FCFE8F1AE7913F3230E0B6C6BA2EDA0F208CB142EA806B52ED745BF28C6BBC5546BE96B58AD41091BD754A0DA030E09D81533A2E38FF8E31A177D6FB70
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...Y..N...._keyhttps://www.joomag.com/Frontend/mobile/viewer/normalize.d0dfb984f88d0dbb9fde.js .https://joomag.com/..b%./.....G...Xr''..!s.@.x`.....)u..A..Eo.....^g.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\18e402f011ac7071_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	273
Entropy (8bit):	5.736246822724068
Encrypted:	false
SSDEEP:	6:mHnYET08NWQASxYOno/Pd0PUTtf2+Awgt65Pl7wCSrlZK6t:6Dg8NWQXnoHdRtfXvgtql8PT
MD5:	7D7C67D9202311508072BA081ED9D25C
SHA1:	3E4FFAB66C8478B823AE2172ABB022A31A105CA7
SHA-256:	C61A8DFE002EEEAA9347043F459E481964BC029629B43B0ED5221562BBCBB171
SHA-512:	CD51F43F37FC555C223A49C3C9C4D267202D7A02F895F7C0338E53370FEE8CF03607A5076664514F295DB6C662355BF81C2D0A2055708AE6E2A2B9841798DA1F
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://cdnjs.cloudflare.com/ajax/libs/jquery-mousewheel/3.1.13/jquery.mousewheel.min.js?isAjax=true&_=1617996282617 .https://joomag.com/M..o%./.....v..]....N.....]a.....aRgQA.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1a841bd9fc7ecccd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	312080
Entropy (8bit):	5.695940156032901
Encrypted:	false
SSDEEP:	6144:l4TltRZCKvWlTiHWFm01vZnrVGNOHpYqup9kjtJhkoyqaM7RGBOPk5s:+TltTvSFmIJlp5jhaM7RGs
MD5:	BB15BE287D3A1F000063C9BBD015618E
SHA1:	85315497A9280E79A364343DFE079C57CF5F17DB
SHA-256:	C3DBE350CEDE8DE0DCA25A091B8DBCDD8F4C012D90D7E62E34620DAFA1652BD5
SHA-512:	A794CE7C71AFD4D76A6581DC6F791124A4360E209739EBF3546E1F232F2CF697D5BD8DFDA1EBC7BA123041C5A8B6E7ED5248566DA27F129CF0AF07DCA2CCB9F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....v....D9BBA9AE86B7DF1F94AD0160B022BE8C39931177A379B1851BA4BA1F2542EC48.....'.....O[.....m.....P.....@.....P.....x.....(S.h..`..... L`.....Qc.g.t...joomag.....a.....a.....QcVq.c....extend....%..a.....QcnZu.....backend...an.....Qen..J....account_manager....a.....Qc...h....title.... Qf.....Account Management....Qe&y.....account_settings.L.a".....Qe.C.6....change_password..D.a.....Qd.n0....new_password..Qd.....New Password. QfbM6.....new_password_help....$QgJog.....Enter the new password....Qdv.m.....old_password..Qd.....Old Password. Qfr.....old_password_help.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1aed43a98452cbb5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	255
Entropy (8bit):	5.802662742469178
Encrypted:	false
SSDEEP:	6:maY4rgdsiQM+HMy2Api6FYoa8iVdwLr7gRK6t:z7GmrdK8iVdq4r
MD5:	E40C68283D2165736F49D86121196D07

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1aed43a98452cbb5_0	
SHA1:	CFF88F64AD848868E1BEC02D3131D77619774883
SHA-256:	058F9858AA6D3C7A49F77B06E3F9C58CB62B6BA6FFBADF7C210715D24AE26CD6
SHA-512:	0F3B3DBFB8E65FEAED3EA92390554F5F2E4DB986601003B9C676B65F7566279091B34E26289AB54D75EF8A71E3ABF03FCB7277F190B234C9E6CFCB4242433FAF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....{...1....._keyhttps://s.adroll.com/pixel/7S36S2RHW5BUVAXH6L4RZE/6TMQVXNPWBG6BOGAF3EFID/LEBFNED4AVAJNBDGU4P5DT.js .https://joomag.com/..4o%./.....AR]..G ....]E./.d.. ..".Hx. .A..Eo.....J.1.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1c6644b795785887_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	37348
Entropy (8bit):	5.4471507543706155
Encrypted:	false
SSDEEP:	384:qlNElu4KGa7Rr6NMQqjqAYLZBayIsSGCo+/YzOe1vKP7h+NAj56ClFuwA7:wCkOa5CBAQ+wUh+46E8
MD5:	F6826B1A85D0816CB495843951AAA761
SHA1:	F3EBB9DAE17CC646BE0ADC94661A2C21B0B3E911
SHA-256:	9C55FDF8DD747DA8AC01EB3C2A55CA40EDD81101E23EBD4ED16319C414D87CDD
SHA-512:	B3290783FEF168D2249660183CB65D4ABB51D5DDC4130C19B606D9D7ACD041798C074CAA4F1BE64E12CC03A2713014FAF1F4891260585100E39B953F891AA931
Malicious:	false
Reputation:	low
Preview:	0\r..m.....<...x....._keyhttps://s.adroll.com/j/roundtrip.js .https://joomag.com/.S.h%./.....g.....Q*r.{.-...S..;..T2Mx..,..ue..A..Eo.....A..Eo.....'.....O....X...yx.....(S.H..`L.....L`.....Qc..Kf....window....Q.@F1.5...__adroll.(S....`.....}.L`:.....LRc".....Qb.....f.....d.....I`....Da4....D...(S....`.....L`R.....Qb.\<s....1.0...Qc.....version...Qb".....exp...Qb.....eexp..Xa....vH7B..Qb.....Math..Qc.a.....random....Qb..k....pv....Qc.1....._ _ar_v4...Qc:....._adc.....QbRWv}...._nad..Qb...+...._Ice..Qc....._broken...Qc.N...._loaded...Qb".0c...._url..Qb".....kwl..Qb..k....._r....Qcb({.....cm_urls...Qc..E...._logs.....a.....Qcr.u.....facebook..1...Qc.Q5.....linkedin..q...Qe:.....consent_networks....M...Qc:.3.....round.....Qc.^IL....substr....Qd....._set_global...Q.P.s.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\202398c31ac24d4a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	681
Entropy (8bit):	5.807168212489162
Encrypted:	false
SSDEEP:	12:1E3xR9oux2peyyQL13CMxGDPMUIZGYxNUCd4+4ogEqrr:1EBRGuyeyyQL1SXDVIIY8CdZ4ogJH
MD5:	4B8FE33ADB57CF625E887D5D29DBCFDF
SHA1:	A1B1FF0CF9E756CF4BE59779E39861114C5424F3
SHA-256:	BB112F70C8F4EB675013177FFD399FAC06019D2B370B45052DEBD2FF29867B3F
SHA-512:	3E460CEA7AD9A2FDCF2C1DA6BA3CBDD1DD6E3D1370C8DE9D2865C2F34D650AFFBCBE9BC0BEAF1AC8A10C89F0D4E2535A2584F5A45D71C0C858E11E1A6D2A9C4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....%....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/1003757157/?random=1617996273414&cv=9&fst=1617996273414&num=1&bg=ffffff&guid=ON&resp=GooglemKTybQhCsO&eid=2505059650&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=120&u_java=false&u_nplug=1&u_nmime=2&gtm=2oa3v0&sendb=1&ig=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fwww.joomag.com%2Fen%2Fsolutions%2Finteractive-content-marketing&tiba=Interactive%20Content%20Marketing%20Platform%7C%20Joomag&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://joomag.com/..n%./.....Z.....U.....y.}..@..(...UXE{..D].i.A..Eo.....f.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2a82640fed18fa5c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	80800
Entropy (8bit):	6.072911172242188
Encrypted:	false
SSDEEP:	1536:Lg6RND0Fq+0qWvBextNPqJBb7JuG7tzGQIEdLXC/g8s:06R0q+0qW4zqJBb7IGVGzEdjC/gd
MD5:	3244B95AB8525686A2019C796E158990
SHA1:	6DCCAAE64D5F1FFF00FE51F5363A8C24866D06DF
SHA-256:	CFFC56A5C0B6723202F502F3AC1E2F3821CB0E16445E1F7C84534846B1D28FF3
SHA-512:	FED50C96805C8C4625CCFE26A1BDAC5A6345052BCA0B2F9ACCCDD9D2C99BDA7966F3EF147334D94220F1B4A4980ABA52970E5E43E5C56717BB57F82ADDC7A9E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2a82640fed18fa5c_0	
Preview:	0\r..m.....@.....0....2CD38408A308D0E86C320ABE6902420E2A496DEA64B2654F31F37C8B5320832A.....'.w.....O....X:...OV.....(.....`...|...<.....<.....(S.D..`B.....L`.....(S.]..`p.....L``....u.Rc.....R.....Qb.2Ay....n.....Qb6.....q.....Qb~..9....r.....Qb.i.....t.....Qb..z%....v.....Qb.g.....x.....Qb..rL....y.....Qb.C.....z.....Qb..E....A.....Qb.!.h....B.....Qb~.....C.....Qbrh/.....F.....Qb...M....E.....Qb^].....D.....Qb.....G.....Qb.....H.....Qb6.....J.....Qb..1a....I.....Qbb\.....K.....Qb.....aa....Qb..dM....L.....Qb.....N.....Qb.....O.....Qb...b....P.....Qb.xQ.....M.....Qb.T.%....da....Qbv.hg....ea....Qb.....Q.....Qb..H"....S.....Qb..R.....R.....QbB.u.....ia....Qb..O.....U.....Qb.....ha....QbV+.m....T.....Qb.^V.....V.....Qb..`@....W.....Qb..."....Z.....Qb.....Y.....Qb.c.....X.....Qb.I.....ba....Qb...i....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\35aec16058a68073_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	9750
Entropy (8bit):	5.933077320850789
Encrypted:	false
SSDEEP:	192:sBjkicSTtYaml1faHGcbsTzExtFFFFFJUFFFFFJyFFFFFJc7pFFFFFJMFFFFFJUp:sPzfYFbsTzExOUkAYGmJQmmfo/
MD5:	EA63EB7DB53AA5A7131CB6D146D75E1B
SHA1:	BEB612EB41C00BC9C06B1EB86148135F4AD9D733
SHA-256:	EE7C32D545F31E9761ADF11AA0172265A6295173ECC454198A79F2457D4FFB7D
SHA-512:	149557EF21F1E44595CA68B37808AAA5268388607E452C80A3984C94A98230E5F998C1D034D88A1840A6CDBB59C9EB9FD4E53CF1E6B452F8AF2D3F6CF4CF60C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....>....K....._keyhttps://s.adroll.com/j/sendrolling.js .https://joomag.com/...h%./.....G.....zk...f..3..N..Z.(.}....JW$...1.A..Eo.....e.jf.....A..Eo.....'..&....O....$....^D.....@.....(S....`n....<L`.....(S.0.`.....L`.....0Rc.....Qb.....t...`....I`....Da.....(S.t.`.....L`.....TRc&.....Qb>.....r...QbV&F.....n.....Qb.d.....e.....Qb.....o.....Qb..Cq....x...d$.....$.....a.`....Da,...~.....(S....`.....4L`.....4Rc.....Qb>-.....d...`$.....`....DaP.....q...Q.@ngw.....require..... QfV.....Cannot find module '..Qbn?^.....'.....QeV5.O....MODULE_NOT_FOUND.9.....a.....Q.@6..{....exports....a.....Qb.0.....call.....(S.P..`\...]..K`....Dn.....&...*..&...*..&.%.*..&.....&.%...%.&.].....,Rc.....I`....Da>.....c..... .....@.-....4P.....%...https://s.adroll.com/j/sendrolling.js...a.....D

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\37e825f21a9f687b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	363
Entropy (8bit):	5.808885544426738
Encrypted:	false
SSDEEP:	6:mRl9YSHT8NWQAlKPUQy4GAGXkrs1aSpOmN/rbK6tcRxEguP+mmnnGOmN/N0:iz8NWQCUUpAAmszXNGRxEguPAnb
MD5:	00FD17E562BCF8DF85E8B336A61E9E53
SHA1:	632BF119237972364E0E2288155F3B99EA02BA50
SHA-256:	31CF3E663DD37DE6A760E57BBC847170E4A861AAC19867693D98C32E6D481481
SHA-512:	CB6BA1C44DD6E0D356EEC898270AEE11C32CF9C056C23585BF4CAB68DD749063ACB8EB75D9ED760243E5B80D102E8AC97ADF679D73E20A87CAD5A47EA987855
Malicious:	false
Reputation:	low
Preview:	0\r..m.....c...2\.'...._keyhttps://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js .https://theicecreamqueen.net/..m%./.....m4F..J..e..,...9.E.}..lNPX`.(.A..Eo.....>.....A..Eo.....m%./.Po..7AEE718E1085D4611B43E5893A05C2D77C418717BB58B53BD3D4FD43BC5E1BEA..m4F..J..e..,...9.E.}..lNPX`.(.A..Eo.....0.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3cf52a5fdd0e540e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1266
Entropy (8bit):	5.616882395743444
Encrypted:	false
SSDEEP:	24:M4c470uZO4c470O6SO4c470a5BO4c470OfRO4c470ltO4c470t1:Vc8PZ/c8p7/c8V/c8xR/c8E/c8Y
MD5:	797193C86E24CB10229B403B27E8333F
SHA1:	7073A3714DAF047FE74F632FBFC9597C24DB1E5E
SHA-256:	6AC8B66ADF3026F0A0E534E120CA883830164DADE64CD2E8282895D8B23249F3
SHA-512:	2247614261B2894C3350939BF6FAB5A40895642791DA5A0A33E16E0066F414883CE43671D1171EFFAC43364ED40D51595119BEE6624106F20538924C01972BE1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O...cE....._keyhttps://rum.monitis.com/get/jsbenchmark.min.js?id=4916 .https://joomag.com/f.gl%./.....C.....lw.H7....k..u.4.....8.q...A..Eo.....A..Eo.....0\r..m.....O...cE....._keyhttps://rum.monitis.com/get/jsbenchmark.min.js?id=4916 .https://joomag.com/...m%./.....%.....lw.H7....k..u.4.....8.q...A..Eo.....A..Eo.....0\r..m.....O...cE....._keyhttps://rum.monitis.com/get/jsbenchmark.min.js?id=4916 .https://joomag.com/A..n%./.....[.....lw.H7....k..u.4.....8.q...A..Eo.....G.....A..Eo.....0\r..m.....O...cE....._keyhttps://rum.monitis.com/get/jsbenchmark.min.js?id=4916 .https://joomag.com/G..n%./.....w.....lw.H7....k..u.4.....8.q...A..Eo.....R.....A..Eo.....0\r..m.....O...cE....._keyhttps://rum.monitis.com/get/jsbenchmark.min.js?id=4916 .https://joomag.com/..Ho%./.....lw.H7....k..u.4....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\45e516dff6cff1b1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	94200
Entropy (8bit):	5.769226172087408
Encrypted:	false
SSDEEP:	1536:WPVfY5rcr3KjTkUajHTzmuEjjEkE68s7NIWDxWl3pDCGsrHEo+9G1qvSPO:0Kr43dZ2gkP8sp39k3lCX4o1qh
MD5:	0C12D07C7BBF672C1B610625AD044498
SHA1:	2E8658A8D930771E387EBF85AB59CB822ED3B0E3
SHA-256:	10779225EE42EAE21598490CA65E20E4F8496682C3FFA3B75A83648ECDF8B856
SHA-512:	13484183F487BBAAE7191743B1EA3B64011E89C0BA95B25D59ED41DF5093B80220AE1B2C503EC5B0B4E9562A94CDABE8CF35C2B9124642E03CE43E2B7B1E7FE9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....W.....7AEE718E1085D4611B43E5893A05C2D77C418717BB58B53BD3D4FD43BC5E1BEA.....'.JN....O ....n..F..s.....!.....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....O.`....I`....Da....*.....Q.@zb.....module....Q.@.....exports...Qc.n.....document.(S.....5.a.....a.....a.....a.....a.....Pc.....exportsa.....I.....@.-....LP.!.....@...https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.jsa.....D`....D`....D`.....`z...&...&..!.&....&.(S....!..`.C.....q.L`.....Rc@.....M.....Qb..N~....d.....QbJ..C....e.....Qb.(.....f.....Qbj6.....h.....S...Qb..r.....j.....Qb.o.....k.....Qb..r....l.....QbR["".....n.....Qb..m....o.....Qb>|.4....p.....Qb&.....q.....Qb..<.....r.....QbZ.%J....s.....R....Qb..Yn....v.....Qbr|.4....w.....Qb.....x.....QbV.....y....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\48a3614fa2ea4442_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.445209281000175
Encrypted:	false
SSDEEP:	3:m+lohq/dA8RzY8ciAnGY/ZMeOFPWFvDftml9tlHCp/l7Z6S1RqMqgHwk5m6tt/pD:mUnYWAnB014rRf6S1RagHwk4iK6t
MD5:	75B38A764609050F7F94BFD2D181C5AD
SHA1:	6F4128A49213B4D72F7C870F7356483391BC7EFE
SHA-256:	569918B8AC118AB02B91BF2AC418B1BB588CFF4709361280E89932DB17A43AE4
SHA-512:	286D4EC34EA078526ECB473D77B75C39752BA27C62ADED3F1E9C37B48391A9E734DCF5B9FE649BF20209BE39BF74FF9F5F6838018B68BA5116EF38DABEB18B5F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L.....H}...._keyhttps://browser.sentry-cdn.com/5.11.2/bundle.min.js .https://joomag.com/...b%./.....[.....'J]._..g.".s0.Y.i..Lp&."n.....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4d1295fcda27fb46_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	345
Entropy (8bit):	5.870591604472839
Encrypted:	false
SSDEEP:	6:mOYGLyINREDfmeuPESbSEfernqK6tEaEMdlVprnBj:63meuPq8tEM7TJ
MD5:	69CBA7D406BB0E753520FA6262C41073
SHA1:	26189765413D41F0087F106A0D05A7CCD83B4AA0
SHA-256:	6AB36338A70EFC5185BDE4F2C27C79305590327EC83E091F8284441BD509C4A4
SHA-512:	D8A7388E79FB47794AD2986EC6796AB6E045CE0E8030FECA1F8F92C023051A78F7BE06FDE425AFF3E029A639E526E4F0EE14CE0ACCC7EF47F15C8628440FB3A1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q....._keyhttps://www.joomag.com/static/js/pages/home.js?_=5.1.8.0 .https://joomag.com/..}h%./.....>.....]zf.).AJ..8.....I..G.[.A..Eo.....A..Eo.....}h%./.....52891DB3131A6676739F92A17901ED3645E899E219551717BE09574A7C8C9DB6]zf.).AJ..8.....I..G.[.A..Eo.....y.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4dc39f0688ebc553_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	48836
Entropy (8bit):	6.172852204656362
Encrypted:	false
SSDEEP:	384:dqYQ6UaKjUstQHGGBrMdtGUiAL56sPjpqeZ+saiE5dreaFPz1hb6DXTVL/QaAVsr:EY5mvQHKTGrgfOvgRdR6wHu5YY+KOb
MD5:	862C3D6C6CEDB1377C78040FEA0306AD

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4dc39f0688ebc553_0	
SHA1:	AF98872453D6538B3EC7EAEA645C3AED40D8A4D8
SHA-256:	1F4ACF2BF60F749F052A53165FD00C9B35382BDABE3D534C178A8FC6EBDEBF15
SHA-512:	E4D3BE79211D4D8F8F4C17ED8DD0E8EEA8F5E0FD824D8B1BBDA25FEDE3FBB0E3A180F0F37E91200033B8E019603D093B4AE7B127786CD9B9EA7CE0A8D8A637FC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....<....>(^...._keyhttps://js.hs-banner.com/5574303.js .https://joomag.com/[..h%./.....&.Z.....p.[.....5.....A..Eo.....A..Eo.....'.....O....8.....$.....0.....I.....d.....(S.)..`.....LL`".....L`.....Qb....._hsp..Qc..Kf....window.....Qb".k,....push.....`.....L`.....Qe:.C....setCookiePolicy.....`.....L`.....aF.....Qc6.....portalId`>.....Qbf.5I....id..`.b....Qc.....domain..F..Qb.|.....path.0Qj.-.[!.../hubspot-analytics-default-policy.....Qc..fQ....label...F..Qc. .....enabled.G..Qe^.&2....privacyPolicy...`..... Qf.k.]....privacyHideDecline..G..Qe.....privacyDefault..G. QfJM.z....privacyPolicyWordingF. QfNJ.v....privacyAcceptWordingF. $Qg.&.....privacyDismissWording...F.$Qg.I&.....privacyDisclaimerWordingF.$Qg.....privacyBannerAccentColorF. Qf...$....privacyBannerType.....Qb.R`R....TOP.. Qf ..U.....cookiesByCategory...F. Qf.P.b..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4de9bd481f502f20_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	229
Entropy (8bit):	5.586639267423462
Encrypted:	false
SSDEEP:	6:mtAgnYGLyIqWAUq0XQf1VYCLwKyarG9MTD4o9K6t:aAgCkq0Xi1q4wKbf/X
MD5:	93ECA45C9D375AE93679E59C6268A1EC
SHA1:	794A6112F7F5CD93D1C2CF9B3C73C07A6608AF9D
SHA-256:	8B6E11910C4F90D998FBB436D762A1E91D08E47E7485F2612452116D305DEE85
SHA-512:	D9EDE0DAFB9FD7E0E56D44E760990F00D0A0A6C840EE6703197C3049435ADF5230BF025C424F7516E8E860D457CA37B42C0F2C491AD6333E2010165AC47695F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....a...;....._keyhttps://www.joomag.com/Frontend/mobile/viewer/15.e64efce9e3c094627307.js .https://joomag.com/..(h%./.....j.s}.?...G.....,M.N..y.....X...A..Eo.....B."..........A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4f99dcb1a864e622_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	58254
Entropy (8bit):	5.798374618596626
Encrypted:	false
SSDEEP:	768:0y1YR9MhBZTaCBggdSOT+S84NjafXGKX/sPBqQJPJ/DOGjBriexMLUVJiFlYDsNG:0ZXzS8AjaPGO/UsGVrbVilTgn0kWgAk3
MD5:	37B6C2F3A6B29B6E69EC9D2B88E22597
SHA1:	4C7856D84412729B7FF289927F00BEA02A219995
SHA-256:	980775885091365D81D1192423E2F4DE9E8E0F76224CA7131574DD8991C61B53
SHA-512:	5D51FF496086340BBA8EDD1F42015B6DEEBC3868F7143F01259652E4F79C2F10E10887D26719817367835D75BF09E0BC6A1E078191EC041CCEBC69B459BEB6A7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f....+.~...._keyhttps://connect.facebook.net/signals/config/295648160646317?v=2.9.33&r=stable .https://joomag.com/...h%./.....$..2.w.M.*...*3.b.b.A:.k[....A..Eo.....$.r.....A..Eo.....'.....O.....>.$(.....X... !.....x.....H.....(S.....`.....\L`*....(S.P.`\....L`.....PRc$.....Qb>-.....d.....Qbn.Ql....c.....O....M...Qb.d.....e...d....$.....$.....I`....Dad.....a.....Q.@6..{....exports....a.....!..(S....`.....E.L`.....\Rc*.....Qb.....f.....Qb..!....h.....S...Qb.y.....j.....Qb...'....k...e.....I`....Da.....(S.....Ia.....%...#.@.-....\P.a.....M...https://connect.facebook.net/signals/config/295648160646317?v=2.9.33&r=stable...a.....D`....D`T...D`.....!!...`....&...&....&....&...(S.I..`.....$L`.....Qd.....postMessage..(S.....O.a.....I...#...&d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5383b090eaa51678_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1176
Entropy (8bit):	5.471526430836125
Encrypted:	false
SSDEEP:	24:2KKRrgKKQt2pgKKnpgKKq71gKKe83gKKRO:2KsgKL2pgK0gKRpgK+3gKKO
MD5:	8CD2EA26D4C5958F45C0BEBA2E2116C4
SHA1:	E6BB949C0C3FC35CC804E22FDBCE145587EAD4E4
SHA-256:	1D2EEC6938557A05579577CA6D9AE0ABB4E2C37A29834DB1825FF5CFDE3A7162
SHA-512:	CA99ADF13A67988C23500706862909C0AE0613E140FC827889CAA2835C13A9DFE31CE6DF7EC20FBD7B5EF1C481C8C54A95C9C904EFC3010E870E64AF0A70DE8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5383b090eaa51678_0	
Preview:	0\r..m.....@....._keyhttps://js.hsleadflows.net/leadflows.js .https://joomag.com/\$.h%./.....T.....8T.ky..^.l.ZH.P]C<..]..! .....z.A..Eo.....O.....A..Eo.....0\r.. m.....@....._keyhttps://js.hsleadflows.net/leadflows.js .https://joomag.com/..m%./..... .....8T.ky..^.l.ZH.P]C<..]..! .....z.A..Eo.....i.....A..Eo.....0\r..m..... @....._keyhttps://js.hsleadflows.net/leadflows.js .https://joomag.com/.l.n%./.....i7.....8T.ky..^.l.ZH.P]C<..]..! .....z.A..Eo.....w.....A..Eo.....0\r..m.....@.... ....._keyhttps://js.hsleadflows.net/leadflows.js .https://joomag.com/]^.n%./.....i.....8T.ky..^.l.ZH.P]C<..]..! .....z.A..Eo.....9.....A..Eo.....0\r..m.....@..... ._keyhttps://js.hsleadflows.net/leadflows.js .https://joomag.com/d.0o%./.....8T.ky..^.l.ZH.P]C<..]..! .....z.A..Eo.....!.....A..Eo.....0\r..m.....@.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\569ae1a688927577_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.479156918319433
Encrypted:	false
SSDEEP:	3:m+letC8RzYP2FycyG8ZFvD6AMGAGXhIL/zHKlltlHCv/mQccIWmlEH3jkeZmrlpD:mnPYeMQGAGXkrq6GQ6oXzYnK6t
MD5:	21EA014EEA9847C0A80A81B81308410A
SHA1:	D28DE1BD2E2D7E505063044AD090C2BC0EE24EE0
SHA-256:	53AD2A201EE73921D189ABB649D30C482BEDCF2068B3A2FB8E0AC65BC4744EA7
SHA-512:	C330A1DE16D7DB342F0217CF35066F0C3D4D1D63D8B5C684FA4206E76738820CC4F65BA3AAFD54A434A9178E3A4D0F613CE44FB2A6D5FF77435E9475D77EE0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N...U.L...._keyhttps://code.jquery.com/jquery-3.1.1.min.js .https://theicecreamqueen.net/X..m%./.....V...w.....R...c.K.....A..Eo.....A..Eo... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\56bafe686ab360ee_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16650
Entropy (8bit):	6.093871424902907
Encrypted:	false
SSDEEP:	384:YuFMwD6CufWKfMCuMaXEu4e8ZyEoNtbTbAK3CN43uJzw:na2jQhUChaAe8ZyESTF
MD5:	86712D55CB18C510CDCCA62F7DEBE3D8
SHA1:	526502BE3A89E7ABA90F81AC4B80C22097A0A8CE
SHA-256:	0AB57AE151811B383CE3C233C7203C2673B84A5E959EB8BF2ABA0E7D6CC4228B
SHA-512:	D90935A39819C297476EBFB0B27FB16CDAC8388B4E94BC0EC299CA04D393B0AC0BE01C3B2914FFEFB9B6244C46F381C7A3FC2CA807D0168E89071A505A3740 D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N.....9....._keyhttps://js.intercomcdn.com/message-modern.58f7c774.js .https://joomag.com/=X.o%./.....uzkRI...y.,.3.6..-.4d.(TR.r...A..Eo.....b9&..... ...A..Eo.....=X.o%./.....uzkRI...y.,.3.6..-.4d.(TR.r...A..Eo.....6{-.....=X.o%./.....uzkRI...y.,.3.6..-.4d.(TR.r...A..Eo.....5..R.....=X.o%./..... .....uzkRI...y.,.3.6..-.4d.(TR.r...A..Eo.....5.:1.....'.....O.....>.....@.....(S.....`.....DL`.....Qc..Kf....window....Q.P..:"....webpackJsonp ..Qb".k,....push....`.....L`.....`.....Ma....Z...`.....`..b,.....C`0...C`@...C`H...C`J...C`....C`....C`....C`....C`....C`.....(S.U..`^.....L`n.....Rc<.....S...Qb._.O....s..... M...Qbn.Ql....c.....Qbj..n....l.....Qb.K.E....p.....Qb6.2.....m.....R.....O...Qb.....f...j.....Qb.....581.`.....Pc.....push.581a

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5e0609edbb009490_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	166312
Entropy (8bit):	5.727446443023032
Encrypted:	false
SSDEEP:	3072:i2MxX8yHfqL24KQntof4KNDlPVOr8si2jXGRpivewiJAHf:RMd8yS64KQCQKNDlNOosi2jXGRpsiOHf
MD5:	F7A761F60DB41211C97101C9C3C89887
SHA1:	039C098C9445448A02A3315249ABC36112BD7FFD
SHA-256:	8B3F3B6FF0ED06C0D90F277820E1E92C4991CB4DA551A4F86B4C0244C00D96DD
SHA-512:	B545B30F282FCF3DEB71A82C660EFA4EA6DAAC9FD8071DADD38BD9248AB57C32ED2471AAC2CD3BC86906DACC49FA79D2C85AD8743DEDC36A55E06732D26 70A6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...nC.....7DACA0907AB9F2860DFD05745591E9C3C22DA13D8576600873CA502753ADFFDD.....'.....O6.....A.T9.....X... !..... .....(S....`.....\L`*....(S.P.`\.....L`.....PRc$.....Qb>-.....d.....Qbn.Ql... .c.....O....M...Qb.d.....e...d....$.....$.....I`....Dad.....a.....Q.@6..{....exports....a.....!..(S....`.....E.L`.....\Rc*.....Qb.....f.....Qb..!.....h.....S...Qb.y.....j.....Qb.. .'....k...e.....I`....Da.....(S.....Ia.....%...#.@.-....\P.a.....M...https://connect.facebook.net/signals/config/290226788268586?v=2.9.33&r=stable...a..... .D`....D`:...D`.....!!..`....&...&....&....&...(S.l..`.....$L`.....Qd.....postMessage..(S.....O.a.....I...#...&d.....$..a.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6158ca99bdaf719d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	139432
Entropy (8bit):	5.836771227530138
Encrypted:	false
SSDEEP:	1536:uayt4AZYpkU0qxGYILGauSqjW7WYVUoV7lvXzU1OVaxDu7TgQ+feSRt1O:uX4AfKyuSeYKe5XzUkjT5+feS9O
MD5:	EC14590BE93F8539FF01534D6A7AE4E3
SHA1:	9AE832A915909FEA03C0431EA5EC705FDEFF2130
SHA-256:	9A2BDDB54AA213BCC3AA239E1EA8F60940CCB1EACF858D64C17FB23573AC08B0
SHA-512:	7EF283A9DB7D613748087C9474EC14510F83C98802B8B2544338DAD7F2108A2D2ED26D5D42DFF7BFD6B4F97225F347B1F3DDA15107CDF543CF8C20931FE72F7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...9."....5DF3A77FFC799DBDD53EFBCF0BF154C4B2A67BA11BD77B1BA4BFF0AB62DFDBDD.....'.FK....O.... .....(...|-..... .....(S.D..`@.....L`.....(S.h.`.....L`.....TRc&.....Qb..{*....w.....e....d..... .....l`....Daz.....(S.....5.a.....a.....Pd.....<computed>.ea`...t...l.....@.-....DP.....5…https://www.googletagmanager.com/gtm.js?id=GTM-WVG733...a.....D`.. ..D` ...D`.....`....&...&....&..1.&...(S...}-..`.Z.....L`n.....Rc^.....&.....Qb.6.....data..Qb.#.....ca....Qbn.....ea....QbR.q`....la....Qb.,u.....na....Qb.|.....sa....Qb6.J.. ...ta....Qbb.L.....ra....Qb.....oa....Qb.4.....ua....Qb6.....xa....Qb..3....za....Qb...G....Aa....Qb...H....Ba....Qb.....Ca....Qb>.....Da....QbV.....Ea....Qb.|.....Ga....Qb..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\63c01e10279ec25e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	559992
Entropy (8bit):	6.23755887439869
Encrypted:	false
SSDEEP:	6144:DwlbcE7O1L71XCXcWHRvVzFnwdIRME3V8Tfl0E6xpLN8QAH8:4jc7gdMkOTfSdLrE8
MD5:	BF2995BDD108144D35861677F5FD793C
SHA1:	08169E6419B385CF88981A4744D14969715C2D9B
SHA-256:	FC02F5739E0C60FBB45321E0C3BE637EFA01D6E0DBD0FCF47F814ACC6AB1D386
SHA-512:	294222F52C6974C4CD40E58EF9A70A8EAE06D5E174565D3F8B8C8AE76D3D605342ED30BCD2A61B315DDC00237BB28AA8829C2E72FB2BD2F5533BCA96FB0C9E AF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...A]._....C8BB778450CEB7894DD9260F9648DC275D2EE80AAC6046590483F0000930225C.....'.w$....O....@...[>4T.....`....2..... ..... .....\&.....D.....p.....X.....D..... .....4...<.....$.....L.....\.....L..... ....H...@.....(S....`,....E.L`.....Q.@rv.....window....Q.P&.....webpackJsonp..Qb.....push.....`.....L`.....`.....Ma.....`.....Qc&(;.....concat.....`.... .....LaN.....E`.....Ec.....E`....Ec.....Ef.....E`.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\65befcac1cde97c2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	329160
Entropy (8bit):	5.920139390457667
Encrypted:	false
SSDEEP:	3072:bXR18U9/qbUV8YinDCnRf4sGmKyF7E02hiGRGLo9ev++7R/jv/NhwlU4ODLFzM7x:JJinlsc27yhi57m+7lcUpe
MD5:	DDA693AE42D5FECC5DB403567871EEA9
SHA1:	8789D368F93804CC1F5646CDAF7C0187AA4E78C2
SHA-256:	73EE339DC193A8B779C8C1FF472C9462E0E50D7FF99500351FEF6597251FF8B8
SHA-512:	7FCB4A272B31BC081C3DCBB76DCD5507F7BCBB165E9A315C2BA1F11A7A2F66F2D58A88D62E63DBCFDF20D0D4179734E64BE6AA063258B96BEC84C24DCCC20DC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....069B05A91C5ACEE5FB0FCD2B1505A2FB3A190AD28658F80DE2174823DCB62590.....'.J.....Od...h...../.....%..... .....L.....,.....h.....`.....$..p.....X.... .....`.....(S....`.....L`.....(S.A..`8.....L`<....`Rc,.....Qb.d.....e.....QbV&F.....n.....Qb>.....r.....S...Qb.....o.....Qb._.O....s.. ...Qb>-.....d...f$.....I`....Da.....(S.M..`P....(L`.....M.....Qe.....hasOwnProperty....Qb.0.....call..Qb".k,....push..QcJE.....shift.....K`....D...x.....*..&...*.. &...*..&..&.|.&.(...i...e%.*..&....&.(...&.(...&.(...&...&.Z.....)..&.%.*....(...&...&.%.*..&..*..&.Y.....&..0..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\66856abd7f544089_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	273

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\66856abd7f544089_0	
Entropy (8bit):	5.72715285802344
Encrypted:	false
SSDEEP:	6:mzYET08NWQASxYOno/Pd0PWip7K6wXDGX8/m4jCbK6t:2g8NWQXnoHdTipuXDGCmLN
MD5:	780AF68D192233B02F81D6BA12630058
SHA1:	B122738D272ED694A623A73F44D6FA565A3922D0
SHA-256:	DE8D61BBADED093379BF5A7A111AC09F69D4711E1F3934C32537FE5B89156626
SHA-512:	153F0D8CE16ECEDF17481CB089019437F9414E95DBAB45DA5AF8FE5529D0975DC16B66E99636EF8D48B392ADF13CF0FEF7D20AE8ACF0425EC7E1182C79837DD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f.0...._keyhttps://cdnjs.cloudflare.com/ajax/libs/jquery-mousewheel/3.1.13/jquery.mousewheel.min.js?isAjax=true&_=1617996262823 .https://joomag.com/..m%./.....3.....>W...6...T...$#....?....E./..A..Eo.....!.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\68cc6d037028d20c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	679
Entropy (8bit):	5.817979485242907
Encrypted:	false
SSDEEP:	12:hE3xeIl1oux2pmYyyQL13CMxGDPM8ihVkhN7Cd8xGnhWT:hEBeI4uyRyyQL1SXDXirkDCd8xGnhU
MD5:	CE8AB2F6A2CAA801713AE9117DBB5EBC
SHA1:	14230DAC8B11B30AF71CFE9856E730547DEA0332
SHA-256:	671C875606737EC54AB90D87B773DC9E60B02246083A584EC7783BB6072C0DA5
SHA-512:	F560882FC2CA9E5DEB204127C1B1F4CC4135FBDFD678B9FEA20F991AA089BD7D9AA5146738EE6EF68D9D0363A63821E2624189B5BD976C67B8599CBAB06C2AE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....#...U....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/1003757157/?random=1617996285268&cv=9&fst=1617996285268&num=1&bg=ffffff&guid=ON&resp=GooglemKTybQhCsO&eid=2505059651&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=120&u_java=false&u_nplug=1&u_nmime=2&gtm=2oa3v0&sendb=1&ig=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fwww.joomag.com%2Fen%2Fsolutions%2Fdigital-publishing&tiba=The%20All-in-One%20Digital%20Publishing%20Platform%20%7C%20Joomag&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://joomag.com/..Do%./.....@y.'.._.....4...3..~.#..A..Eo.....c.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6b1b9d51f4f5cab5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.5964628478697716
Encrypted:	false
SSDEEP:	6:mAfYGLyIqWA5nZx7w54vNyZPNixcLh+7DK6t:kpZxoi0PNi
MD5:	8800944DAB69636949861557404D9F5B
SHA1:	C39FF4D9091CBEB23A7303FB949D9B3B451B342E
SHA-256:	55FEC1EBDD1C663C020CB94FF190A9449E1CB0D11563BF76FA851BD89FC241B5
SHA-512:	8D9CCA27902771B4A136413857804ABF577E9056C6161C932335CA5515AD293F189030F2305D0F705C92F9A619E1F661DC325D2CBABC1F8C410B3534D5544060
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g...8....._keyhttps://www.joomag.com/Frontend/mobile/viewer/manifest.6ab342fa4d7e7af5331a.js .https://joomag.com/o.b%./.....l....1{.h#....(..C.j.X.T. ai.A..Eo.....l.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7371003c8c6a9d18_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	341
Entropy (8bit):	5.889543139581875
Encrypted:	false
SSDEEP:	6:meFnYGLyINRsSxYeuPk3lA5Hnv/zlbK6tGSOlmcgSdDiE2hS2Hnvx:QLUYeuPkVa3XQmcZYE2hS25
MD5:	547649CAD712D34B67E698CA6DDBDEBD
SHA1:	CD051D88F5BFEE99C448BD6D8CE1C56CDF37739B
SHA-256:	C9445386063A23BE2DA8C6D637073EECA2333187E0AF645F8F8455B561733473
SHA-512:	552AF5F0B886B30AA7BE76E506596B2A31C640775ABE6E3BFF104586AF1BCF399F60B8B882E7F86E328C8484710F052E23BF8E1E1CE96B659F3F071FE968273B
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7371003c8c6a9d18_0	
Reputation:	low
Preview:	0\r..m.....M....#....._keyhttps://www.joomag.com/static/js/joomag.js?_=5.1.8.0 .https://joomag.com/.v{h%./.....5.....x&.|.....#.....O.B..5..3b...A..Eo.....<.....A..Eo... .....v{h%./.....D6AB9E303CE87B7F01CBADEA275E8E4EB21FB8DA472CD6BB51943767E5054D94.x&.|.....#.....O.B..5..3b...A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7b5d3be33a96cdb3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3162
Entropy (8bit):	5.537197820068832
Encrypted:	false
SSDEEP:	48:QklpbnEGXM/xkl1TMoty206FRXfbBeFLfpnFrFLZMey1D4grXN3Vz:QjxFoQ20fNpFA91D4ox
MD5:	39B8DA120DC55C78E252880AF5ED57D7
SHA1:	6613B312B81B6183DAC7CEB4991BA1E4A149A5A2
SHA-256:	5920CABD3A37BAE35DF44B825365F75BA953CD1B1D95DFEA821BF4891CA3A237
SHA-512:	FADE6E087AB0600C47809C1236D8F2A80A12EBB25E91442BB0C1B6C7E0566DEFE96E1EF4E4F7D228096180D7030DEBE7D382BAAF0EB37DCF138F546DAAB862 CA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....j...pH`o...._keyhttps://s.adroll.com/j/pre/7S36S2RHW5BUVAXH6L4RZE/6TMQVXNPWBG6BOGAF3EFID/index.js .https://joomag.com/6..h%./.....2.. *.8A\....F."..b...s...G.....A..Eo.....RHU.....A..Eo.....6..h%./.(.....'.....O.....$:.....0.....(S.<..`0.....L`.....(S.0.`.....L`.....(S.U..`b.....L`H....xRc8..... .....Qbn.Ql....c.....Qbj..n....l.....Qb..]x....y.....Qb...'....k.....Qb._.....z.....Qb6.2.....m.....Qb.....q.....Qb..{*....w.....Qb~.....v...i$.....l`....Da,....#...(S.. ...la$...J.....@.-....`P.q.....Q...https://s.adroll.com/j/pre/7S36S2RHW5BUVAXH6L4RZE/6TMQVXNPWBG6BOGAF3EFID/index.js...a.....D`....D`@...D`.....`...`,...&...&.. ..&..q.&....&.(S....IaT.....!.....d.....&.(S...Ia.....a...d.....&.(S...Ia...._.....d.....&.(S.....5.a.....a.....Qd^..W...._install_cmpa.....I

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\83137b52fc11f0b5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	350
Entropy (8bit):	5.885684167304161
Encrypted:	false
SSDEEP:	6:mvYGLylNRED1EMeuPKAPXVLXtXK6tig+GxCaJgCjSSbW/UB4VLXtK:TdXeuPNXRX7rFxCESSbW/UB4RX
MD5:	AA0D64FFB10906D7F9F0218339B27E26
SHA1:	E79F023F8406095B23092FA1E7C2A89CC04E2D80
SHA-256:	1F88CDEBED8CDB895BC5C4C65CD82CB77FE6AE9314EA0640483F1B33332B2B84
SHA-512:	5BB97AAD371D3E51B793F316C385D256FE216E91CF53BA09688FF1D691411D6D6201EDF0F7188EBCCD2E9527F9BE67E0C99777A5423ECA192ABD9271DA78E04 8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V....T.}...._keyhttps://www.joomag.com/static/js/pages/solutions.js?_=5.1.8.0 .https://joomag.com/...m%./.....1.....I..o#.....u...{..i...+.....A..Eo.....~.I..... A..Eo.....m%./.....922AEAD3999397874287A570609B4133E9A71C813B87A04F4BA7DA7B3E4C1FBBI..o#.....u...{..i...+.....A..Eo.....|..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\83b9c3db1088f864_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	5.717403673672304
Encrypted:	false
SSDEEP:	6:mY2nYiRDHjfRpA7eIAX3TH5R2DU3eJsyAlK6t:KxDHIeB3L5gDG1/
MD5:	DC713F2D0FF09CD0D851A917B9D73A33
SHA1:	BBFDDD223833CF2672C959960330EC137D7792CA
SHA-256:	AF5E47A99778BFEDFA83E3FC680DA53CDD9B86E108BD1F10F7DB298B9FA8DB56
SHA-512:	EEAA2E442AF465D963DBFAA5760B37B6056F36B492E7A3FFDB73C78C5AD459A1BA225BD092573294A31C46317352C9A4FB625AD15FD93014F827EF7A187A9D1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....x....._keyhttps://c.s-microsoft.com/en-gb/CMSScripts/script.jsx?k=8c84dc53-9dee-f42a-46b1-5a93c0e43d70 .https://microsoft.com/]J.l%./.....1o.. ....h.....KP..e.9.k..A..Eo.....,.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\87166bed915ccad5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\87166bed915ccad5_0	
Size (bytes):	333744
Entropy (8bit):	5.674495817743544
Encrypted:	false
SSDEEP:	3072:t+TeS+Vv2+A2DWxG0Hl0wKgoyWOniU5SBWO/3U+Bi5VX3ZJZ6YOe7vj052ihVyKm:MT0kpnxGsljKgoEO/AYm
MD5:	AC01693C18421FC1ADBC09F4BF52AE8F
SHA1:	3B27CF0AA3541AD4498AD5DA7584FFA5E0F9FF94
SHA-256:	F71DA0796039E76D6A9A0BA98F960435BD61805C14757DEDFC8AD33C27A9A974
SHA-512:	60F971431B2B00FC2EF6B12493F233B10F9F4C425F2E4FA558FB4AB883D4538857A2AD2B38F3DE33F25001E06E104C2FE30901B1DB1E8820A0FB6360BBFEC35B
Malicious:	false
Reputation:	low
Preview:	0\r..m......@...;>.....A8F6097574AC1BA3E1E7B63FED30E86CD98338E89187154B5DE85C4AA87C7CE6.............'.......OP........"..................@.. ....$..................................$...D..X......................@....7...d......... ....(S.....`.....!.L`......Q.@...)....window....Q.P...9....webpackJsonp..Qb..ol....push.....`......L`.......`......Ma....`...`.........b...........C`....C`....C`....C`....C`....C`....C`....C`....C`".. .C`$...C`(...C`H...C`^...C``...C`b...C`d...C`f...C`h...C`j...C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C `....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`....C`...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\87fd1924f833e73a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	131904
Entropy (8bit):	5.725930884213589
Encrypted:	false
SSDEEP:	1536:PFY/8P3b5yJEgn2tpj7HmH5S3Pa/AMBY2Lcs2SjKaV7dNFpzFvNMD44w:tYNag2tpj7GZSf8BRLcs26KqdRzj
MD5:	4EF4716860C0500B5D6DA4070B1EFF78
SHA1:	7844C4580CC7E592918DC6E59FB2E54166A6A78A
SHA-256:	5B1034988448060C2EBE7BA8D35932DE334673D3FA0A6E092FFE970FD7D2C018
SHA-512:	7E88699F2417268004C2EE375957AB641F019D51648F38F5A52FBE0BD86A857CE4491E913A3243641E6A9BC312541686FAEC76A29AC2637FF3706E09D18930EA
Malicious:	false
Reputation:	low
Preview:	0\r..m......@.....<.....09B1AA11C2005038CD981BE279116E954CC01CFA96798BCC216747131820F437.............'..m....O+.......v~... ....,...................(S....`.....XL`(.....Qb..}T....fbq...Qc.Q^.....2.9.33....Qc.......version...Qc........stable....Qe..ie.... _releaseSegment......`......M`......Qe.'.....global_config.....Qe..b.....pendingConfigs...(S.P.`\.....L`.....PRc$................Qb>-......d.....Qbn.Ql....c......O....M...Qb.d.....e...d.... $.......$.......I`....Da.....6......a..........Q.@6..{....exports....a.............(S....`.......L`@....tRc6...............Qb.......f..........Qb..!.....h......S...Qb.y......j.....Qb...'....k.....Qbj..n....l.....Qb6.2.. ...m.....QbV&F.....n...h...................................I`....Da|....6.......(S.P..`X.....L`........HQp..##9...this hasn't been initialised - super() hasn't been called..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\88c2694a38162e86_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	32413
Entropy (8bit):	5.084257573492091
Encrypted:	false
SSDEEP:	384:gPQPxzc2FPLCqss2tCCT/CFNIbqEUVZedSn7zYZjT5ymvBsY8a91LN7vVE0zhaua:58WrmZsgQwOWSY7ruCxFwaCjig1R
MD5:	057B947520663AC405D52A1BABAC1DA7
SHA1:	87DED97D95DD197D5E57DD0B93E737A3EA5BB7FB
SHA-256:	83EA8A5416E01A04DC8214ABC4A2772734C0026D5F50F1D07C72EAA55A132F24
SHA-512:	CE1B844D93782234DD0564C3086863CB8000D5973E3A4358A54337A56223662B6E19921FC59B6FC92A07BCE48E83ADF9A187FF1918CAF9948025213ACDFA656E
Malicious:	false
Reputation:	low
Preview:	0\r..m......M....K-....._keyhttps://js.intercomcdn.com/vendor-modern.a5ba650d.js .https://joomag.com/..cl%./.....................s...!h^..$..i.F....t.2....xG.A..Eo........~..........A..Eo.. ....'.......O.....}.................(...H...0..(S...I...`F".......L`n.....Qc..Kf....window....Q.P..:"....webpackJsonp..Qb".k,....push.....` ......L`.......`......Ma....^...`.......`.....y.La8........E`.....E`....E`.....Ea........E`....Ea.........E`.....E`.....Ea.........Eb............E`....Ec...............E`.....Ea.........E`.....Ek.............................. ....E`.....E`.....Eo..E`.....Er...................................................................E`.....Eb............E`.....E`.....Ek........................... ....E.!...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8c50196a1e0f9ecd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	672
Entropy (8bit):	5.755360359394251
Encrypted:	false
SSDEEP:	12:5E3xCdWFIJdsoux2peyyQL13CMxGDPM9tlN7Cdenp1:5EBCdWFIJdVuyeyyQL1SXDOtlpCd+p1
MD5:	7D727B57346A37A7AF828E651943DAEE
SHA1:	FB56033091FD234C509F4FAB54CC30016851332E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8c50196a1e0f9ecd_0	
SHA-256:	35169630159A4D8F05692E1801170FD3DD983CF6830A6C907B3E5C5ED96825DB
SHA-512:	5555D25FD20ED17727832FCC2A2B85BF7711E0BBC446E1517DF6A374953DC17C29F6FF8CC651B3C5E2C5BAA7E4A28B018DE4A8F4D715B3075507441E410F485
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/1003757157/?random=1617996280828&cv=9&fst=1617996280828&num=1&bg=ffffff&guid=ON&resp=GooglemKTybQhCsO&eid=2505059650&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=120&u_java=false&u_nplug=1&u_nmime=2&gtm=2oa3v0&sendb=1&ig=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fwww.joomag.com%2Fen%2Fsolutions%2Fcorporate-communications&tiba=Corporate%20Communications%20Platform%20%7C%20Joomag&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://joomag.com/F..o%./.....x.....~....j.wV.....s.c?Ew.~.....=...A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\91721bc070d4628d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	234
Entropy (8bit):	5.484132511235112
Encrypted:	false
SSDEEP:	6:mEqEY68E9xEEUgLErvGAGXkrKFZ1NMmwdYusp0Ar4cZK6t:lqQYgfAAmeZHMOXtDT
MD5:	8F544493679F14C06F6C1EFE03629159
SHA1:	E7DC6C4BA2FB6607B3717605EFEC01F87F24CD86
SHA-256:	93E18CF1E45BC9D89D36875094BA79491D13765B4619FCBA9B57A924AFA62C18
SHA-512:	D975A57605B5BA3BCCFDA982AE0BC9B1677D1D72AD8D8D48369737B3EE5D5CD678637B6657190F3D0BE66FFF4074A9286A10F78CD91DABADDF0DEC934245B0C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f....._keyhttps://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js .https://theicecreamqueen.net/.. m%./.....(.....wJ..XT.M....!..q2.....i%. ...A..Eo.....H&.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9890963327d9ee09_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	339
Entropy (8bit):	5.871094488802147
Encrypted:	false
SSDEEP:	6:m2/PY4rgdsiQM+HMnfIAWn5r6PbkhXofYe4K4RK6tx6GhhXofYe4K4G:P/7GmmfIAW5rjqj4bVqj
MD5:	F8ABC39D86EE95C980830F65629325A5
SHA1:	7E35A0E854722C7F54B5857D90191156A75D521C
SHA-256:	9B9971D9014F07B26891906DFF8FD8D74EF8FE3C1B6CD3F65F9F237786B00A3B
SHA-512:	CCC94ECC2EBB7C389DCE5902C9C1A6A0B83210DDB821DA0EE322B3DC98C9D57384B97600D27D00EF93294E99F824D039FD6F8CF8D0368B7BE6EC5EFADDFC596
Malicious:	false
Reputation:	low
Preview:	0\r..m.....{....g'....._keyhttps://s.adroll.com/pixel/7S36S2RHW5BUVAXH6L4RZE/6TMQVXNPWBG6BOGAF3EFID/LD55UB2QDFC4VI5DKZ4AM3.js .https://joomag.com/^1.m%./.....!.....16.P.....2W.s2...Z]....)...%%}j.A..Eo.....kd.....A..Eo.....^1.m%./.....16.P.....2W.s2...Z]....)...%%}j.A..Eo.....].9.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\989b6fe145516e59_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	340
Entropy (8bit):	5.825583566257617
Encrypted:	false
SSDEEP:	6:mOLPYOXdTAqxAXLMAun5PZPY47TLyu4rbK6tGomnwpF9CXUSRZVTjr7TLyu4rfll:FnXBuk5h1bl+Pp3wXLTVTjrbl
MD5:	B182BF63C86EC6852BB9BEAB6B0D5A35
SHA1:	9C5DE0CB3767C8900DDFD7750C3B1D37E94DB318
SHA-256:	3255F13F5A249F7876072C211FF076A133213266F5045CC9C251DEE24D89FB25
SHA-512:	37B0297B6BCD017B89B74F90A97C0B20630E74D2DA76A7019BCD1049F4DAFA388A47B3216F250FAE9B4B1E8AF0305F6A5D18F520BB599B5A6E58629039C3711C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L....._keyhttps://js.intercomcdn.com/frame-modern.f881becc.js .https://joomag.com/2.cl%./.....6F.....u.MoS..E.....J..D.A..Eo.....Vd.....A..Eo... .....2.cl%./. ...069B05A91C5ACEE5FB0FCD2B1505A2FB3A190AD28658F80DE2174823DCB625906F.....u.MoS..E.....J..D.A..Eo.....DL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9ac614ffd44f5d33_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	6872
Entropy (8bit):	5.482432127012055
Encrypted:	false
SSDEEP:	192:KUnWInW9eYJKdidNR9H/2MBbi8cKE33BU:KUBWlK4/2MBbL1E33G
MD5:	7BEE66672DA9F80C9C263D58108390A2
SHA1:	6D10757CB35A1970E4E49BDCD67DB02B8FB31C8F
SHA-256:	FC8036142C8F4F39B85A18F57521F250DA0279DFCD21AFE8CB8581336D3F171E
SHA-512:	D5C69BA0AFFBE0696588594A2A3266CEAE77FF291DD89E03C5165BC1BD5AB4652BCA57D2EA226727F98AAABFADA3502BE3DD741837C2E60BB93BE67AAD90814D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....8...vq.'...._keyhttps://js.hsadspixel.net/fb.js .https://joomag.com/..h%./.....:.;j.....{XB.B...F....t...I.<..A..Eo.....4.Z.....A..Eo.....'.$.....O. ...x...<*Ey.....(S.\..`n.....L`.....(S...`(....XL`(....HRc .....Qb.d.....e.....QbV&F.....n.....Qb.....t.....Qb>.....r...c$.....I`....Da.....(S...`.....L`..... .Q.@6..{....exports..$..a.....S.C..Qbj..n....I...H.....a.....Qb.0.....call.....K`....D}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...&...&.'..W.... .-...(.....,Rc.....`....Da@...8.....a.....e..... P.....@....@.-....,P.....https://js.hsadspixel.net/fb.js.a.....D`....D`P...D`.....`d...&...&....&....&.(S.....Pc.....t. dlbpr.a.....I.....d.....&.(S.X..`l.....L`.....Qb.....o.....e.....a.....G...C...K`....Dp(... .....&.(...&.Z.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9d6dba672108c09e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.606767706862604
Encrypted:	false
SSDEEP:	6:m0XYGLyIq72RKiB6qzSPsN55A763OXeWyWnXzK6t:NSr2RdrSP45UeAl
MD5:	21F472CD587248872586ABBD7D76757F
SHA1:	5319F9E8A41F0C286A2E18F8350F5C28BA8CEF93
SHA-256:	18DFDFDCD52B8D24B77ECB891008C2473D1868E64D4AF592AF349F0768923649
SHA-512:	90519EF3DD539A5C02B9D143FE50D2A3A7661866D2682D181168428B1FB4855F1D6C8393350031DE34BAE8935BADAB7DC9FF38F2E19B5281D56E8E1AEBD92D5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....c...}....._keyhttps://www.joomag.com/Frontend/pixel/joomag-pixel.3df7f73f177625835141.js .https://joomag.com/...b%./.....pO6.<...5.._@..3O..g.. ._H.m....A..Eo.....p.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9e1cef9c2a427a5f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	103096
Entropy (8bit):	5.5976222487822875
Encrypted:	false
SSDEEP:	1536:r1hdf4jddN/ElYSrDsJstpCcMZXolCnm3EKmTdBs4P64sZCmL:7df43N83rDEdmTmTkj
MD5:	E020B8D055001DB35A4A828F386EA2EC
SHA1:	AC8CCC2B02E08A72CD0723D1F4243A6C90B9B0D0
SHA-256:	FFB4C3F6EB5B0DC66F2B050E652E3ED69E0B9C432E3CED8BD47B4CF7BE954809
SHA-512:	7494656D1E911C8503D5F617716C2BFE8ED1B99D4DD11E3DCAEF643C99C5DC66B1E9CEA2550F0DCFF7C7C00EC98DF2AC96E66AD37646EE36CCE73ADCEC10645
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....922AEAD3999397874287A570609B4133E9A71C813B87A04F4BA7DA7B3E4C1FBB.....'.R$....O#...X.....(7..... .....(S....`h....xL`8....(S.U..`b.....L`V....@Rc.....Qb.Z.2....t.....Qb.7.....e.....S.b.....I`....Da.....(S.....Ia.... N.....@.-....LP.!.....=...https://www.joomag.com/static/js/pages/solutions.js?_=5.1.8.0...a.....D`....D`....D`.....`....&...&....&..!.&.(S.....5.a.....a.....Qdj.x;.... queueTriggera|.....I.....d.....&...(S.....Pd.....t.trigger...a.....I.....d.....&.(S.....Pd.....t.destroy...a....`...I..d.....&.(S.....Pd.....t.disable...a}.... ...I..d.....&.(S.....Pc.....t.enablea.....I..d.....&.(S.....Pc.....t.next..a....(...I..d.....&.(S.....Pd.....t.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9ff14046406d6375_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	342
Entropy (8bit):	5.905322250524128
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9ff14046406d6375_0	
SSDEEP:	6:mplllVYGLSmXZCLRaRphNPAngAAEi7V+YgK6twmSKdQfOKe21wZoZAAEi7V+YA:s/1Pfb0i7VSGmVdQfHe21qoui7Vw
MD5:	C816C5943469036B02AEF3A64F8D91DA
SHA1:	0895639EF5ECB138969D48DA082E7012435061DA
SHA-256:	6CA1566712F2ED225DD331636F83724540391BCAF13449BACC30AB6D6923398A
SHA-512:	3A3C3AD89CC5258E9C76B254EBD365A2C006448DB817C51C52D02FC338789D91EB77CB11FE457AB1EA841C2100E8643EA170BAD2ACC945A284310295EFE75BC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N....)Q....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-WVG733 .https://joomag.com/G.h%./.....&t.<...^4....).'.r.G..H.f...`&..A..Eo.....A..Eo.....G.h%./.. ..5DF3A77FFC799DBDD53EFBCF0BF154C4B2A67BA11BD77B1BA4BFF0AB62DFDBDD&t.<...^4....).'.r.G..H.f...`&..A..Eo.....%...L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a262d627eec5cc8b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	233
Entropy (8bit):	5.610580927347868
Encrypted:	false
SSDEEP:	6:mmWYGLyIqWAt71dGtWVN581Hqsc8lM5tbK6t:v3Ma8Zc8O5tN
MD5:	16FE93279CB441F99B2BE3677120A0E1
SHA1:	0BB059D9FCB0825224251EED85C9F6BF3D3DA5FB
SHA-256:	F99A2C92E3AC5705137233344A152D8006DA0D5F6DB9B372DCAB0A3C25981CDB
SHA-512:	A38F2A0E631F529DA57EDB2BB89BC5B0D0EB81585912E7BA04C5A5F99E48CC794720569945CFBBBFB55305230FE95CBB1663B689A6AB06FF9EFE6DA8E7858B6D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....e...7.*....._keyhttps://www.joomag.com/Frontend/mobile/viewer/vendor.7bc4df7aaac8424047c3.js .https://joomag.com/@.b%./.....F.Y.BQ`?.|..q .W.+..._7NT..A..Eo.....i.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ab12a7b7c55c605f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	506
Entropy (8bit):	5.787151903519588
Encrypted:	false
SSDEEP:	12:HXm04fG15eTNypHipX+1ETNypuUp+1+nqdsJ/HlWNyp++1okTNyp:HXQfiARyp66ERyprUwqa/HlQyptokRyp
MD5:	AE2BA0C21870C817581F879FB40AED27
SHA1:	43EB7AD7E5D9FB53F1FC74C3F0194667BF1431E2
SHA-256:	E1C961F703894F8AF7280B71937CF10E3D25EE4EB2D8CA0FFE12E2C631ED40E9
SHA-512:	C07BB05B73B1CFFB99FB059D8E130E185F570BE4F3FB395B2F3BAE8C0FBF04A0DFD11445376C8781C0F8E175B1B6CA8E0CD87B540B3709893F3331622B05CBA4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....J....i_+...._keyhttps://js.intercomcdn.com/app-modern.517ec28b.js .https://joomag.com/.o%./.....2.....P.....W.....@....g.8.|"p.ew-...A..Eo.....(.....A..Eo.....o%./.....P.....W.....@....g.8.|"p.ew-...A..Eo.....PU.....o%./....C8BB778450CEB7894DD9260F9648DC275D2EE80AAC6046590483F0000930225C.P.....W.....@....g.8.|"p.ew-...A..Eo.....4.L.....o%./.....P.....W.....@....g.8.|"p.ew-...A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\abcc6ae9f8e1acb2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.473117870299715
Encrypted:	false
SSDEEP:	3:m+lesLA8RzYrSLyIKEKclEPVeuhVDftv5VtlHCPltl/x9v9R2UIq89koz4m+p5lH:mKYGLylluNeuPodtdvN+9kon8RK6t
MD5:	274A603E0E58B02A5EE860A318853C00
SHA1:	7D01AD048DBF21178AB49749156D4AEA35589352
SHA-256:	137AA8AC52C7419715CDF7707951FBC8DEBE79648B7D0536D50C261C037DE105
SHA-512:	98A8AF14B113D6BEA98B7DEAB67945BCE593EF145AC9003A3F5D060228ABE4CA38D01FD89065520D9DDFF99DDF8A4225522E74AEA1855E034FD5A295C3BE0AB6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\abcc6ae9f8e1acb2_0	
Preview:	0\r..m.....N....._keyhttps://www.joomag.com//static/locale/en.js?_=5.1.8.0 .https://joomag.com/..b%./.....Y.....k.v.Y.3...(....&..S..f..:B.`u..A..Eo.....DZ.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b2009de9dba4a7bb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	273
Entropy (8bit):	5.715376274639777
Encrypted:	false
SSDEEP:	6:mS4EYET08NWQASxYOno/Pd0PNbUwSXxn32Rl4gRK6t:b1g8NWQXnoHdVnxnG7Dr
MD5:	E0604EC4340D8CD8CE9FA275CEB591CD
SHA1:	660E333C65917E849EF1B941DD61737414134966
SHA-256:	6C03F67EB5A413C8B8A0B04F6510FCBE7BB558A3A54CB7314141CCB912572E72
SHA-512:	F0B98C5F52A3F1D06FA710051B634697544A1E8AD2A0C75B3F88F41464D9213388E02240A83ADF780D6EC3A6891360C73B2FF0A7EB68F4BFFDF7E349666783D7
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://cdnjs.cloudflare.com/ajax/libs/jquery-mousewheel/3.1.13/jquery.mousewheel.min.js?isAjax=true&_=1617996276252 .https://joomag.com/..n%./.....+g.....O.8.O.....Y.SIT...(...9O.[.w.A..Eo.....N.x.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b450020f7ef934d5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	255
Entropy (8bit):	5.920093035457789
Encrypted:	false
SSDEEP:	6:mxY4rgdsiQM+HMBr5miztU+GfSkh+4MAnK6t:y7Gme9mJ+GfSkh+7Ap
MD5:	A014C91D1D6EC220CFE3B5D6969D66C6
SHA1:	A24F4D30DEF4F41E79D7D5F37EC93F64F51E4533
SHA-256:	FC3EDD1D0537AC09933A416CEE79BDDC4DDE2DF2A8CB5EE8377890252F131A6B
SHA-512:	FFE2A56AE8EA2645F1EB714FB2D1174F35A382D8859B693909CE38AD96C4818CE207822C1B99EF3EFD5B681432D5DED3062FDCA8706C24BE6FB39BD09FD503 4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....{...v+.3...._keyhttps://s.adroll.com/pixel/7S36S2RHW5BUVAXH6L4RZE/6TMQVXNPWBG6BOGAF3EFID/WN42DWEAGNDBBGFACV55I7.js .https://joom ag.com/\..h%./.....'.....v.T.W.Qp.~.u.Y...k..&..A..Eo.....6%.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b63b937d58459cf2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	273
Entropy (8bit):	5.765371661056424
Encrypted:	false
SSDEEP:	6:mfEYET08NWQASxYOno/Pd0PP7NpJ0v6TvzDZLGp4/K6t:o0g8NWQXnoHd4nevUD1GpW
MD5:	7904EAA3C634616B03FA1B33D32AB1A7
SHA1:	1DB76D7D15B0CD4F650DB2C214D4D79541475BE3
SHA-256:	A79A99B2F460C8E3906364CDBB55AC0599F551249AA9151FE87563FF9CE7FC05
SHA-512:	91AC8ABB6BDDC310826EDEB79E55058D33DECB3F0C2C12B68BB1E44E29505EA4A4A5B8F31B9C80A89429A3178ADCD73DE2B65CC50E615FADF93830D1D908 A0B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....J`TL...._keyhttps://cdnjs.cloudflare.com/ajax/libs/jquery-mousewheel/3.1.13/jquery.mousewheel.min.js?isAjax=true&_=1617996257425 .https://joomag .com/...m%./.....u#....a..q.....K....3i.b...A..Eo.....<.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b6d41f41415a5d23_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.6651376506804905
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b6d41f41415a5d23_0	
SSDEEP:	3:m+lFtC8RzYrSLSELDXZCLRZLtmOv/tlHCl4h/t2spOWNhvCi+1U16RmUqhl/lpK+:mqPYGLSmXZCLRFpyQIzXvR6AhnK6t
MD5:	6495263A9CCFB7A90AC648B1C406C640
SHA1:	0F7D1F0682A8079318B030AB47598DA9A0242693
SHA-256:	0148E57431F08F2C071D0C16DC922E8F11E7785A5DB9F4E042D2454344EED700
SHA-512:	57F13DE3E2BDE63BD71CFFFF22959DC6793CC46E034520BCD7E84D382811ED9D13B05940AED1A85135293D281A1315292CBB25F5F424C8CFC5FE52094626BA4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O....z.o...._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-KDXRF52 .https://joomag.com/9X.b%./.....SL..L..<H.h....|..3....-#.....A..Eo.....+`.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b8d56c7282a9959b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	366
Entropy (8bit):	5.873115677378245
Encrypted:	false
SSDEEP:	6:mE8YAWGUJ3XXCzFvNpOADtr8/4ZprdVkDK6tcSK2lJvwrC4PvQ/4ZprCl:JdipvDrQgZpxSOUPvQQgZp
MD5:	993AE2083397D34A4CFAECADC1DEE7AA
SHA1:	BA1316BAC6C3AE8A06591012C59D6136A1FCAE4C
SHA-256:	99D1D6FE2148F05D9908438A9DB84B646FAD777B5863BBE2BE4AAB1C5968113C
SHA-512:	4E9DEE9496DBF931610DCE8B9752620B6650ED84EE603ED9E3D8EC1C29E96B58B1D01666E644BFBE11CAF4EA3D1DF5C4C8ED94204FF1857B187FCAF4B3B0CB5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f.....8...._keyhttps://connect.facebook.net/signals/config/290226788268586?v=2.9.33&r=stable .https://joomag.com/...h%./.....n.d.iT..+6..N.....A..Eo.....5.p.....A..Eo.....h%./.....7DACA0907AB9F2860DFD05745591E9C3C22DA13D8576600873CA502753ADFFDD.....n.d.iT..+6..N.....A..Eo.....vkiL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b9c9b6043be491b2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	240
Entropy (8bit):	5.504248670674005
Encrypted:	false
SSDEEP:	6:mf/lXYET08NaYWbVOqZvGAGXkrqye1FRYa9J04JsRK6t:0/Ng8NaY8ZeAAmIE1
MD5:	C9E71601E43FF094B979AAD874D3FC8E
SHA1:	6D8F02154B4FABE504968F64BA23FAEA9923609C
SHA-256:	6EC08A36E9CAF8AC00B225198BFD49681736ED3FB75EF40A06D596FB533D12B6
SHA-512:	665C08BC199743AF0B5F4295C3CA11DCBBB833109FF7A0F127D637F52E1B586608E25113033CB0919BAF9E0E8C1DCAF5903D2B92A5413D9E3272DA049C448BC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....l....F....._keyhttps://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js .https://theicecreamqueen.net/. m%./..... .....}...bp>("..IH..{..<.T....?"..T..A..Eo.....v:.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bce8477a65cd8197_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	335
Entropy (8bit):	5.891805411913403
Encrypted:	false
SSDEEP:	6:mw5YAWQf2574YZ0t+1hKyGxqTH4HOtbK6tH9YyJw3KyGxqTH4v:dLe5E3+/dmqTHXNp9YjdmqTHS
MD5:	38361DA643A02AF7CBB828E1E208F1CB
SHA1:	AF548B8E466F0C488721A7C8153B6229A43458CD
SHA-256:	52BCEEC8BD594A463A0DF854C5D3F6AB7997972A299BBF7015DC33633541AF0A
SHA-512:	1787D632409846AE0C793A9809E918F8CD71FF84DD89EFDBEA5ECA0EB9A9FA0F4ABE90B96CED6B65BCD4353F68378E0769E7D4B151B7E545AF8A8FAD65095C6A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....G...<t$r...._keyhttps://connect.facebook.net/en_US/fbevents.js .https://joomag.com/.k.h%./.....N.PSy.o....". .(u....$Ty..../.A..Eo.....{.#T.....A..Eo.....k.h%./.....09B1AA11C2005038CD981BE279116E954CC01CFA96798BCC216747131820F437.N.PSy.o....". .(u....$Ty..../.A..Eo.....x.(.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\be0d93bfbf442987_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	202
Entropy (8bit):	5.476412458253223
Encrypted:	false
SSDEEP:	3:m+lCQl/gOA8RzYrSLLiMIwJJSftsp1+9tlHCm/l/mWY6ruGVHuidkoMmyrlpK5kt:mCYGL+MIwJJaep1+Am/luIrmgnIK6t
MD5:	21F96CB02D921CE24E406E75631EFF2A
SHA1:	954656DB293215F65ACDABE33EF085071BF47BF8
SHA-256:	52E4A3373B16AA64D62A877355C96D2B799CA1C5A75E25A0A48B4371182B7689
SHA-512:	B20D9BCB0B91E8C8BE10C22494F569E787837086B459BAFE1BADE5F001558E16681D0F011C7ACD942CE503CDC82873E7912DEBC305089D1E450B7422C682F05
Malicious:	false
Reputation:	low
Preview:	0\r..m.....F.....+...._keyhttps://www.google-analytics.com/analytics.js .https://joomag.com/.L.b%./.....}.....3{...T.k.._..l.K..X.....W.....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c0b2aab84f0a50bc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	46709
Entropy (8bit):	5.732554792891765
Encrypted:	false
SSDEEP:	768:ttLaUC8FShvn8skXEQqmw4qneVyCoWIOE:ttibWEQqmwVnHCoWHE
MD5:	639D62A7D3CAE48F8A3C5DABAE886FED
SHA1:	BE49C481275F82974C0016F469568E5BD5C17D58
SHA-256:	46680E109A2CBACC55E4C11ADD2EC91FAE568B806E805C4F6B87D8E61761A570
SHA-512:	5D5F216A3EBEB23D097A0F88D39D28293F353B06AA8B24AEFBBF0C268F1015B59100B6902BEAB963433A50D2F8EB86750FBA2CCE1AE98914D23B92B1067BCA7C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....E.....Y....._keyhttps://js-agent.newrelic.com/nr-1208.min.js .https://joomag.com/}.9h%./...../.....M.c.6....R...6#.....D...#.....A..Eo.....A/2.....A..Eo.....'.dz....O.....!.....(S.....`.....].L`.....(S.h.`.....L`.....HRc .....Qb.i.....t.....Qb.2Ay....n.....Qb~..9....r.....Qb. ../....o...c....$.....I`....Da....8....(S...`.....,L`.....4Rc.....Qb.?.....e...`$.....`....Da6.....Q...Q.Pn..y...__nr_require.... Qf:..j....Cannot find module '..QbrT8....'.....a... .....Q.@.S.....exports....a.....Qb.....call..1&.(S.P.`\...]..K`....Dn.....&...*..&...*..&.%.*..&.....&.%...%.&.]....,Rc.....I`....Da....<.....#....c..... .....@.-....8P .....,...https://js-agent.newrelic.com/nr-1208.min.jsa.....D`....D`X...D`.....`....&...&....&..q.&...&&.(S.,..`.....L`.....(S.x.`....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c0ec2433cf77f682_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	13251
Entropy (8bit):	5.7950157997973415
Encrypted:	false
SSDEEP:	192:K8SHtBI6FDvnaYNoRxqKWArQhNmH0IDawtoALz8hqfvM4D2ZTVUb3:d6FbahRVmhkUIXCqfFaTVUb3
MD5:	A2F1B00A8CABC6323C56BF7CDE9D431D
SHA1:	707E2D20E83BA2FF3F41E895A17590B00A18CBA0
SHA-256:	067C2AEBBB606E8DF758168EEF832BF31C8C7BEF50C2A2C84C6F5DEA56D7F661
SHA-512:	F174868041F536217F5799FE6A2B84DF8561E2F90CF832AC25BC5110450C64B05F464BBB87E7B007D55C8CBEE1A21A8D7AE21C0BE6B7A5720C19F76B65443E1C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....;...3.i...._keyhttps://use.typekit.net/olb8zpk.js .https://joomag.com/.W,h%./.....;4.u...}.6.....a...D..''d../..A..Eo.....r.rg.....A..Eo.....'..F....O....X2....w.....$.....(S.d..`.....$L`.....Qc.....window....Q.@.a.....Typekit.....a>.....M...QcP.>.....1029652...Qb.^K.....c.....`.....M`.....Qe.....tk-proxima-nova.(Qh6..K....''proxima-nova'',sans-serif.....Qb&.&.....fi.....`..... Mf.....V...Z...^....*....Qb..._....fc.....`..... L`.....,a.....Qb.....id..`.....Qc^.....family....Qd''.....proxima-nova..Qb...;....src..lQy.#.._...https://use.typekit.net/af/1eef01/00000000000000000000148ac/23/{format}{?primer,subset_id,fvd,v}...Qd..Z.....descriptors...,a.....Qc..c.....weight....Qb.....900..q..!...Qc... ....display.....Qd.;.....subset_id...`.....,a.....`.....Q.....lQy..+._...https://use.typekit.net/af/bc719c/00000000000000001499c/23/{f

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c1a5eee687c36bec_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	742
Entropy (8bit):	5.779764135104783
Encrypted:	false
SSDEEP:	12:OE3xvLoux2pmYyyQL13CMxGDP7JsxSNg48meqkhNGICdDSsUXT:OEBv8uyRyyQL1SXDTzgdqkbCdusUD

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c1a5eee687c36bec_0

MD5:	2E01F85B00042C310490EBCF641BB709
SHA1:	D59662943DB011EC7C5091DB063EB7B5FE260A1C
SHA-256:	F5280BF296023D46695663AC7E65D9734B0A155BF697F16AD6FFF93489FC8A09
SHA-512:	4E2B14E93EE9BF3F8F3456FE56B1CE267D9831DB311A20A19EE80326AA3DAF89BB33CF020E4D83BE36BA7187DBC0CC86951A6DEB36DA52148A37501355D73E1
Malicious:	false
Reputation:	low
Preview:	0\r..m......b...>..c...._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/1003757157/?random=1617996237276&cv=9&fst=1617996237276&num=1&bg=ffffff&guid=ON&resp=GooglemKTybQhCsO&eid=2505059651&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=120&u_java=false&u_nplug=1&u_nmime=2&gtm=2oa3v0&sendb=1&ig=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fwww.joomag.com%2F%3Fref%3Dviewer_ad%26utm_source%3Dviewer_ad_create%26utm_medium%3Dnon-paid%26utm_campaign%3Djm_leads&tiba=Digital%20Publishing%20Platform%20for%20Everyone%20%7C%20Joomag&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://joomag.com/.^jl%./.....................C.IU...$2....L..u...4./.H....T.A..Eo......RA...........A..Eo..................

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c243fa307356206a_0

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	31774
Entropy (8bit):	5.812441671454958
Encrypted:	false
SSDEEP:	384:Xltt4H6iIRTpOkNL6wzd2MG5UTfnoL/3iyiFJjeAG29mu4ZZIEBL:Xlt6H63RTxfzwMdTfoLiXJtMnIE
MD5:	50FD465A91CC44EE4E52CA87F6242960
SHA1:	48F80923C5FAC957207B9E7D4CCBFBA596B73543
SHA-256:	0DD464E1ECF1FF1236782F3E1D6669B1D3847279BABEA489C337F24F43ACEB1F
SHA-512:	882B036A5BEA49694E9C67C0CF8DE7D18B623DA0AA283EA5D7647A3779D7C14113D4A53F93D5F5ADE81B6A377A6CFCF5C503E11178ADB507D04E002733035E 6
Malicious:	false
Reputation:	low
Preview:	0\r..m......R...}.(1...._keyhttps://js.intercomcdn.com/vendors~app-modern.4c248a1f.js .https://joomag.com/s..o%./.............z.......G.o...U.e.7...h.j.ll....P...l@...A..Eo...................A..Eo..............................'.......O.....y...J..(S.....`.....!.L`......Qc........window....Q.P..~.....webpackJsonp..Qb... ....push.....`......L`.......`......Ma....`...`.........b............C`....C`....C`....C`....C`....C`....C`....C`....C`....C`"...C`$...C`(...C`H...C`^...C``...C`b...C`d...C`f...C`h...C`j...C`....C`....C`..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c32afd9997a26c41_0

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.468250726368395
Encrypted:	false
SSDEEP:	6:mgPYlNYpSVkyGAGXkr0Xx16Nwl5blfkb4jK6t:/pSVOAAmCLRMa
MD5:	82A39189DB6617AA30C27F84FC3006C3
SHA1:	BE93C80F64EA19167A570A65A84CE72D4409122B
SHA-256:	FD5783C96B3A3B27A833D5CDDAF3E3FBE05FF06B9A0ED26BD65A6BADE3C4C583
SHA-512:	C1E2F6C539D825D9EB4A0801BEC9C2F448F96AFF8FE8B7380B35DACF55EA213968C8C21BCD9D072BA52CFE10633F9DF1004524C450B621A4412D0A64CA489D8
Malicious:	false
Reputation:	low
Preview:	0\r..m......L...f......._keyhttps://kit.fontawesome.com/585b051251.js .https://theicecreamqueen.net/...m%./.............L...........X...\.%.).+......Lnd.@.C..A..Eo.......!.&.........A..Eo.................

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c5aafbc7a17c355c_0

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	559992
Entropy (8bit):	6.237218427355762
Encrypted:	false
SSDEEP:	6144:i/IbcEcASGxaFiR6XcbuVNDw3XpAxQ1OGj9LK8pLN8QAH0:EyjLATSSNGp9LrE0
MD5:	31670169E5F0747798958E31A48B26E2
SHA1:	857C7334A81841F253D0FD9C2FD02AC8EF1CFF52
SHA-256:	2EF953460DA4659274AEE4958624C03F5B419B648D92A12D683FF88DDEC72696
SHA-512:	B70163F0429A1554A812593F620DE222F9A88967D8AEAE564F2695D5B81DAB612330CC3999D3CC7E13EDB57A653A0C521F1F4F88DC5E417F3F398D5C5788F2F
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c5aafbc7a17c355c_0	
Reputation:	low
Preview:	0\r..m.....@...D.w3....6A8564BF832B626C3EA2EC37C4F591ECAB1B1BF1B2863B39D969A05F2F4510D6.....'.w$....O....@...<b.\|.....`....2..... ..... .....\&.....D.....p.....X.....D..... .....4...<.....$.....L.....\.....L..... ....H...@.....(S.....`,....E.L`.....Qc..Kf....window....Q.P..:"....webpackJsonp..Qb".k,....push.....`.....L`.....`.....Ma.....`.....Qc.....concat.....`..... ..LaN.....E`.....Ec.....E`....Ec.....Ef.....E`..

Static File Info

No static file info

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 21:23:43.768594980 CEST	49745	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:43.769243956 CEST	49746	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:43.847744942 CEST	49748	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:43.862880945 CEST	443	49745	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:43.863776922 CEST	443	49746	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:43.863807917 CEST	49745	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:43.863867998 CEST	49746	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:43.864033937 CEST	49745	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:43.864207029 CEST	49746	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:43.944385052 CEST	443	49748	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:43.944514036 CEST	49748	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:43.944730997 CEST	49748	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:43.960165977 CEST	443	49746	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:43.960207939 CEST	443	49745	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:43.961122990 CEST	443	49745	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:43.961168051 CEST	443	49745	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:43.961205959 CEST	443	49745	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:43.961232901 CEST	443	49745	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:43.961275101 CEST	49745	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:43.961304903 CEST	49745	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:43.978663921 CEST	443	49745	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:43.978781939 CEST	443	49745	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:43.978857994 CEST	49745	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:43.979263067 CEST	443	49746	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:43.979305983 CEST	443	49746	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:43.979343891 CEST	443	49746	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:43.979372025 CEST	443	49746	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:43.979420900 CEST	49746	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:43.979448080 CEST	49746	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:43.997793913 CEST	443	49746	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:43.997831106 CEST	443	49746	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:43.997904062 CEST	49746	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:44.017954111 CEST	49745	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:44.018501043 CEST	49746	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:44.018644094 CEST	49746	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:44.018824100 CEST	49745	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:44.019201994 CEST	49745	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:44.039777994 CEST	443	49748	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.039822102 CEST	443	49748	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.039904118 CEST	443	49748	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.039947033 CEST	443	49748	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.039974928 CEST	443	49748	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.039979935 CEST	49748	443	192.168.2.4	209.95.50.27

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 21:23:44.040040016 CEST	49748	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:44.053837061 CEST	443	49748	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.053889036 CEST	443	49748	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.053968906 CEST	49748	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:44.054775953 CEST	49748	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:44.112488031 CEST	443	49745	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.112862110 CEST	443	49745	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.112981081 CEST	49745	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:44.113118887 CEST	49745	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:44.113439083 CEST	443	49746	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.113473892 CEST	443	49746	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.113498926 CEST	443	49745	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.113533974 CEST	443	49746	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.113583088 CEST	49746	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:44.113615036 CEST	49746	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:44.131721020 CEST	443	49745	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.134072065 CEST	49745	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:44.149349928 CEST	443	49748	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.149637938 CEST	443	49748	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.149671078 CEST	443	49748	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.149753094 CEST	49748	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:44.158155918 CEST	49753	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:44.251312017 CEST	443	49745	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.252943993 CEST	443	49753	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.253129005 CEST	49753	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:44.253305912 CEST	49753	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:44.347878933 CEST	443	49753	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.348484039 CEST	443	49753	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.348517895 CEST	443	49753	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.348541975 CEST	443	49753	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.348557949 CEST	443	49753	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.348613024 CEST	49753	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:44.348654032 CEST	49753	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:44.350863934 CEST	443	49753	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.350893021 CEST	443	49753	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.350967884 CEST	49753	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:44.407079935 CEST	49753	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:44.407218933 CEST	49753	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:44.407447100 CEST	49753	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:44.502113104 CEST	443	49753	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.502346992 CEST	443	49753	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.502367020 CEST	443	49753	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.502470016 CEST	443	49753	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.502512932 CEST	49753	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:44.502856970 CEST	49753	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:44.533164024 CEST	443	49753	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.533198118 CEST	443	49753	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.533217907 CEST	443	49753	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.533237934 CEST	443	49753	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.533273935 CEST	443	49753	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.533293009 CEST	443	49753	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.533314943 CEST	443	49753	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.533338070 CEST	443	49753	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.533359051 CEST	443	49753	209.95.50.27	192.168.2.4
Apr 9, 2021 21:23:44.533365011 CEST	49753	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:44.533416986 CEST	49753	443	192.168.2.4	209.95.50.27
Apr 9, 2021 21:23:44.533423901 CEST	49753	443	192.168.2.4	209.95.50.27

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 9, 2021 21:23:43.595530033 CEST	192.168.2.4	8.8.8.8	0xb3d7	Standard query (0)	joom.ag	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:44.141838074 CEST	192.168.2.4	8.8.8.8	0xa2ec	Standard query (0)	viewer.joomag.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 9, 2021 21:23:44.604124069 CEST	192.168.2.4	8.8.8.8	0x2bcc	Standard query (0)	www.joomag.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:44.605923891 CEST	192.168.2.4	8.8.8.8	0xe71	Standard query (0)	browser.sentry-cdn.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:45.696775913 CEST	192.168.2.4	8.8.8.8	0x5651	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:46.116576910 CEST	192.168.2.4	8.8.8.8	0xf22d	Standard query (0)	www.google.ch	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:46.288826942 CEST	192.168.2.4	8.8.8.8	0x93b2	Standard query (0)	use.typekit.net	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:46.613571882 CEST	192.168.2.4	8.8.8.8	0xf4ec	Standard query (0)	s9.joomag.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:46.670409918 CEST	192.168.2.4	8.8.8.8	0xc5b4	Standard query (0)	p.typekit.net	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:47.182848930 CEST	192.168.2.4	8.8.8.8	0x76c7	Standard query (0)	js-agent.newrelic.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:47.227894068 CEST	192.168.2.4	8.8.8.8	0xb9c3	Standard query (0)	an3.joomag.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:47.310935020 CEST	192.168.2.4	8.8.8.8	0xb375	Standard query (0)	bam-cell.nr-data.net	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:47.722717047 CEST	192.168.2.4	8.8.8.8	0x68e	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:47.986970901 CEST	192.168.2.4	8.8.8.8	0xaaaf	Standard query (0)	www.joomag.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:52.036037922 CEST	192.168.2.4	8.8.8.8	0x60f0	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:52.592138052 CEST	192.168.2.4	8.8.8.8	0xff60	Standard query (0)	js.hs-scripts.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:52.592192888 CEST	192.168.2.4	8.8.8.8	0x7d12	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:52.594890118 CEST	192.168.2.4	8.8.8.8	0xba0a	Standard query (0)	s.adroll.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:52.746912956 CEST	192.168.2.4	8.8.8.8	0xaf4f	Standard query (0)	d.adroll.mgr.consensu.org	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:53.044053078 CEST	192.168.2.4	8.8.8.8	0x5048	Standard query (0)	d.adroll.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:53.044378996 CEST	192.168.2.4	8.8.8.8	0xd1d	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:53.749232054 CEST	192.168.2.4	8.8.8.8	0x9eb4	Standard query (0)	js.hsleadflows.net	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:53.749855042 CEST	192.168.2.4	8.8.8.8	0xb9a6	Standard query (0)	js.hs-banner.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:53.750500917 CEST	192.168.2.4	8.8.8.8	0xa400	Standard query (0)	js.hs-analytics.net	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:53.751137972 CEST	192.168.2.4	8.8.8.8	0xf3c2	Standard query (0)	js.hsadspixel.net	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.542772055 CEST	192.168.2.4	8.8.8.8	0x91ba	Standard query (0)	pixel.advertising.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.544234037 CEST	192.168.2.4	8.8.8.8	0x23a7	Standard query (0)	dsum-sec.casalemedia.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.546933889 CEST	192.168.2.4	8.8.8.8	0x890c	Standard query (0)	pixel.rubiconproject.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.548218966 CEST	192.168.2.4	8.8.8.8	0x724f	Standard query (0)	sync.outbrain.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.549491882 CEST	192.168.2.4	8.8.8.8	0xa30a	Standard query (0)	ads.yahoo.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.609191895 CEST	192.168.2.4	8.8.8.8	0xe017	Standard query (0)	simage2.pubmatic.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.617549896 CEST	192.168.2.4	8.8.8.8	0x6be8	Standard query (0)	sync.taboola.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.620064974 CEST	192.168.2.4	8.8.8.8	0x7d15	Standard query (0)	eb2.3lift.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.622607946 CEST	192.168.2.4	8.8.8.8	0x36ad	Standard query (0)	x.bidswitch.net	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.624809980 CEST	192.168.2.4	8.8.8.8	0xe51a	Standard query (0)	ib.adnxs.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.626497030 CEST	192.168.2.4	8.8.8.8	0x42c4	Standard query (0)	us-u.openx.net	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:55.847058058 CEST	192.168.2.4	8.8.8.8	0xe51a	Standard query (0)	ib.adnxs.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:55.847124100 CEST	192.168.2.4	8.8.8.8	0x36ad	Standard query (0)	x.bidswitch.net	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:55.847136974 CEST	192.168.2.4	8.8.8.8	0x7d15	Standard query (0)	eb2.3lift.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 9, 2021 21:23:55.961056948 CEST	192.168.2.4	8.8.8.8	0x7f09	Standard query (0)	idsync.rlcdn.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:55.963073969 CEST	192.168.2.4	8.8.8.8	0x1316	Standard query (0)	cm.g.doubleclick.net	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:56.465755939 CEST	192.168.2.4	8.8.8.8	0x7468	Standard query (0)	ups.analytics.yahoo.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:56.988560915 CEST	192.168.2.4	8.8.8.8	0xa271	Standard query (0)	track.hubspot.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:56.990151882 CEST	192.168.2.4	8.8.8.8	0xe382	Standard query (0)	api.hubapi.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:57.004674911 CEST	192.168.2.4	8.8.8.8	0x798	Standard query (0)	rum.monitis.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:57.008038044 CEST	192.168.2.4	8.8.8.8	0x8937	Standard query (0)	widget.intercom.io	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:57.021375895 CEST	192.168.2.4	8.8.8.8	0x2493	Standard query (0)	forms.hubspot.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:57.122914076 CEST	192.168.2.4	8.8.8.8	0x3bc1	Standard query (0)	js.intercomcdn.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:57.482604027 CEST	192.168.2.4	8.8.8.8	0x7b3b	Standard query (0)	api-iam.intercom.io	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:57.573492050 CEST	192.168.2.4	8.8.8.8	0xe314	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:57.779489994 CEST	192.168.2.4	8.8.8.8	0xf3e1	Standard query (0)	d.adroll.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:58.690859079 CEST	192.168.2.4	8.8.8.8	0x2fa4	Standard query (0)	nexus-websocket-a.intercom.io	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:00.304374933 CEST	192.168.2.4	8.8.8.8	0xdd4e	Standard query (0)	northcentralusr-notifyp.svc.ms	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:02.367439985 CEST	192.168.2.4	8.8.8.8	0xb336	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:02.371035099 CEST	192.168.2.4	8.8.8.8	0x27d7	Standard query (0)	assets.onestore.ms	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:06.312427044 CEST	192.168.2.4	8.8.8.8	0xe283	Standard query (0)	theicecreamqueen.net	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:07.675744057 CEST	192.168.2.4	8.8.8.8	0xd842	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:07.678323030 CEST	192.168.2.4	8.8.8.8	0x1474	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:07.681094885 CEST	192.168.2.4	8.8.8.8	0x8789	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:09.225282907 CEST	192.168.2.4	8.8.8.8	0x54b9	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:11.772816896 CEST	192.168.2.4	8.8.8.8	0x87fa	Standard query (0)	theicecreamqueen.net	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.083446026 CEST	192.168.2.4	8.8.8.8	0x34b4	Standard query (0)	pixel.advertising.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.084237099 CEST	192.168.2.4	8.8.8.8	0x707	Standard query (0)	dsum-sec.casalemedia.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.205085039 CEST	192.168.2.4	8.8.8.8	0x426e	Standard query (0)	pixel.rubiconproject.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.211801052 CEST	192.168.2.4	8.8.8.8	0x9503	Standard query (0)	ups.analytics.yahoo.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.215095043 CEST	192.168.2.4	8.8.8.8	0xb02f	Standard query (0)	sync.outbrain.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.326809883 CEST	192.168.2.4	8.8.8.8	0xbc22	Standard query (0)	simage2.pubmatic.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.343965054 CEST	192.168.2.4	8.8.8.8	0xc4e7	Standard query (0)	ads.yahoo.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.450757980 CEST	192.168.2.4	8.8.8.8	0x7cac	Standard query (0)	sync.taboola.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.465143919 CEST	192.168.2.4	8.8.8.8	0x4a52	Standard query (0)	eb2.3lift.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.566205978 CEST	192.168.2.4	8.8.8.8	0x29d0	Standard query (0)	x.bidswitch.net	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.689348936 CEST	192.168.2.4	8.8.8.8	0x231b	Standard query (0)	idsync.rlcdn.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.808912992 CEST	192.168.2.4	8.8.8.8	0x59c	Standard query (0)	us-u.openx.net	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.828532934 CEST	192.168.2.4	8.8.8.8	0x1d2d	Standard query (0)	ib.adnxs.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.931225061 CEST	192.168.2.4	8.8.8.8	0xdf35	Standard query (0)	cm.g.doubleclick.net	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:49.186388016 CEST	192.168.2.4	8.8.8.8	0xd831	Standard query (0)	www.joomag.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 9, 2021 21:24:49.187026978 CEST	192.168.2.4	8.8.8.8	0xe2d2	Standard query (0)	use.typekit.net	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:51.960472107 CEST	192.168.2.4	8.8.8.8	0x8175	Standard query (0)	bam-cell.nr-data.net	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:55.528873920 CEST	192.168.2.4	8.8.8.8	0x9d64	Standard query (0)	static.intercomassets.com	A (IP address)	IN (0x0001)
Apr 9, 2021 21:25:57.907912016 CEST	192.168.2.4	8.8.8.8	0xbaaa	Standard query (0)	nexus-websocket-a.intercom.io	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 9, 2021 21:23:43.767710924 CEST	8.8.8.8	192.168.2.4	0xb3d7	No error (0)	joom.ag		209.95.50.27	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:44.156253099 CEST	8.8.8.8	192.168.2.4	0xa2ec	No error (0)	viewer.joomag.com	lb.joomag.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:44.156253099 CEST	8.8.8.8	192.168.2.4	0xa2ec	No error (0)	lb.joomag.com		209.95.50.27	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:44.618549109 CEST	8.8.8.8	192.168.2.4	0xe71	No error (0)	browser.sentry-cdn.com		151.101.66.217	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:44.618549109 CEST	8.8.8.8	192.168.2.4	0xe71	No error (0)	browser.sentry-cdn.com		151.101.130.217	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:44.618549109 CEST	8.8.8.8	192.168.2.4	0xe71	No error (0)	browser.sentry-cdn.com		151.101.2.217	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:44.618549109 CEST	8.8.8.8	192.168.2.4	0xe71	No error (0)	browser.sentry-cdn.com		151.101.194.217	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:44.625566959 CEST	8.8.8.8	192.168.2.4	0x2bcc	No error (0)	www.joomag.com	lb.joomag.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:44.625566959 CEST	8.8.8.8	192.168.2.4	0x2bcc	No error (0)	lb.joomag.com		209.95.50.27	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:45.723650932 CEST	8.8.8.8	192.168.2.4	0x5651	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:45.723650932 CEST	8.8.8.8	192.168.2.4	0x5651	No error (0)	stats.l.doubleclick.net		74.125.143.157	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:45.723650932 CEST	8.8.8.8	192.168.2.4	0x5651	No error (0)	stats.l.doubleclick.net		74.125.143.155	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:45.723650932 CEST	8.8.8.8	192.168.2.4	0x5651	No error (0)	stats.l.doubleclick.net		74.125.143.154	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:45.723650932 CEST	8.8.8.8	192.168.2.4	0x5651	No error (0)	stats.l.doubleclick.net		74.125.143.156	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:46.129996061 CEST	8.8.8.8	192.168.2.4	0xf22d	No error (0)	www.google.ch		216.58.215.227	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:46.307245970 CEST	8.8.8.8	192.168.2.4	0x93b2	No error (0)	use.typekit.net	use-stls.adobe.com.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:46.626341105 CEST	8.8.8.8	192.168.2.4	0xf4ec	No error (0)	s9.joomag.com		107.182.226.40	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:46.688163042 CEST	8.8.8.8	192.168.2.4	0xc5b4	No error (0)	p.typekit.net	p.typekit.net-v3.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:47.195719957 CEST	8.8.8.8	192.168.2.4	0x76c7	No error (0)	js-agent.newrelic.com	f4.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:47.242810011 CEST	8.8.8.8	192.168.2.4	0xb9c3	No error (0)	an3.joomag.com		209.95.50.25	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:47.329777002 CEST	8.8.8.8	192.168.2.4	0xb375	No error (0)	bam-cell.nr-data.net	tls12.newrelic.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 9, 2021 21:23:47.750629902 CEST	8.8.8.8	192.168.2.4	0x68e	No error (0)	clients2.google usercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:47.750629902 CEST	8.8.8.8	192.168.2.4	0x68e	No error (0)	googlehosted.l.googleusercontent.com		172.217.168.33	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:48.002032042 CEST	8.8.8.8	192.168.2.4	0xaaaf	No error (0)	www.joomag.com	lb.joomag.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:48.002032042 CEST	8.8.8.8	192.168.2.4	0xaaaf	No error (0)	lb.joomag.com		209.95.50.27	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:52.054482937 CEST	8.8.8.8	192.168.2.4	0x60f0	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:52.054482937 CEST	8.8.8.8	192.168.2.4	0x60f0	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:52.610811949 CEST	8.8.8.8	192.168.2.4	0x7d12	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:52.610811949 CEST	8.8.8.8	192.168.2.4	0x7d12	No error (0)	scontent.xx.fbcdn.net		157.240.17.15	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:52.612402916 CEST	8.8.8.8	192.168.2.4	0xff60	No error (0)	js.hs-scripts.com		104.17.214.204	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:52.612402916 CEST	8.8.8.8	192.168.2.4	0xff60	No error (0)	js.hs-scripts.com		104.17.212.204	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:52.612402916 CEST	8.8.8.8	192.168.2.4	0xff60	No error (0)	js.hs-scripts.com		104.17.211.204	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:52.612402916 CEST	8.8.8.8	192.168.2.4	0xff60	No error (0)	js.hs-scripts.com		104.17.213.204	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:52.612402916 CEST	8.8.8.8	192.168.2.4	0xff60	No error (0)	js.hs-scripts.com		104.17.210.204	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:52.614744902 CEST	8.8.8.8	192.168.2.4	0xba0a	No error (0)	s.adroll.com	wildcard.adroll.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:52.779445887 CEST	8.8.8.8	192.168.2.4	0xaf4f	No error (0)	d.adroll.mgr.consensu.org	d.adroll.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:52.779445887 CEST	8.8.8.8	192.168.2.4	0xaf4f	No error (0)	d.adroll.com	adserver-vpc-alb-3-890571764.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:52.779445887 CEST	8.8.8.8	192.168.2.4	0xaf4f	No error (0)	adserver-vpc-alb-3-890571764.eu-west-1.elb.amazonaws.com		3.248.28.111	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:52.779445887 CEST	8.8.8.8	192.168.2.4	0xaf4f	No error (0)	adserver-vpc-alb-3-890571764.eu-west-1.elb.amazonaws.com		54.195.19.148	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:53.058757067 CEST	8.8.8.8	192.168.2.4	0xd1d	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:53.058757067 CEST	8.8.8.8	192.168.2.4	0xd1d	No error (0)	star-mini.c10r.facebook.com		157.240.219.35	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:53.059573889 CEST	8.8.8.8	192.168.2.4	0x5048	No error (0)	d.adroll.com	adserver-vpc-alb-2-1264451658.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:53.059573889 CEST	8.8.8.8	192.168.2.4	0x5048	No error (0)	adserver-vpc-alb-2-1264451658.eu-west-1.elb.amazonaws.com		34.252.196.107	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 9, 2021 21:23:53.059573889 CEST	8.8.8.8	192.168.2.4	0x5048	No error (0)	adserver-vpc-alb-2-1264451658.eu-west-1.elb.amazonaws.com		54.74.23.153	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:53.771240950 CEST	8.8.8.8	192.168.2.4	0xb9a6	No error (0)	js.hs-banner.com		104.18.20.191	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:53.771240950 CEST	8.8.8.8	192.168.2.4	0xb9a6	No error (0)	js.hs-banner.com		104.18.21.191	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:53.772497892 CEST	8.8.8.8	192.168.2.4	0x9eb4	No error (0)	js.hsleadflows.net		104.17.230.204	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:53.772497892 CEST	8.8.8.8	192.168.2.4	0x9eb4	No error (0)	js.hsleadflows.net		104.17.234.204	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:53.772497892 CEST	8.8.8.8	192.168.2.4	0x9eb4	No error (0)	js.hsleadflows.net		104.17.232.204	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:53.772497892 CEST	8.8.8.8	192.168.2.4	0x9eb4	No error (0)	js.hsleadflows.net		104.17.231.204	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:53.772497892 CEST	8.8.8.8	192.168.2.4	0x9eb4	No error (0)	js.hsleadflows.net		104.17.233.204	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:53.772563934 CEST	8.8.8.8	192.168.2.4	0xf3c2	No error (0)	js.hsadspixel.net		104.17.114.176	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:53.772563934 CEST	8.8.8.8	192.168.2.4	0xf3c2	No error (0)	js.hsadspixel.net		104.17.116.176	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:53.772563934 CEST	8.8.8.8	192.168.2.4	0xf3c2	No error (0)	js.hsadspixel.net		104.17.112.176	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:53.772563934 CEST	8.8.8.8	192.168.2.4	0xf3c2	No error (0)	js.hsadspixel.net		104.17.113.176	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:53.772563934 CEST	8.8.8.8	192.168.2.4	0xf3c2	No error (0)	js.hsadspixel.net		104.17.115.176	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:53.773186922 CEST	8.8.8.8	192.168.2.4	0xa400	No error (0)	js.hs-analytics.net		104.17.68.176	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:53.773186922 CEST	8.8.8.8	192.168.2.4	0xa400	No error (0)	js.hs-analytics.net		104.17.67.176	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:53.773186922 CEST	8.8.8.8	192.168.2.4	0xa400	No error (0)	js.hs-analytics.net		104.17.70.176	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:53.773186922 CEST	8.8.8.8	192.168.2.4	0xa400	No error (0)	js.hs-analytics.net		104.17.71.176	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:53.773186922 CEST	8.8.8.8	192.168.2.4	0xa400	No error (0)	js.hs-analytics.net		104.17.69.176	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.557252884 CEST	8.8.8.8	192.168.2.4	0x91ba	No error (0)	pixel.advertising.com	prod.ups-adcom.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:54.557252884 CEST	8.8.8.8	192.168.2.4	0x91ba	No error (0)	prod.ups-adcom.aolp-ds-prd.aws.oath.cloud	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:54.557252884 CEST	8.8.8.8	192.168.2.4	0x91ba	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		18.197.99.6	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.557252884 CEST	8.8.8.8	192.168.2.4	0x91ba	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		52.28.254.214	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.557252884 CEST	8.8.8.8	192.168.2.4	0x91ba	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		35.156.106.231	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.557252884 CEST	8.8.8.8	192.168.2.4	0x91ba	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		18.184.153.186	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 9, 2021 21:23:54.557252884 CEST	8.8.8.8	192.168.2.4	0x91ba	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		52.59.28.101	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.557252884 CEST	8.8.8.8	192.168.2.4	0x91ba	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		3.126.63.176	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.557252884 CEST	8.8.8.8	192.168.2.4	0x91ba	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		52.59.102.119	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.557252884 CEST	8.8.8.8	192.168.2.4	0x91ba	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		35.156.153.71	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.562283993 CEST	8.8.8.8	192.168.2.4	0x724f	No error (0)	sync.outbrain.com	alldcs.outbrain.org		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:54.562283993 CEST	8.8.8.8	192.168.2.4	0x724f	No error (0)	alldcs.outbrain.org	chidc2.outbrain.org		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:54.562283993 CEST	8.8.8.8	192.168.2.4	0x724f	No error (0)	chidc2.outbrain.org		64.74.236.159	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.563925028 CEST	8.8.8.8	192.168.2.4	0x23a7	No error (0)	dsum-sec.casalemedia.com	dsum-sec.casalemedia.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:54.565227985 CEST	8.8.8.8	192.168.2.4	0xa30a	No error (0)	ads.yahoo.com	edge.gycpi.b.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:54.565227985 CEST	8.8.8.8	192.168.2.4	0xa30a	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.23	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.565227985 CEST	8.8.8.8	192.168.2.4	0xa30a	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.22	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.590061903 CEST	8.8.8.8	192.168.2.4	0x890c	No error (0)	pixel.rubiconproject.com	pixel.rubiconproject.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:54.622522116 CEST	8.8.8.8	192.168.2.4	0xe017	No error (0)	simage2.pubmatic.com	pug-lhrc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:54.622522116 CEST	8.8.8.8	192.168.2.4	0xe017	No error (0)	pug-lhrc.pubmatic.com	pug-lhr.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:54.622522116 CEST	8.8.8.8	192.168.2.4	0xe017	No error (0)	pug-lhr.pubmatic.com		185.64.190.80	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.633012056 CEST	8.8.8.8	192.168.2.4	0x7d15	No error (0)	eb2.3lift.com	eu-eb2.3lift.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:54.633012056 CEST	8.8.8.8	192.168.2.4	0x7d15	No error (0)	eu-eb2.3lift.com	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:54.633012056 CEST	8.8.8.8	192.168.2.4	0x7d15	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		3.121.70.57	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.633012056 CEST	8.8.8.8	192.168.2.4	0x7d15	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		52.57.162.23	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.633012056 CEST	8.8.8.8	192.168.2.4	0x7d15	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		18.184.39.197	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 9, 2021 21:23:54.633012056 CEST	8.8.8.8	192.168.2.4	0x7d15	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		18.158.85.202	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.633012056 CEST	8.8.8.8	192.168.2.4	0x7d15	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		3.120.52.49	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.633012056 CEST	8.8.8.8	192.168.2.4	0x7d15	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		3.124.88.100	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.633012056 CEST	8.8.8.8	192.168.2.4	0x7d15	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		3.122.89.158	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.633012056 CEST	8.8.8.8	192.168.2.4	0x7d15	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		18.157.239.120	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.635550022 CEST	8.8.8.8	192.168.2.4	0x36ad	No error (0)	x.bidswitch.net	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:54.635550022 CEST	8.8.8.8	192.168.2.4	0x36ad	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		18.158.181.33	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.635550022 CEST	8.8.8.8	192.168.2.4	0x36ad	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		52.29.191.126	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.635550022 CEST	8.8.8.8	192.168.2.4	0x36ad	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		52.28.196.155	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.635550022 CEST	8.8.8.8	192.168.2.4	0x36ad	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		35.157.221.90	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.635550022 CEST	8.8.8.8	192.168.2.4	0x36ad	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		35.158.179.12	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.635550022 CEST	8.8.8.8	192.168.2.4	0x36ad	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		3.120.52.76	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.635550022 CEST	8.8.8.8	192.168.2.4	0x36ad	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		52.28.120.199	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.635550022 CEST	8.8.8.8	192.168.2.4	0x36ad	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		52.58.146.86	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.637259960 CEST	8.8.8.8	192.168.2.4	0xe51a	No error (0)	ib.adnxs.com	g.geogslb.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 9, 2021 21:23:54.637259960 CEST	8.8.8.8	192.168.2.4	0xe51a	No error (0)	g.geogslb.com	ib.anycast.adnxs.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:54.637259960 CEST	8.8.8.8	192.168.2.4	0xe51a	No error (0)	ib.anycast.adnxs.com		185.33.221.89	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.637259960 CEST	8.8.8.8	192.168.2.4	0xe51a	No error (0)	ib.anycast.adnxs.com		185.33.223.178	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.637259960 CEST	8.8.8.8	192.168.2.4	0xe51a	No error (0)	ib.anycast.adnxs.com		185.33.221.90	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.637259960 CEST	8.8.8.8	192.168.2.4	0xe51a	No error (0)	ib.anycast.adnxs.com		185.33.220.243	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.637259960 CEST	8.8.8.8	192.168.2.4	0xe51a	No error (0)	ib.anycast.adnxs.com		185.33.220.244	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.637259960 CEST	8.8.8.8	192.168.2.4	0xe51a	No error (0)	ib.anycast.adnxs.com		185.33.220.241	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.637259960 CEST	8.8.8.8	192.168.2.4	0xe51a	No error (0)	ib.anycast.adnxs.com		185.33.221.15	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.637259960 CEST	8.8.8.8	192.168.2.4	0xe51a	No error (0)	ib.anycast.adnxs.com		185.33.221.53	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.637643099 CEST	8.8.8.8	192.168.2.4	0x6be8	No error (0)	sync.taboola.com	am-sync.taboola.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:54.637643099 CEST	8.8.8.8	192.168.2.4	0x6be8	No error (0)	am-sync.taboola.com	am-vip001.taboola.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:54.637643099 CEST	8.8.8.8	192.168.2.4	0x6be8	No error (0)	am-vip001.taboola.com		141.226.228.48	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.638844967 CEST	8.8.8.8	192.168.2.4	0x42c4	No error (0)	us-u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:54.638844967 CEST	8.8.8.8	192.168.2.4	0x42c4	No error (0)	us-u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:55.861896038 CEST	8.8.8.8	192.168.2.4	0xe51a	No error (0)	ib.adnxs.com	g.geogslb.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:55.861896038 CEST	8.8.8.8	192.168.2.4	0xe51a	No error (0)	g.geogslb.com	ib.anycast.adnxs.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:55.861896038 CEST	8.8.8.8	192.168.2.4	0xe51a	No error (0)	ib.anycast.adnxs.com		185.33.221.91	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:55.861896038 CEST	8.8.8.8	192.168.2.4	0xe51a	No error (0)	ib.anycast.adnxs.com		185.33.221.90	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:55.861896038 CEST	8.8.8.8	192.168.2.4	0xe51a	No error (0)	ib.anycast.adnxs.com		185.33.221.50	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:55.861896038 CEST	8.8.8.8	192.168.2.4	0xe51a	No error (0)	ib.anycast.adnxs.com		185.33.221.89	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:55.861896038 CEST	8.8.8.8	192.168.2.4	0xe51a	No error (0)	ib.anycast.adnxs.com		185.33.221.15	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:55.861896038 CEST	8.8.8.8	192.168.2.4	0xe51a	No error (0)	ib.anycast.adnxs.com		185.33.221.11	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:55.861896038 CEST	8.8.8.8	192.168.2.4	0xe51a	No error (0)	ib.anycast.adnxs.com		185.33.220.241	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:55.861896038 CEST	8.8.8.8	192.168.2.4	0xe51a	No error (0)	ib.anycast.adnxs.com		185.33.223.178	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:55.861943960 CEST	8.8.8.8	192.168.2.4	0x36ad	No error (0)	x.bidswitch.net	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 9, 2021 21:23:55.861943960 CEST	8.8.8.8	192.168.2.4	0x36ad	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		18.158.181.33	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:55.861943960 CEST	8.8.8.8	192.168.2.4	0x36ad	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		52.29.191.126	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:55.861943960 CEST	8.8.8.8	192.168.2.4	0x36ad	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		52.28.196.155	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:55.861943960 CEST	8.8.8.8	192.168.2.4	0x36ad	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		35.157.221.90	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:55.861943960 CEST	8.8.8.8	192.168.2.4	0x36ad	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		35.158.179.12	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:55.861943960 CEST	8.8.8.8	192.168.2.4	0x36ad	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		3.120.52.76	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:55.861943960 CEST	8.8.8.8	192.168.2.4	0x36ad	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		52.28.120.199	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:55.861943960 CEST	8.8.8.8	192.168.2.4	0x36ad	No error (0)	alb-aws-fr-bswx-3-1125904451.eu-central-1.elb.amazonaws.com		52.58.146.86	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:55.861974001 CEST	8.8.8.8	192.168.2.4	0x7d15	No error (0)	eb2.3lift.com	eu-eb2.3lift.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:55.861974001 CEST	8.8.8.8	192.168.2.4	0x7d15	No error (0)	eu-eb2.3lift.com	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:55.861974001 CEST	8.8.8.8	192.168.2.4	0x7d15	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		3.121.70.57	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:55.861974001 CEST	8.8.8.8	192.168.2.4	0x7d15	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		52.57.162.23	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:55.861974001 CEST	8.8.8.8	192.168.2.4	0x7d15	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		18.184.39.197	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:55.861974001 CEST	8.8.8.8	192.168.2.4	0x7d15	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		18.158.85.202	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:55.861974001 CEST	8.8.8.8	192.168.2.4	0x7d15	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		3.120.52.49	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 9, 2021 21:23:55.861974001 CEST	8.8.8.8	192.168.2.4	0x7d15	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		3.124.88.100	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:55.861974001 CEST	8.8.8.8	192.168.2.4	0x7d15	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		3.122.89.158	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:55.861974001 CEST	8.8.8.8	192.168.2.4	0x7d15	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		18.157.239.120	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:55.982029915 CEST	8.8.8.8	192.168.2.4	0x7f09	No error (0)	idsync.rlcdn.com		35.244.174.68	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:55.989803076 CEST	8.8.8.8	192.168.2.4	0x1316	No error (0)	cm.g.doubleclick.net		172.217.168.66	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:56.478852034 CEST	8.8.8.8	192.168.2.4	0x7468	No error (0)	ups.analytics.yahoo.com	prod.ups-ats.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:56.478852034 CEST	8.8.8.8	192.168.2.4	0x7468	No error (0)	prod.ups-ats.aolp-ds-prd.aws.oath.cloud	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:56.478852034 CEST	8.8.8.8	192.168.2.4	0x7468	No error (0)	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud		3.126.56.137	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:56.478852034 CEST	8.8.8.8	192.168.2.4	0x7468	No error (0)	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud		18.156.0.31	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:57.008891106 CEST	8.8.8.8	192.168.2.4	0xa271	No error (0)	track.hubspot.com		104.19.155.83	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:57.008891106 CEST	8.8.8.8	192.168.2.4	0xa271	No error (0)	track.hubspot.com		104.19.154.83	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:57.013842106 CEST	8.8.8.8	192.168.2.4	0xe382	No error (0)	api.hubapi.com		104.17.200.204	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:57.013842106 CEST	8.8.8.8	192.168.2.4	0xe382	No error (0)	api.hubapi.com		104.17.202.204	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:57.013842106 CEST	8.8.8.8	192.168.2.4	0xe382	No error (0)	api.hubapi.com		104.17.204.204	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:57.013842106 CEST	8.8.8.8	192.168.2.4	0xe382	No error (0)	api.hubapi.com		104.17.201.204	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:57.013842106 CEST	8.8.8.8	192.168.2.4	0xe382	No error (0)	api.hubapi.com		104.17.203.204	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:57.017453909 CEST	8.8.8.8	192.168.2.4	0x798	No error (0)	rum.monitis.com		192.111.140.242	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:57.029947042 CEST	8.8.8.8	192.168.2.4	0x8937	No error (0)	widget.intercom.io		13.32.25.95	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:57.029947042 CEST	8.8.8.8	192.168.2.4	0x8937	No error (0)	widget.intercom.io		13.32.25.127	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:57.029947042 CEST	8.8.8.8	192.168.2.4	0x8937	No error (0)	widget.intercom.io		13.32.25.27	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:57.029947042 CEST	8.8.8.8	192.168.2.4	0x8937	No error (0)	widget.intercom.io		13.32.25.37	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:57.040031910 CEST	8.8.8.8	192.168.2.4	0x2493	No error (0)	forms.hubspot.com		104.19.154.83	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 9, 2021 21:23:57.040031910 CEST	8.8.8.8	192.168.2.4	0x2493	No error (0)	forms.hubspot.com		104.19.155.83	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:57.138544083 CEST	8.8.8.8	192.168.2.4	0x3bc1	No error (0)	js.intercomcdn.com		99.86.3.104	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:57.138544083 CEST	8.8.8.8	192.168.2.4	0x3bc1	No error (0)	js.intercomcdn.com		99.86.3.13	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:57.138544083 CEST	8.8.8.8	192.168.2.4	0x3bc1	No error (0)	js.intercomcdn.com		99.86.3.105	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:57.138544083 CEST	8.8.8.8	192.168.2.4	0x3bc1	No error (0)	js.intercomcdn.com		99.86.3.118	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:57.496629000 CEST	8.8.8.8	192.168.2.4	0x7b3b	No error (0)	api-iam.intercom.io		75.2.88.188	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:57.496629000 CEST	8.8.8.8	192.168.2.4	0x7b3b	No error (0)	api-iam.intercom.io		99.83.219.81	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:57.587362051 CEST	8.8.8.8	192.168.2.4	0xe314	No error (0)	googleads.g.doubleclick.net		216.58.215.226	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:57.794850111 CEST	8.8.8.8	192.168.2.4	0xf3e1	No error (0)	d.adroll.com	adserver-vpc-alb-3-890571764.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:23:57.794850111 CEST	8.8.8.8	192.168.2.4	0xf3e1	No error (0)	adserver-vpc-alb-3-890571764.eu-west-1.elb.amazonaws.com		54.195.19.148	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:57.794850111 CEST	8.8.8.8	192.168.2.4	0xf3e1	No error (0)	adserver-vpc-alb-3-890571764.eu-west-1.elb.amazonaws.com		3.248.28.111	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:58.705239058 CEST	8.8.8.8	192.168.2.4	0x2fa4	No error (0)	nexus-websocket-a.intercom.io		35.170.0.145	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:58.705239058 CEST	8.8.8.8	192.168.2.4	0x2fa4	No error (0)	nexus-websocket-a.intercom.io		34.237.73.95	A (IP address)	IN (0x0001)
Apr 9, 2021 21:23:58.705239058 CEST	8.8.8.8	192.168.2.4	0x2fa4	No error (0)	nexus-websocket-a.intercom.io		35.174.127.31	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:00.333194017 CEST	8.8.8.8	192.168.2.4	0xdd4e	No error (0)	northcentralusr-notifyp.svc.ms	svc-ms.spo-0008.spo-msedge.net		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:24:02.390223026 CEST	8.8.8.8	192.168.2.4	0xb336	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:24:02.409730911 CEST	8.8.8.8	192.168.2.4	0x27d7	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:24:06.337681055 CEST	8.8.8.8	192.168.2.4	0xe283	No error (0)	theicecreamqueen.net		69.49.230.229	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:07.688308001 CEST	8.8.8.8	192.168.2.4	0xd842	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:24:07.700241089 CEST	8.8.8.8	192.168.2.4	0x8789	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:24:07.708213091 CEST	8.8.8.8	192.168.2.4	0x1474	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:07.708213091 CEST	8.8.8.8	192.168.2.4	0x1474	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:09.243722916 CEST	8.8.8.8	192.168.2.4	0x54b9	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 9, 2021 21:24:11.813965082 CEST	8.8.8.8	192.168.2.4	0x87fa	No error (0)	theicecrea mqueen.net		69.49.230.229	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.098193884 CEST	8.8.8.8	192.168.2.4	0x34b4	No error (0)	pixel.adve rtising.com	prod.ups-adcom.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:24:21.098193884 CEST	8.8.8.8	192.168.2.4	0x34b4	No error (0)	prod.ups-a dcom.aolp-ds-prd.aws .oath.cloud	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:24:21.098193884 CEST	8.8.8.8	192.168.2.4	0x34b4	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oa th.cloud		52.59.102.119	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.098193884 CEST	8.8.8.8	192.168.2.4	0x34b4	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oa th.cloud		52.59.28.101	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.098193884 CEST	8.8.8.8	192.168.2.4	0x34b4	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oa th.cloud		3.126.63.176	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.098193884 CEST	8.8.8.8	192.168.2.4	0x34b4	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oa th.cloud		35.156.153.71	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.098193884 CEST	8.8.8.8	192.168.2.4	0x34b4	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oa th.cloud		52.57.10.248	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.098193884 CEST	8.8.8.8	192.168.2.4	0x34b4	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oa th.cloud		35.156.106.231	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.098193884 CEST	8.8.8.8	192.168.2.4	0x34b4	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oa th.cloud		18.197.99.6	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.098193884 CEST	8.8.8.8	192.168.2.4	0x34b4	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oa th.cloud		18.197.47.23	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.110223055 CEST	8.8.8.8	192.168.2.4	0x707	No error (0)	dsum-sec.c asalemedia.com	dsum-sec.casalemedia.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:24:21.225148916 CEST	8.8.8.8	192.168.2.4	0x9503	No error (0)	ups.analyt ics.yahoo.com	prod.ups-ats.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:24:21.225148916 CEST	8.8.8.8	192.168.2.4	0x9503	No error (0)	prod.ups-a ts.aolp-ds-prd.aws.o ath.cloud	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:24:21.225148916 CEST	8.8.8.8	192.168.2.4	0x9503	No error (0)	prod.ups-ats.eu-central-1.aolp-ds-prd.aw s.oath.cloud		18.156.0.31	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.225148916 CEST	8.8.8.8	192.168.2.4	0x9503	No error (0)	prod.ups-ats.eu-central-1.aolp-ds-prd.aw s.oath.cloud		3.126.56.137	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.226351023 CEST	8.8.8.8	192.168.2.4	0x426e	No error (0)	pixel.rubi conproject.com	pixel.rubiconproject.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:24:21.230165005 CEST	8.8.8.8	192.168.2.4	0xb02f	No error (0)	sync.outbr ain.com	alldcs.outbrain.org		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:24:21.230165005 CEST	8.8.8.8	192.168.2.4	0xb02f	No error (0)	alldcs.out brain.org	chidc2.outbrain.org		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:24:21.230165005 CEST	8.8.8.8	192.168.2.4	0xb02f	No error (0)	chidc2.out brain.org		50.31.142.31	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.342442989 CEST	8.8.8.8	192.168.2.4	0xbc22	No error (0)	simage2.pu bmatic.com	pug22000nfc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:24:21.342442989 CEST	8.8.8.8	192.168.2.4	0xbc22	No error (0)	pug22000nf c.pubmatic.com	pug22000nf.pubmatic.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 9, 2021 21:24:21.342442989 CEST	8.8.8.8	192.168.2.4	0xbc22	No error (0)	pug22000nf.pubmatic.com		185.64.189.110	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.359169006 CEST	8.8.8.8	192.168.2.4	0xc4e7	No error (0)	ads.yahoo.com	edge.gycpi.b.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:24:21.359169006 CEST	8.8.8.8	192.168.2.4	0xc4e7	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.22	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.359169006 CEST	8.8.8.8	192.168.2.4	0xc4e7	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.23	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.477369070 CEST	8.8.8.8	192.168.2.4	0x4a52	No error (0)	eb2.3lift.com	eu-eb2.3lift.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:24:21.477369070 CEST	8.8.8.8	192.168.2.4	0x4a52	No error (0)	eu-eb2.3lift.com	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:24:21.477369070 CEST	8.8.8.8	192.168.2.4	0x4a52	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		18.158.81.184	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.477369070 CEST	8.8.8.8	192.168.2.4	0x4a52	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		18.158.85.202	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.477369070 CEST	8.8.8.8	192.168.2.4	0x4a52	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		3.64.73.215	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.477369070 CEST	8.8.8.8	192.168.2.4	0x4a52	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		18.157.239.120	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.477369070 CEST	8.8.8.8	192.168.2.4	0x4a52	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		3.120.52.49	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.477369070 CEST	8.8.8.8	192.168.2.4	0x4a52	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		3.124.88.100	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.477369070 CEST	8.8.8.8	192.168.2.4	0x4a52	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		3.122.89.158	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.477369070 CEST	8.8.8.8	192.168.2.4	0x4a52	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		3.121.70.57	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.482018948 CEST	8.8.8.8	192.168.2.4	0x7cac	No error (0)	sync.taboola.com	am-sync.taboola.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:24:21.482018948 CEST	8.8.8.8	192.168.2.4	0x7cac	No error (0)	am-sync.taboola.com	am-vip001.taboola.com		CNAME (Canonical name)	IN (0x0001)

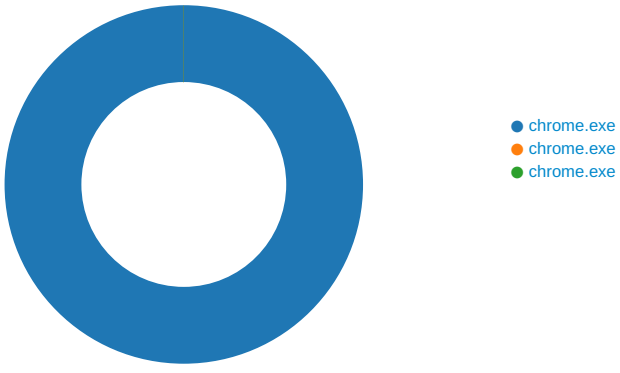
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 9, 2021 21:24:21.482018948 CEST	8.8.8.8	192.168.2.4	0x7cac	No error (0)	am-vip001.taboola.com		141.226.228.48	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.578795910 CEST	8.8.8.8	192.168.2.4	0x29d0	No error (0)	x.bidswitch.net	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:24:21.578795910 CEST	8.8.8.8	192.168.2.4	0x29d0	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		35.156.223.207	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.578795910 CEST	8.8.8.8	192.168.2.4	0x29d0	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		3.121.79.35	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.578795910 CEST	8.8.8.8	192.168.2.4	0x29d0	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		18.185.180.173	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.578795910 CEST	8.8.8.8	192.168.2.4	0x29d0	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		52.58.182.33	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.578795910 CEST	8.8.8.8	192.168.2.4	0x29d0	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		3.124.46.162	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.578795910 CEST	8.8.8.8	192.168.2.4	0x29d0	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		18.195.54.133	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.578795910 CEST	8.8.8.8	192.168.2.4	0x29d0	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		52.58.45.227	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.578795910 CEST	8.8.8.8	192.168.2.4	0x29d0	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		3.120.242.149	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.703289032 CEST	8.8.8.8	192.168.2.4	0x231b	No error (0)	idsync.rlcdn.com		35.244.174.68	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.821638107 CEST	8.8.8.8	192.168.2.4	0x59c	No error (0)	us-u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.821638107 CEST	8.8.8.8	192.168.2.4	0x59c	No error (0)	us-u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.841597080 CEST	8.8.8.8	192.168.2.4	0x1d2d	No error (0)	ib.adnxs.com	g.geogslb.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:24:21.841597080 CEST	8.8.8.8	192.168.2.4	0x1d2d	No error (0)	g.geogslb.com	ib.anycast.adnxs.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:24:21.841597080 CEST	8.8.8.8	192.168.2.4	0x1d2d	No error (0)	ib.anycast.adnxs.com		185.33.221.89	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.841597080 CEST	8.8.8.8	192.168.2.4	0x1d2d	No error (0)	ib.anycast.adnxs.com		185.33.223.178	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.841597080 CEST	8.8.8.8	192.168.2.4	0x1d2d	No error (0)	ib.anycast.adnxs.com		185.33.221.90	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.841597080 CEST	8.8.8.8	192.168.2.4	0x1d2d	No error (0)	ib.anycast.adnxs.com		185.33.220.243	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.841597080 CEST	8.8.8.8	192.168.2.4	0x1d2d	No error (0)	ib.anycast.adnxs.com		185.33.220.244	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.841597080 CEST	8.8.8.8	192.168.2.4	0x1d2d	No error (0)	ib.anycast.adnxs.com		185.33.220.241	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 9, 2021 21:24:21.841597080 CEST	8.8.8.8	192.168.2.4	0x1d2d	No error (0)	ib.anycast.adnxs.com		185.33.221.15	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.841597080 CEST	8.8.8.8	192.168.2.4	0x1d2d	No error (0)	ib.anycast.adnxs.com		185.33.221.53	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:21.945502043 CEST	8.8.8.8	192.168.2.4	0xdf35	No error (0)	cm.g.doubleclick.net		172.217.168.66	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:49.200807095 CEST	8.8.8.8	192.168.2.4	0xd831	No error (0)	www.joomag.com	lb.joomag.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:24:49.200807095 CEST	8.8.8.8	192.168.2.4	0xd831	No error (0)	lb.joomag.com		209.95.50.27	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:49.208025932 CEST	8.8.8.8	192.168.2.4	0xe2d2	No error (0)	use.typekit.net	use-stls.adobe.com.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:24:51.974050999 CEST	8.8.8.8	192.168.2.4	0x8175	No error (0)	bam-cell.nr-data.net	tls12.newrelic.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:24:55.549638987 CEST	8.8.8.8	192.168.2.4	0x9d64	No error (0)	static.intercomassets.com	d2065cca9qi4ey.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 21:24:55.549638987 CEST	8.8.8.8	192.168.2.4	0x9d64	No error (0)	d2065cca9qi4ey.cloudfront.net		99.86.3.39	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:55.549638987 CEST	8.8.8.8	192.168.2.4	0x9d64	No error (0)	d2065cca9qi4ey.cloudfront.net		99.86.3.98	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:55.549638987 CEST	8.8.8.8	192.168.2.4	0x9d64	No error (0)	d2065cca9qi4ey.cloudfront.net		99.86.3.80	A (IP address)	IN (0x0001)
Apr 9, 2021 21:24:55.549638987 CEST	8.8.8.8	192.168.2.4	0x9d64	No error (0)	d2065cca9qi4ey.cloudfront.net		99.86.3.84	A (IP address)	IN (0x0001)
Apr 9, 2021 21:25:57.922729015 CEST	8.8.8.8	192.168.2.4	0xbaaa	No error (0)	nexus-websocket-a.intercom.io		35.174.127.31	A (IP address)	IN (0x0001)
Apr 9, 2021 21:25:57.922729015 CEST	8.8.8.8	192.168.2.4	0xbaaa	No error (0)	nexus-websocket-a.intercom.io		35.170.0.145	A (IP address)	IN (0x0001)
Apr 9, 2021 21:25:57.922729015 CEST	8.8.8.8	192.168.2.4	0xbaaa	No error (0)	nexus-websocket-a.intercom.io		34.237.73.95	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 6896 Parent PID: 1284

General

Start time:	21:23:38
Start date:	09/04/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://joom.ag/Ja5I'
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
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

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}	dr	unicode	0	1	success or wait	1	7FF609CBFC4B	RegSetValueExW

Analysis Process: chrome.exe PID: 6000 Parent PID: 6896

General

Start time:	21:23:39
Start date:	09/04/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1316,17158847015543384734,7560515483952834825,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1800 /prefetch:8
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6

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

Registry Activities

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

Analysis Process: chrome.exe PID: 6216 Parent PID: 6896

General

Start time:	21:24:59
Start date:	09/04/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1316,17158847015543384734,7560515483952834825,131072 --lang=en-GB --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=6788 /prefetch:8
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly