



ID: 356207
Cookbook: browseurl.jbs
Time: 18:58:11
Date: 22/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report http://storangegoogleapiddp.agilecrm.com 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Dropped Files 4
Sigma Overview 4
Signature Overview 5
Phishing: 5
Compliance: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 11
Public 12
Private 12
General Information 13
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 15
IPs 15
Domains 15
ASN 15
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
Static File Info 49
No static file info 49
Network Behavior 49
Network Port Distribution 49
TCP Packets 49
UDP Packets 51
DNS Queries 53
DNS Answers 54
HTTP Request Dependency Graph 60
HTTP Packets 60
HTTPS Packets 60
Code Manipulations 61
Statistics 61

Behavior 61
System Behavior 61
Analysis Process: iexplore.exe PID: 3948 Parent PID: 792 62
General 62
File Activities 62
Registry Activities 62
Analysis Process: iexplore.exe PID: 5500 Parent PID: 3948 62
General 62
File Activities 62
Registry Activities 63
Disassembly 63

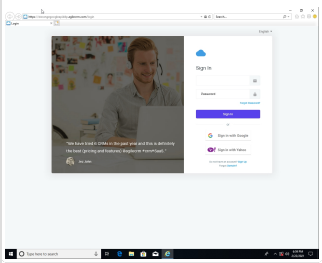
Analysis Report http://storangegoogleapiddp.agilecrm.c…

Overview

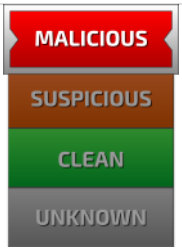
General Information

Sample URL:	http://storangegoogleapiddp.agilecrm.com
Analysis ID:	356207

Most interesting Screenshot:



Detection



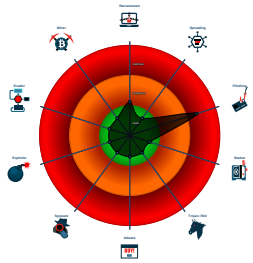
HTMLPhisher

Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish_10
- Phishing site detected (based on log…
- Found iframes
- HTML title does not match URL

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 3948 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5500 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3948 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\login[2].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\login[1].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\login[1].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\login[3].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\login[2].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Click to see the 2 entries

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

Phishing:



Yara detected HtmlPhish_10

Phishing site detected (based on logo template match)

Compliance:



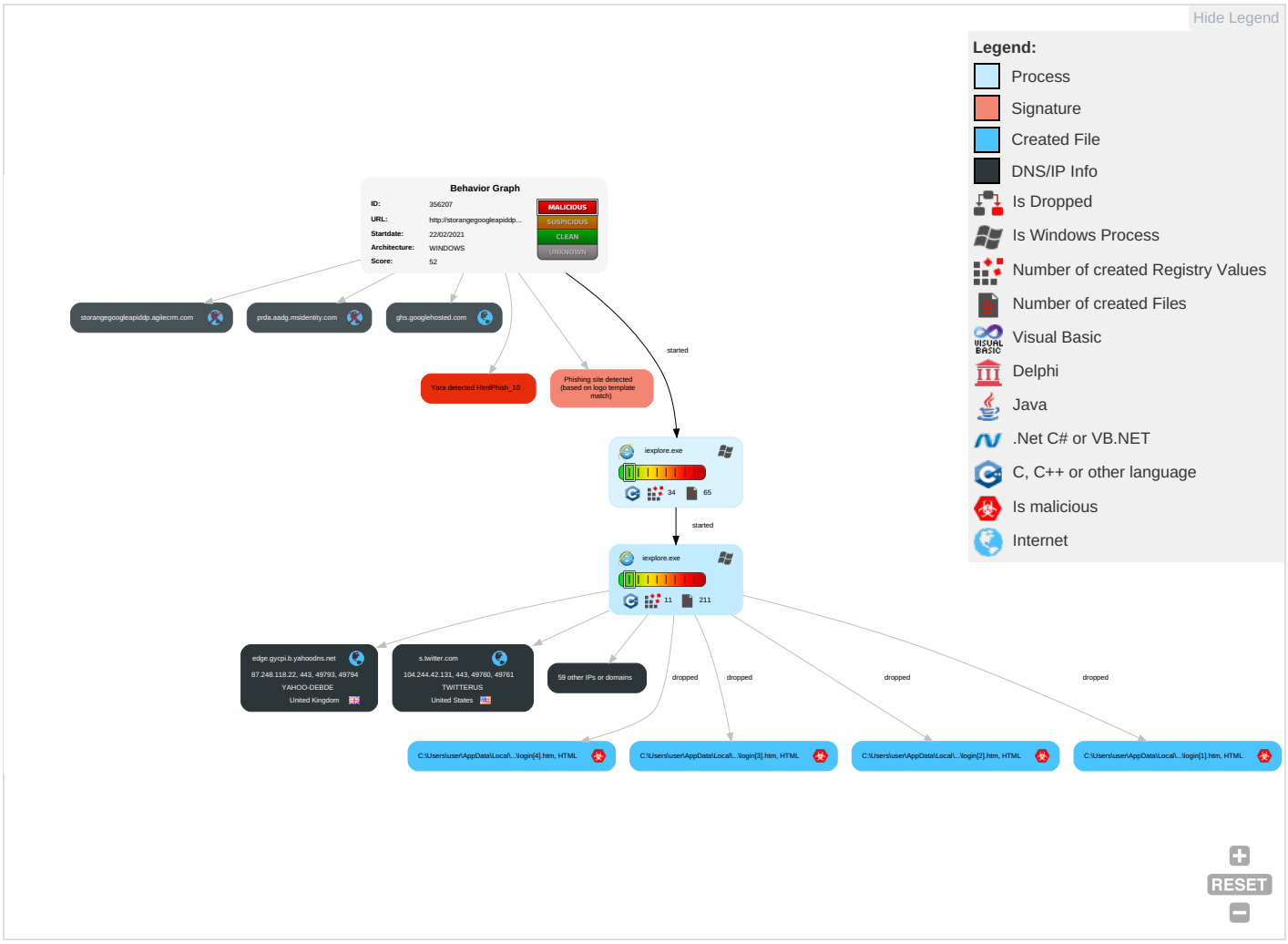
Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Drive-by Compromise 1	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap	

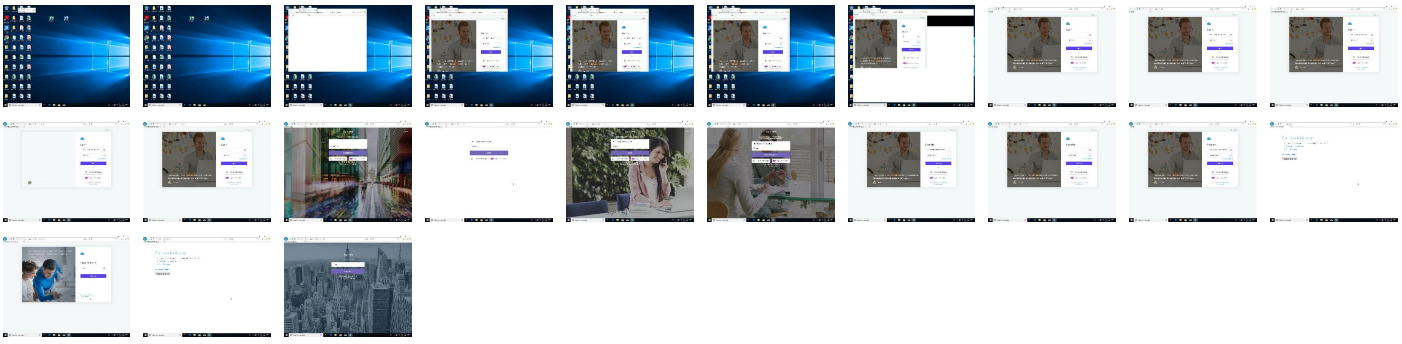
Behavior Graph

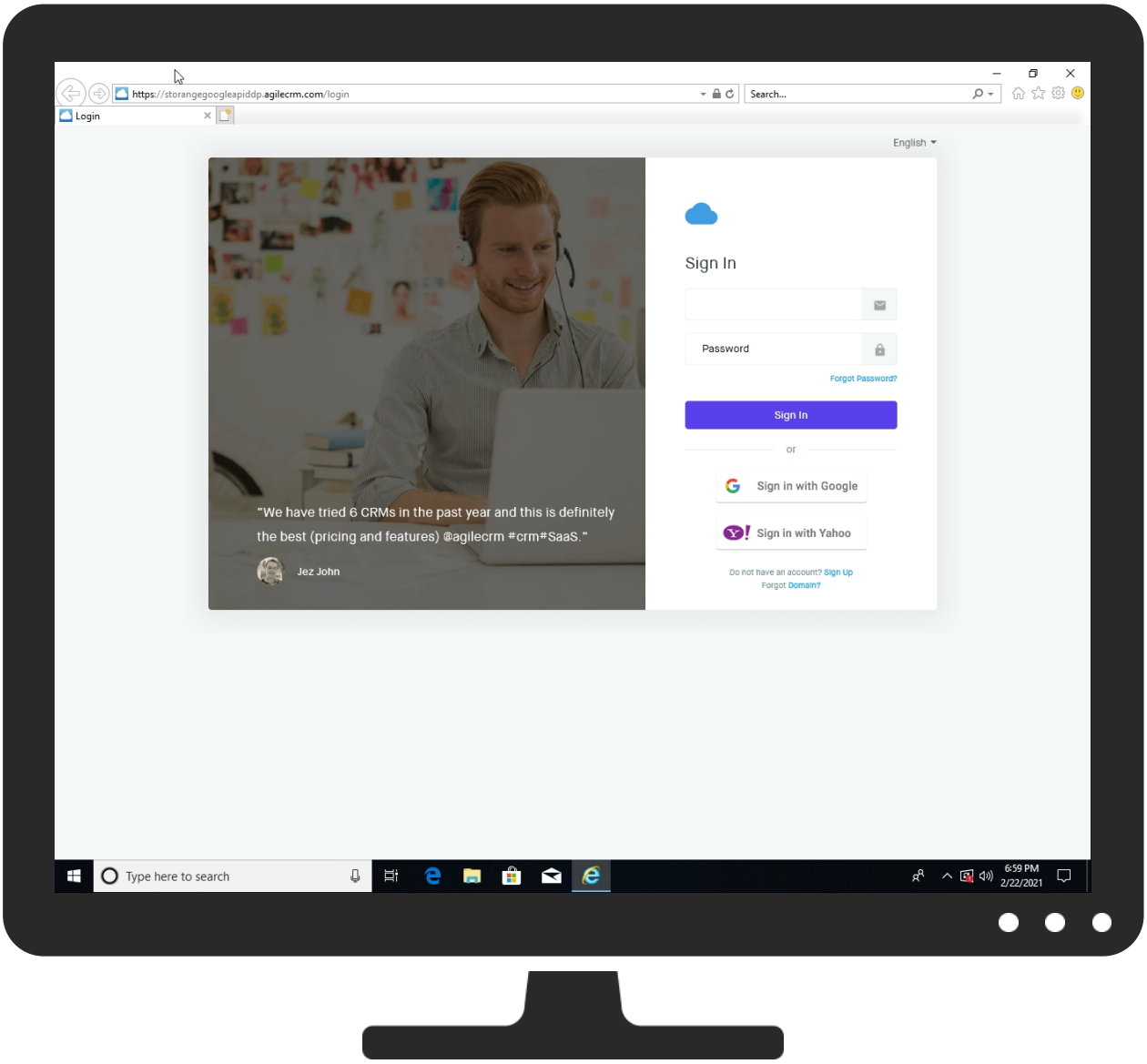


Screenshots

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://storangegoogleapiddp.agilecrm.com	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
platform.twitter.map.fastly.net	0%	Virustotal		Browse
nydc1.outbrain.org	0%	Virustotal		Browse
prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud	0%	Virustotal		Browse
www.google.co.uk	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://storangegoogleapiddp.agilecRoot	0%	Avira URL Cloud	safe	
http://https://storangegoogleapiddp.Root	0%	Avira URL Cloud	safe	
http://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://https://test55-dot-sandbox-dot-agilecrmbeta.appspot.com/flatfull/images/user-default.jpg	0%	Avira URL Cloud	safe	
http://arshaw.com/fullcalendar/	0%	Avira URL Cloud	safe	
http://https://www.agilecrm.c	0%	Avira URL Cloud	safe	
http://https://~domain.agilecrm.com/sendemail/document/~docid/~contactid	0%	Avira URL Cloud	safe	
http://https://cdn01.boxcdn.net/js/static/select.js	0%	Avira URL Cloud	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://static.ads-twitter.com/uwt.js	0%	URL Reputation	safe	
http://https://static.ads-twitter.com/uwt.js	0%	URL Reputation	safe	
http://https://static.ads-twitter.com/uwt.js	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://www.agle1.me?utm_source=powered-by&	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pug-lhr.pubmatic.com	185.64.190.80	true	false		high
alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com	54.93.211.166	true	false		high
d1gwclp1pmzk26.cloudfront.net	99.86.162.148	true	false		high
platform.twitter.map.fastly.net	151.101.12.157	true	false	• 0%, Virustotal, Browse	unknown
scontent.xx.fbcdn.net	31.13.92.14	true	false		high
idsync.rlcdn.com	34.120.207.148	true	false		high
s3.amazonaws.com	52.216.76.206	true	false		high
t.co	104.244.42.69	true	false		high
adserver-vpc-alb-1-1446435489.eu-west-1.elb.amazonaws.com	54.246.184.51	true	false		high
pagead.l.doubleclick.net	172.217.16.130	true	false		high
cdnjs.cloudflare.com	104.16.18.94	true	false		high
am-vip001.taboola.com	141.226.228.48	true	false		high
doxhze3l6s7v9.cloudfront.net	13.226.175.122	true	false		high
pagead46.l.doubleclick.net	172.217.23.98	true	false		high
nydc1.outbrain.org	64.202.112.127	true	false	• 0%, Virustotal, Browse	unknown
us-u.openx.net	34.98.64.218	true	false		high
s.twitter.com	104.244.42.131	true	false		high
stats.l.doubleclick.net	173.194.76.155	true	false		high
prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud	3.126.63.176	true	false	• 0%, Virustotal, Browse	unknown
dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com	18.158.74.203	true	false		high
www.google.co.uk	142.250.186.35	true	false	• 0%, Virustotal, Browse	unknown
ib.anycast.adnxs.com	37.252.172.45	true	false		high
prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud	18.156.0.31	true	false		unknown
ghs.googlehosted.com	142.250.185.179	true	false		unknown
adserver-vpc-alb-3-890571764.eu-west-1.elb.amazonaws.com	52.209.227.220	true	false		high
edge.gycpi.b.yahoodns.net	87.248.118.22	true	false		unknown
static.ads-twitter.com	unknown	unknown	false		unknown
d.adroll.mgr.consensu.org	unknown	unknown	false		unknown
d.adroll.com	unknown	unknown	false		high
cdn.jsdelivr.net	unknown	unknown	false		high
stats2.agilecrm.com	unknown	unknown	false		high
ups.analytics.yahoo.com	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
ads.yahoo.com	unknown	unknown	false		high

Copyright null 2021

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cm.g.doubleclick.net	unknown	unknown	false		high
pixel.advertising.com	unknown	unknown	false		high
sync.outbrain.com	unknown	unknown	false		high
sync.taboola.com	unknown	unknown	false		high
x.bidswitch.net	unknown	unknown	false		unknown
pixel.rubiconproject.com	unknown	unknown	false		high
www.clickcease.com	unknown	unknown	false		high
s.adroll.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
analytics.twitter.com	unknown	unknown	false		high
our.agilecrm.com	unknown	unknown	false		high
simage2.pubmatic.com	unknown	unknown	false		high
googleads.g.doubleclick.net	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
storangegoogleapiddp.agilecrm.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://storangegoogleapiddp.agilecrm.com/login?lang=es	false		high
http://https://storangegoogleapiddp.agilecrm.com/forgot-domain	false		high
http://https://storangegoogleapiddp.agilecrm.com/login?lang=fr	false		high
http://https://storangegoogleapiddp.agilecrm.com/forgot-password	false		high
http://storangegoogleapiddp.agilecrm.com/	false		high
http://https://storangegoogleapiddp.agilecrm.com/login?lang=pt	false		high
http://https://storangegoogleapiddp.agilecrm.com/login?lang=en	false		high
http://https://storangegoogleapiddp.agilecrm.com/login	false		high

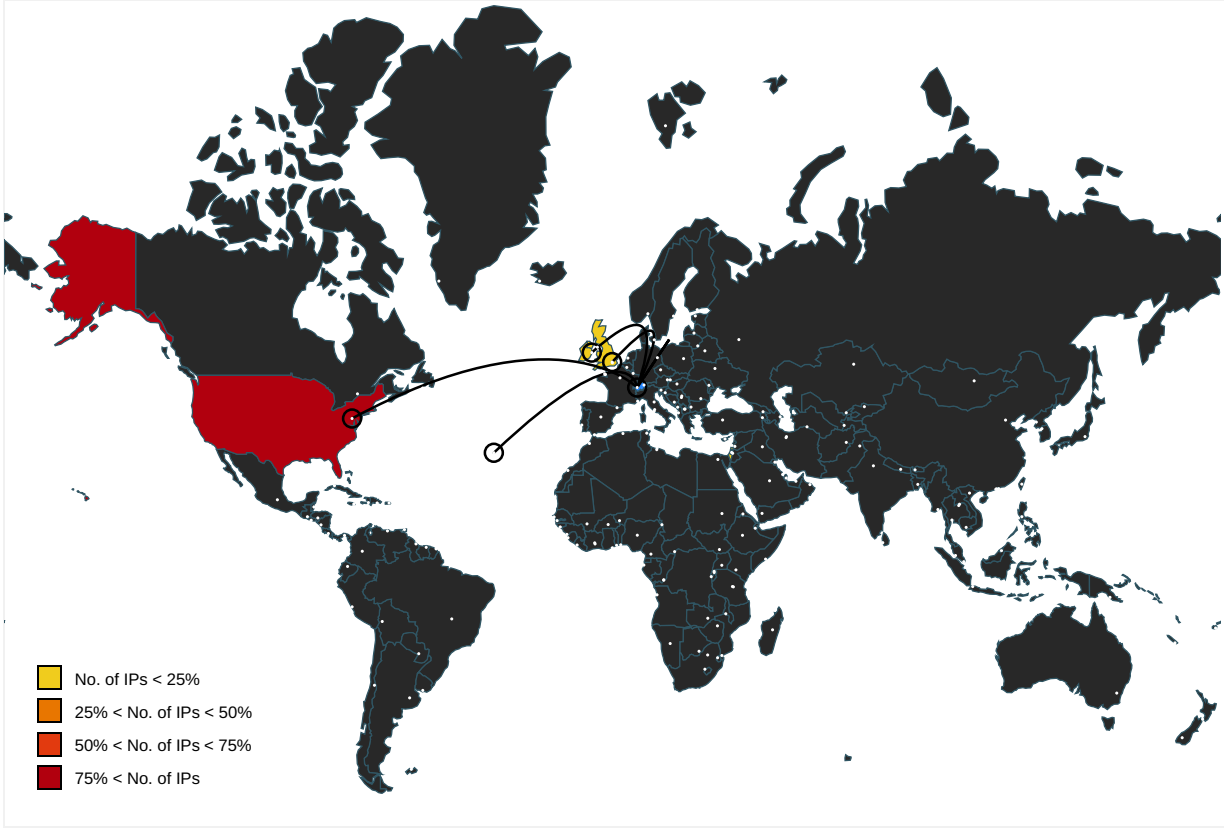
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdnjs.cloudflare.com/ajax/libs/intl-tel-input/9.2.4/js/intlTelInput.min.js	js-all-min-3[2].js0.2.dr, js-all-min-3[1].js2.2.dr, js-all-min-3[2].js.2.dr, js-all-min-3[1].js0.2.dr, js-all-min-3[1].js1.2.dr	false		high
http://https://my.agilecrm.com/registercrm.com/forgot-password	~DFCC22ACC9E6B30BEA.TMP.1.dr	false		high
http://https://secure.gravatar.com/avatar/	js-all-min-3[1].js1.2.dr	false		high
http://https://www.agilecrm.com/	login[2].htm.2.dr, login[1].htm0.2.dr, forgot-password[1].htm.2.dr	false		high
http://https://storangegoogleapiddp.agilecrm.com/flatfull/preload-js-src-iframe.html	~DFCC22ACC9E6B30BEA.TMP.1.dr	false		high
http://https://www.slideshare.net/slideshow/embed_code/32115990	ru[1].js.2.dr	false		high
http://https://my.agilecrm.com/register?utm_affiliate=	js-all-min-3[2].js0.2.dr, js-all-min-3[1].js2.2.dr, js-all-min-3[2].js.2.dr, js-all-min-3[1].js0.2.dr, js-all-min-3[1].js1.2.dr	false		high
http://salescal.agilecrm.com	js-all-min-4[2].js0.2.dr, js-all-min-4[1].js0.2.dr, js-all-min-4[2].js.2.dr	false		high
http://https://storangegoogleapiddp.agilecrm.com/login	~DFCC22ACC9E6B30BEA.TMP.1.dr, {1063455E-7583-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://s3.amazonaws.com/agilecrm/panel/uploaded-logo/a317/1490689109731/gdrive.png	js-all-min-3[1].js2.2.dr, js-all-min-3[2].js.2.dr	false		high
http://https://www.linkedin.com/search/results/people/?keywords=	js-all-min-2[2].js.2.dr, js-all-min-2[2].js0.2.dr, js-all-min-2[1].js1.2.dr	false		high
http://https://d.adroll.com	roundtrip[1].js.2.dr	false		high
http://https://github.com/select2/select2/blob/master/LICENSE.md	js-all-min-2[2].js.2.dr	false		high
http://getbootstrap.com/javascript/#buttons	b-bootstrap[1].js.2.dr	false		high
http://https://s.adroll.com	roundtrip[1].js.2.dr	false		high
http://https://s3.amazonaws.com/agilecrm/	js-all-min-1[2].js.2.dr	false		high
http://https://storangegoogleapiddp.agilecRoot	{1063455E-7583-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://storangegoogleapiddp.Root	{1063455E-7583-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.youtube.com/embed/aBUQVVXrf2I	portlets[2].js0.2.dr, portlets[1].js2.2.dr, portlets[1].js0.2.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/intl-tel-input/9.2.4/js/utils.js	js-all-min-3[2].js0.2.dr, js-all-min-3[1].js2.2.dr, js-all-min-3[2].js.2.dr, js-all-min-3[1].js0.2.dr, js-all-min-3[1].js1.2.dr	false		high
http://https://storangegoogleapiddp.agilecrm.com/flatfull/preload-js-srRoot	{1063455E-7583-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://www.lemoda.net/maths/bezier-length/index.html	js-all-min-4[2].js1.2.dr	false		high
http://https://github.com/twbs/bootstrap/issues/14093	b-bootstrap[1].js.2.dr	false		high
http://getbootstrap.com/javascript/#tooltip	b-bootstrap[1].js.2.dr	false		high
http://https://doxhze3l6s7v9.cloudfront.net/beta/static/img/agile-loader.gif	js-all-min-4[2].js0.2.dr, js-all-min-4[1].js0.2.dr, js-all-min-4[2].js.2.dr	false		high
http://https://agilecrm.s3.amazonaws.com/videos/thumbs/default.png	js-all-min-4[2].js1.2.dr, js-all-min-4[2].js0.2.dr, js-all-min-4[1].js0.2.dr, js-all-min-4[1].js1.2.dr, js-all-min-4[2].js.2.dr	false		high
http://https://connect.facebook.net/en_US/fbevents.js	js-all-min-3[2].js0.2.dr, js-all-min-3[1].js2.2.dr, js-all-min-3[1].js.2.dr	false		high
http://getbootstrap.com)	bootstrap.v3.min[1].js.2.dr	false	• Avira URL Cloud: safe	low
http://https://github.com/krux/postscribe/blob/master/LICENSE.	gtm[1].js.2.dr	false		high
http://https://twitter.com/intent/tweet?url=	js-all-min-4[2].js1.2.dr, js-all-min-4[2].js0.2.dr, js-all-min-4[1].js.2.dr	false		high
http://https://test55-dot-sandbox-dot-agilecrmbeta.appspot.com/flatfull/images/user-default.jpg	ru[1].js.2.dr, pt[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://stats.g.doubleclick.net/j/collect	analytics[1].js.2.dr	false		high
http://https://storangegoogleapiddp.agilecrm.com/loginom/dp.agilecrm.com/login?lang=ptLogin	{1063455E-7583-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://benknowscode.wordpress.com/2012/09/14/path-interpolation-using-cubic-bezier-and-control-point	js-all-min-4[2].js1.2.dr	false		high
http://www.agilecrm.com/?utm_source=affiliates&utm_medium=web&utm_campaign=	fr[1].js.2.dr	false		high
http://arshaw.com/fullcalendar/	js-all-min-4[2].js1.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.agilecrm.com/?utm_source=affiliates&utm_medium=web&utm_campaign=	fr[1].js.2.dr, it[1].js.2.dr	false		high
http://https://www.agilecrm.com/dp.agilecrm.com/login?lang=pt	~DFCC22ACC9E6B30BEA.TMP.1.dr	false		high
http://https://s.adroll.com/j/ad-container.js	roundtrip[1].js.2.dr	false		high
http://https://www.agilecrm.c	{1063455E-7583-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://~domain.agilecrm.com/sendemail/document/~docid/~contactid	js-all-min-4[2].js1.2.dr, js-all-min-4[2].js0.2.dr, js-all-min-4[1].js0.2.dr, js-all-min-4[1].js1.2.dr, js-all-min-4[2].js.2.dr	false	• Avira URL Cloud: safe	low
http://https://media.twiliocdn.com/sdk/js/client/v1.7/twilio.min.js	js-all-min-2[2].js.2.dr, js-all-min-2[2].js0.2.dr, js-all-min-2[1].js0.2.dr	false		high
http://https://storangegoogleapiddp.agilecrm.com/login?ls-src-iframe.html	{1063455E-7583-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://www.modernizr.com/)	b-bootstrap[1].js.2.dr	false		high
http://https://storangegoogleapiddp.agilecrm.com/login?lang=fr	~DFCC22ACC9E6B30BEA.TMP.1.dr	false		high
http://https://storangegoogleapiddp.agilecrm.com/favicon.ico~	imagestore.dat.2.dr	false		high
http://https://cdn01.boxcdn.net/js/static/select.js	js-all-min-2[2].js.2.dr, js-all-min-2[2].js0.2.dr, js-all-min-2[1].js1.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cct.google/taggy/agent.js	gtm[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.agilecrm.com/support.html	ru[1].js.2.dr, es[1].js.2.dr, pt[1].js.2.dr, fr[1].js.2.dr	false		high
http://https://static.ads-twitter.com/uwt.js	gtm[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://storangegoogleapiddp.agilecrm.com/loginc-iframe.html	{1063455E-7583-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://doxhze3l6s7v9.cloudfront.net/beta/static/images/agilecrm-logo.jpg	js-all-min-3[2].js0.2.dr, js-all-min-3[1].js2.2.dr, js-all-min-3[2].js.2.dr, js-all-min-3[1].js0.2.dr, js-all-min-3[1].js1.2.dr	false		high
http://getbootstrap.com/javascript/#tabs	b-bootstrap[1].js.2.dr	false		high
http://https://storangegoogleapiddp.agilecrm.com/forgot-domain	~DFCC22ACC9E6B30BEA.TMP.1.dr	false		high
http://https://d1gwclp1pmzk26.cloudfront.net/agile/stats/min/app/v11/agile-min.js	agile-cloud[1].js.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://doxhze3l6s7v9.cloudfront.net/beta/static/img/android-new.svg	portlets[2].js0.2.dr, portlets[1].js2.2.dr	false		high
http://https://storangegoogleapiddp.agilecrm.com/loginm/registercrm.com/forgot-passwordogin	{1063455E-7583-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://www.agilecrm.com/blog/feed/	js-all-min-2[2].js.2.dr, js-all-min-2[2].js0.2.dr, js-all-min-2[1].js2.2.dr	false		high
http://https://www.google.%/ads/ga-audiences	analytics[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	bootstrap.v3.min[1].js.2.dr	false		high
http://https://static.woopra.com/js/woopra.js	js-all-min-3[2].js0.2.dr, js-all-min-3[1].js2.2.dr, js-all-min-3[1].js.2.dr	false		high
http://https://s3.amazonaws.com/agilecrm/panel/uploaded-logo/a317/1492593925097/edoc1.png	js-all-min-3[1].js2.2.dr, js-all-min-3[2].js.2.dr	false		high
http://https://doxhze3l6s7v9.cloudfront.net/app/static/img/iphone-new.svg	portlets[2].js0.2.dr, portlets[1].js2.2.dr	false		high
http://https://storangegoogleapiddp.agilecrm.com/login?lang=es	~DFCC22ACC9E6B30BEA.TMP.1.dr	false		high
http://https://doxhze3l6s7v9.cloudfront.net/app/static/img/Android.svg	ru[1].js.2.dr, pt[1].js.2.dr	false		high
http://https://storangegoogleapiddp.agilecrm.com/login?lang=en	~DFCC22ACC9E6B30BEA.TMP.1.dr	false		high
http://https://www.youtube.com/embed/0PcHh2OjagU	fr[1].js.2.dr	false		high
http://https://storangegoogleapiddp.agilecrm.com/forgot-domaindb	~DFCC22ACC9E6B30BEA.TMP.1.dr	false		high
http://https://www.youtube.com/embed/LQOiZ8AhF0A	fr[1].js.2.dr	false		high
http://www.agle1.me?utm_source=powered-by&	js-all-min-2[2].js.2.dr, js-all-min-2[2].js0.2.dr, js-all-min-2[1].js0.2.dr, js-all-min-2[1].js2.2.dr	false	• Avira URL Cloud: safe	unknown
http://supportcal.agilecrm.com	js-all-min-4[2].js.2.dr	false		high
http://https://doxhze3l6s7v9.cloudfront.net/img/default-404.png	js-all-min-4[2].js0.2.dr, js-all-min-4[1].js0.2.dr, js-all-min-4[2].js.2.dr	false		high
http://corner.squareup.com/2012/07/smoother-signatures.html	js-all-min-4[2].js1.2.dr	false		high
http://https://d1gwclp1pmzk26.cloudfront.net/agile/agile-cloud.js	login[2].htm.2.dr	false		high
http://https://secure.gravatar.com/avatar/d41d8cd98f00b204e9800998ecf8427e.jpg?s=50&d=https%3A//dpm72z3	ru[1].js.2.dr	false		high
http://https://github.com/szimek/signature_pad	js-all-min-4[2].js1.2.dr	false		high
http://https://s3.amazonaws.com/agilecrm/panel/uploaded-logo/a317/1490792217282/send-mail%2B(1).png	ru[1].js.2.dr, es[1].js.2.dr, pt[1].js.2.dr, fr[1].js.2.dr	false		high
http://https://storangegoogleapiddp.agilecrm.com/forgot-password	~DFCC22ACC9E6B30BEA.TMP.1.dr	false		high
http://https://storangegoogleapiddp.agilecrm.com/loginapiddp.agilecrm.com/login?lang=itLogin	{1063455E-7583-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://getbootstrap.com/javascript/#scrollspy	b-bootstrap[1].js.2.dr	false		high
http://a.adroll.com	roundtrip[1].js.2.dr	false		high
http://getbootstrap.com/javascript/#collapse	b-bootstrap[1].js.2.dr	false		high
http://https://restcountries.eu/rest/v1/name/	js-all-min-2[1].js2.2.dr	false		high
http://www.agilecrm.com	forgot-domain[1].htm.2.dr	false		high
http://https://github.com/agilecrm/agile-popups#usage	ru[1].js.2.dr, es[1].js.2.dr, pt[1].js.2.dr, fr[1].js.2.dr	false		high
http://getbootstrap.com/javascript/#modals	b-bootstrap[1].js.2.dr	false		high
http://https://storangegoogleapiddp.agilecrm.com/forgot-password.Esqueci	~DFCC22ACC9E6B30BEA.TMP.1.dr	false		high
http://https://s.adroll.com/j/roundtrip.js	gtm[1].js.2.dr	false		high
http://https://storangegoogleapiddp.agilecrm.com/loginapiddp.agilecrm.com/login?lang=frLogin	{1063455E-7583-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://storangegoogleapiddp.agilecrm.com/loginapiddp.agilecrm.com/login?lang=ruLogin	{1063455E-7583-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://getbootstrap.com/javascript/#transitions	b-bootstrap[1].js.2.dr	false		high
http://https://storangegoogleapiddp.agilecrm.com/login?lang=pt	~DFCC22ACC9E6B30BEA.TMP.1.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.226.175.122	unknown	United States		16509	AMAZON-02US	false
52.209.227.220	unknown	United States		16509	AMAZON-02US	false
173.194.76.155	unknown	United States		15169	GOOGLEUS	false
3.126.63.176	unknown	United States		16509	AMAZON-02US	false
99.86.162.148	unknown	United States		16509	AMAZON-02US	false
31.13.92.14	unknown	Ireland		32934	FACEBOOKUS	false
18.158.74.203	unknown	United States		16509	AMAZON-02US	false
185.64.190.80	unknown	United Kingdom		62713	AS-PUBMATICUS	false
54.246.184.51	unknown	United States		16509	AMAZON-02US	false
172.217.23.98	unknown	United States		15169	GOOGLEUS	false
141.226.228.48	unknown	Israel		200478	TABOOLA-ASIL	false
142.250.74.194	unknown	United States		15169	GOOGLEUS	false
37.252.172.45	unknown	European Union		29990	ASN-APPNEXUS	false
104.16.18.94	unknown	United States		13335	CLOUDFLARENETUS	false
142.250.186.35	unknown	United States		15169	GOOGLEUS	false
104.244.42.69	unknown	United States		13414	TWITTERUS	false
87.248.118.22	unknown	United Kingdom		203220	YAHOO-DEBDE	false
142.250.185.179	unknown	United States		15169	GOOGLEUS	false
64.202.112.127	unknown	United States		22075	AS-OUTBRAINUS	false
34.120.207.148	unknown	United States		15169	GOOGLEUS	false
104.244.42.131	unknown	United States		13414	TWITTERUS	false
54.93.211.166	unknown	United States		16509	AMAZON-02US	false
52.216.76.206	unknown	United States		16509	AMAZON-02US	false
34.98.64.218	unknown	United States		15169	GOOGLEUS	false
18.156.0.31	unknown	United States		16509	AMAZON-02US	false
172.217.16.130	unknown	United States		15169	GOOGLEUS	false
151.101.12.157	unknown	United States		54113	FASTLYUS	false

Private

IP
192.168.2.1

Copyright null 2021

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356207
Start date:	22.02.2021
Start time:	18:58:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://storangegoogleapiddp.agilecrm.com
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	14
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:	mal52.phis.win@3/136@34/28
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://storangegoogleapiddp.agilecrm.com/login?lang=en • Browsing link: https://storangegoogleapiddp.agilecrm.com/login?lang=es • Browsing link: https://storangegoogleapiddp.agilecrm.com/login?lang=it • Browsing link: https://storangegoogleapiddp.agilecrm.com/login?lang=ru • Browsing link: https://storangegoogleapiddp.agilecrm.com/login?lang=fr • Browsing link: https://storangegoogleapiddp.agilecrm.com/login?lang=pt • Browsing link: https://www.agilecrm.com/ • Browsing link: https://storangegoogleapiddp.agilecrm.com/forgot-password • Browsing link: https://storangegoogleapiddp.agilecrm.com/register • Browsing link: https://storangegoogleapiddp.agilecrm.com/forgot-domain

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 168.61.161.212, 52.147.198.201, 13.64.90.137, 88.221.62.148, 142.250.185.202, 142.250.186.104, 151.101.2.109, 151.101.66.109, 151.101.130.109, 151.101.194.109, 172.217.16.142, 184.30.24.121, 204.79.197.200, 13.107.21.200, 172.67.68.112, 104.26.13.59, 104.26.12.59, 142.250.185.164, 184.30.24.241, 69.173.144.138, 69.173.144.139, 69.173.144.165, 152.199.19.161, 184.30.24.56, 104.42.151.234, 20.190.160.134, 20.190.160.8, 20.190.160.129, 20.190.160.73, 20.190.160.6, 20.190.160.69, 20.190.160.136, 20.190.160.71, 40.88.32.150, 51.11.168.160, 2.20.142.209, 2.20.142.210, 51.103.5.186 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, fs-wildcard.microsoft.com.edgekey.net, e11290.dspg.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, login.live.com, www.clickcease.com.cdn.cloudflare.net, audownload.windowsupdate.nsatc.net, www.google.com, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net, www.google-analytics.com, fonts.googleapis.com, fs.microsoft.com, dual-a-0001.a-msedge.net, skypedataprdcolcus17.cloudapp.net, www.tm.a.prd.aadg.akadns.net, wildcard.adroll.com.edgekey.net, blobcollector.events.data.trafficmanager.net, dsum-sec.casalemedia.com.edgekey.net, e4007.g.akamaiedge.net, cs9.wpc.v0cdn.net, au.download.windowsupdate.com.edgesuite.net, www.googleadservices.com, pixel.rubiconproject.net.akadns.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, iecvlist.microsoft.com, wns.notify.trafficmanager.net, go.microsoft.com, e8037.g.akamaiedge.net, www.googletagmanager.com, bat.bing.com, prod.fs.microsoft.com.akadns.net, dualstack.f3.shared.global.fastly.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, www-google-analytics.l.google.com, ie9comview.vo.msecnd.net, www-googletagmanager.l.google.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, login.msa.msidentity.com, skypedataprdcoleus16.cloudapp.net, bat-bing-com.a-0001.a-msedge.net, go.microsoft.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, vip2-par02p.wns.notify.trafficmanager.net • 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 NtDeviceIoControlFile calls found. • Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\KF0W15PX\storangegoogleapiddp.agilecrm[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	4.91429191399241
Encrypted:	false
SSDEEP:	192:AO9F0IB9A0IB9c0O69j0O69j0O69c0O69c0dH9R0dH930dH930F2920F29r0F29X:f9F0I9A0I9c0d9j0d9j0d9c0d9c019RQ
MD5:	7C8BDEEB64D8FED2B3E4B33EB532ED9A
SHA1:	2B8171BFD695A419D6A7C809C5CAE7045E986507
SHA-256:	58FC63DFFCE27D3EB9133935C6C411D2332AC2EC7753FB56545FB6A5831196B7
SHA-512:	96CDF52EA5A2DDE0297E5257FF9ACDBA70E3D6ED163C5B8247F8287926A84D44C5FBCE8C69B55C8D75E12CEEBDD7476D9E3652FF6D5407011C1F6C7F041F9 3E
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="_uetsid" value="14d8e860758311eb86278ded896e289b" ltime="3600247712" htime="30869903" /><item name="_uetsid_exp" value="Wed, 24 Feb 2021 02:59:01 GMT" ltime="3600247712" htime="30869903" /><item name="_uetvid" value="14d98790758311eb8bfe25059e976afa" ltime="3600247712" htime="30869903" /><item name="_uetvid_exp" value="Thu, 11 Mar 2021 08:59:01 GMT" ltime="3600247712" htime="30869903" /></root><root><item name="_uetsid" value="14d8e860758311eb86278ded896e289b" ltime="3797467712" htime="30869903" /><item name="_uetsid_exp" value="Wed, 24 Feb 2021 02:59:21 GMT" ltime="3797467712" htime="30869903" /><item name="_uetvid" value="14d98790758311eb8bfe25059e976afa" ltime="3600247712" htime="30869903" /><item name="_uetvid_exp" value="Thu, 11 Mar 2021 08:59:01 GMT" ltime="3600247712" htime="30869903" /></root><root><item name="_uetsid" value="14d8e860758311eb86278ded896e289b" ltime="3797467712" htime="30869903" /><item name="_uetsid_exp" value="Wed, 24 Feb 2021 02

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{1063455C-7583-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.85522332072783
Encrypted:	false
SSDEEP:	48:IwiGcprn7GwpLRG/ap8SGIpcNUGvnZpvNF7GoSqp9NFUiGo4tpmNQZUoWGWII9N9:rWZnVZV2SWNdtNhfNatMNfNYNRfNRsX
MD5:	E039D0C35FA33551E35B0B6AEB7C8453
SHA1:	437E4955BA08A8FC5BD9685EB64835A2C8D6AA55
SHA-256:	0B73A953B0B64258F13E7F18C6C19D3F81EB4754514634D3E6E2AEC0B4461F48
SHA-512:	48B7115E1C874699C3762FF3277B3B862B316D62D4EE2DADF972D135ED581F21C1C6F278BE7D04ABB5CE2F94FFAA7A3EE95BB06BD63BB4CB19681C294030396 3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{1063455C-7583-11EB-90E4-ECF4BB862DED}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{1063455E-7583-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	200316
Entropy (8bit):	2.75251750498267
Encrypted:	false
SSDEEP:	768:34CIoYM02krC0VLxIngXjlFek52o88ZmlP02wdPlmXFxa:iFt
MD5:	B3AFB98C0BCD04BEF8B8DA2BD6272575
SHA1:	E55624656DBE9DC317F9C94BE53058EA8F0FF5BE
SHA-256:	661B212A20E9835D732F038589919E83C0D36793560CAFCDABADD40E42F6689F
SHA-512:	029536E96010678C2668EBD74E3EAADCBF1D30BF9553EEA25128A9F481695DC29B7B173950092FCEA2F27A9A1E62B1BD611B2D40859E2240D43EA953D2ED151
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{19D90101-7583-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5643342469021078
Encrypted:	false
SSDEEP:	48:IwmGcprzGwpamG4pQGGrapbSxGQpKmG7HpR6TGIpG:r6ZtQW6IBSLART+A
MD5:	B0F1B1FE54BF3E98C9EEB64B627E0A3A
SHA1:	10A7D9737E56EF3AC70F98BBC383626EC1FDE6FB
SHA-256:	B8E5FAF372F30BDDB1AF79D14616C1644DEC4C22969556D61864D7650E394529
SHA-512:	4841A74A23530417AB06AC03866C626BD3857B31B3F1B9FAAECC9CFD8478DACC67FC2ED69B88FED508D2D10C60FA54D83179B60375C72FA3C5B0ECBAB2994 C1
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	1294
Entropy (8bit):	5.141892106579026
Encrypted:	false
SSDEEP:	24:+uHfTaNOmjlMq/jpxMwdjRQ0UrMIgQb8pswoDvh6nFqtbO:+uH6OmR3xRnU1Yuwyhi8O
MD5:	0D349E0F280FD1E285781C50DB847462
SHA1:	E3E59ADCC725B90AEA8A4FB22F6D5471CB343B34
SHA-256:	E85B4D9C9BECF1CCF7B5AD2AEC4B70E9EFD7A85C894DE3569FE195890FA9FD42
SHA-512:	DEFBBB6E4DEBFA342F7D8D15E1DCD885AB46EFBEF730C8288C24D6B309E43E92C25E38F5002EA9B652C4BD05921697895D681E144B3425239EE6B540EC3C85 C4
Malicious:	false
Reputation:	low
Preview:	5.h.t.t.p.s.:././.s.t.o.r.a.n.g.e.g.o.o.g.l.e.a.p.i.d.d.p...a.g.i.l.e.c.r.m...c.o.m./.f.a.v.i.c.o.n...i.c.o.~..... .h.....(..... ....p...p...p...p...p...p...o...q...p...q...q ...q...p...p...p...u...u...u...u...u...u...u...u...v...u...u...u...u...u...u...u...{$..{$...,..;..=..:..<..=..<..=..>..<..5..}).z#..z#...)..E.....6...)..7..... .....|..0..N.....9..V.....B..J.....B..I..o..... .....[..J..S..P..b.....Y..P..S..Y..X..U.....T..Y..Y.._..._..^..i.....x..]..._..`..f..f..f..e..b..a..|.....d..f..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\141590300270327[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\141590300270327[1].js	
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	492644
Entropy (8bit):	5.466759589515212
Encrypted:	false
SSDEEP:	6144:Rk1HWCSntDV/H4K3V/H486EPjQHWuH3Hpxk1HWCSntDV/H4K3V/H486EPjQHWuHF:f6E46E2
MD5:	8B9BABEEB620E5C5D82D7165F3B2D305
SHA1:	BAF1E6354E6EAC227159BA78F67FA1BA34792FB0
SHA-256:	9A749F82068531D2A35F42D01F42E1947F0B54793BE832785980477048DFBB55
SHA-512:	025F2C13DFF2079911ED293B96D959B6A4EB5BFA3E3B80BE20112EDEF59ECA05F0909E1760A79541FE3175048C524332B332FFEC534639B4081AB893CCFF3C5D
Malicious:	false
Reputation:	low
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\141590300270327[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	246322
Entropy (8bit):	5.466759589515212
Encrypted:	false
SSDEEP:	6144:Rk1HWCSntDV/H4K3V/H486EPjQHWuH3HpH:f6E2
MD5:	348AFD7BD47729F11B6FED351FBC991C
SHA1:	49D7DD41559F7A8FE8C0C39BC69B44AB6D8A746E
SHA-256:	113E5E2F3912C9271BC8D2BB386DE5F649F9326F1CC308100F493EEC0B90223F
SHA-512:	9C8A8E325D37F63DB367D1899C1F1BCC4243FBA327F53C2C1816C1AD326A7B41F4B5D65622BABC24F5B1D09F0601BD5536109A9912D91295133B27EDAD75515
Malicious:	false
Reputation:	low
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\agile-min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	C source, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	64261
Entropy (8bit):	5.453547763855676
Encrypted:	false
SSDEEP:	1536:Eb49cD6LWunM8GsRZBZDmsPY/QBU9eyMHDDcbzprsaWzUTC4H9z3PXBBxKpSA9:X9cTsPYZ97Bc
MD5:	F2B5B11FADB71A368726E5C3359858EE
SHA1:	84E11C7FBB064F7A2B022B18F7DB13180A05165A
SHA-256:	3DFA9239012B3CD2737CDB2B0370DC9F9C253D38883F48ACE64590E0CDD8B7C5
SHA-512:	5470A3154942144249AE3DD89A5CBA48DC150301EC3D7790595C18076DD5A5A7324BC2A9CA66338A85A42234C425064B497237E2B0CD99D57C3E62822F8CFB37
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://d1gwclp1pmzk26.cloudfront.net/agile/stats/min/app/v11/agile-min.js
Preview:	function agile_createContact(r,c){var b={};var e=[];for(var s in r){if(r.hasOwnProperty(s)&&s!="tags"&&s!="lead_score"&&s!="agile_source"){e.push(agile_property JSON(s,r[s]))}}var k=agile_read_cookie(agile_guid.cookie_original_ref);var f=agile_read_cookie(agile_guid.cookie_tags);var j=agile_read_cookie(agile_guid.cookie _score);var t=agile_read_cookie(agile_guid.cookie_campaigns);var p=agile_getUtmParamsAsProperties();var a=agile_read_data("agile-browser-id");var l=agile_guid.g et();b.properties=e;if(k){e.push(agile_propertyJSON("original_ref",k))}if(p&&p.size!=0){try{e.push.apply(e,p)}catch(d){console.debug("Error occured while pushing utm para ms "+d)}}if(r.tags){var h=r.tags;var m=h.trim().replace("/ /g"," ");m=m.replace("/, /g",",");b.tags=m.split(",");for(var o=0;o<b.tags.length;o++){b.tags[o]=b.tags[o].trim()}}if(f){ agile_delete_cookie(agile_guid.cookie_tags);var m=f.trim().replace("/ /g"," ");m=m.replace("/, /g",",");var g=m.split(",");if(b.tags){for(var o=0;o<g.length;o++){b.tags.p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\agile-webrules-min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\agile-webrules-min[1].js	
Category:	downloaded
Size (bytes):	39245
Entropy (8bit):	5.389699995272089
Encrypted:	false
SSDEEP:	768:+P+jPJ5ycb1ZKp01Zzyd0rsZG4ihqIeJ4rQkR58zlOUnknDDP2SYPSfA5aIX8rUC:+P+jPJ5yc3Od0rs0cwP0kOUoohWKUI6k
MD5:	8905DC1D776F9BCE281CDBCA7A515B7F
SHA1:	0F7356312660595ECB0AADE73EC86A1BDC2B8FBC
SHA-256:	E260B9C304598205A322374408F2E2718ACAB63E585AF74E41FB69179D3B4337
SHA-512:	CB5D64B3E42A179D4DD26A939CFB490D5389B07EF01E33C5B77ADF3B1C5CC9806244834EDE145075B334456D6F257D3C55FAC2470F2EA4A8D21EB4C62C188AF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://s3.amazonaws.com/agilecrm/web-rules-static/agile-webrules-min.js
Preview:	function _agile_execute_action(action){switch(action.action){case"MODAL_POPUP":_agile_when(action,function(){_agile_show_modal(action)});break;case"FORM":_agile_when(action,function(){_agile_show_modal(action)});break;case"CORNER_NOTY":_agile_when(action,function(){_agile_show_noty(action)});break;case"ASSIGN_CAMPAIGN":_agile.add_campaign({id:action.RHS});break;case"UNSUBSCRIBE_CAMPAIGN":_agile.unsubscribe_campaign({id:action.RHS});break;case"ADD_TAG":_agile_tag_web_rule_actions.toadd.push(action.RHS);break;case"REMOVE_TAG":_agile_tag_web_rule_actions.toremove.push(action.RHS);break;case"JAVA_SCRIPT":eval("["+action.popup_text.value+"]");break;case"ADD_SCORE":_agile.add_score(action.RHS);break;case"SUBTRACT_SCORE":action.RHS=action.RHS<0?action.RHS:-action.RHS,_agile.add_score(action.RHS);break;case"CALL_POPUP":_agile_when(action,function(){_agile_show_modal(action)});break;case"SITE_BAR":_agile_when(action,function(){_agile_show_site_bar(action)});break;case"REQUEST_PUSH_POPUP":agile_

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\agilecrm-login-new[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 548 x 566, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	100510
Entropy (8bit):	7.969387154178837
Encrypted:	false
SSDEEP:	3072:YpsZFzE3MaZU0FU2nzVnZeS/4EOwwpj4mFjLJ2RheS:9Fz5pIRZTXYjDS
MD5:	373C57701DF7A3C77225A320F9A2B414
SHA1:	313D0E794F218F7C76B5AF04535DFC087E6F1195
SHA-256:	FF0540CDFC6C99543553FE5852D85800CCDE895AA49A09A4DA46C267EDC10B73
SHA-512:	4B93678AF97572CB3DC08711DCEBB8F951D81BCBB418D55228752F12E97FC327A10ADA54DC9610A54103A0AC908210AE008177828EAA1FE360D848439C57F3C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/static/images/agilecrm-login-new.png
Preview:	.PNG.....IHDR...$...6.....W3c.....PLTEdb]ec^ed`ba\b`Z``Yec_baZeeba^Xd`Z`^U]\VebZb`WYXRXVP\[Tcc]e`We^X_\U`\Qb`Tc^U``\QOI\YQf]UURL^]XWTN^ZO RQKMJCHE?JHAZZTMLE\YMcM8TTOFC<^ZS]\QONHDA:YUIPMFeP;hgdUQI]H8`E4h\UhfaZVNYXLY@0ZE6]E4^@0\WIYUF`K8@=6`dYgQEB?8d]RgYQX>,<92 ?;3gWNZYOaN;gUFdZLYC3eZS^D1IIC]_UU?/MJ?gUJU;*bZP[B0fL=g\QKG=74,`G8:70...WRDcH9HD9dJ;fNAPL@I2....?-.fZOP<,9'.4&.9*.S8&0#.eaRSOCC1.fO#aI5SRD*' .aA12/%`ZKUVIg[HN5!\B3[_[[</31*=*.U]_,..5$....%#.fRAM7& ..H3$eaLbN@JH9DA4UB3G=0D3$=- gY@JB4N8*cUIgb&aVL"..0 .WI8gM'0+"bQE`_EVP@^J=\OBOJ:\I3D-.gQ.A8,S`#f_?``M(..^UCcC6\\N]SHA=/H8&Z8+f`EP@0;8+V\XaWF'..82%%XL>, .gH.+,%gT8HVXB.#d\5__?P<$[Q(SM<\R:`U?>3)S2)mkfgc.UB)a9,QE:O,#PF2!..XG/J4* RM$OPBM[[fC@gF7FG!gL.?ZZG(.]XGg;Hg5AU80DRTgJK>NQgRS5..d[)Z0'?F<gc8c97?!.KC*d.0_B*Xa2...T+?/VW8IMI6GLOK7@8.WWAGL`#7/8/8@J.NQ.ZWC.0. ..=...YIDATx...L[u....6m.*Gkq.5...S.`....@.N.....,L..... .....Xi..J) ...%..A.....\.#.Q.....k9.5./..J[(.}..w....u...U.TJdB.....|...Rq..0t...]m...\....x.soL....y|fx.....x<l..y<.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\btn_yahoo_signin[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 187 x 43, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	3878
Entropy (8bit):	7.800827357922713
Encrypted:	false
SSDEEP:	96:w2N6hz7Roc3qGqPM/FigXRz51TG3GZOdhhL1LO8ZMPZzX:Yhz/dqU/FPwvvpZuzX
MD5:	57B468AFD47B3BA274F2BDF7AAA5A81F
SHA1:	A213D1F58992C57FACBE85AC2A1793B1782014C3
SHA-256:	B46CFD8EA5259F75A865F1B401A5C05A60EC805B45A7692D46C6072B380C7AC7
SHA-512:	559F5C75FDEF7421448F2623FACDF4EE95F3049636610855B4E0D78D880415FC5CAFB041CC306D6F3F2E9992462914BE313F30FE4F0AF64890DFE5D7EAF84ECB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://storangegoogleapiddp.agilecrm.com/images/btn_yahoo_signin.png
Preview:	.PNG.....IHDR.....+..... ..)....tEXtSoftware.Adobe ImageReadyq.e<...#iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c140 79.160451, 2017/05/06-01:08:21 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CC (Macintosh)" xmpMM:InstanceID="xmp.iid:4D3445B05C1211E8A0D78AAC04758936" xmpMM:DocumentID="xmp.did:4D3445B15C1211E8A0D78AAC04758936"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:4D3445AE5C1211E8A0D78AAC04758936" stRef:documentID="xmp.did:4D3445AF5C1211E8A0D78AAC04758936"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>..-.....IDATx..].IT.....|.....up. ..BC.....*.h+P.RUH...Z.RU.PE.i.Z"...qI.Z.....0.C}.....z....[..8.EO..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\fbevents[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	280128
Entropy (8bit):	5.3917536957896575
Encrypted:	false
SSDEEP:	3072:5OQRj1SVBYDGKOQRj1SVBYDGKOQRj1SVBYDG2:5OCJS8DGKOCJS8DGKOCJS8DG2
MD5:	A30952DC0D1CB4C1DD74447AD09B2EF6
SHA1:	AD6E2CED66B5B38EEED3D7C8AF9125BAA0FEE67A
SHA-256:	687E72C3A15BFA15B011C391EA82FD80BDCA0554F80B97D1259300B51DA31D94
SHA-512:	3C0D4DB2DE0A0E582ACD708AD69312640CBFC6E1F33737A34B447E522E52EC7D6FC9662760FA84A6DEE7DC044AE1618D08B48D879CCE93C700B60A32AD013 8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://connect.facebook.net/en_US/fbevents.js
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\handlebars.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	44084
Entropy (8bit):	5.527841208101969
Encrypted:	false
SSDEEP:	768:ruQFfD7x7JAOB5iWVvU+rhLaaul1TO8cBs+6FyHAl:ruQhDtuavVd39u+9Al
MD5:	594CC6EE15FBFC40C3211778B6882431
SHA1:	68CF61223F35B310D37D65FC8BD39C86768DCCC4
SHA-256:	2DC9A1C2111185E85B712BBA38D54BE78740CC9AE1A128A0A8393E37767D81AE
SHA-512:	33AF81CD573D2B1D4D73D0B558BB433E1F39D9013F1F04D0A8BFE7B73A7308817966639B057DBFCE63F18C5CF28B0D62CCAFB116A26C97F724A16B53808AC14
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/handlebars.js/1.3.0/handlebars.min.js
Preview:	/*!.. handlebars v1.3.0..Copyright (C) 2011 by Yehuda Katz..Permission is hereby granted, free of charge, to any person obtaining a copy.of this software and associated d ocumentation files (the "Software"), to deal.in the Software without restriction, including without limitation the rights.to use, copy, modify, merge, publish, distribute, sublicense, and/or sell.copies of the Software, and to permit persons to whom the Software is.furnished to do so, subject to the following conditions:..The above copyright notice and this permission notice shall be included in.all copies or substantial portions of the Software...THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,.FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE.AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER.LIABILITY, WH ETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,.OUT O

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\head.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines
Category:	downloaded
Size (bytes):	9680
Entropy (8bit):	5.241537457604115
Encrypted:	false
SSDEEP:	192:vwFWRF4U5LRSwFKd+F5FDP8Zn/J3vUkHVyRVy/DpAC4NWx59l32UgyfMYeR:vRH5LRSSKd+jFIFcUyHy7pAC4kx5r32X
MD5:	CDA51F90890BC6411432994F00EC49C5
SHA1:	8C9495C76D5AA00D3DFB88653C362FBA9F10CBB2
SHA-256:	FB4F642E1C0008A5C53C3BEAA38C4C32F8B8FAE5C5B11676B9819B78DD54F2C2
SHA-512:	F0D93FCE84CA8CD8B19CCD79C178E9176E8A4782E7F3B71CE58965739C4FE78C306DC2A79630009F624FFAD6004BCFB87BBB3F5CAF174E20C7D0BB70D9F9A 05
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/headjs/1.0.3/head.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\head.min[1].js	
Preview:	./*! head.core - v1.0.2 */.(function(n,t){"use strict";function r(n){a[a.length]=n}function k(n){var t=new RegExp(" ?\\b"+n+"\\b");c.className=c.className.replace(t,"")}function p(n,t){for(var i=0,r=n.length;i<r;i++)t.call(n,n[i],i)}function tt(){var t,e,f,o;c.className=c.className.replace(/ (w-|eq-|gt-|gte-|lt-|lte-|portrait|no-portrait|landscape|no-landscape)\d+/g,"");t=n.innerWidth||c.clientWidth;e=n.outerWidth||n.screen.width;u.screen.innerWidth=t;u.screen.outerWidth=e;r("w-"+t);p(i.screens,function(n){t>n?(i.screensCss.gt&&r("gt-"+n),i.screensCss.gte&&r("gte-"+n)):t<n?(i.screensCss.lt&&r("lt-"+n),i.screensCss.lte&&r("lte-"+n)):t===n&&(i.screensCss.lte&&r("lte-"+n),i.screensCss.eq&&r("e-q"+n),i.screensCss.gte&&r("gte-"+n))});f=n.innerHeight||c.clientHeight;o=n.outerHeight||n.screen.height;u.screen.innerHeight=f;u.screen.outerHeight=o;u.feature("portrait",f>t);u.feature("landscape",f<t)}function it(){n.clearTimeout(b);b=n.setTimeout(tt,50)}var y=n.document,rt=n.navigator,ut=n.loca

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	93100
Entropy (8bit):	5.300526104474089
Encrypted:	false
SSDEEP:	1536:q4mCgi8DyCuXXFiJ+L0kJQsJVPEKLQRZdC/RlfDknv+p0WzH/IoSZ7qABZnu0sFv:qGsKXlI2p0WPSbDrstfam
MD5:	E0E0559014B222245DEB26B6AE8BD940
SHA1:	E2F3603E23711F6446F278A411D905623D65201E
SHA-256:	89A15E9C40BC6B14809F236EE8CD3ED1EA42393C1F6CA55C7855CD779B3F922E
SHA-512:	60740DA8F871B8263675DB2421B0E565FC18E95C772F7C3D5916F224263CD71A6A2E6ACCEAB2F6F8BA1C0607951F0198F525D87D0589FA57045B1D5F292DACF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/jquery/1.10.2/jquery.min.js
Preview:	/*! jQuery v1.10.2 | (c) 2005, 2013 jQuery Foundation, Inc. | jquery.org/license.//@ sourceMappingURL=jquery.min.map.*/.(function(e,t){var n,r,i=typeof t,o=e.location,a=e.document,s=a.documentElement,l=e.jQuery,u=e.$,c={},p=[],f="1.10.2",d=p.concat,h=p.push,g=p.slice,m=p.indexOf,y=c.toString,v=c.hasOwnProperty,b=f.trim,x=function(e,t){return new x.fn.init(e,t,r)},w=/[+-]?(?:\d*\.\|)\d+(?:[eE][+-]?\d+\|)/.source,T=/\S+/g,C=/^[\s\uFEFF\xA0]+\|[\s\uFEFF\xA0]+$/g,N=/^(?:\s*(<[\w\W]+>)[^>]*|#([\w-]*))$/,k=/^<(\w+)\s*\/?>(?:<\/\1>\|)$/,E=/^[\],:{}\s]*$/,S=/(?:^|:|,)(?:\s*\[)+/g,A=/\\(?:["\\\/bfnrt]|u[\da-fA-F]{4})/g,j=/"[^"\\\r\n]*"|true|false|null|-?(?:\d+\.|)\d+(?:[eE][+-]?\d+|)/g,D=/^-ms-/,L=/-([\da-z])/gi,H=function(e,t){return t.toUpperCase()},q=function(e){(a.addEventListener||"load"===e.type||"complete"===a.readyState)&&(_(),x.ready())},_=function(){a.addEventListener?(a.removeEventListener("DOMContentLoaded",q,!1),e.removeEventListener("load",q,!1)):(a.detachEvent("onreadystatechange",q)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\js-all-min-1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	613284
Entropy (8bit):	5.360812227993317
Encrypted:	false
SSDEEP:	12288:9MtVRCbPg0+YDCg1Ppvpm0ECf5k8k10Nmee:9MtVRCbPg0+Ymg1Ppvpm0ECf5k8k10NG
MD5:	1B8A96D86ADF001130EC48A0853A10DA
SHA1:	39448826DE7AD5B270E5F887787366904AEEC862
SHA-256:	5F7AF2AA288DB2FAFAFC3F91162E9A28578D1A68FB06F79AE9FAE0BA3C4E7BF4
SHA-512:	BAD31A382C801070C8B488D939535295545C5563F0B5A33875C9B35851ABF0C3B455295CEE087FD34F624B31C244306AA41B2C0B60F908B1FE1DCF98FC5BD5F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/68-7/jscore/min/locales/fr/js-all-min-1.js?_=68-7.432843952504576280
Preview:	Backbone.View.prototype.close=function(){this.remove();this.unbind();if(this.onClose){this.onClose()}};var BaseModel=Backbone.Model.extend({});var BaseCollection=Backbone.Collection.extend({model:BaseModel,initialize:function(b,a){this.restKey=a.restKey;if(a.sortKey){this.sortKey=a.sortKey}if(a.descending){this.descending=a.descending}this.sort_collection=a.sort_collection;if(this.sort_collection==false){this.comparator=false}},comparator:function(a){if(this.sortKey){if(this.descending==true){return -a.get(this.sortKey)}return a.get(this.sortKey)}return a.get("id")},parse:function(a){if(a&&a[this.restKey]){return a[this.restKey]}return a}});var Base_List_View=Backbone.View.extend({events:{"click .delete":"deleteItem","click .edit":"edit","delete-checked .agile_delete":"deleteItem","click .delete-model":"deleteModel","click .delete-confirm":"deleteConfirm","click .delete-with-confirmation":"deleteModelAfterConfirmation",},initialize:function(){_.bindAll(this,"render","deleteItem","edit"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\js-all-min-2[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	887995
Entropy (8bit):	5.3795445754419156
Encrypted:	false
SSDEEP:	24576:WmFRktzKZIUMytIur2fcvEVfQ6gRNPLUCHXF4CR:WmFRktzKZIU/tIur2fcvEVfQ6gRNPLUg
MD5:	9C2849E88E6AE1B10BA0DE70E2525F97
SHA1:	119BDA2AA423A8B59053A357E159EFE6AE7DE50A
SHA-256:	AE7C6F7391A1E550E1C39D3627AA742558179C452EF54CE55C16339B92F1AFDF
SHA-512:	35F12D6F8406EBDB84F355EA3312B9EC56B6E04674F637D7B749B57299680F4E3BDEC8EEDC88A5E442584406E4F43D9BC8D453E883BA6CC0554EA4E4F3B8BC5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/68-7/jscore/min/locales/fr/js-all-min-2.js?_=68-7.432843952504576280

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\js-all-min-2[1].js	
Preview:	function initWebruleChartsUI(a){initDateRangeforForm(a);a()}function showWebruleGraphs(a){showBar("core/api/webrule-analytics/web/graphreports/"+a+getOptions()+"&type=date","line-daily-chart","daily","Count",null);showBar("core/api/webrule-analytics/web/graphreports/"+a+getOptions()+"&type=hour","line-hourly-chart","hourly","Count",null);showBar("core/api/webrule-analytics/web/graphreports/"+a+getOptions()+"&type=day","line-weekly-chart","weekly","Count",null)}function getOptions(){var b="?";var a=$("#range").html().split("-");var e=getUTCMidNightEpochFromDate(new Date(a[0]));var g=$.trim(a[1]);if(g){g=g+" 23:59:59"}var c=getUTCMidNightEpochFromDate(new Date(g));c+=(((23*60*60)+(59*60)+59)*1000);b+=("start_time="+e+"&end_time="+c);var j=new Date();b+=("&time_zone="+j.getTimezoneOffset());if($("#frequency").length>0){var f=$("#frequency").val();b+=("&frequency="+f)}if($("#filter").length>0){var h=$("#filter").val();if(h!=""&&h!="ALL"){b+=("&filter="+h)}}return b}function get_webrule_tab

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\js-all-min-2[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	886005
Entropy (8bit):	5.376978991878418
Encrypted:	false
SSDEEP:	24576:WPNnk3OKPqUbzV40rmncvEVcQYxRNbLaaaSssYR:WPNnk3OKPqU3V40rmncvEVcQYxRNbLat
MD5:	1BABCDA64989FA6D7C847822A67E84F4
SHA1:	56751B5BA5F796FA46EBC997B717FF30581A8168
SHA-256:	D8E2F2E035591011CF50FDB0413A23FA9334561B11E828C6E8624DFE81419843
SHA-512:	78E2E6C97A3166E173423190176ADDE388C0425B6C262B18CBF5CAD0F9B3BD4142D90AEFD53AC8EBD2154F7E690DBF8CF3E17D66EF45098328A095D48DF8463
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/68-7/jscore/min/locales/pt/js-all-min-2.js?_=68-7.432843952504576280
Preview:	function initWebruleChartsUI(a){initDateRangeforForm(a);a()}function showWebruleGraphs(a){showBar("core/api/webrule-analytics/web/graphreports/"+a+getOptions()+"&type=date","line-daily-chart","daily","Count",null);showBar("core/api/webrule-analytics/web/graphreports/"+a+getOptions()+"&type=hour","line-hourly-chart","hourly","Count",null);showBar("core/api/webrule-analytics/web/graphreports/"+a+getOptions()+"&type=day","line-weekly-chart","weekly","Count",null)}function getOptions(){var b="?";var a=$("#range").html().split("-");var e=getUTCMidNightEpochFromDate(new Date(a[0]));var g=$.trim(a[1]);if(g){g=g+" 23:59:59"}var c=getUTCMidNightEpochFromDate(new Date(g));c+=(((23*60*60)+(59*60)+59)*1000);b+=("start_time="+e+"&end_time="+c);var j=new Date();b+=("&time_zone="+j.getTimezoneOffset());if($("#frequency").length>0){var f=$("#frequency").val();b+=("&frequency="+f)}if($("#filter").length>0){var h=$("#filter").val();if(h!=""&&h!="ALL"){b+=("&filter="+h)}}return b}function get_webrule_tab

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\js-all-min-3[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	928603
Entropy (8bit):	5.6934228465105825
Encrypted:	false
SSDEEP:	12288:bwtktfY9/OfVMxnrMUQfsQpz+4YzDvDAqFRB:bwB9/OfVMxnoUQvQEqrB
MD5:	FC345EB7A8E959280B02D48F5609E65C
SHA1:	1AA545F9D3E0AB550305E3997895F1BAB6505CE3
SHA-256:	A727B5D0EEE9815FD348F8AC5B136A8F90DD6C4EB2243CA974DAC7AC712F30AF
SHA-512:	95AACB848745C02A6C41B1DFA8B73AB73414A7CDFEB9217A555C694148BA7D1D33F7EB0B8B5A7ACA5D8D5D2D6737EA9B597FB0F3D9FF5CCF677FED65A1A108EE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/68-7/jscore/min/locales/fr/js-all-min-3.js?_=68-7.432843952504576280
Preview:	var Email_Template_Events=Base_Model_View.extend({events:{"click .merge-field":"onMergeFieldSelect","click .add-attachment-select":"onAddAttachmentSelect","click .add-attachment-confirm":"onAddAttachmentConfirm","click .add-attachment-cancel":"onAddAttachmentCancel","click .add-tpl-attachment-confirm":"onTemplateAddAttachmentConfirm","click .add-tpl-attachment-cancel":"onTemplateAddAttachmentCancel","change #attachment-select":"onChangedAttachment",},onMergeFieldSelect:function(c){c.preventDefault();var b=$(c.currentTarget).attr("name");var d=$("#email-template-html").val();var f=$("#email-template-html").data("wysihtml5");if(f){editor.focus();f.editor.composer.commands.exec("insertHTML","{{"+b+"}}")}},onAddAttachmentSelect:function(g){g.preventDefault();var b=$(g.currentTarget);var f=$(b).closest("div");$(b).css("display","none");f.find(".attachment-document-select").css("display","inline");var c="<option value='{{id}}' network_type='{{titleFromEnums network_type}}' size='{{size}}'>{{

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\js-all-min-3[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	927699
Entropy (8bit):	5.69226611973665
Encrypted:	false
SSDEEP:	12288:UOX7sspr/OLVWxnjEUQIzIXz64YzDSYAqmRw:UO9r/OLVWxnYUQbKeq6w
MD5:	CDE52788C4B8FE4C85DB4F4DBC99DEA8
SHA1:	6324BADCD603846D687B9F24885BA1AD4ED01FBB
SHA-256:	1655AD71879BB8805E0A070FF0C9B05796CF9FB34E091B7FDC9328500F9AEB92

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\js-all-min-3[2].js	
SHA-512:	FB622611BF62FF2ECE9C8A2A0DC0DBE47304444421E8C55A4F6C27BD8C6714E807A0B4CBEA196F65B69EFF4E38C3676DA957F3F3E86B65559D7AB0C8768CDEEA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/68-7/jscore/min/locales/pt/js-all-min-3.js?_=68-7.432843952504576280
Preview:	var Email_Template_Events=Base_Model_View.extend({events:{"click .merge-field":"onMergeFieldSelect","click .add-attachment-select":"onAddAttachmentSelect","click .add-attachment-confirm":"onAddAttachmentConfirm","click .add-attachment-cancel":"onAddAttachmentCancel","click .add-tpl-attachment-confirm":"onTemplateAddAttachmentConfirm","click .add-tpl-attachment-cancel":"onTemplateAddAttachmentCancel","change #attachment-select":"onChangedAttachment",},onMergeFieldSelect:function(c){c.preventDefault();var b=$(c.currentTarget).attr("name");var d=$("#email-template-html").val();var f=$("#email-template-html").data("wysihtml5");if(f){editor.focus();f.editor.composer.commands.exec("insertHTML","{{"+b+"}}")}},onAddAttachmentSelect:function(g){g.preventDefault();var b=$(g.currentTarget);var f=$(b).closest("div");$(b).css("display","none");f.find(".attachment-document-select").css("display","inline");var c="<option value='{{id}}' network_type='{{titleFromEnums network_type}}' size='{{size}}'>{{

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jstz.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	5340
Entropy (8bit):	5.232128612886495
Encrypted:	false
SSDEEP:	96:xWLyvd0TDZAEc8nx/ZcxjeWx3lQqDiuBfJqbohoA4t4RSVwRdK8249rz1O:xWLXDhn5eQDXBfQbsoA4twSVMIUDO
MD5:	FB43A70ADF8DDF0853FFA88734D22B21
SHA1:	3D465833E59F8F3C721A82E49CFF071067D5FFFA
SHA-256:	538F30288AA121EB73B8F5408EAF086BD42AE067460DC99BB859F4A18950BAE0
SHA-512:	B956532379221403F4EB82A43D233E90D268BFA817DAE3092598E872655A9C40F51DC00734392BCF847C73D0E3EE840B17E58A78E41724361D4DC7A1A5A0B119
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/jstimezonedetect/1.0.4/jstz.min.js
Preview:	/*! jstz - v1.0.4 - 2012-12-18 */.(function(e){var t=function(){"use strict";var e="s",n=function(e){var t=-e.getTimezoneOffset();return t!==null?t:0},r=function(e,t,n){var r=new Date;return e!==undefined&&r.setFullYear(e),r.setDate(n),r.setMonth(t),r},i=function(e){return n(r(e,0,2))},s=function(e){return n(r(e,5,2))},o=function(e){var t=e.getMonth()>7?s(e.getFullYear()):i(e.getFullYear()),r=n(e);return t-r!==0},u=function(){var t=i(),n=s(),r=i()-s();return r<0?t+",1":r>0?n+",1,"+e:t+",0"},a=function(){var e=u();return new t.TimeZone(t.olson.timezones[e])},f=function(e){var t=new Date(2010,6,15,1,0,0,0),n={"America/Denver":new Date(2011,2,13,3,0,0,0),"America/Mazatlan":new Date(2011,3,3,3,0,0,0),"America/Chicago":new Date(2011,2,13,3,0,0,0),"America/Mexico_City":new Date(2011,3,3,3,0,0,0),"America/Asuncion":new Date(2012,9,7,3,0,0,0),"America/Santiago":new Date(2012,9,3,3,0,0,0),"America/Campo_Grande":new Date(2012,9,21,5,0,0,0),"America/Montevideo":new Date(2011,9,2,3,0,0,0),"America

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\login-v2-min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	477678
Entropy (8bit):	5.095264903923995
Encrypted:	false
SSDEEP:	1536:VQaFWRrhwX80XFLoU9l/C4H2xwZt20AKusFBxNgivTr7jObP3/3jjoACpjajUjLW:Vc3b/mWo1mleY883duvcchR/jYmwYL
MD5:	845FAC4DA2E22E5D380B6BF428598318
SHA1:	C1CF465D42E612F1419F9E5C46D6794891CE4D4F
SHA-256:	1D415D77E0FA07238C5046F21956153CA64879C23B62104169DE838F74C8A82F
SHA-512:	4A63B49F71585DB63B4A42208031988918495 3DC00DCCCAAD846EA5100671B06EB9C0EB73C96FF21017AE732D12FBC8CFE1DDAE2E0B7FBE73755054715A411DE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://storangegoogleapiddp.agilecrm.com/flatfull/css/min/login-v2-min.css
Preview:	/*! normalize.css v3.0.0 | MIT License | git.io/normalize */html{font-family:'PT Sans',"Helvetica Neue",Helvetica,Arial,sans-serif;-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%}body{margin:0}article,aside,details,figcaption,figure,footer,header,hgroup,main,nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-align:baseline}audio:not([controls]){display:none;height:0}[hidden],template{display:none}a{background:0}a:active,a:hover{outline:0}b,strong{font-weight:700}dfn{font-style:italic}h1{margin:.67em 0}mark{background:#ff0;color:#000}sub,sup{font-size:75%;line-height:0;position:relative;vertical-align:baseline}sup{top:-.5em}sub{bottom:-.25em}img{border:0}svg:not(:root){overflow:hidden}hr{-moz-box-sizing:content-box;box-sizing:content-box;height:0}pre{overflow:auto}code,kbd,pre,samp{font-size:1em}button,input,optgroup,select,textarea{color:inherit;font:inherit;margin:0}button{overflow:visible}button,select{text-transform:none}button,html i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\login[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	16636
Entropy (8bit):	5.323873689084472
Encrypted:	false
SSDEEP:	384:Mx7LBJmMrHT7C7ILizZMYoxGh0TsEUMJNRwo8mTp4S2yZGclUdzZ:YfeMzCGMoIhOJu5WuRZ
MD5:	396828F13258F161C12DABF4B1AFB67C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\login[1].htm	
SHA1:	A72B7C196FD7F4B4C8745F969D14399C3B476328
SHA-256:	C42245F68F57FA1D5D2E04B440FDEFEF58786F1C69E19384A6C9740FB4B59582
SHA-512:	8B228A324167DAB09926079316C889FB9CEC7C4618729D9CC6FB64FCB0F352E139D0D2653B5FA7C0050B44CBCA0F16B3CC262AA6FDDB954065A98D255B17F7A
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\login[1].htm, Author: Joe Security • Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\login[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://storangegoogleapiddp.agilecrm.com/login?lang=es
Preview:	.....<!DOCTYPE html>..<html lang="es" style="background:transparent;">.<head>.<meta charset="utf-8">.<meta name="globalsign-domain-verification". .content="-r3RJ0a7Q59atalBdQQIvI2DYIhVYtVrtYuRdNXENx" />.<title>Iniciar sesi.n</title>.<meta name="viewport" content="width=device-width, initial-scale=1.0 maximum-scale=1">.<meta name="description" content="">.<meta name="author" content="">.<meta name="robots" content="noindex, nofollow">..<link rel="stylesheet" type="text/css" href="/flatfull/css/min/login-min.css" />..<link href="https://fonts.googleapis.com/css?family=Roboto" rel="stylesheet">.. Include ios meta tags -->.<link rel="apple-touch-icon" href="ios/touch-icon-iphone.png">.<link rel="apple-touch-icon" sizes="76x76" href="ios/touch-icon-ipad.png">.<link rel="apple-touch-icon" sizes="120x120" href="ios/touch-icon-iphone-retina.png">.<link rel="apple-touch-icon" sizes="152x152" href="ios/touch-icon-ipad-retina.png">..<link rel="apple-touch-startup-image" href="i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\login[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	17424
Entropy (8bit):	5.60296679021902
Encrypted:	false
SSDEEP:	384:LUc7LDJmMiHymC3LWzZME4oxGh0TsEUMJNRVkZEvMMSb9v0vclUd0Z:Qcf0MpmCb/oIhOJ7kZpb9v0EuqZ
MD5:	3C1363A3AC6B0606EF01868AC1EB1C61
SHA1:	A4E8F88F0D596326C033674EBBBC359C0A63F144
SHA-256:	99A331ECD051A83F515B37DED41BFD17F2A26AE92AA58BB5B0D997B3C24AC41C
SHA-512:	E3C63E2A9C1169289BC3283FC35263295C864CB5C471BD2273CD894294BB9D500C45E8AEC612C2A65868EE9EBC0E1CA47955DC2D30BB628338BF234E117358
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\login[2].htm, Author: Joe Security • Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\login[2].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://storangegoogleapiddp.agilecrm.com/login?lang=ru
Preview:	.....<!DOCTYPE html>..<html lang="ru" style="background:transparent;">.<head>.<meta charset="utf-8">.<meta name="globalsign-domain-verification"..content="-r3RJ0a7Q59atalBdQQIvI2DYIhVYtVrtYuRdNXENx" />.<title>.....</title>.<meta name="viewport" content="width=device-width, initial-scale=1.0 maximum-scale=1">.<meta name="description" content="">.<meta name="author" content="">.<meta name="robots" content="noindex, nofollow">..<link rel="stylesheet" type="text/css" href="/flatfull/css/min/login-min.css" />..<link href="https://fonts.googleapis.com/css?family=Roboto" rel="stylesheet">.. Include ios meta tags -->.<link rel="apple-touch-icon" href="ios/touch-icon-iphone.png">.<link rel="apple-touch-icon" sizes="76x76" href="ios/touch-icon-ipad.png">.<link rel="apple-touch-icon" sizes="120x120" href="ios/touch-icon-iphone-retina.png">.<link rel="apple-touch-icon" sizes="152x152" href="ios/touch-icon-ipad-retina.png">..<link rel="apple-touch-startup-image" href="ios/st

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\login[3].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	23512
Entropy (8bit):	5.341743413296907
Encrypted:	false
SSDEEP:	384:E3GLnhsfFM8QVWnMzg4Jo6IvYff+1T7csMhUe2tNroxGh7TsEkMmNzdm7uWtISTE:acYFM8QonM/WYft2oIhn6zYnwtB
MD5:	B9285E748E5E23ECA09E86FD2DBA138E
SHA1:	3FB8426F6530F05784487F1003EF9382FAC1D0AD
SHA-256:	375B90AB11D1FBE2DF5436A63231848BB43D17A47CC4D4855084D59FD5445C68
SHA-512:	3E21F0EA2A6C86A319D02F723B12882DC0E59FAC85384B31B96EA7D5D0317733F55411D2CD7180380D90BD9B8C5ABAC496DC9C245B0EBC60659E3FD6B340C09
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\login[3].htm, Author: Joe Security • Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\login[3].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://storangegoogleapiddp.agilecrm.com/login?lang=fr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\login[3].htm	
Preview:	.....<!DOCTYPE html>..<html lang="fr" style="background:transparent;">.<head>.<meta charset="utf-8">.<meta name="globalsign-domain-verification"..content="-r3RJ0a7Q59atalBdQQIvI2DYIhVYtVrtYuRdNXENx" />.<title>Se connecter </title>.<meta name="viewport" content="width=device-width, initial-scale=1.0 maximum-scale=1">.<meta name="description" content="">.<meta name="author" content="">.<meta name="robots" content="noindex, nofollow">..<link rel="stylesheet" type="text/css" href="/flatfull/css/min/login-v2-min.css" />..<link href="https://fonts.googleapis.com/css?family=Roboto" rel="stylesheet">. Include ios meta tags -->.<link rel="apple-touch-icon" href="ios/touch-icon-iphone.png">.<link rel="apple-touch-icon" sizes="76x76" href="ios/touch-icon-ipad.png">.<link rel="apple-touch-icon" sizes="120x120" href="ios/touch-icon-iphone-retina.png">.<link rel="apple-touch-icon" sizes="152x152" href="ios/touch-icon-ipad-retina.png">..<link rel="apple-touch-startup-image" href="i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\login[4].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	23304
Entropy (8bit):	5.3337194258137
Encrypted:	false
SSDEEP:	384:0yGLnhsfFM8QVWnMz+4Jo6IvobVC1T5csMhUdtNroxGh7TsEkMmNzdmnMISeSocH:dcYFM8QonM1WobooIhn6zNDZB
MD5:	1E707B9AAA24B585038C231B2F96431E
SHA1:	C61D67F32F8B70A21C7A941507BA6E5D347F9768
SHA-256:	01A02B486D2CAF8F494887F99C10946E9FC9C1421C82BB1AE7C169884B4E91F2
SHA-512:	D5C08C7D4D49DB8F8B4A1FFD05ECA087688AEE00C3729951DA950DDDAFE05321DDE1A4892B79FAC1B1438C991345EF110348AC8883ABBF96D82855A8E816AC EA
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\login[4].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://storangegoogleapiddp.agilecrm.com/login?lang=pt
Preview:	.....<!DOCTYPE html>..<html lang="pt" style="background:transparent;">.<head>.<meta charset="utf-8">.<meta name="globalsign-domain-verification"..content="-r3RJ0a7Q59atalBdQQIvI2DYIhVYtVrtYuRdNXENx" />.<title>Entrar</title>.<meta name="viewport" content="width=device-width, initial-scale=1.0 maximum-scale=1">.<meta name="description" content="">.<meta name="author" content="">.<meta name="robots" content="noindex, nofollow">..<link rel="stylesheet" type="text/css" href="/flatfull/css/min/login-v2-min.css" />..<link href="https://fonts.googleapis.com/css?family=Roboto" rel="stylesheet">. Include ios meta tags -->.<link rel="apple-touch-icon" href="ios/touch-icon-iphone.png">.<link rel="apple-touch-icon" sizes="76x76" href="ios/touch-icon-ipad.png">.<link rel="apple-touch-icon" sizes="120x120" href="ios/touch-icon-iphone-retina.png">.<link rel="apple-touch-icon" sizes="152x152" href="ios/touch-icon-ipad-retina.png">..<link rel="apple-touch-startup-image" href="ios/star

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\material-icons[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	81239
Entropy (8bit):	4.804483759150772
Encrypted:	false
SSDEEP:	768:mR5bYP+Br3ytblioDT/PE7EGG/wRfKJOvij:mR5bYur3ioaEGG/wRfKJOvij
MD5:	0ECF02538FA8D12A71B28701DDA1E38B
SHA1:	9237BF70621D0877FC486202CEED3596D957B70F
SHA-256:	9B761341F115717D96F152E22381EF83737D4C3A1CC8F8D31860AC6F0DD03978
SHA-512:	A197AAA81A2447A64A1443B36ACF572CF5F53639AED57DBB9E713D16FAD332A4E6735C0B40720836D931EF6157D452997DAFBA2DF7C2C69A360C6DEFF57057F A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://storangegoogleapiddp.agilecrm.com/flatfull/css/material-theme/min/material-icons.css
Preview:	@font-face {. font-family: 'Material Icons';. font-style: normal;. font-weight: 400;. src: url(/flatfull/css/material-theme/icon/MaterialIcons-Regular.eot); /* For IE6-8 */. src: local('Material Icons'),. local('MaterialIcons-Regular'),. url(/flatfull/css/material-theme/icon/MaterialIcons-Regular.woff2) format('woff2'),. url(/flatfull/css/material-theme/icon/MaterialIcons-Regular.woff) format('woff'),. url(/flatfull/css/material-theme/icon/MaterialIcons-Regular.ttf) format('truetype');.}.material-icons {. font-family: 'Material Icons';. font-weight: normal;. font-style: normal;. font-size: 1.2em; /* Preferred icon size */. display: inline-block;. line-height: 1;. text-transform: none;. letter-spacing: normal;. word-wrap: normal;. white-space: nowrap;. direction: ltr;.. /* Support for all WebKit browsers. */. -webkit-font-smoothing: antialiased;. /* Support for Safari and Chrome. */. text-rendering: optimizeLegibility;.. /* Support for Firef

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\portlets[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	485102
Entropy (8bit):	5.567103663323704
Encrypted:	false
SSDEEP:	6144:RrngsrCreBeBZBnBUg+OGmxElOem1EOOnO1mREVb26KF++fWKB+XKlK7Kh+tK5+j:TOGmxElOem1EJO1mRERa/v5DU
MD5:	7E2D00A0EBFD1C10BDDBDD900D74A5A3
SHA1:	813478E7D4C516DCCECDC4B534DE6F5BDFB22D65
SHA-256:	846864BD6FFBD0F94B4BA8D834565C82371B6FB2D17B3D6F92AF447020B47A42

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\portlets[1].js	
SHA-512:	C724A0E8835E8E9355C4C9EEAD59D322EC05E3F1BEC2DDC3CF77563DCC34E566AEDFF61D4B5C9403DAD05DDCED991F89061B9BB61B13F6371550F431C8A85B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/68-7/tpl/min/precompiled/locales/en/portlets.js?_=68-7.432843952504576280
Preview:	(function(){var b=Handlebars.template,a=Handlebars.templates=Handlebars.templates||{};a["marketing-video-modal-template"]=b(function(f,g,d,c,e){this.compilerInfo=[4,">= 1.0.0"];d=this.merge(d,f.helpers);e=e||{};return'\n. \n... \n.... \n.....<button class="close" data-dismiss="modal">×</button>\n.....<h3 class="modal-title">Marketing Tutorial</h3>. \n.... \n..... \n..... \n.....<iframe style="width:100%;" height="345" src="//www.youtube.com/embed/KP8feLANFZA?enablejsapi=10&autoplay=1&showinfo=0" frameborder="0" allowfullscreen></iframe>\n..... \n.... \n... \n. \n.\n'});a["mobile-app-options-template"]=b(function(g,m,f,l,k){this.compilerInfo=[4,">= 1.0.0"];f=this.merge(f,g.helpers);k=k||{};var j="",d,h,r,p=this,i="function",n=f.blockHelperMissing;function e(t,s){return" "}functio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\portlets[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	487840
Entropy (8bit):	5.542128937530664
Encrypted:	false
SSDEEP:	6144:seBWC0+n8e7W+0Re6Wr06DcJ90b464jrJI4wrJb4HrJDz77fLqHGaPD9B4IrJwTS:seBWC0Re7W+0Re6Wr0bmFN
MD5:	B49CA25346834326B3C57BE911B79930
SHA1:	EB746DB9062BDACAA7BDFAE1765FC9614D93C97A
SHA-256:	AF4128008B3A3D3E54526C3E30100B0759E9F21A894CE1C9F896DBEA1655E66D
SHA-512:	203E2FAAD3746D52EF0144D9E0C24BAAECF910AE26E9730B27AC79639DA38A914A8B57AD7233972E9725D43D21A0C1A46E5215BB5068E9ECB247A5E4F623F3A3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/68-7/tpl/min/precompiled/locales/pt/portlets.js?_=68-7.432843952504576280
Preview:	(function(){var b=Handlebars.template,a=Handlebars.templates=Handlebars.templates||{};a["marketing-video-modal-template"]=b(function(f,g,d,c,e){this.compilerInfo=[4,">= 1.0.0"];d=this.merge(d,f.helpers);e=e||{};return'\n. \n... \n.... \n.....<button class="close" data-dismiss="modal">×</button>\n.....<h3 class="modal-title">Marketing Tutorial</h3>. \n.... \n..... \n..... \n.....<iframe style="width:100%;" height="345" src="//www.youtube.com/embed/KP8feLANFZA?enablejsapi=10&autoplay=1&showinfo=0" frameborder="0" allowfullscreen></iframe>\n..... \n.... \n... \n. \n.\n'});a["mobile-app-options-template"]=b(function(g,m,f,l,k){this.compilerInfo=[4,">= 1.0.0"];f=this.merge(f,g.helpers);k=k||{};var j="",d,h,r,p=this,i="function",n=f.blockHelperMissing;function e(t,s){return" "}functio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\pt[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2139559
Entropy (8bit):	5.402660462434653
Encrypted:	false
SSDEEP:	12288:Z3lPdWfzlzdDfllidtfpJlb1iGK+vcQp7bzbxM9HEv9M0QbDkuRaZ0XrwArI1Egc:Zy1iGKSpluBXrwArI1EgRBOlbZ
MD5:	873EFFDFCB7750078D236B1ACB2AFA1B
SHA1:	1A5A8CF9F72D9E44EAD525709770D21EA4C76554
SHA-256:	6906E4B1A412682579D0D6933EB6716A6A76EA49092D1D08724F8CBA31124C13
SHA-512:	C53E6FECA58DA73B5100212E0C7420FD3BA6EE0EB97E727FEFC900756003695F5958C16DA691F26E98F0482A825664C2AC9BC86A3B8520BD37AB19A1B3C5E45
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/68-7/tpl/min/precompiled/locales/pt/pt.js?_=68-7.432843952504576280
Preview:	(function(){var b=Handlebars.template,a=Handlebars.templates=Handlebars.templates||{};a["account-delete-step2-template"]=b(function(f,g,d,c,e){this.compilerInfo=[4,">=1.0.0"];d=this.merge(d,f.helpers);e=e||{};return'\n \n \n \n <button type="button" class="close" data-dismiss="modal" aria-hidden="true">x</button>\n <h3 class="modal-title">Pedido de Cancelamento Recebido</h3>\n \n \n Lamentamos v.-lo sair. A Nossa Equipa de Suporte entrar. em contato consigo dentro de 48 horas, para saber mais sobre a raz.o de nos deixar. Por favor, observea sua subscri..o mantem-se ativa e a nossa Equipa de Suporte ir. ajud.-lo com o processo posterior. \n..Para saber o status do pedido, por favorEscreva-nos.\n. \n \n \n <a href="#" class="btn btn-prim

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\sourcesanspro-light[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 26540, version 1.1
Category:	downloaded
Size (bytes):	26540
Entropy (8bit):	7.977869110731841
Encrypted:	false
SSDEEP:	768:pxmiFOp6DJjMOBvrxmvIhZNfNI59xQyEDd:aiMpojMjvIzI59xgDd
MD5:	7951903BFF82A82E7CDE0396DFC9D80C
SHA1:	189F5D517CAA3E32F01736FFF6A921C5068ECF92

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\sourcesanspro-light[1].woff	
SHA-256:	E42643595230DB6D887CF16BA0E06F4FD0CE9C50E8931CBBD6E0167A0D960743
SHA-512:	8B58763DAC4D0E7EA018CC78CA744A10CF0FD0CE1CAFEEF377D848DA7DA83F4029CFE6FDC78967FEA26D2642EA58AC40686A716B006AEBC40A518EA8F58CD C85
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://storangegoogleapiddp.agilecrm.com/flatfull/font/sourcesanspro/sourcesanspro-light.woff
Preview:	wOFF.....g.....D.....FFTM...l.....jNi.OS/2.....T...`Z[.9cmap.....T...cvt ...x...(...(.s..fpgm.....s.Y.7gasp.....glyf.....0...\T...head..5H...3...6.r..hhea..5 |.....$.a.!hmtx..5.....Y*.kern..7.....IhQ1S.loca..Ql.....O89.maxp..SP... ... ...Cname..Sp.....;.qX.ipost..e\.....).b.Jprep..g`...K...K-h.y.....ZE.....\.\|x.c`f..... .....,.,.LL,@.;.P....].\....(..l...7....'....0.h .....x.b```.b..F.....1.,.....%.d.2.1.g4d.f:.t...3.3.3.....l.....B...%!%...../.....b@.%. . ..e.....O...?...?.....{.....z.....}.....<0.w..9. {...l@...L@..U.d.+.;.'.7./.....''@J.*.j...Z.:.z...F.&.f...V.6.v...N...n...^.>.~...A.....GDFE....'$&%3ttv.N..`.e+..\.v...7l.u....v....CIZz....E...9.]s.J..2+...cX..9....gHii.y...7o]....0. ..w..e.o.fh.k..8i..3...?.....'j.....(.,.0.....3.....>...~.....x.]..N.0...|...,$[V.*W.28.P.@.|..R+...)...<..-/.....]|w.;..O..I...K.O

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\sourcesanspro[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 27248, version 1.1
Category:	downloaded
Size (bytes):	27248
Entropy (8bit):	7.972379249220342
Encrypted:	false
SSDEEP:	768:jWlE/bWHGQQsYNRlPNez2pToQ19Uxx8UR9YSzfF1O:jrbazqOz29GRCSq
MD5:	C4F39C8CEF7F1746DA98C25E82B76F29
SHA1:	D368079E8789E98AD4831B570E096BA28ED365D6
SHA-256:	13AE7E5A59DE6CEF3C3CEDEAA348B17157B3CBC2B1BC9607C6D84CED4D137269
SHA-512:	97CE4C37A9FAD34763D851D4F0EB58717F6F5CDA7C36F493A4E4576E4D07D2263AFE2D44B7CD8D3EC34FE67A4B551518CD7E4A905D549A8492784C135BED0F 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://storangegoogleapiddp.agilecrm.com/flatfull/font/sourcesanspro/sourcesanspro.woff
Preview:	wOFF.....jp.....FFTM...l.....jNi.OS/2.....W...`Z...cmap.....T...cvt ...|...(...(....fpgm.....s.Y.7gasp.....glyf...../...[$..head..4....3...6.f..hhea..4. .....$.U..hmtx..4.....&.kern..7....:..R..p.6loca..TH.....)...maxp..V,.. ... ...7name..VL.....;@...epost..h .....).b.Jprep..j$...K...K.....ZE.....\.~x.c`f\|.8.....)..... B3.1.1*.E.Y..Y...X..v.....8.8.280.*.2.....\|.QP..q2H..... .....U.x.b```.b..F.....1.,.....%.d.2.1.g4d.f:.t...3.3.3.....l.....B...%!%...../.....b@.%. . ..e.....O...?...?.....{.....z.....} .....<0.w..9.{...l@...L@..U.d.+.;.'.7./.....''@J.*.j...Z.:.z...F.&.f...V.6.v...N...n...^.>.~...A.....GDFE....'$&%3ttv.N..`.e+..\.v...7l.u....v....CIZz....E...9.]s.J..2+...cX..9....gHi i.y...7o]....0...w..e.o.fh.k..8i..3...?.....'j.....D.R.V.....3.....>...~.....x.]..N.0...|...,$[V.*W.28.P.@.|..R+...)...<..-/.....]|w.;..O..I..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\web-rules[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	126818
Entropy (8bit):	5.280094166862753
Encrypted:	false
SSDEEP:	3072:Us/lO8DlOpeW38ekWIN5WIrlHlHDlOiWo:Us/lOClOpeW38ekWIHWIrlHlHDlOiWo
MD5:	9B02BABB7F376463BA1DBAE8A839C1E5
SHA1:	764D34B21A822D6A2C405B7E32040004629DA9DB
SHA-256:	21381869302C20150FCC59B820C74851640086320B1C325EC73893D91D1A5531
SHA-512:	4B4386D72BDFF3EA2ABABEBD6FA5D7F2758E30C0472E5C06F045340479E57E2AD4066DAAFA2F01C25A1ABCAA8F70B6A5609B37519F5CE3323B82EF0076CE25 00
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://our.agilecrm.com/core/js/api/web-rules?callback=json903640739649397&id=jo22gpvhr34r2mccjaekgsm7oh
Preview:	json903640739649397(..[{"cursor":null,"count":null,"id":4540766905171968,"name":"CSM - Live chat","disabled":false,"rule_type":"WEBRULE","rules":[{"LHS":"page", "CONDITION":"MATCHES","RHS":"agilecrm.com/#live-chat","RHS_NEW":null,"nested_condition":null,"nested_lhs":null,"nested_rhs":null,"business_hours_time_from":null ,"business_hours_time_to":null,"business_hours_time_zone":null,"ruleType":"Contact"}],"actions":[{"action":"ADD_TAG","RHS":"Chat CSM","position":null,"popup_pat tern":null,"title":null,"popup_text":null,"delay":null,"timer":0,"redirect_url":null}],"position":0,"country":"GB","created_time":1530715876,"updated_time":0},{"cursor":null,"count ":null,"id":4555792445603840,"name":"Feedback - CSM","disabled":false,"rule_type":"WEBRULE","rules":[{"LHS":"page","CONDITION":"MATCHES","RHS":"agilec rm.com/#ticket-feedback","RHS_NEW":null,"nested_condition":null,"nested_lhs":null,"nested_rhs":null,"business_hours_time_from":null,"business_hours_time_to":nul l,"business_hours_time_zone":n

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\141590300270327[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	738966
Entropy (8bit):	5.466759589515212
Encrypted:	false
SSDEEP:	6144:Rk1HWCSntDV/H4K3V/H486EPjQHWuH3Hpxk1HWCSntDV/H4K3V/H486EPjQHWuHw:f6E46E46E2
MD5:	260F14367D13992845A8A2CD7D9A9D38

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\141590300270327[1].js	
SHA1:	750DA2B38A728A88A859503168FE8A4FA3C1E4A3
SHA-256:	E71CFBF5FA8D9761538A059B7EE0BD3AAB0805569D4C59D9CFEBA75EF0DD6594
SHA-512:	B49546D2DD08016F5D16C2C8D772D3E4D60839279BB14A2696E3B44D251DCD906C4DED1F4B5B8999102022C092CD05B7DCB1A3CDD6213C1590819088CDB506
Malicious:	false
Reputation:	low
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\141590300270327[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	246322
Entropy (8bit):	5.466759589515212
Encrypted:	false
SSDEEP:	6144:Rk1HWCSntDV/H4K3V/H486EPjQHWuH3HpH:f6E2
MD5:	348AFD7BD47729F11B6FED351FBC991C
SHA1:	49D7DD41559F7A8FE8C0C39BC69B44AB6D8A746E
SHA-256:	113E5E2F3912C9271BC8D2BB386DE5F649F9326F1CC308100F493EEC0B90223F
SHA-512:	9C8A8E325D37F63DB367D1899C1F1BCC4243FBA327F53C2C1816C1AD326A7B41F4B5D65622BABC24F5B1D09F0601BD5536109A9912D91295133B27EDAD75515
Malicious:	false
Reputation:	low
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Jez-John[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 48x48, frames 3
Category:	downloaded
Size (bytes):	1234
Entropy (8bit):	7.238191080760754
Encrypted:	false
SSDEEP:	24:j/wOS8RjZV/Qv6Z7pVnwkpOjyL7qoK4gB9YL2aiRCCz:joOSW6SBXwY7zdgB9qi8Cz
MD5:	366D781FD669685A7288F4D128AE2099
SHA1:	0DA48843A8CF0233E97C20E69AE8F8524A1609AD
SHA-256:	ED5BF061CA56DAE905F3DAA76B4349B6DE9961A32810326B3A1B3E8BC9A0077E
SHA-512:	459BA344CF4814D7AF422363C262BCA44EA1B8F3F39EC695305F4D74307185003D43579318256F748B073B48A87D3A7F728BD6480872363402FAD363C7767CAE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/static/images/Jez-John.jpeg
Preview:	......JFIF.....C.....!.....'.."#%%%..),($+!$%$...C.....$...$$$

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\app[1].css	
SHA-512:	B13E363383168B9B42C4DC16D7CE35A5BDF6236460CA3984CDDC757133EDDCA698C1C19CB928E2F290FDF961999BE002F6653A00D24813BCE7DF504D2BDDA A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://storangegoogleapiddp.agilecrm.com/flatfull/css/app.css
Preview:	/* .*/.@font-face {. font-family: 'Source Sans Pro';. font-style: normal;. font-weight: 300;. /*src: local('Source Sans Pro Light'), local('SourceSansPro-Light'), url('../font/sourcesanspro/sourcesanspro-light.woff') format('woff'); */. src: local('Source Sans Pro Light'), local('SourceSansPro-Light'), url(https://fonts.gstatic.com/s/sourcesanspro/v9/toadOcfmlt9b38dHJxOBGD_j0nMiB9fPhg_k1wdK2h0.woff2) format('woff2');.}.@font-face {. font-family: 'Source Sans Pro';. font-style: normal;. font-weight: 400;. /* src: local('Source Sans Pro'), local('SourceSansPro-Regular'), url('../font/sourcesanspro/sourcesanspro.woff') format('woff');\ */. src: local('Source Sans Pro'), local('SourceSansPro-Regular'), url(https://fonts.gstatic.com/s/sourcesanspro/v9/ODelI1aHBYDBqgeIAH2zlNOAHFN6BivSraYkjhveRHY.woff2) format('woff2');. }.@font-face {. font-family: 'Source Sans Pro';. font-style: normal;. font-weight: 700;. /*src: local('Source Sans Pro Bold'), local('SourceSansPro-Bold'), url(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\b-bootstrap[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	68485
Entropy (8bit):	4.869645680512931
Encrypted:	false
SSDEEP:	768:7S5JiCkWDNS9rT7jncg3nV6LbqekfZZFqUWZPBVUiWf8A:hWD0VdekAPT1WkA
MD5:	6BA086DFC337AA2AE3DD65C5A7C1F543
SHA1:	3A9313F4892283AB68591D1338F0DA8DD7DB4A98
SHA-256:	9269707A5E396686202A52D5FCF95192BFEE208EC44A1149EF48155E4E1956ED
SHA-512:	BF72DC242261D4761229276778E872E5E5946A47106CC9334715F6C2C9A85454F5FB2CB40C381EAAD6C6E87B9AFA34A01ABD00D8BE9863F74A7E37C52491E0D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://storangegoogleapiddp.agilecrm.com/flatfull/final-lib/final-lib-1/b-bootstrap.js
Preview:	/*!. * Bootstrap v3.3.1 (http://getbootstrap.com). * Copyright 2011-2014 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */..if (typeof jQuery === 'undefined') {. throw new Error('Bootstrap\'s JavaScript requires jQuery').}..+function ($) {. var version = $.fn.jquery.split(' ')[0].split('.'). if ((version[0] < 2 && version[1] < 9) \|\| (version[0] == 1 && version[1] == 9 && version[2] < 1)) {. throw new Error('Bootstrap\'s JavaScript requires jQuery version 1.9.1 or higher'). }.}(jQuery);../* ========== ==========. * Bootstrap: transition.js v3.3.1. * http://getbootstrap.com/javascript/#transitions. * ========== ==========. * Copyright 2011-2014 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). * ========== */...+function ($) {. 'us

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\backbone-min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	16540
Entropy (8bit):	5.070750399515814
Encrypted:	false
SSDEEP:	384:SdPKqLOA20f7KtDvK2VxfxjA5QsjqOmPRNECw9:SAblxhI
MD5:	32AA69CB3FED6ADDF3520DE7FE0AA358
SHA1:	7E9F2AC45C3F56DADD19F47B45AEEFF81EBD3BBD
SHA-256:	F8EBD4A80D00E5AB3973EE784FD545D453903EA28537750674AF9CD21EB5C701
SHA-512:	9FD88B91D8BD502E2C9D2E7EC6B737850ECB511D3929F43D004C17FA638793D5539927DDCEE456ED8025A93F04637BA8CE1148F5183EFA693001A234082C5EE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/static/flatfull/final-lib/min/backbone-min.js
Preview:	/*! This is the customized file. .Here we overrided the add event in collection for infiniscroll addAll event. .If you want to upgrade the backbone to latest version please use the set instead od addAll(our customized ecent) for infiniscroll*/.../*! Backbone.js 0.9.2 */..(function(){var t,e=this,i=e.Backbone,s=Array.prototype.slice,n=Array.prototype.splice;t="undefined"!=typeof exports?exports:e.Backbone={},t.VERSION="0.9.2";var r=e._;!r&&"undefined"!=typeof require&&(r=require("underscore"));var o=e.jQuery||e.Zepto||e.ender;t.setDomLibrary=function(t){o=t},t.noConflict=function(){return e.Backbone=i,this},t.emulateHTTP=!1,t.emulateJSON=!1;var a=/\s+/,h=t.Events={on:function(t,e,i){var s,n,r,o,h;if(!e)return this;for(t=t.split(a),s=this._callbacks||(this._callbacks={});n=t.shift();)r=(h=s[n])?h.tail:{},r.next=o={},r.context=i,r.callback=e,s[n]={tail:o,next:h?h.next:r};return this},off:function(t,e,i){var s,n,o,h,c,u;if(n=this._callbacks){if(!t&&!e&&!i)return delete this._callbacks,this

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bat[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	28050
Entropy (8bit):	5.310811127038129
Encrypted:	false
SSDEEP:	384:otUVCwh9wC22xo1nB4KZjhbwM05Jkr9qNHfs9nB/wDSliNqCET8zT7QAEqny7YOI:pCwhBRHDOZwDhzT7QSnKYO56
MD5:	F07693F6368C988ACD20DE4362479103
SHA1:	D04355E119FAC2C9104C4FE98015E22F3F181D93

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bat[1].js	
SHA-256:	4DD6C09DDCB0E53A6290CC1DF35224856073BA5F89D4134BD7C69E4FD9C6F515
SHA-512:	1A0BD6850F3E7744216FA133493FA0D686EBB815B23ED2F2F511CEA982FC79794D882EDCE8DCB22670E455B94BA7EF2FE6EFC7E95710DD3243CBF54E65449A6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bat.bing.com/bat.js
Preview:	function UET(o){this.stringExists=function(n){return n&&n.length>0};this.domain="bat.bing.com";this.URLLENGTHLIMIT=4096;this.pageLoadEvt="pageLoad";this.customEvt="custom";this.pageViewEvt="page_view";o.Ver=o.Ver!==undefined&&(o.Ver===="1"||o.Ver===1)?1:2;this.uetConfig={};this.beaconParams={};this.supportsCORS=this.supportsXDR=!1;this.paramValidations={string_currency:{type:"regex",regex:/^[a-zA-Z]{3}$/,error:"{p} value must be ISO standard currency code"},number:{type:"num",digits:3,max:999999999999},integer:{type:"num",digits:0,max:999999999999},hct_los:{type:"num",digits:0,max:30},date:{type:"regex",regex:/^\d{4}-\d{2}-\d{2}$/,error:"{p} value must be in YYYY-MM-DD date format"},"enum":{type:"enum",error:"{p} value must be one of the allowed values"},array:{type:"array",error:"{p} must be an array with 1+ elements"}};this.knownParams={event_action:{beacon:"ea"},event_category:{beacon:"ec"},event_label:{beacon:"el"},event_value:{type:"number",beacon:"ev"},page_title:{},page_location:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bootstrap.v3.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	35601
Entropy (8bit):	5.178356022236213
Encrypted:	false
SSDEEP:	768:91+7/uRE672wlNrDMlbGqXYu+jS1s8ep0s1QfrXf8X8GvpZOWQ:DFRx7zYyS1WOv8fpZDQ
MD5:	2616D3564578D8F845813483352802A9
SHA1:	5ADA7C103FC1DEABC925CC1FDBBB6E451C21FC70
SHA-256:	F971B901AEB9E55B07D472AFEE09BD5AE05159E1119DBD16D993E473565E7FC0
SHA-512:	E3D8BC8FD58B0AC1D9FC444F21F2DAD94DEFDE536AF2AADB6ACE768AE0BCA9F9C9274161B076FC546CED174F23CC7495A8C5049AB00BE19C75F6310E91ABEDC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://storangegoogleapiddp.agilecrm.com/flatfull/lib/bootstrap.v3.min.js
Preview:	/*!. * Bootstrap v3.3.1 (http://getbootstrap.com). * Copyright 2011-2014 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.if("undefined"==typeof jQuery)throw new Error("Bootstrap's JavaScript requires jQuery");+function(a){var b=a.fn.jquery.split(" ")[0].split(".");if(b[0]<2&&b[1]<9||1==b[0]&&9==b[1]&&b[2]<1)throw new Error("Bootstrap's JavaScript requires jQuery version 1.9.1 or higher")}(jQuery),+function(a){"use strict";function b(){var a=document.createElement("bootstrap"),b={WebkitTransition:"webkitTransitionEnd",MozTransition:"transitionend",OTransition:"oTransitionEnd otransitionend",transition:"transitionend"};for(var c in b)if(void 0!==a.style[c])return{end:b[c]};return!1}a.fn.emulateTransitionEnd=function(b){var c=!1,d=this;a(this).one("bsTransitionEnd",function(){c=!0});var e=function(){c||a(d).trigger(a.support.transition.end)};return setTimeout(e,b),this},a(function(){a.support.transition=b(),a.support.transition&&(a.event.spe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\buildings-low[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop CS3 Windows, datetime=2015:10:15 11:11:57], progressive, precision 8, 1920x830, frames 3
Category:	downloaded
Size (bytes):	99308
Entropy (8bit):	7.898429249413108
Encrypted:	false
SSDEEP:	1536:lYdrSnv8oAOVhpDWac3eSasT6lHqn6Jh435PT85CiLefm:3vgOVhxm3pqLPOBTACiLlm
MD5:	15D3C83DA7CA9BC6F5C988A0A6981E60
SHA1:	B4C7C2CA577779FAA9212B41F49455042BE436F1
SHA-256:	07284F2415B5C17594394D895E9F51EDC5EEEED1E7560CB4D55084270D6FAA71
SHA-512:	70C0ADDDD2AE7EE97F0AFA23C171733A5CAD30883833383EB477A1F3BCB5EB8618668333E146159CDE8EECFC0203AACF223E72EFC388D1E90086E1C97789472
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/static//images/buildings-low.jpg
Preview:	......JFIF.....H.H.....BExif..MM.*.....b.....j.(.....1.....r.2.....i.....'.....'.Adobe Photoshop CS3 Windows.2015:10:15 11:11:57.....>.....&.(.....H.....H.....JFIF.....H.H.....Adobe_CM.....Adobe.d.....E...".....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWgw.....5....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?.}.>..o.~w...4...v.{[....!..|O..j<I.$....kg..... ..IL.6..3.....a?...zL..|.....n.....5SwP...C...`:..U[?$.C.""....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\buildings[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1920x830, frames 3
Category:	downloaded
Size (bytes):	274863
Entropy (8bit):	7.975417863855154
Encrypted:	false
SSDEEP:	6144:vdVjkxgD8sj86yZ0BWzrW6DocsjiXUF8mgzDyHhY11BF6:1VYgo6l8rWa8iXdXj36

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\buildings[1].jpg	
MD5:	BB41524F25FC87C7AB87B83C94B7499E
SHA1:	9AA379E7DDE363E7823D8AB9DAF7557E758EBB74
SHA-256:	975435A2F2543242F8761CBDC64EF53573758B40905041DA6D628B291CFC74E8
SHA-512:	9569C0E7CC4D4A6B5473F8D5D87161801D99889A7B7F0501CFCCA54FDDD756F5883DEEEC71D299576B30D2C0CAD724C56AE7358D752CCC7C9A8941A27843E8F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/static//images/buildings.jpg
Preview:	......JFIF.....C..... ("..&...#0$&*+-.-."251,5(,-,...C.....,...,,,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\font[1].css	
SHA1:	838B8BF949B69E9294F3796CD942F99D60DF3EE9
SHA-256:	363B9AC2659653FB3E5DE2B6A6F34103C67D6C1A26AA19C9E420C6189E69567A
SHA-512:	F02ECDA000B0A68BE391A49BF9FC1AC14BE04AAB4213A21008AF1C7262A58EEC77838904FD9A5EB5D8EAFE7F1ABF0C82406FCA7164A7AFCC6FF9A671C4CC6B87
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://storangegoogleapiddp.agilecrm.com/flatfull/css/font.css
Preview:	@font-face {. font-family: 'Source Sans Pro';. font-style: normal;. font-weight: 300;. src: local('Source Sans Pro Light'), local('SourceSansPro-Light'), url('../font/sourcesanspro/sourcesanspro-light.woff') format('woff');.}.@font-face {. font-family: 'Source Sans Pro';. font-style: normal;. font-weight: 400;. src: local('Source Sans Pro'), local('SourceSansPro-Regular'), url('../font/sourcesanspro/sourcesanspro.woff') format('woff');.}.@font-face {. font-family: 'Source Sans Pro';. font-style: normal;. font-weight: 700;. src: local('Source Sans Pro Bold'), local('SourceSansPro-Bold'), url('../font/sourcesanspro/sourcesanspro-bold.woff') format('woff');.}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Reputation:	low
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\it[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2138834
Entropy (8bit):	5.384461113913953
Encrypted:	false
SSDEEP:	12288:4KlPdWfLlzdDfBlidtfS5jpliGKDBtpft5N9MN+29CMpy2HxDI7up/woXrwArg1C:4fliGKBf59ZujXrwArg1EgRBk/b9
MD5:	2D73E84FB85CA0371CBB9F5F6F50D12A
SHA1:	741FA5833EA232B463BDEC546E855BE686ECA652
SHA-256:	A0D64439C6E5AEFC32122A817E944C0FDE2F913E32C9968D79D40BEA83BBD5F9
SHA-512:	9988541E750AC6A147417A40BBC852297CE6E9B7B609C612D11983B390E4EA92FF0A12F1732137083110D458BF3C5858F3BE418CF659D8F73A0635CE1755F3C4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/68-7/tpl/min/precompiled/locales/it/it.js?_=68-7.432843952504576280
Preview:	(function(){var b=Handlebars.template,a=Handlebars.templates=Handlebars.templates||{};a["account-delete-step2-template"]=b(function(f,g,d,c,e){this.compilerInfo=[4,">=1.0.0"];d=this.merge(d,f.helpers);e=e||{};return"\n \n \n \n <button type="button" class="close" data-dismiss="modal" aria-hidden="true">x</button>\n <h3 class="modal-title">Richiesta di Cancellazione Ricevuta </h3>\n \n \n Siamo spiacenti che ci lasci. Il nostro team di Supporto ti contatter. entro 48 ore per saperne di pi. sul motivo del tuo abbandono. Ti preghiamo di notare che la tua sottoscrizione . ancora attiva e il nostro team di Supporto ti offrir. aiuto per il processo successivo. \n..Per conoscere lo stato della richiesta, ti preghiamo di scrivici.\n. \n \n \n <

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\js-all-min-1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	613158
Entropy (8bit):	5.358961046409701
Encrypted:	false
SSDEEP:	12288:zMtVRSPg0+YaCg1Ppk5n0ECf5k8k10Omee:zMtVRSPg0+Ybg1Ppk5n0ECf5k8k10Om1
MD5:	C5A2D08547176DAF5F1DB4D522D5BC19
SHA1:	ED697BDFC4EB6B1336314B11FA36CF6D21B5FB4F
SHA-256:	7D59E8616594B16E14EE2185A1BE307C88D471805B4FAA582615A3BA0428D866

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\js-all-min-1[1].js	
SHA-512:	683ADA6B3FC5B78820D85FD1749F9C6C43A1583DBAF233FCFB4A7A3B332531A29D20CB79EFBAB4E9E4AD861CE9B4AEC586F659925157FA1399781882193E646
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/68-7/jscore/min/locales/it/js-all-min-1.js?_=68-7.432843952504576280
Preview:	Backbone.View.prototype.close=function(){this.remove();this.unbind();if(this.onClose){this.onClose()}};var BaseModel=Backbone.Model.extend({});var BaseCollection=Backbone.Collection.extend({model:BaseModel,initialize:function(b,a){this.restKey=a.restKey;if(a.sortKey){this.sortKey=a.sortKey}if(a.descending){this.descending=a.descending}this.sort_collection=a.sort_collection;if(this.sort_collection==false){this.comparator=false}},comparator:function(a){if(this.sortKey){if(this.descending==true){return -a.get(this.sortKey)}return a.get(this.sortKey)}return a.get("id")},parse:function(a){if(a&&a[this.restKey]){return a[this.restKey]}return a}});var Base_List_View=Backbone.View.extend({events:{"click .delete":"deleteItem","click .edit":"edit","delete-checked .agile_delete":"deleteItem","click .delete-model":"deleteModel","click .delete-confirm":"deleteConfirm","click .delete-with-confirmation":"deleteModelAfterConfirmation",},initialize:function(){_.bindAll(this,"render","deleteItem","edit"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\js-all-min-1[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	613180
Entropy (8bit):	5.360071156226274
Encrypted:	false
SSDEEP:	12288:IMtVR20Pg0+YDCg1Ppa540ECf5k8k10hmee:IMtVR20Pg0+Ymg1Ppa540ECf5k8k10hG
MD5:	D5A5763E2E4B9806AB035013094F407F
SHA1:	853CFA7CF3F648938EBD8DBE055B40497F9B14E4
SHA-256:	B4EDFDA4F4AD506830502F91134A3C605AC44C3EA027E0649731733B577C9F70
SHA-512:	C8237CF02579B6BF97F6381ADBDAE981A4B91A475A90B12CB479F1785B8D18AC61AE34C98BF4BC1D42C16438E9C3871520058B675CFD23386353EE5043AF1CD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/68-7/jscore/min/locales/pt/js-all-min-1.js?_=68-7.432843952504576280
Preview:	Backbone.View.prototype.close=function(){this.remove();this.unbind();if(this.onClose){this.onClose()}};var BaseModel=Backbone.Model.extend({});var BaseCollection=Backbone.Collection.extend({model:BaseModel,initialize:function(b,a){this.restKey=a.restKey;if(a.sortKey){this.sortKey=a.sortKey}if(a.descending){this.descending=a.descending}this.sort_collection=a.sort_collection;if(this.sort_collection==false){this.comparator=false}},comparator:function(a){if(this.sortKey){if(this.descending==true){return -a.get(this.sortKey)}return a.get(this.sortKey)}return a.get("id")},parse:function(a){if(a&&a[this.restKey]){return a[this.restKey]}return a}});var Base_List_View=Backbone.View.extend({events:{"click .delete":"deleteItem","click .edit":"edit","delete-checked .agile_delete":"deleteItem","click .delete-model":"deleteModel","click .delete-confirm":"deleteConfirm","click .delete-with-confirmation":"deleteModelAfterConfirmation",},initialize:function(){_.bindAll(this,"render","deleteItem","edit"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\js-all-min-2[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	886401
Entropy (8bit):	5.3668675154292975
Encrypted:	false
SSDEEP:	24576:WChhqXVKt9UtbfIbr2hcvEV5QV2RNhLoaWqKrUR:WChhqXVKt9UdfIbr2hcvEV5QV2RNhLo8
MD5:	F79BEF13B6B3D6D885B4950D5C18D8E7
SHA1:	BE250902DC24384D495F4CC2BA4628C8FFCC9902
SHA-256:	E7B380687DA50C1AC4A56405C879F08BDFF42E4657569BFDA5212EE1A78339AD
SHA-512:	B97F01C27DD99D97CF364B68C66ED5225979CB2FBEFD9DCC6F3D1EAA66B683326B1B4DF70651E7E0F78C2E829C49CCE9DB4992E539A8A1C7D3E7B04C7849E14
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/68-7/jscore/min/locales/it/js-all-min-2.js?_=68-7.432843952504576280
Preview:	function initWebruleChartsUI(a){initDateRangeforForm(a);a()}function showWebruleGraphs(a){showBar("core/api/webrule-analytics/web/graphreports/"+a+getOptions()+"&type=date","line-daily-chart","daily","Count",null);showBar("core/api/webrule-analytics/web/graphreports/"+a+getOptions()+"&type=hour","line-hourly-chart","hourly","Count",null);showBar("core/api/webrule-analytics/web/graphreports/"+a+getOptions()+"&type=day","line-weekly-chart","weekly","Count",null)}function getOptions(){var b="?";var a=$("#range").html().split("-");var e=getUTCMidNightEpochFromDate(new Date(a[0]));var g=$.trim(a[1]);if(g){g=g+" 23:59:59"}var c=getUTCMidNightEpochFromDate(new Date(g));c+=(((23*60*60)+(59*60)+59)*1000);b+=("start_time="+e+"&end_time="+c);var j=new Date();b+=("&time_zone="+j.getTimezoneOffset());if($("#frequency").length>0){var f=$("#frequency").val();b+=("&frequency="+f)}if($("#filter").length>0){var h=$("#filter").val();if(h!=""&&h!="ALL"){b+=("&filter="+h)}}return b}function get_webrule_tab

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\js-all-min-3[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	927913
Entropy (8bit):	5.688985168062615
Encrypted:	false
SSDEEP:	12288:sSYN7iPp/OfVMxnrMUQnqKpzG4YzD0nzqoM+:sSHp/OfVMxnoUQdkKqz+
MD5:	4211302AD79A5125ADF2BAA336F691E9
SHA1:	40CB53220F8BB0FFB3E2DA31B2F282AC6B1D461F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\js-all-min-3[1].js	
SHA-256:	7ED3612CB61F9A41C60240734053290E10946E4A9F25B5E43064E8DA673761DB
SHA-512:	CC794A695A3D1F8790192E98D07C7993B8D8E0448A3680A0DDE17D144AE7B500E75273D636DA44FD2FE4CE6DC4A5AD9D91E64A8A2B7C2A54511D077127730F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/68-7/jscore/min/locales/it/js-all-min-3.js?_=68-7.432843952504576280
Preview:	var Email_Template_Events=Base_Model_View.extend({events:{"click .merge-field":"onMergeFieldSelect","click .add-attachment-select":"onAddAttachmentSelect","click .add-attachment-confirm":"onAddAttachmentConfirm","click .add-attachment-cancel":"onAddAttachmentCancel","click .add-tpl-attachment-confirm":"onTemplateAddAttachmentConfirm","click .add-tpl-attachment-cancel":"onTemplateAddAttachmentCancel","change #attachment-select":"onChangedAttachment",},onMergeFieldSelect:function(c){c.preventDefault();var b=$(c.currentTarget).attr("name");var d=$("#email-template-html").val();var f=$("#email-template-html").data("wysihtml5");if(f){editor.focus();f.editor.composer.commands.exec("insertHTML","{{"+b+"}}")}},onAddAttachmentSelect:function(g){g.preventDefault();var b=$(g.currentTarget);var f=$(b).closest("div");$(b).css("display","none");f.find(".attachment-document-select").css("display","inline");var c="<option value='{{id}}' network_type='{{titleFromEnums network_type}}' size='{{size}}'>{{

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\js-all-min-4[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	1116581
Entropy (8bit):	5.39301615051039
Encrypted:	false
SSDEEP:	6144:oYXLFuWAkYvY3b/29SLjHZ2zmygCt4cr6HJWjwcDvawIByzJ9cDGx03tSZZV1MKf:HeH9Pr//ooc/TQazK
MD5:	1A58271F0ECAA285ED89AFFC6C9AEDF9
SHA1:	FF826E2029F1E220B104CC94FE4A1AB3AB6E3F94
SHA-256:	5D802C8A5B6FBE3A0E3822C66CBDCAADEE93C97719DD835563993DA0350CE156
SHA-512:	2B796FDFCBE0A74970D1A21C126E4AA526FA858D1B12BA9655C92DFFB2C09674F2E412F2A8F4D4D121B461A4495EE2683B227BB0CBF009F6CDCCE20DBB4C4F11
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/68-7/jscore/min/locales/it/js-all-min-4.js?_=68-7.432843952504576280
Preview:	var recent_view;var recent_view_update_required=false;var MAX_RECENT=6;function populate_recent_menu(){if(!recent_view){var b=[];try{b=JSON.parse(localStorage.recentItems)}catch(c){}recent_view=new Base_Collection_View({restKey:"contacts",templateKey:"recent-menu",data:b,individual_tag_name:"li",sort_collection:false,postRenderCallback:function(d){$("#recent-menu").append($(d).html())}});if(recent_view.collection.length==0){$("#recent-menu>ul").html('<li class="list-group-item" style="border:none">Nessuna Attivit. Recente ');hideTransitionBar()}else{recent_view.render(true)}}function add_recent_view(d){if(recent_view==undefined){populate_recent_menu()}if(!recent_view.collection.get(d.get("id"))){if(recent_view.collection.length>=MAX_RECENT){recent_view.collection.pop({silent:true})}recent_view.collection.unshift(d)}else{recent_view.collection.remove(d,{silent:true});recent_view.collection.unshift(d)}recent_view_update_required=true;va

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\js-all-min-4[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	1116602
Entropy (8bit):	5.401681668516682
Encrypted:	false
SSDEEP:	6144:OYUtqufAPe2oVb/4pSLXLtMkmyNpN+NdWkviwIByzj9cXGVPiIdY/Q0bL804yxbo:qnk9wv//oWQ/TVmzQ
MD5:	8D4E19A7369D4C29C90FF88A04BAF427
SHA1:	1F154037A0A1B56BEB0A0FED44235AC2E18366B0
SHA-256:	B8D0BCDE0FD161BC3224C91FEBE75EAAECFB2C1B0DDDC1C1CA44B1458F429089
SHA-512:	C18D9D6E30883A2CBE380439D7F63B8DB93FE6F8E116EBCEEBE74EF55A8021495FDFCE6A0B3504839A945DE33F813CE145F7DE90D478B7BA07D3D4295502342
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/68-7/jscore/min/locales/pt/js-all-min-4.js?_=68-7.432843952504576280
Preview:	var recent_view;var recent_view_update_required=false;var MAX_RECENT=6;function populate_recent_menu(){if(!recent_view){var b=[];try{b=JSON.parse(localStorage.recentItems)}catch(c){}recent_view=new Base_Collection_View({restKey:"contacts",templateKey:"recent-menu",data:b,individual_tag_name:"li",sort_collection:false,postRenderCallback:function(d){$("#recent-menu").append($(d).html())}});if(recent_view.collection.length==0){$("#recent-menu>ul").html('<li class="list-group-item" style="border:none">Nenhuma Atividade Recente ');hideTransitionBar()}else{recent_view.render(true)}}function add_recent_view(d){if(recent_view==undefined){populate_recent_menu()}if(!recent_view.collection.get(d.get("id"))){if(recent_view.collection.length>=MAX_RECENT){recent_view.collection.pop({silent:true})}recent_view.collection.unshift(d)}else{recent_view.collection.remove(d,{silent:true});recent_view.collection.unshift(d)}recent_view_update_required=true;var

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\lib-all-new-1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	186681
Entropy (8bit):	5.348402763621212
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\lib-all-new-1[1].js	
SSDEEP:	3072:r0PilzHpcrXMDrRYoPyTKtO8HOdQ1zbJOHSwCV:r0PilzJcrXMDrWcyWEDi1r
MD5:	AFEE25A40F7D8553164CE80680DB27D3
SHA1:	5A31E1701468886700222827 97A8038A8C3B7343
SHA-256:	FA5D2C83DCCBEA32DDE227118578E608D763B30FFD716A7E57C16287806ED03A
SHA-512:	08265EFA9A93B21AF410948657E2BB9AEF47413CD67845AA4360421968543A06CF612D53A613DAC94F460DCA3B97D3FB333E82F059BF4A7DC1595A5E86EEC8B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/static/flatfull/final-lib/min/lib-all-new-1.js?_=68-7.432843952504576280
Preview:	(function(b,a,c){b.curCSS=b.css;b.browser={};b.browser.msie=false;b.browser.version=0;if(navigator.userAgent.match(/MSIE ([0-9]+)\./)){b.browser.msie=true;b.browser.version=RegExp.$1}})(jQuery,window);./*!. * Bootstrap v3.3.1 (http://getbootstrap.com). * Copyright 2011-2014 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.if(typeof jQuery==="undefined"){throw new Error("Bootstrap's JavaScript requires jQuery")}+function(b){var a=b.fn.jquery.split(" ")[0].split(".");if((a[0]<2&&a[1]<9)||(a[0]==1&&a[1]==9&&a[2]<1)){throw new Error("Bootstrap's JavaScript requires jQuery version 1.9.1 or higher")}}(jQuery);+function(b){function a(){var e=document.createElement("bootstrap");var d={WebkitTransition:"webkitTransitionEnd",MozTransition:"transitionend",OTransition:"oTransitionEnd otransitionend",transition:"transitionend"};for(var c in d){if(e.style[c]!==undefined){return{end:d[c]}}}return false}b.fn.emulateTransitionEnd=function(e){var d=false;va

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\login-2-high-prog[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], progressive, precision 8, 1537x867, frames 3
Category:	downloaded
Size (bytes):	145130
Entropy (8bit):	7.983833082548584
Encrypted:	false
SSDEEP:	3072:nDmPN8Uw9KZquQvJGtuJDnePkHiBBEn19BgOa8eHTQ3W:DCN8fiJYJQeiBBs6V7TWW
MD5:	731572D41FB3F1B4970A11C89EA2DC00
SHA1:	E7B7E8F18EA60AEEE01E796321D3F3D8B011A54C
SHA-256:	3DE8CBF61481F4AE110E625785D58ED768B90D724E60F871C4210540BB0B1098
SHA-512:	EC6EE7FAD8ECBEE1A55FF134983896D2FF9E2C9FC19AE109D2135E8EDF32C845A5CF5AC6FAEB4C8C155C52351D409594DA2EC97EA228FD6AE324AB0D56ED B7B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/static/images/login-2-high-prog.jpg
Preview:	.....Exif..II*.....Ducky.....2...../http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c067 79.157747, 2015/03/30-23:40:42 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CC 2015 (Windows)" xmpMM:InstanceID="xmp.iid:59754D6BE04D11E595A9CF4B180858AF" xmpMM:DocumentID="xmp.did:59754D6CE04D11E595A9CF4B180858AF"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:59754D69E04D11E595A9CF4B180858AF" stRef:documentID="xmp.did:59754D6AE04D11E595A9CF4B180858AF"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>...!Adobe.d.....0..7V...C.....#"""#"""...C.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\login-8-high-prog[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], progressive, precision 8, 1537x867, frames 3
Category:	downloaded
Size (bytes):	216449
Entropy (8bit):	7.986406720294414
Encrypted:	false
SSDEEP:	6144:3e70FcIV7ljJXYcT+M2JBr/HtvtVHFRJIFmdJkQs2Me:O70FbV73Ycq1/NnlRJIFm/kQs2D
MD5:	0AF723FFDF2A51BA3C344026E930A999
SHA1:	1FEC9172F9AEE7023A2B842DD759610D3526821D
SHA-256:	A0E9B743744A258C22899FC087CD7C0D40F60FD19C94EF7A2D1AB20399B28A3F
SHA-512:	C9F474DDC236B3DD1F54D68E0C794C548BD92C41D1D2A7BBD6B5DA6CB9D9E74EFA0E735596F4A2EB7E028D893A5BEE6F19B0C8E4BB93AF540F045AA7BD56 504
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/static/images/login-8-high-prog.jpg
Preview:	.....Exif..II*.....Ducky.....2...../http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c067 79.157747, 2015/03/30-23:40:42 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CC 2015 (Windows)" xmpMM:InstanceID="xmp.iid:03A41EADE04D11E5AFC0C405CF786883" xmpMM:DocumentID="xmp.did:03A41EAEE04D11E5AFC0C405CF786883"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:03A41EABE04D11E5AFC0C405CF786883" stRef:documentID="xmp.did:03A41EACE04D11E5AFC0C405CF786883"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>...!Adobe.d.....N....C.....#"""#"""...C.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\login[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	23132

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\login[1].htm	
Entropy (8bit):	5.324523761361377
Encrypted:	false
SSDEEP:	384:BBGLnhsfFM8QVWnMzI4Jo6IvYgl8FTdcsMhUpttNroxGh7TsEkMmNzdmlaStUoVp:HcYFM8QonM/WYgI9oIhn6zvBuB
MD5:	964DC1E6B388EFECA94B1AE693E26565
SHA1:	F11DEE51B50072AC76AF2085EC303CE665ADC4A1
SHA-256:	1E18489BEA1FE663EE7D60033035DC8EAF75B78F6C198B8E4D69121448BEA0C5
SHA-512:	FA09D0EBB44FA752B78F621F081B106225E5CA18CB5BCBBC6C59167F5E2357D99B487642E33E84E83D7D9FEBAB92BC1E448DD21C7AD6B3138F6C6BB344C367 46
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://storangegoogleapiddp.agilecrm.com/login
Preview:	.....<!DOCTYPE html>..<html lang="en" style="background:transparent;">.<head>.<meta charset="utf-8">.<meta name="globalsign-domain-verification". .content="-r3RJ0a7Q59atalBdQQIvI2DYIhVYtVrtYuRdNXENx" />.<title>Login</title>.<meta name="viewport" content="width=device-width, initial-scale=1.0 maximum-scale=1">.<meta name="description" content="">.<meta name="author" content="">.<meta name="robots" content="noindex, nofollow">..<link rel="stylesheet" type="text/css" href="/flatfull/css/min/login-v2-min.css" />..<link href="https://fonts.googleapis.com/css?family=Roboto" rel="stylesheet">. Include ios meta tags -->.<link rel="apple-touch-icon" href="ios/touch-icon-iphone.png">.<link rel="apple-touch-icon" sizes="76x76" href="ios/touch-icon-ipad.png">.<link rel="apple-touch-icon" sizes="120x120" href="ios/touch-icon-iphone-retina.png">.<link rel="apple-touch-icon" sizes="152x152" href="ios/touch-icon-ipad-retina.png">..<link rel="apple-touch-startup-image" href="ios/start

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\login[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	23132
Entropy (8bit):	5.324523761361377
Encrypted:	false
SSDEEP:	384:BBGLnhsfFM8QVWnMzI4Jo6IvYgl8FTdcsMhUpttNroxGh7TsEkMmNzdmlaStUoVp:HcYFM8QonM/WYgI9oIhn6zvBuB
MD5:	964DC1E6B388EFECA94B1AE693E26565
SHA1:	F11DEE51B50072AC76AF2085EC303CE665ADC4A1
SHA-256:	1E18489BEA1FE663EE7D60033035DC8EAF75B78F6C198B8E4D69121448BEA0C5
SHA-512:	FA09D0EBB44FA752B78F621F081B106225E5CA18CB5BCBBC6C59167F5E2357D99B487642E33E84E83D7D9FEBAB92BC1E448DD21C7AD6B3138F6C6BB344C367 46
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://storangegoogleapiddp.agilecrm.com/login?lang=en
Preview:	.....<!DOCTYPE html>..<html lang="en" style="background:transparent;">.<head>.<meta charset="utf-8">.<meta name="globalsign-domain-verification". .content="-r3RJ0a7Q59atalBdQQIvI2DYIhVYtVrtYuRdNXENx" />.<title>Login</title>.<meta name="viewport" content="width=device-width, initial-scale=1.0 maximum-scale=1">.<meta name="description" content="">.<meta name="author" content="">.<meta name="robots" content="noindex, nofollow">..<link rel="stylesheet" type="text/css" href="/flatfull/css/min/login-v2-min.css" />..<link href="https://fonts.googleapis.com/css?family=Roboto" rel="stylesheet">. Include ios meta tags -->.<link rel="apple-touch-icon" href="ios/touch-icon-iphone.png">.<link rel="apple-touch-icon" sizes="76x76" href="ios/touch-icon-ipad.png">.<link rel="apple-touch-icon" sizes="120x120" href="ios/touch-icon-iphone-retina.png">.<link rel="apple-touch-icon" sizes="152x152" href="ios/touch-icon-ipad-retina.png">..<link rel="apple-touch-startup-image" href="ios/start

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\login[3].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	16595
Entropy (8bit):	5.306308388052489
Encrypted:	false
SSDEEP:	384:hNL7L3JmMOHbC7LjzZM3oxGh0TsEUMJNR9EUmoc6SFgclUdUZ:ffIMACvioIhOJsbu+Z
MD5:	318870BC5E0A055D459D4CA531C08F1A
SHA1:	36A6BBA0B779C12ADF0F9231F6D53107251C9EC6
SHA-256:	405BBD9B9A520B8E9B6ECFFD72590777C7EE97CC8B72D52E3C71D634B01E72F1
SHA-512:	090E67175AB5F3BB1AC7D983DDAE1CB0954D6247F0C2674E9A397B7E783813590ECA2D514288C01FCDCCDFF08E82B6F04B1B18F520F4DA19ED6F7CB7CB0E 5D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://storangegoogleapiddp.agilecrm.com/login?lang=it
Preview:	.....<!DOCTYPE html>..<html lang="it" style="background:transparent;">.<head>.<meta charset="utf-8">.<meta name="globalsign-domain-verification"..content="-r3RJ0a7Q59atalBdQQIvI2DYIhVYtVrtYuRdNXENx" />.<title>Accedi </title>.<meta name="viewport" content="width=device-width, initial-scale=1.0 maximum-scale=1">. <meta name="description" content="">.<meta name="author" content="">.<meta name="robots" content="noindex, nofollow">..<link rel="stylesheet" type="text/css" href="/flatfull/css/min/login-min.css" />..<link href="https://fonts.googleapis.com/css?family=Roboto" rel="stylesheet">.. Include ios meta tags -->.<link rel="apple-touch-icon" href="ios/touch-icon-iphone.png">.<link rel="apple-touch-icon" sizes="76x76" href="ios/touch-icon-ipad.png">.<link rel="apple-touch-icon" sizes="120x120" href="ios/touch-icon-iphone-retina.png">.<link rel="apple-touch-icon" sizes="152x152" href="ios/touch-icon-ipad-retina.png">..<link rel="apple-touch-startup-image" href="ios/star

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\maisonneue-bold-webfont[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\maisonneue-bold-webfont[1].eot	
File Type:	Embedded OpenType (EOT), Maison Neue Bold family
Category:	downloaded
Size (bytes):	25596
Entropy (8bit):	7.969283620699325
Encrypted:	false
SSDEEP:	768:j64Lx4UlWFTXq7uUNlkTvioYoDeUNCEp98dd0b6:j64LOtNrDeGlpudd0W
MD5:	588124B750E01023C48420A3A8F8741C
SHA1:	AEFC8D8BEFD1546E181EDF7283ED804366A09935
SHA-256:	6986B3E0F0C1184DE69D2602F52F6AF0946C6C9D60454035CFB3A595726BE73D
SHA-512:	F8B4AB6A691DA4824D40A55929B10068B7DD134AE0F447997616AFFAB908593242D046F3EF59B150E5F383320FEBB27887AFF0025EB67F840C840095DA2D773F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://storangegoogleapiddp.agilecrm.com/flatfull/css/material-theme/font/maisonneue-bold-webfont.eot?
Preview:	.c...c.....LP....{ .P..... ....L..... .M.a.i.s.o.n. .N.e.u.e. .B.o.l.d.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .2...0.0.3...0.M.a.i.s.o.n. .N.e.u.e. .B.o.l.d. .R.e.g.u.l.a.r.....BSGP.....Bx.B~.I.....xZg.icyR..&c..4o4F..w....[.yM...R.Y.N&.1.V.'-.[+.....jorr...q.....o..>B].>-.e...._.....*y..UE&.z..s.W.....X..'B...SV...#.2?. ...8.....O]^..y.._U 4.KB.....bE. .*.....M<...=.o.Q..v..(E.D..r._(.6}...../n.....;...m..3.z..@n.y...f..].QFPB.!.....`E4*L.._.....D.(.....i7?..o)..l.fk.0c..2j..G...|..E.....''..U..R7..D..2...t...$..X^.d.....W ..HV.$...).S.U.7..Re.H.W(&26.d..;'.|..1.Of....I..J6.k....;).m..-...J?Ho9...+.90:..M(.i.....I...OB.y%..E..j0.....r..+s*.].....AM....M$s...e.0B....\.x+..|.FD../....6 ..]..... (f...t.uqUr.P..b/ ..U.{...+.7..tA.&.\.+..E.A.^ly.L..]..?uF..fi.....L.....E/.?(..C...3....o_...=...>..z..o..K=.....6....#&.....].03Pe.....0j@..x.O#S....\.0..-.)]Z.w.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\maisonneue-light-webfont[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Maison Neue Light family
Category:	downloaded
Size (bytes):	25024
Entropy (8bit):	7.970331078456057
Encrypted:	false
SSDEEP:	384:Nxtfrckz+/r2TxMk0ClRHKjc2mTtqVYOXvEScW5/sP4bfCA50iIH:Nxtjvz+/r2Tp0ClRH8cB09MSV10N
MD5:	81540179158B57246265C215CFAFAD19
SHA1:	7267D2694EDD2A1DF76302E303BE4F7626839173
SHA-256:	109D3149908C606F7C9782D28ADB270CD4254098824A4BEF6C05232DBDEB8569
SHA-512:	E9A2C80D783F4B720635FB49C4E763C9169BEF565AA57798A85777E406A8F569FB9A1C9EB08C8EFED7CA9D2D834EDD48A552CEE8CAD7699AD6B450256CBDA B8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://storangegoogleapiddp.agilecrm.com/flatfull/css/material-theme/font/maisonneue-light-webfont.eot?
Preview:	.a...`.....LP....{ .P..... .....".M.a.i.s.o.n. .N.e.u.e. .L.i.g.h.t.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .2...0.0.3...2.M.a.i.s.o.n. .N.e.u.e. .L.i.g.h.t. .R.e. g.u.l.a.r.....BSGP.....h.A..A..I.....xZg.icyR..&c..4o4F..w....[.yM...R.Y.N)6.1.V.'.u^.....\..r...p.....p.....Z.....F3.....T..eM.....%...ptQ7$r....:.xV.....x..Y.#.b.....''l...k...Y..... #5.....plj.b...43.5..8.....I.....V...e.K9.N..N.O....0q.r..X..<...6.G..Rr..[.!?.....Xf..k.....b;.A.D.ko.....L..<.CG.....j...^.....0x..*..j8.@....r..kE.P...^...h.....e...i.Y....G#...,..b./.*y 0Pd.>.R.X2V....Y.....)2H).@.m....g.....4D...0.>..q..S.....!....a.@...J..pT..=...S..P../..r7.... M12L.5...r(..).S&..E.(..]Z5@...A.2`YeW..w.w@b.....z.T.S.i..?$A.d..a..7p..X[D.''o. #.....>1.^.. .xF./YMF.....'...)..~o....3.k.Y..V/.$..,...H.o..R.. l.5.''.0.j..P..P.~a3t(#+._...~G3u.8.C..s.]...@.....<...!..d..0.l.(R0..|....$.K!-...:..<.T..x..$.D...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\portlets[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	487413
Entropy (8bit):	5.536881658715278
Encrypted:	false
SSDEEP:	6144:CeBWC0ge7W+0Ve6Wr0QsgX93X7rIlvxxW4jrJa4wrJS4HrJvz7pfLDcGpXHXfbb7:CeBWC0ge7W+0Ve6Wr0acTL
MD5:	BA828AA6E5636C727E290F6A1BBEBEFD
SHA1:	FC0B0D856A6AD7C4B25D4E209273982C2D2EECA2
SHA-256:	C8D3595B93A5DD0E51B187B0D1DB9114FB816D79ADF5FDEC3436BDD0FB6CA4EB
SHA-512:	73A3F0FB448B8329F91D0B87C80D38D3FBE0B7662D0340E592CBE621E1291AF01C9525BDEA4BE7564FA1DED1BC9321338FD0E2F90F09D3D6A4D01F3A6C6EFC 6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/68-7/tpl/min/precompiled/locales/it/portlets.js?_=68-7.432843952504576280
Preview:	(function(){var b=Handlebars.template,a=Handlebars.templates=Handlebars.templates||{};a["marketing-video-modal-template"]=b(function(f,g,d,c,e){this.compilerInfo= [4,">= 1.0.0"];d=this.merge(d,f.helpers);e=e||{};return'\n. \n... \n.... \n.....<button cl ass="close" data-dismiss="modal">×</button>\n.....<h3 class="modal-title">Marketing Tutorial</h3>. \n.... \n..... \n..... \n.....<iframe style="width:100%;" height="345" src="//www.youtube.com/embed/KP8feLANFZA?enablejsa pi=10&autoplay=1&showinfo=0" frameborder="0" allowfullscreen></iframe>\n..... \n..... \n... \n. \n.\n'});a["mobile-app-options-template"]=b(function (g,m,f,l,k){this.compilerInfo=[4,">= 1.0.0"];f=this.merge(f,g.helpers);k=k||{};var j="",d,h,r,p=this,i="function",n=f.blockHelperMissing;function e(t,s){return" "}functio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\roundtrip[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\roundtrip[1].js	
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	41069
Entropy (8bit):	5.409336380661595
Encrypted:	false
SSDEEP:	768:2v5UOTGnoBVKQIhGIN6CmxJCC4/xJYtwZ9fuie6pc+tSuC:eU4HKQ0qkBZbSd
MD5:	C7F615E15AD1A7E8133DF2608B479F02
SHA1:	C5651E9D483313B82EE42A7C6EE9041F765A3C01
SHA-256:	D2AC0CA5E77BCD857442C67F81703931D79B862B0018B0F1EF687616BBADDFE2
SHA-512:	6CFD9E42ACB7E8F83A8188C3D931D70A512D722A559B9B30519CA5346C6F22C4FAE10D567A94B4E4519541E5524FB6BABC888CD2F08991ADDE2C0623594D02(D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://s.adroll.com/j/roundtrip.js
Preview:	window.__adroll||(function(){function f(){this.version="1.0";this.exp=8760;this.eexp=720;this.pv=1E11*Math.random();this.__adc="__ar_v4";this._nad=0;this._lce=null;this._loaded=this._broken=!1;this._url=2E3;this._kwl=300;this._r={};this.cm_urls=[];this._logs=[];this.consent_networks={facebook:"f",linkedin:"linkedin"};for(var a=Array(4),b=0;b<a.length;b++)a[b]=(Math.round(1E11*Math.random()).toString(16)+Array(9).join("0")).substr(0,8);this._set_global("adroll_sid",a.join(""));this._has_global("adroll_adv_id")&&(this.load_experiment_js(),.this.init_pixchk(),this._load_precheck_js(),this.trigger_gtm_consent_event(),["adroll_adv_id","adroll_pix_id"].forEach(function(a){window.hasOwnProperty(a)&&("string"===typeof window[a]||window[a]instanceof String)&&(window[a]=window[a].replace(/[^A-Z0-9_]/g,""))}))};f.prototype.load_consent_banner=function(){window.document.getElementById("__adroll_consent_banner_el")||this.add_script_element("s.adroll.com/j/consent_tcfv2.js",{id:"__adroll_consent_ban

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\sendrolling[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	9882
Entropy (8bit):	5.285883354346058
Encrypted:	false
SSDEEP:	192:7F1mV9Z+rsnFNkmFNea1YHB/21v2BaL74A+kEaEBjMwH:7F1DgFNlNea1IB/picA+baEBjfH
MD5:	062104CC4FBE261FE3AD021F9F25A6E6
SHA1:	E22806A4D24D63A44608A2396F46D3867213F076
SHA-256:	2E4320F083852424C933BB6FB3D766C84EC4C088B7B87CF1C9AB7A34D5CFDC3C
SHA-512:	EE98610435AF6379D09EE03613F983D32FB27349394071EE58903019DE29080C6D2A62AF036C4548BDFE3B05479574E7F48F7B41549A3DBFDA25754E6F7E38E2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://s.adroll.com/j/sendrolling.js
Preview:	!function(){function t(e,n,r){function o(d,a){if(!n[d]){if(!e[d]){var i="function"==typeof require&&require;if(!a&&i)return i(d,!0);if(x)return x(d,!0);var l=new Error("Cannot find module '"+d+"'");throw l.code="MODULE_NOT_FOUND",l}var c=n[d]={exports:{}};e[d][0].call(c.exports,function(t){var n=e[d][1][t];return o(n||t)},c,c.exports,t,e,n,r)}return n[d].exports}for(var x="function"==typeof require&&require,d=0;d<r.length;d++)o(r[d]);return o}return t}({1:[function(t,e,n){"use strict";var r=t("sendrolling-core");!function(){var t=!1,e=!0;"string"==typeof window.adroll_emc_mode&&(window.adroll_emc_mode.indexOf("blur")>=0&&(t=!0),-1===window.adroll_emc_mode.indexOf("click")&&(e=!1)),window.document.body.addEventListener?(window.document.body.addEventListener("submit",r.submitHandler,!1),t&&window.document.body.addEventListener("blur",r.blurHandler,!0),e&&window.document.body.addEventListener("change",r.changeClickHandler,!0)):window.document.body.attachEvent&&(window.document.body.atta

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\72AVEQ7A3VCKZOATQLBUDH[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	4487
Entropy (8bit):	5.4430434981858955
Encrypted:	false
SSDEEP:	48:yM/7O6LnlUOCXCT7HvlSJmws9Kgksiwk7QX7HAfKsbjyZhwagw+xZ8Sg9uo9qdTZ:rHPAJhUUmHA9WZ2Q+xZjaITJdVJzl
MD5:	F9E9309682852486014D1A6B44020D01
SHA1:	000C116D323320AA359D086CBD37E7A474FE2006
SHA-256:	5282E038028AF403AD051AD904D851A5E3829E8164E06E8D0C77ABA1CE74B6A2
SHA-512:	6F5FE22C6D2229B0695549696226D0D2DF757C91B59D4C8D499BF652DC3E614D712822B227B31395E61107FC9DDEFCE3A60F0C600A638842D260F04B1A1C97D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://s.adroll.com/pixel/BZO5CPBFBZCFTNZIHK6ETU/4LLU4IYDB5FVLLYNDBY6QT/72AVEQ7A3VCKZOATQLBUDH.js
Preview:	(function () {. var scheme = (("https:" == document.location.protocol) ? "https" : "http");. var adnxs_domain = 'secure.adnxs.com';. var aol_domain = 'secure.leadback.advertising.com';. window.adroll_seg_eid = "72AVEQ7A3VCKZOATQLBUDH";. var rule = ["*", "*"];. if (scheme=='http') { adnxs_domain = 'ib.adnxs.com'; aol_domain = 'leadback.advertising.com';}. var el = document.createElement("div");. el.style["width"] = "1px";. el.style["height"] = "1px";. el.style["display"] = "inline";. el.style["position"] = "absolute";. var cm_urls = ["/cm/r/out?advertisable=BZO5CPBFBZCFTNZIHK6ETU","/cm/b/out?advertisable=BZO5CPBFBZCFTNZIHK6ETU","/cm/x/out?advertisable=BZO5CPBFBZCFTNZIHK6ETU","/cm/l/out?advertisable=BZO5CPBFBZCFTNZIHK6ETU","/cm/o/out?advertisable=BZO5CPBFBZCFTNZIHK6ETU","/cm/g/out?advertisable=BZO5CPBFBZCFTNZIHK6ETU&google_nid=adroll5"];. var img_tag = '\n';. var content = '';. for(var i = 0; i < cm_urls

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\MaterialIcons-Regular[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 57620, version 1.1
Category:	downloaded
Size (bytes):	57620
Entropy (8bit):	**7.993800967896546**
Encrypted:	**true**
SSDEEP:	1536:P9yja4UYomqS8baDYbAa21lgFehL6aP7onO2Vu:lyHBUbaza21l9hhPcXE
MD5:	012CF6A10129E2275D79D6ADAC7F3B02
SHA1:	C6C953C2CCB2CA9ABB21DB8DBF473B5A435F0082
SHA-256:	C4A1BAEC300D09E03A8380B85918267EE80FAAE8E00C6C56B48E2E74B1D9B38D
SHA-512:	0AB5E18EE3972FCD599EAD183D81CD38D8C559A5E87CA86EEBCB6A2CFAE2078A27495E3B5824AAC6EBDDC08F57D594B2CF692813134A1E002B28505EB7C3472
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://storangegoogleapiddp.agilecrm.com/flatfull/css/material-theme/icon/MaterialIcons-Regular.woff
Preview:	wOFF.....t.....GDEF...D...#...$...SGPOS...h...-...6...GSUB....'?..iP..QOS/2..(....@...`.s"ccmap..).....1.gasp...,4.....glyf..,<.....r...Y.head.....5...6.. .Nhhea...D.....$....hmtx...\...9....j.iFloca.....j.maxp..... ... .'..name...<.....z..5.post..... ...2x.c`d``..b. f.Bf.u..... ..(.....W.x.c`d``.b.c0a`.I,.c.``a.....2..U.P...p.....x..... %=.;...a....m.m.m.m...l...l.UVwW.L....F...J..*...=]Bq... ....B..O...D.8O2.....>.....J.V9}.].x{..7.}.5.....?...=..|..G?{..'.|..=D.$%.R...%b.@.dG.[~W..R].^W.t..V....?.IN...s.s...3 .wWuwuOuou_v.tGx.k.6.....n.^....y3.....?.....~..`A.....Y).[Q2|s.&._2.B").0SRA..p...~A.}.f.....Y."<>$)..y...2.Z.".~./;.!i!..s.K..n9.E...K..zF...j...".&8..O...@.. I.T!..H.*)h.E_..NJ..../IH..G....^..._.c..HK..T.G~.h..x.AF%F.k...._&R..\;..ti.i.bk.C...vdy+.Nu.....1..$e.JTE.. ...E..4.%d..Fg.;D.}f.G.QO.Do..}Z.R.K.A.B.Py}...v..x...O:q8*7]._

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284FD
Malicious:	false
Reputation:	low
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\agile-cloud[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	706
Entropy (8bit):	5.088564285486566
Encrypted:	false
SSDEEP:	12:A3EMGSiuLCXhWEMGSKLuJN7Vr4A6qKIVxRnmE2uHnOm5jRMN+DRWULd5jShWEMGV:8EHtkCxWEH/UvUAnmE2uHOSjRMURWU5s
MD5:	4B6D55CC10835A44A57ADF885C285E4D
SHA1:	E0674AD212E3D0C9B54401B8E49502B201E77F95
SHA-256:	77659A8F46F482D83B81C2789CC9BF8C094A94F5B954940B7E3711505E6C707D
SHA-512:	5ADE0596AABAC1A406744EDA86E491C6EBDC64BB4AFBAE01EBD0D16938CFA93570876CE2C5992283667038B09405F7A16FE2D5334438A5A60850DB90B747F83D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://d1gwclp1pmzk26.cloudfront.net/agile/agile-cloud.js
Preview:	function _agile_load_cloud_file(){try{if(!document.body){clearInterval(_agile_body_load_interval_timer);_agile_body_load_interval_timer=setInterval(function(){_agile_load_cloud_file()},100);return}clearInterval(_agile_body_load_interval_timer);var d=window.navigator&&window.navigator.appVersion.split("MSIE");if(parseFloat(d[1])){d=parseFloat(d[1])}var a="https://d1gwclp1pmzk26.cloudfront.net/agile/stats/min/app/v11/agile-min.js";var c=document.createElement("script");c.type="text/javascript";c.async=true;c.src=a+((d&&d==10)?"?t="+new Date().getTime():"");document.getElementsByTagName("body")[0].appendChild(c)}catch(b){}}var _agile_body_load_interval_timer;(function(){_agile_load_cloud_file()})();.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\agilecrm-forgot-password[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\agilecrm-forgot-password[1].jpg	
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 548x566, frames 3
Category:	downloaded
Size (bytes):	33500
Entropy (8bit):	7.95937657228855
Encrypted:	false
SSDEEP:	768:m1Mra9FjQOabZ5eeeqnZj2tUpfO3ry0xdOFAcmL9J:QWhnUiY3209/BJ
MD5:	AA8CBA703AF2D8D9452B223F9F1E0EFD
SHA1:	27F7CAFD1BEBA7FE49CFADB745A15543A4976109
SHA-256:	94641C17832ED22BA7FC65E61E9E6CD96D4B5EE7E21B94759BBF172220C19567
SHA-512:	79AC424E0AB8E609514499C484DB2FD8A7292651A4B09C3775BAE12E112E0AB5F55ACDA68B3803F7783D07CE3E583CF5C9E524D6D03B5332A4A2212F7DB3C48
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://storangegoogleapiddp.agilecrm.com/images/flatfull/agilecrm-forgot-password.jpg
Preview:	.....JFIF.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=====.. ....6.$.....H..I.....@$P..(PX.BW8.....@....H..+.B...@..!.B.. .... ., ...!B.....2.4.<. .B..].b.!,.$H....$!.... .@.....H... AB..T...I.B..!....@.*H....X..HB.. .B..*@....@...T..B..L.Q6.....B...V.! BX..... T .....!.. ...(IEQ...A.....i B.$.`.! B..+... .@.....H....T..BJ.LGI5.....!.B.(V. K...T..!.B..".... .B.H..@... $IUI...!....!.!...!... K,..B. ..B...@..HT....P...BV...A5.....!.V.,....X*H@..!.B..!.....P..@T.....g^.:.....@....,.%....X*HB..... .....P.....*T..BUB...t..@.. ..Qb.I`.%...H@...B.....T.*B.H..T. (PX.B!s.w..y.T.!.@.....!,...H..$!.B.. .T..T.!P.!R.HTX.+..gV...8.*B.. .aR...K.....X.!....@B...B.@.. ..HB...\.u.=6.....B....*BX%.B.XX.B@.$..B..B...@B....!R.!D..K.@..IMC...!.@..%.X. ..XX.... B@. .R. .@....HT..P.(TP.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\bootstrap.v3.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	99192
Entropy (8bit):	5.102586838867807
Encrypted:	false
SSDEEP:	768:6LBd2mvjOh9z8ZWcirwGxwa+Bh8NWHF7ZAY1tRriX109Zj8vLv/Fj:w4gZWRrhwl805Zdo092vp
MD5:	50FF14AE7DE4AF978D015BCFE3C5D535
SHA1:	1A5B41AAC5F3088505DA7061820B167EBEA581B7
SHA-256:	940EBEDD5472EBFD3AF4A2EB76D98F4E73EC7D2A571FC999F22436F4FF5AE0D4
SHA-512:	E1D06C80180164892AB5BA95983A40EE3AD819DB673B3D7631D3EE46237862ECB79AE9207621C269E59BF774872345079D1B19DC2DB88B6A6BC4E8DAC7970EE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://storangegoogleapiddp.agilecrm.com/flatfull/css/bootstrap.v3.min.css
Preview:	/*! normalize.css v3.0.0 | MIT License | git.io/normalize *//*@import url(https://fonts.googleapis.com/css?family=Ubuntu|PT+Sans);*/html{font-family:'PT Sans',"Helvetica Neue",Helvetica,Arial,sans-serif;-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%}body{margin:0}article,aside,details,figcaption,figure,footer,header,hgroup,main,nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-align:baseline}audio:not([controls]){display:none;height:0}[hidden],template{display:none}a{background:0 0}a:active,a:hover{outline:0}b,strong{font-weight:700}dfn{font-style:italic}h1{margin:.67em 0}mark{background:#ff0;color:#000}sub,sup{font-size:75%;line-height:0;position:relative;vertical-align:baseline}sup{top:-.5em}sub{bottom:-.25em}img{border:0}svg:not(:root){overflow:hidden}hr{-moz-box-sizing:content-box;box-sizing:content-box;height:0}pre{overflow:auto}code,kbd,pre,samp{font-size:1em}button,input,optgroup,select,textarea{color:inherit;font:inherit;margin

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\browser-detect[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	3175
Entropy (8bit):	5.020950479285938
Encrypted:	false
SSDEEP:	48:uJ3IvqOyef1NkjRo2rhmthFL4KcwztZ0T5oBI:c3rOyTjRo2rNUINoBI
MD5:	5EDE2CBC925DFDC005D963872D89B10C
SHA1:	A72B4254C2FBF8DD525BCEF51FBFA67332A0F60C
SHA-256:	13097C4FADC8E77726ABA557150EFF3D8F7DECBD810B251AE258EA79EEC9BAE0
SHA-512:	9F7D35793B437CC32FAD24015B00CB7A97712D27CADCA09D5DE844C330AA965058DE66B9955334C414B4C28A1CD57410876636B152399B87DDC1A0D572247E4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://storangegoogleapiddp.agilecrm.com/flatfull/lib/browser-detect.js
Preview:	var BrowserDetect = {..init : function() {...this.browser = this.searchString(this.dataBrowser).....|| "An unknown browser";...this.version = this.searchVersion(navigator.userAgent).....|| this.searchVersion(navigator.appVersion).....|| this.searchMobileVersion(navigator.userAgent).....|| "An unknown version";...this.OS = this.searchString(this.dataOS) || "unknown";..},..searchString : function(data) {...for (var i = 0; i < data.length; i++) {....var dataString = data[i].string;....var dataProp = data[i].prop;....var match = data[i].match;....this.versionSearchString = data[i].versionSearch.....|| data[i].identity;.....if (match && dataString.match(match)).....return data[i].identity;.....if (dataString) {.....if (dataString.indexOf(data[i].subString) != -1).....return data[i].identity;....} else if (dataProp).....return data[i].identity;...}..},..searchMobileVersion : function(dataString) {....try {....match = dataString.match(/Mobile SafariV([\d.]+)/);....if (match).....return pa

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\btn_google_signin[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\btn_google_signin[1].png	
File Type:	PNG image data, 187 x 43, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4373
Entropy (8bit):	7.842941938721296
Encrypted:	false
SSDEEP:	96:w2pVF4tvYKTnu+m4cC23oy+xn/LjWiXaGqzbaukCu7:lMgK7u0eoZx/LDXatzbaukV7
MD5:	E91029696EC46FD49FAB987BCDC42623
SHA1:	04D479CE442CA95119AB60B57D2869F3D86C448E
SHA-256:	33CB037CB95920498610903DCF335E848F8C19B001686F74DB0BA404AD670ECC
SHA-512:	3C1FA18744002E3D27EB65B4EFDCEF6B1597C439C3F1A3E8577B98B410E2B78770278AE9DF0A93C3CDC52AE3E0BC22C54E4BB076603A31ADFE291E3660F485 2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://storangegoogleapiddp.agilecrm.com/images/btn_google_signin.png
Preview:	.PNG.....IHDR.....+..... ..)....tEXtSoftware.Adobe ImageReadyq.e<...#iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c140 79.160451, 2017/05/06-01:08:21 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CC (Macintosh)" xmpMM:InstanceID="xmp.iid:52E2D2375C0111E8A0D78AAC04758936" xmpMM:DocumentID="xmp.did:52E2D2385C0111E8A0D78AAC04758936"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:52E2D2355C0111E8A0D78AAC04758936" stRef:documentID="xmp.did:52E2D2365C0111E8A0D78AAC04758936"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.c.....IDATx...P.W..$..'...b..P"..jM.#RJ+Wu...d.;..c...j.Z[..zw:.y....;^..A5:.rNJ'...a,..&"..@.....{....Z..-.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/errorPageStrings.js
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the website you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\es[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\es[1].js	
Category:	downloaded
Size (bytes):	2138884
Entropy (8bit):	5.381928430638528
Encrypted:	false
SSDEEP:	12288:VvJd50bXJ85PbEJD5Fb0wFeo1CGqC7kIp7hRvie9HyTueBtlJKuhO9uXrwArC1EZ:V/Q1CGq6pLunXrwArC1EgRBJEbf
MD5:	71A4F04E361B2DBB4A53E345006D3CDA
SHA1:	A1EBCCA10269608AC18584E3B8F21C78C054A1AE
SHA-256:	33AD6B5FED52CC9A2749AE770F7F1A6EC79F450E2FE66F36F7F5804E2A8C1B4B
SHA-512:	E49831D45711FDD3F6EEF33E8DB0144099011DBD38CD80114318E3990BB16B79FF3D979019633E02C2A761CE703F0A56A5DA7AF17C4743B43797E91C5F1AE392
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/68-7/tpl/min/precompiled/locales/es/es.js?_=68-7.432843952504576280
Preview:	(function(){var b=Handlebars.template,a=Handlebars.templates=Handlebars.templates||{};a["account-delete-step2-template"]=b(function(f,g,d,c,e){this.compilerInfo=[4,">= 1.0.0"];d=this.merge(d,f.helpers);e=e||{};return"\n \n \n \n <button type="button" class="close" data-dismiss="modal" aria-hidden="true">x</button>\n <h3 class="modal-title">Solicitud de cancelaci.n recibida</h3>\n \n \n Lo sentimos verte salir. Nuestro equipo de soporte se pondr. en contacto con usted dentro de 48 horas para saber m.s acerca de la raz.n para salir de nosotros. tenga en cuentasu suscripci.n todav.a est. activo y nuestro equipo de soporte le ayudar. con el proceso. \n..Para conocer el estado de la solicit ud, por favorEscr.benos.\n. \n \n \n <a href="#" c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 16x16, 32 bits/pixel
Category:	downloaded
Size (bytes):	1150
Entropy (8bit):	5.070967419123253
Encrypted:	false
SSDEEP:	24:XjlMq/jpxMwdjRQ0UrMIgQb8pswoDvh6nFqt:XR3xRnU1Yuwyhi
MD5:	C3E7DBA5797F011DCE297376E9B27048
SHA1:	1CDBD0F782C6D40C3E2882D964028444C2A18CAB
SHA-256:	74E79946A6E7903FE9AFAF4FB862E490952DB64A3A8543DE15C50AFB8A930FB1
SHA-512:	A1F57B1740264A1A2365C72EAB4CF23150C511C1577B79A8DD888E38FB188A609FCBBF8A37AC9E7044670752DB78D4D0D361749C5BB9A9D5569473B271FC509
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://storangegoogleapiddp.agilecrm.com/favicon.ico
Preview:	..... .h.....(..... ....p...p...p...p...p...p...o...q...p...q...q...q...p...p...p...u...u...u...u...u...u...u...u...v...u...u...u...u...u...u...u...{$..{$...,..;..=..:..<..=..<..=..>..<..5..})..z#..z#...)..E.....6...)..7.....|..0..N.....9..V..... .....B..J.....B..l..o.....[..J..S..P..b.....Y..P..S..Y..X..U.....T..Y.. Y.._.._..^..i.....x..]..._..`..f..f..f..e..b..a..|.....d..f..f..f..l..k..l..l..l..n..j..r.....i..l..m..l..k...q...r...r...q...r...s...q...p..n..o...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\fingerprint2.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	33059
Entropy (8bit):	5.552325876758583
Encrypted:	false
SSDEEP:	384:mrOolNy6BbFbGIORv1QpjXuBsbJxEtogqMttHnX+z1rX4/AZGPWq9qjrreC:sTy6HBOTQpzh8dttORc/A2d92
MD5:	42E38317F0366CE8879F8FDDE3951209
SHA1:	F9BD051772F651FBE77347B7E157DFB02C50D9B4
SHA-256:	AB14B83B703B88EC1243E63622A83C5E963C972A5CAE867A22AE03D5B96FF0AC
SHA-512:	0C6DCAC6411D843092BADA0968DC9A7D9201E80C9AC6696007C5CB6748FA5DC938AB6AA9D48BA146B2203CEA3253F9F970D34015A38D5C3C729E7B8254FFBD 3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.jsdelivr.net/fingerprintjs2/1.1.2/fingerprint2.min.js
Preview:	!function(e,t,i){"use strict";"undefined"!=typeof module&&module.exports?module.exports=i():"function"==typeof define&&define.amd?define(i):t[e]=i()}("Fingerprint2",this, function(){"use strict";Array.prototype.indexOf||(Array.prototype.indexOf=function(e,t){var i;if(null==this)throw new TypeError('"this' is null or undefined");var a=Objec t(this),r=a.length>>>0;if(0===r)return-1;var n=+t||0;if(Math.abs(n)===1/0&&(n=0),n>=r)return-1;for(i=Math.max(n>=0?n:r-Math.abs(n),0);r>i;){if(i in a&&a[i]===e)return i;i ++}return-1});var e=function(e){var t={swfContainerId:"fingerprintjs2",swfPath:"flash/compiled/FontList.swf",detectScreenOrientation:!0,sortPluginsFor:[/palemoon/i]};this .options=this.extend(e,t),this.nativeForEach=Array.prototype.forEach,this.nativeMap=Array.prototype.map};return e.prototype={extend:function(e,t){if(null==e)return t;for(var i in e)null!=e[i]&&t[i]!==e[i]&&(t[i]=e[i]);return t},log:function(e){window.console&&console.log(e)},get:function(e){var t=[];t=this.userAgentKey

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\forgot-domain[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\forgot-domain[1].htm	
Size (bytes):	7102
Entropy (8bit):	5.347765908278054
Encrypted:	false
SSDEEP:	192:pVos+qLyWhWAHl6r1gavoxIwlKLilWniJNz:pVoqLyeWAHl6roxIwMLiV7
MD5:	3FF4ECBE656DA1FC236D2BDFA5E9389B
SHA1:	C037A2FCD3723F82D940F0F0E6DF84D86A3D2846
SHA-256:	D14142C77F382DA4B4CA37288141638FEAA65E15C56E62B9F5C384621E063C1A
SHA-512:	387B5AB178D5A1FFF399302107508F5194092DD683816F3D0A9958742643CD2E06AA4928448D84EBB84E012B88388702A94474EE4C4C56B8B61D3815AF84D251
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://storangegoogleapiddp.agilecrm.com/forgot-domain
Preview:	.....<!DOCTYPE html>.<html lang="pt">.<head>.<meta charset="utf-8">. <meta name="globalsign-domain-verification" content="-r3RJ0a7Q59atalBdQQIvI2DYIhV YtVrtYuRdNXENx"/>.<title>Esqueci o Dom.nio</title>.<meta name="viewport" content="width=device-width, initial-scale=1.0 maximum-scale=1">.<meta name="descriptio n" content="">.<meta name="author" content="">.. Le styles -->.<link rel="stylesheet" type="text/css" href="/flatfull/css/bootstrap.v3.min.css" />.<link rel="stylesheet" type="text/css" href="/flatfull/css/font.css" />.<link rel="stylesheet" type="text/css" href="/flatfull/css/app.css" />.<link rel="stylesheet" href="//maxcdn.bootstrapcdn.com/fon t-awesome/4.3.0/css/font-awesome.min.css">.. Include ios meta tags -->.<link rel="apple-touch-icon" href="ios/touch-icon-iphone.png">.<link rel="apple-touch-icon" sizes ="76x76" href="ios/touch-icon-ipad.png">.<link rel="apple-touch-icon" sizes="120x120" href="ios/touch-icon-iphone-retina.png">.<link rel="apple-touch-icon"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\fr[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2151070
Entropy (8bit):	5.4070538131450085
Encrypted:	false
SSDEEP:	12288:jwlPdWfylzdDfelidtfNRE846f7YiGKeQEpC60WzlHTrKD9mbnuD/hpjbutcLkbb:jaR5YiGKOCVuvXrwArg1EgRBwHbv
MD5:	FAE699AC2B3A4546AD6396680A2978AB
SHA1:	BC95E0DDD9E25246FB19D017FCDD78D485A1FF8C
SHA-256:	E7E028064664E13CCF97C24978E735B578796E8756298712B221A30A224D50DC
SHA-512:	76B7700176060970CC9F63920A42EA8FAE3C5131C2D695DD484646D16CCCF51E59080339BF0EBA7B807E82E3EF4F8DEC17519C33000141F0D2E44679D5B7F170
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/68-7/tpl/min/precompiled/locales/fr/fr.js?_=68-7.432843952504576280
Preview:	(function(){var b=Handlebars.template,a=Handlebars.templates=Handlebars.templates||{};a["account-delete-step2-template"]=b(function(f,g,d,c,e){this.compilerInfo=[4,">= 1.0.0"];d=this.merge(d,f.helpers);e=e||{};return'\n \n \n \n <button type="button" class="close" data-dismiss="modal" aria-hidden="true">x</button>\n <h3 class="modal-title">Requ.te d'Annulation re.ue </h3>\n \n \n Nous sommes d.sol.s de vous voir partir. Notre .quipe de support vous contactera dans les 48 heures pour en savoir plus sur la raison de notre d.part. Notez s'il vous pla.t votre abonnement est encore actif et notre .quipe de support vous aidera avec le processus suivant. \n..Pour conna.tre l'.ta t de la requ.te, veuillez .crivez-nous .\n. \n \n \n

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\gtm[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	138962
Entropy (8bit):	5.5017159232312105
Encrypted:	false
SSDEEP:	3072:frIDM3DXduLJ/B0Va8a4XJLIJG3/r4dGIVSIRcaW:frYMzduYXdLIYjlVS
MD5:	3ABC80BF7F6D98224639981221B15A1B
SHA1:	760F8DB7C26DD9A1AD2147B579DFFE65BEC3997B
SHA-256:	5A4DBCC7EBE2CFEBF8DAF9B7EAFB9F692F22A9798BB5E570B22326BB4D90B3BB
SHA-512:	4D97874341D0CEA18E559EFB380E33A2850476BCD5F0141B5CE84447172B6620360870CEC5708F1BD28EBF4A2CA6313F769F5F7FC32377CAA9C4DE6D81D252A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.googletagmanager.com/gtm.js?id=GTM-MSGJPW4
Preview:	.// Copyright 2012 Google Inc. All rights reserved..(function(){..var data = {."resource": {. "version":"36",. . "macros":[{. "function":"__e". },{. "function":"__gas",. "vtp_cookieDomain":"auto",. "vtp_doubleClick":false,. "vtp_setTrackerName":false,. "vtp_useDebugVersion":false,. "vtp_useHashAutoLink":false,. " vtp_decorateFormsAutoLink":false,. "vtp_enableLinkId":false,. "vtp_enableEcommerce":false,. "vtp_trackingId":"UA-44894190-1",. "vtp_enableRecaptchaOpt ion":false,. "vtp_enableUaRlsa":false,. "vtp_enableUseInternalVersion":false. },{. "function":"__u",. "vtp_enableMultiQueryKeys":false,. "vtp_enableIgno reEmptyQueryParam":false. },{. "function":"__u",. "vtp_component":"URL",. "vtp_enableMultiQueryKeys":false,. "vtp_enableIgnoreEmptyQueryParam":fals e. },{. "function":"__gas",. "vtp_cookieDomain":"auto",. "vtp_doubleClick":false,. "vtp_setTracke

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\index[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\index[1].js	
Size (bytes):	1365
Entropy (8bit):	5.255420526934427
Encrypted:	false
SSDEEP:	24:2TI+MkB5mE9CuWOeWHrtqRHmmKHUKi/+u6O6G54HNHVMlqZ//5glZUW+fHn:CmKC9OeArtGFMioO6G54HVm5Z59KH
MD5:	3996D65282DD996EE0D7D4C90C139158
SHA1:	D4BD057ADF54CAF48F9591086FD3A23677C1CB72
SHA-256:	CBCE85E96B7752208CE15A09EA4D5A58B792EDC9E77F1C5CCF46C01935970F9D
SHA-512:	F14B5D2A8F96DD65107CBD8A3DAB23E6574207EEBC1BB426A74F1A523AABA753C5F45670E4865727104F19CB52744D90E6F054B5454899B0A4B511715994C3B7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://s.adroll.com/j/pre/BZO5CPBFBZCFTNZIHK6ETU/4LLU4IYDB5FVLLYNDBY6QT/index.js
Preview:	(function(f){(function(a){if(a._has_global("__cmp"))a._install_cmp=function(){};else{a._cmp_calls=[];a._set_global("__cmp",function(c,d,e){"ping"===c?e({gdprAppliesGlobally:!1,cmpLoaded:!1}):a._cmp_calls.push([c,d,e])});var f={getVendorConsents:function(c){var d=a._global("__adroll_consent"),e=a._global("__adroll_consent_data"),f=a._global("__adroll_consent_is_gdpr");e=e.euconsent||"";var h=a.b64toint(e.substr(22,4)),m=a.b64toint(e.substr(26,3))>>2,k={},g={},b,l=a._is_defined;if(c&&c.length)for(b=.0;b<c.length;b++)g[c[b]]=l(d[c[b]])?d[c[b]]:null;else{for(b in d)d.hasOwnProperty(b)&&(g[b]=d[b]);for(b=1;b<=m;b++)g[b]=l(d[b])?d[b]:null}for(b=1;24>=b;b++)k[b]=!(isNaN(h)||!(h&1<<24-b));return[{metadata:e.substr(0,18)+e.substr(20,2),gdprApplies:!!f,hasGlobalScope:!1,purposeConsents:k,vendorConsents:g},!0]},getConsentData:function(c){if(c&&"1.1"!==String(c))return[null,!1];c=a._global("__adroll_consent_data");var d=a._global("__adroll_consent_is_gdpr");return[{consentData:c.euconsent||"",gdpr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\js-all-min-1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	613090
Entropy (8bit):	5.359367968657734
Encrypted:	false
SSDEEP:	12288:UMBpRXKPg0+YDCg1PpejU0ECf5k8k10Dmee:UMBpRXKPg0+Ymg1PpejU0ECf5k8k10DG
MD5:	3CF2EC97A41036DC0A905DE856A1B2A5
SHA1:	1FA08EDD753687837C5A0956DADCFC7D34E1A645
SHA-256:	B74B1DC6DDEF5AE0E8AEE43A163D3ABE535B26AB2E412ACAD6942E3489E935F3
SHA-512:	8E04997ECD9F3C662A086E7DD6EED1959AC5FE28E6C87F1AAA229FE3574B3281309121AE042B73E0D2AB58A021EF722661F66F08C0D89004451EA5744D4DD14
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/68-7/jscore/min/locales/es/js-all-min-1.js?_=68-7.432843952504576280
Preview:	Backbone.View.prototype.close=function(){this.remove();this.unbind();if(this.onClose){this.onClose()}};var BaseModel=Backbone.Model.extend({});var BaseCollection=Backbone.Collection.extend({model:BaseModel,initialize:function(b,a){this.restKey=a.restKey;if(a.sortKey){this.sortKey=a.sortKey}if(a.descending){this.descending=a.descending}this.sort_collection=a.sort_collection;if(this.sort_collection==false){this.comparator=false}},comparator:function(a){if(this.sortKey){if(this.descending==true){return -a.get(this.sortKey)}return a.get(this.sortKey)}return a.get("id")},parse:function(a){if(a&&a[this.restKey]){return a[this.restKey]}return a}});var Base_List_View=Backbone.View.extend({events:{"click .delete":"deleteItem","click .edit":"edit","delete-checked .agile_delete":"deleteItem","click .delete-model":"deleteModel","click .delete-confirm":"deleteConfirm","click .delete-with-confirmation":"deleteModelAfterConfirmation",},initialize:function(){_.bindAll(this,"render","deleteItem","edit"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\js-all-min-2[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	886172
Entropy (8bit):	5.371633191362873
Encrypted:	false
SSDEEP:	24576:W3jdk3xKznUMvQ43rmucvEV8QpxRNqLaaH/t0qR:W3jdk3xKznU0Q43rmucvEV8QpxRNqLaG
MD5:	72399F9F5A9B48761AAB9B2563C9A77A
SHA1:	823B0C65F706AB71C7C4C10617A0561D47149689
SHA-256:	B52626E5FC3D4BF097CDE33B699A496D1F555F8EA25C29AF0BC4B15F57844B01
SHA-512:	7EC7CA33F4129417DE669AA108737C2F942969B8E5E0D04D6C28879026BC50718C6BDA5C8BA0846EADC7E2C5746E6CC4BB7CE1C0BB3796E69CE047674AE35ACC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/68-7/jscore/min/locales/es/js-all-min-2.js?_=68-7.432843952504576280
Preview:	function initWebruleChartsUI(a){initDateRangeforForm(a);a()}function showWebruleGraphs(a){showBar("core/api/webrule-analytics/web/graphreports/"+a+getOptions()+"&type=date","line-daily-chart","daily","Count",null);showBar("core/api/webrule-analytics/web/graphreports/"+a+getOptions()+"&type=hour","line-hourly-chart","hourly","Count",null);showBar("core/api/webrule-analytics/web/graphreports/"+a+getOptions()+"&type=day","line-weekly-chart","weekly","Count",null)}function getOptions(){var b="?";var a=$("#range").html().split("-");var e=getUTCMidNightEpochFromDate(new Date(a[0]));var g=$.trim(a[1]);if(g){g=g+" 23:59:59"}var c=getUTCMidNightEpochFromDate(new Date(g));c+=(((23*60*60)+(59*60)+59)*1000);b+=("start_time="+e+"&end_time="+c);var j=new Date();b+=("&time_zone="+j.getTimezoneOffset());if($("#frequency").length>0){var f=$("#frequency").val();b+=("&frequency="+f)}if($("#filter").length>0){var h=$("#filter").val();if(h!=""&&h!="ALL"){b+=("&filter="+h)}}return b}function get_webrule_tab

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\js-all-min-3[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\js-all-min-3[1].js	
Category:	downloaded
Size (bytes):	927718
Entropy (8bit):	5.689965085069192
Encrypted:	false
SSDEEP:	12288:ilNmqBdK/OLVWxnjEUQLfGpza4YzD0OZqLfT:ilFK/OLVWxnYUQqM/qrT
MD5:	88B935ECA3E6C5E3DFAA9998A4D4C544
SHA1:	7E0552CA3C52B63224151D8DDF40326CE421745F
SHA-256:	858B36E49CEAA2FF5D01C533E18ECEDD3C8485FE6182C16776876AA2CB7D0DD5
SHA-512:	7F28AB0CB35E1428FC972CCBBFEF2101914773942CDD5F8A0F9C52E10163B9462E9826337F5449CDCD6EEF52E751CD93FE4F71C05E9555F44578690B0A1447F4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/68-7/jscore/min/locales/es/js-all-min-3.js?_=68-7.432843952504576280
Preview:	var Email_Template_Events=Base_Model_View.extend({events:{"click .merge-field":"onMergeFieldSelect","click .add-attachment-select":"onAddAttachmentSelect","click .add-attachment-confirm":"onAddAttachmentConfirm","click .add-attachment-cancel":"onAddAttachmentCancel","click .add-tpl-attachment-confirm":"onTemplateAddAttachmentConfirm","click .add-tpl-attachment-cancel":"onTemplateAddAttachmentCancel","change #attachment-select":"onChangedAttachment",},onMergeFieldSelect:function(c){c.preventDefault();var b=$(c.currentTarget).attr("name");var d=$("#email-template-html").val();var f=$("#email-template-html").data("wysihtml5");if(f){editor.focus();f.editor.composer.commands.exec("insertHTML","{{"+b+"}}")}},onAddAttachmentSelect:function(g){g.preventDefault();var b=$(g.currentTarget);var f=$(b).closest("div");$(b).css("display","none");f.find(".attachment-document-select").css("display","inline");var c="<option value='{{id}}' network_type='{{titleFromEnums network_type}}' size='{{size}}'>{{

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\js-all-min-4[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	1115884
Entropy (8bit):	5.396702302321378
Encrypted:	false
SSDEEP:	6144:qYIc9uXAOenmgb/qVSLxf9uLmyXHW/yCWKvxwIByzU9cvN5RzLrNoHR4eLiQe6Gx:o2v9hY//t5C/TL7zg
MD5:	7A141E8E2DFB35A8EB50808DAD8256C2
SHA1:	803F2F2B284F1EEC874A70C5922CCC513DCF0ABA
SHA-256:	3808F7D8786E5A544469E7414B2E563F8CA78B2D850752CCD7AECAE33614EEFD
SHA-512:	2684F0B88BA5CE6BD47FA0710B40AEADF1051AC828AD9C02CB6522F7C3ACF38E62B38A405F460AE2641AFC8790FCB235DF2C4A7ED742AD0CA53A37CEB2AF0F17
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/68-7/jscore/min/locales/es/js-all-min-4.js?_=68-7.432843952504576280
Preview:	var recent_view;var recent_view_update_required=false;var MAX_RECENT=6;function populate_recent_menu(){if(!recent_view){var b=[];try{b=JSON.parse(localStorage.recentItems)}catch(c){}recent_view=new Base_Collection_View({restKey:"contacts",templateKey:"recent-menu",data:b,individual_tag_name:"li",sort_collection:false,postRenderCallback:function(d){$("#recent-menu").append($(d).html())}});if(recent_view.collection.length==0){$("#recent-menu>ul").html('<li class="list-group-item" style="border:none">No hay actividad reciente ');hideTransitionBar()}else{recent_view.render(true)}}}function add_recent_view(d){if(recent_view==undefined){populate_recent_menu()}if(!recent_view.collection.get(d.get("id"))){if(recent_view.collection.length>=MAX_RECENT){recent_view.collection.pop({silent:true})}recent_view.collection.unshift(d)}else{recent_view.collection.remove(d,{silent:true});recent_view.collection.unshift(d)}recent_view_update_required=true;var

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\js-all-min-4[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	1118776
Entropy (8bit):	5.402149603574942
Encrypted:	false
SSDEEP:	6144:pYKG9uFAUC8DIb/aaSLZvpBhmyUrb6JyWLvewIByzC9WBYkHQ/vCmPp65N6nCelY:W/39zvnrAcD/hBRzW
MD5:	BADABB3AF1BB723FFB0E781036FDC6E9
SHA1:	D96063F552FAC0D615D527D7EB106CB56EE28AFC
SHA-256:	F2EE62B339F4C44083C3BE47E727369473CE074925C0FA2DA07EC144617AD7CB
SHA-512:	1714A841FC389ADA9858F5DB4A048677E884C462EF5D4BA83D6C58CEF5FB37385D7A1745E0D7E2B5EC8348578AFD692F86393E66F187EFF85D8E476CAAABA56C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/68-7/jscore/min/locales/fr/js-all-min-4.js?_=68-7.432843952504576280
Preview:	var recent_view;var recent_view_update_required=false;var MAX_RECENT=6;function populate_recent_menu(){if(!recent_view){var b=[];try{b=JSON.parse(localStorage.recentItems)}catch(c){}recent_view=new Base_Collection_View({restKey:"contacts",templateKey:"recent-menu",data:b,individual_tag_name:"li",sort_collection:false,postRenderCallback:function(d){$("#recent-menu").append($(d).html())}});if(recent_view.collection.length==0){$("#recent-menu>ul").html('<li class="list-group-item" style="border:none">Aucune Activit. R.cente ');hideTransitionBar()}else{recent_view.render(true)}}}function add_recent_view(d){if(recent_view==undefined){populate_recent_menu()}if(!recent_view.collection.get(d.get("id"))){if(recent_view.collection.length>=MAX_RECENT){recent_view.collection.pop({silent:true})}recent_view.collection.unshift(d)}else{recent_view.collection.remove(d,{silent:true});recent_view.collection.unshift(d)}recent_view_update_required=true;va

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\localize[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	3682
Entropy (8bit):	4.840907939868298
Encrypted:	false
SSDEEP:	96:Tx6G1OUxPjrl+EuqEZNubbZ5/qN6xqmb/:TU03POubn/qN6xqmb/
MD5:	DA508945086CB8BD958D641FA4408E65
SHA1:	AA24BA80252A1D58944BB3DF77BE6256B733EFA3
SHA-256:	6F7F1F9FEF8DFB5A85455F8BE46BDF50A251E7962E4A406759A833F5584A6BE8
SHA-512:	C5DAF986F5DC2BE29154D1BE4D5D393A09418B46BF7710163951A6122711EE2065E6EBA77620040C964BCA24E937D74FAC803A8882B948912B54DA5179CB30DI
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://storangegoogleapiddp.agilecrm.com/locales/html5/localize.js?_=
Preview:	/**. * HTML5 Validations Customization . */.function _agile_set_custom_validate(input){..input.setCustomValidity(getCustomValidity(input)); .}..// Reset to default & Val idate.function _agile_reset_custom_validate(input){. input.setCustomValidity("");.. if(input.checkValidity()). input.setCustomValidity("");.. // input.reportValidit y();.}.//regular expressions for the &#39.function escapeRegExp(str) {. return str.replace(/([.*+?^=!:${}()|\[\]\/\\])/g, "\\$1");.}.// Returns the exact error based on the validity check point of the field.function getCustomValidity(input){..var type = input.type;. // If val is Empty..if(input.validity.valueMissing){. if(input.nodeName == "SELECT"). return localeJSON["invalid-select-one"];. else {. if(type == "number" && input.validity.badInput){. return localeJSON["enter-number-only"];. }. return localeJSON["invalid-default"];. }.. }. // If field not

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\login-min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	165126
Entropy (8bit):	5.104488981482596
Encrypted:	false
SSDEEP:	768:J/BbQy/NOX9z8FWcirwGxwa+BL8NWLPDFaM1vRriX1U9Hj8/Lv/Fq/vXCUgv3eOl:VQaFWRrhwX80XFLoU9I/C4H2xwL
MD5:	4036963EE242F2E75DA8447C9ECD0BC1
SHA1:	61133B8AF204888EF4B59528CC0EF5948A3198DA
SHA-256:	F0B7DDAA6346FFB175035EF6BCE96D21E477165C31603CB6024509503337C35D
SHA-512:	FF82DB6AB991293792263B42785DDA77078F57BD08821CE961971FA53FA47AC770CB2638E7F98169CC9B23317EEAED188607A7A5D9995BEB00AF452027822431
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://storangegoogleapiddp.agilecrm.com/flatfull/css/min/login-min.css
Preview:	/*! normalize.css v3.0.0 | MIT License | git.io/normalize */html{font-family:'PT Sans','Helvetica Neue',Helvetica,Arial,sans-serif;-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%}body{margin:0}article,aside,details,figcaption,figure,footer,header,hgroup,main,nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-align:baseline}audio:not([controls]){display:none;height:0}[hidden],template{display:none}a{background:0}a:active,a:hover{outline:0}b,strong{font-weight:700}dfn{font-style:italic}h1{margin:.67em 0}mark{background:#ff0;color:#000}sub,sup{font-size:75%;line-height:0;position:relative;vertical-align:baseline}sup{top:-.5em}sub{bottom:-.25em}img{border:0}svg:not(:root){overflow:hidden}hr{-moz-box-sizing:content-box;box-sizing:content-box;height:0}pre{overflow:auto}code,kbd,pre,samp{font-size:1em}button,input,optgroup,select,textarea{color:inherit;font:inherit;margin:0}button{overflow:visible}button,select{text-transform:none}button,html i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\portlets[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	487743
Entropy (8bit):	5.542421323808416
Encrypted:	false
SSDEEP:	6144:ceBWC01e7W+0Be6Wr0QA2AV9Zy1m4jrJT4wrJz4HrJIz7CfLeOGattNs4IrJhT2:ceBWC01e7W+0Be6Wr0Q+TbN
MD5:	E60648CDE8B0CFB057EE39ECB2B2A6E7
SHA1:	54BC22E8DEBF95B0AC92E8CD8DC519172DD8A3A0
SHA-256:	0A0F2166D8FD648B41A298A7CA7C74783F1897BFE63D0180BA6CCE1828A81BA3
SHA-512:	19EB607B3AFF563EFC6AD20499B1D7D15E0F296C648747BFB09A282C5FFA2484A17261DE1A9A33C6A92CE89DAAC9F9002D3F5D11A2EA3DD9E4FE5E6D7FEFF(A5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/68-7/tpl/min/precompiled/locales/es/portlets.js?_=68-7.432843952504576280
Preview:	(function(){var b=Handlebars.template,a=Handlebars.templates=Handlebars.templates||{};a["marketing-video-modal-template"]=b(function(f,g,d,c,e){this.compilerInfo=[4,">= 1.0.0"];d=this.merge(d,f.helpers);e=e||{};return'\n. \n... \n.... \n.....<button class="close" data-dismiss="modal">×</button>\n.....<h3 class="modal-title">Marketing Tutorial</h3>. \n.... \n..... \n..... \n.....<iframe style="width:100%;" height="345" src="//www.youtube.com/embed/KP8feLANFZA?enablejsapi=10&autoplay=1&showinfo=0" frameborder="0" allowfullscreen></iframe>\n..... \n..... \n... \n. \n.\n'});a["mobile-app-options-template"]=b(function(g,m,f,l,k){this.compilerInfo=[4,">= 1.0.0"];f=this.merge(f,g.helpers);k=k||{};var j="",d,h,r,p=this,i="function",n=f.blockHelperMissing;function e(t,s){return" "}functio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\portlets[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	489127
Entropy (8bit):	5.560681550245632
Encrypted:	false
SSDEEP:	6144:qeBWC0Te7W+0pe6Wr0XSc91kYG9xt2L4jrJh4wrJl4HrJlz7HfLcBGaCV+3QyS42:qeBWC0Te7W+0pe6Wr0w36QV
MD5:	219D58FE717D777E848158DBBAD2FA91
SHA1:	DFB8295DA48238EA437D779D20F7E1880038E038
SHA-256:	C49BF9E54E3023FF713EAF0D98EA4282CC28075511ED208134F7054C04D912C3
SHA-512:	3C3010DA591469E694C73B0A7723E4B6CB5D14C597E5574DCA4E5BEB41F59C984E0B33CE678DD4365D027A420AF6692F37F61FAB5F7D02240FCFF9BC5F0E2E F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://doxhze3l6s7v9.cloudfront.net/app/68-7/tpl/min/precompiled/locales/fr/portlets.js?_=68-7.432843952504576280
Preview:	(function(){var b=Handlebars.template,a=Handlebars.templates=Handlebars.templates||{};a["marketing-video-modal-template"]=b(function(f,g,d,c,e){this.compilerInfo=[4,">= 1.0.0"];d=this.merge(d,f.helpers);e=e||{};return'\n. \n... \n.... \n.....<button class="close" data-dismiss="modal">×</button>\n.....<h3 class="modal-title">Marketing Tutorial</h3>. \n.... \n..... \n..... \n.....<iframe style="width:100%;" height="345" src="//www.youtube.com/embed/KP8feLANFZA?enablejsapi=10&autoplay=1&showinfo=0" frameborder="0" allowfullscreen></iframe>\n..... \n.... \n... \n. \n.\n'});a["mobile-app-options-template"]=b(function(g,m,f,l,k){this.compilerInfo=[4,">= 1.0.0"];f=this.merge(f,g.helpers);k=k||{};var j="",d,h,r,p=this,i="function",n=f.blockHelperMissing;function e(t,s){return" "}functio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\preload-js-src-iframe[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	2267
Entropy (8bit):	5.557467892378066
Encrypted:	false
SSDEEP:	48:u4NN+SF/CwtPSD3CgBk6IdTXqtVz0FNrl/arH20rH+ZrrH8Z2rH8Z1rHsrH57rvj:uAVID3Jk6Id7yVzCr1r9r8r7rwrMrVr7
MD5:	AF643D26A4282A3FBC0867868E010C68
SHA1:	DE98B19785074CBBCE3C4FA6A1BE62BC1C3DFA18
SHA-256:	5C400891A9AF59120153A78B743D68426066D69FDA47D3416A85AAD054A55BCA
SHA-512:	7B0AA51BA29C24C7C43F555DCBDFED1AD4571A91E6C4892859FA009D5A3940DC5047B45CB53737003CAD34A7969D9198A54497F18923D1635E9EAE1CB2873D 6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://storangegoogleapiddp.agilecrm.com/flatfull/preload-js-src-iframe.html
Preview:	<!DOCTYPE html>..<html>.<head>..<script src='//cdnjs.cloudflare.com/ajax/libs/headjs/1.0.3/head.min.js'></script>.</head>.<body>. <script type="text/javascript">. ..window.onerror = function(message, url, lineNumber) { ... // maybe some handling? ... return true; // prevents browser error messages ...};. ..function get_cloudfront_path(type){....if(type == "static").....return "<%=CLOUDFRONT_STATIC_FILES_PATH%>";....else if(type == "lib").....return "<%=CLOUDFRONT_TEMPLATE_LIB_PATH%>";....else if(type == "version").....return "<%=_AGILE_VERSION%>";...}.. var CLOUDFRONT_STATIC_FILES_PATH = parent.get_cloudfront_path("static");. var CLOUDFRONT_TEMPLATE_LIB_PATH = parent.get_cloudfront_path("lib");. var _AGILE_VERSION = parent.get_cloudfront_path("version");. var _AGILE_LANGUAGE = parent.get_cloudfront_path("language");. if(window.location.href.indexOf("localhost:88") != -1). {. ..CLOUDFRONT_TEMPLATE_LIB_PATH = "/";. ..CLOUDFRO

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\sourcesanspro-bold[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 26608, version 1.1
Category:	downloaded
Size (bytes):	26608
Entropy (8bit):	7.974669615291045
Encrypted:	false
SSDEEP:	768:FVqxq2EkrZYsAq+Lqw4my+7utXUxA87W/m5cLYV:f1ErCPq0BuJrLS
MD5:	1146F3F229F5A3D3C711F0922EA2EB87
SHA1:	5534E9EB2BE04D8A5223489EA9FC9C305AAAB9C9
SHA-256:	5A86FA4090AD9E6F6F5D0CB9CCDFD96DB22E77BFB787BD28085E6BAA376F81E8
SHA-512:	E75940CC0F1DB8431D1849FE1FEF9C576C214F550FB163F298785DDF329FF6215AF42544271639C86BAC037857762419A6C6E9C003E72EE39CEDEFFCCEDF659
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://storangegoogleapiddp.agilecrm.com/flatfull/font/sourcesanspro/sourcesanspro-bold.woff
Preview:	wOFF.....g.....L.....FFTM...l.....jNi.OS/2.....V...`[.cmap.....T...cvt ...|...(...(...ifpgm.....s.Y.7gasp.....glyf...../%..Zx....head..3....4...6...&hhea..4.....$....hmtx..4(.....kern..6D.....N.,..loca..Q.....$maxp..S.... ... ...:name..S.....;4....post..e.....).b.Jprep..g....K...KE.....ZE.....\.yx.c`f.....).....B3.1.1*.E...Y...X..v.....8.8.2(0.*.2.....|.QP..q2H..S...r.....x.b```.b..F.....1.,.....%.d.2.1.g4d.f:.t...3.3.3.....l.....B...%!%...../.....b@.%. . ..e.....O...?...?.....{.....z.....}.....<0.w..9.{...l@...L@..U.d.+.;.'.7./.....@J.*.j...Z.:.z...F.&.f...V.6.v...N...n...^.>.~...A.....GDFE....'$&%3ttv.N..`.e+..\.v...7l.u....v....CIZz....E...9.]s.J..2+...cX..9....gHii.y...7o]....0...w..e.o.fh.k..8i..3...?.....'j.....s.....3.....>...~.....x.]..N.0...\|...,$[V.*W.28.P.@.|..R+...)...<..-/.....]|w.;..O..I..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\stat[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	69273
Entropy (8bit):	5.431073120117305
Encrypted:	false
SSDEEP:	768:tVCTCtD+2Ky4+R9c7oOOyFrTA+SrL4h6lrJg35CAdzYOTQpz0egx5DJ5gZwOvwOr:trgEajNOg35CAdzYT0egxhJc6M
MD5:	876E4861A1BABB46D5B0CFA36D35C226
SHA1:	7D5A06F60AE9A41F29ADBF2EF6799271E63F63A2
SHA-256:	8B327691CFBC4BBFD8B8A7F6EC49D5ABFD01E44E8DED46A34330CBFFC6F435B5
SHA-512:	B9097443A8864F1DD1A2EC68BEBE2F4E24D023B2EFCB799C37CCE01380620C7FB4D2EBCC860C5037ED7B33B021BB9B7CFB2805F3622C3B01B38C9FEC5AD9723
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.clickcease.com/monitor/stat.js
Preview:	!function(){"use strict";function u(e,t,n,r,o,a,i){try{var c=e[a](i),u=c.value}catch(e){return void n(e)}c.done?t(u):Promise.resolve(u).then(r,o)}function a(c){return function(){var e=this,i=arguments;return new Promise(function(t,n){var r=c.apply(e,i);function o(e){u(r,t,n,o,a,"next",e)}function a(e){u(r,t,n,o,a,"throw",e)}o(void 0)})}}function i(e,t){if(!(e instanceof t))throw new TypeError("Cannot call a class as a function")}function r(e,t){for(var n=0;n<t.length;n++){var r=t[n];r.enumerable=r.enumerable||!1,r.configurable=!0,"value"in r&&(r.writable=!0),Object.defineProperty(e,r.key,r)}}function c(e,t,n){return t&&r(e.prototype,t),n&&r(e,n),e}function o(e,t,n){return t in e?Object.defineProperty(e,t,{value:n,enumerable:!0,configurable:!0,writable:!0}):e[t]=n,e}function l(e,t){return function(e){if(Array.isArray(e))return e}(e)||function(e,t){if("undefined"==typeof Symbol||!(Symbol.iterator in Object(e)))return;var n=[],r=!0,o=!1,a=void 0;try{for(var i,c=e[Symbol.iterator]();!(r=(i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\web-rules[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	126819
Entropy (8bit):	5.280063708274555
Encrypted:	false
SSDEEP:	3072:ds/lO8DlOpeW38ekWIN5WIrlHlHDlOiWo:ds/lOClOpeW38ekWIHWIrlHlHDlOiWo
MD5:	D22E889DEF1FF13AF9391214005022CF
SHA1:	942EBBE8ED5AF87EE4F473A89D52848A664A2874
SHA-256:	77A6E2D472B67370674ADFA603ADB9AA4753A1EB59DF5227C6D2F24FC5A91E91
SHA-512:	A85B6F6E9A938B49A6020C5CC55C3261AE1C7A0BCD060269F328B30D1B09DF9F8F1D493A88297D4A241D65C3659014F25AEDBD5068E60D5ED14005D9892B314
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://our.agilecrm.com/core/js/api/web-rules?callback=json7821660555536009&id=jo22gpvhr34r2mccjaekgsm7oh
Preview:	json7821660555536009(..[{"cursor":null,"count":null,"id":4540766905171968,"name":"CSM - Live chat","disabled":false,"rule_type":"WEBRULE","rules":[{"LHS":"page","CONDITION":"MATCHES","RHS":"agilecrm.com/#live-chat","RHS_NEW":null,"nested_condition":null,"nested_lhs":null,"nested_rhs":null,"business_hours_time_from":null,"business_hours_time_to":null,"business_hours_time_zone":null,"ruleType":"Contact"}],"actions":[{"action":"ADD_TAG","RHS":"Chat CSM","position":null,"popup_pattern":null,"title":null,"popup_text":null,"delay":null,"timer":0,"redirect_url":null}],"position":0,"country":"GB","created_time":1530715876,"updated_time":0},{"cursor":null,"count":null,"id":4555792445603840,"name":"Feedback - CSM","disabled":false,"rule_type":"WEBRULE","rules":[{"LHS":"page","CONDITION":"MATCHES","RHS":"agilecrm.com/#ticket-feedback","RHS_NEW":null,"nested_condition":null,"nested_lhs":null,"nested_rhs":null,"business_hours_time_from":null,"business_hours_time_to":null,"business_hours_time_zone":

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\web-rules[2]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	126819
Entropy (8bit):	5.280091141547827
Encrypted:	false
SSDEEP:	3072:Ts/lO8DlOpeW38ekWIN5WIrlHlHDlOiWo:Ts/lOClOpeW38ekWIHWIrlHlHDlOiWo
MD5:	03ECCB7FBD0182E7B856C1AB3722B5B9
SHA1:	B82855464BC55E63FCFAEB6BA53E6195D28D07BA
SHA-256:	02E0FBE6AF251DD58192AF2669AA25EF10846E87A3CEA2132C3A37888F2F3A8D
SHA-512:	21D994466E05D0791CB081C33D2C3B4E1AFD25D067F7183A68F248D80268CB63534DC459AD5C2848899FF74B2CD191B54335F0D3DF5E4B3239D4C424E3F00EC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://our.agilecrm.com/core/js/api/web-rules?callback=json7679780226056252&id=jo22gpvhr34r2mccjaekgsm7oh
Preview:	json7679780226056252(..[{"cursor":null,"count":null,"id":4540766905171968,"name":"CSM - Live chat","disabled":false,"rule_type":"WEBRULE","rules":[{"LHS":"page","CONDITION":"MATCHES","RHS":"agilecrm.com/#live-chat","RHS_NEW":null,"nested_condition":null,"nested_lhs":null,"nested_rhs":null,"business_hours_time_from":null,"business_hours_time_to":null,"business_hours_time_zone":null,"ruleType":"Contact"}],"actions":[{"action":"ADD_TAG","RHS":"Chat CSM","position":null,"popup_pattern":null,"title":null,"popup_text":null,"delay":null,"timer":0,"redirect_url":null}],"position":0,"country":"GB","created_time":1530715876,"updated_time":0},{"cursor":null,"count":null,"id":4555792445603840,"name":"Feedback - CSM","disabled":false,"rule_type":"WEBRULE","rules":[{"LHS":"page","CONDITION":"MATCHES","RHS":"agilecrm.com/#ticket-feedback","RHS_NEW":null,"nested_condition":null,"nested_lhs":null,"nested_rhs":null,"business_hours_time_from":null,"business_hours_time_to":null,"business_hours_time_zone":

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\web-rules[3]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	126819
Entropy (8bit):	5.280109315427302
Encrypted:	false
SSDEEP:	3072:Ws/lO8DlOpeW38ekWIN5WIrlHlHDlOiWo:Ws/lOClOpeW38ekWIHWIrlHlHDlOiWo
MD5:	D89A7BD827B9DADB1156417EC1EC6CF3
SHA1:	3CA0BA626AF7F6ED89B20B3C482DD9C15E3404DC
SHA-256:	00B278C55F4ED809E0035A7712830645221A5F72307FE28C9826E49ED2A1DE31
SHA-512:	51820C1C058D816ADD46C38635788861CED561E5A3A192589F7082DC16906C0E2DA644750CB6ECD13D39CE7CAC98C8071E397D9C63DD16E190A13F8499014A6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://our.agilecrm.com/core/js/api/web-rules?callback=json9764156231984684&id=jo22gpvhr34r2mccjaekgsm7oh
Preview:	json9764156231984684(..[{"cursor":null,"count":null,"id":4540766905171968,"name":"CSM - Live chat","disabled":false,"rule_type":"WEBRULE","rules":[{"LHS":"page","CONDITION":"MATCHES","RHS":"agilecrm.com/#live-chat","RHS_NEW":null,"nested_condition":null,"nested_lhs":null,"nested_rhs":null,"business_hours_time_from":null,"business_hours_time_to":null,"business_hours_time_zone":null,"ruleType":"Contact"}],"actions":[{"action":"ADD_TAG","RHS":"Chat CSM","position":null,"popup_pattern":null,"title":null,"popup_text":null,"delay":null,"timer":0,"redirect_url":null}],"position":0,"country":"GB","created_time":1530715876,"updated_time":0},{"cursor":null,"count":null,"id":4555792445603840,"name":"Feedback - CSM","disabled":false,"rule_type":"WEBRULE","rules":[{"LHS":"page","CONDITION":"MATCHES","RHS":"agilecrm.com/#ticket-feedback","RHS_NEW":null,"nested_condition":null,"nested_lhs":null,"nested_rhs":null,"business_hours_time_from":null,"business_hours_time_to":null,"business_hours_time_zone":

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\web-rules[4]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	126819
Entropy (8bit):	5.280116067238086
Encrypted:	false
SSDEEP:	3072:Ms/lO8DlOpeW38ekWIN5WIrlHlHDlOiWo:Ms/lOClOpeW38ekWIHWIrlHlHDlOiWo
MD5:	6427BA6BFDC74E9846774739897D5C04
SHA1:	52CF51333557D349C9596C33D07E087DE08D4550
SHA-256:	2070DC2184C4591093C865488372EBE7F0DAA119C70561DCFF898F136C8C19AF
SHA-512:	B3EE1D434575C62E7BC29EEAA5264CBCAC300F20A04469A2D933F3F67FCA9677B789D414FDB10283EF10A7269CD60760ACD97CAACB186ED69B17771B0DEFE40F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://our.agilecrm.com/core/js/api/web-rules?callback=json7766037593507772&id=jo22gpvhr34r2mccjaekgsm7oh
Preview:	json7766037593507772(..[{"cursor":null,"count":null,"id":4540766905171968,"name":"CSM - Live chat","disabled":false,"rule_type":"WEBRULE","rules":[{"LHS":"page","CONDITION":"MATCHES","RHS":"agilecrm.com/#live-chat","RHS_NEW":null,"nested_condition":null,"nested_lhs":null,"nested_rhs":null,"business_hours_time_from":null,"business_hours_time_to":null,"business_hours_time_zone":null,"ruleType":"Contact"}],"actions":[{"action":"ADD_TAG","RHS":"Chat CSM","position":null,"popup_pattern":null,"title":null,"popup_text":null,"delay":null,"timer":0,"redirect_url":null}],"position":0,"country":"GB","created_time":1530715876,"updated_time":0},{"cursor":null,"count":null,"id":4555792445603840,"name":"Feedback - CSM","disabled":false,"rule_type":"WEBRULE","rules":[{"LHS":"page","CONDITION":"MATCHES","RHS":"agilecrm.com/#ticket-feedback","RHS_NEW":null,"nested_condition":null,"nested_lhs":null,"nested_rhs":null,"business_hours_time_from":null,"business_hours_time_to":null,"business_hours_time_zone":

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\141590300270327[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	246322
Entropy (8bit):	5.466759589515212
Encrypted:	false
SSDEEP:	6144:Rk1HWCSntDV/H4K3V/H486EPjQHWuH3HpH:f6E2
MD5:	348AFD7BD47729F11B6FED351FBC991C
SHA1:	49D7DD41559F7A8FE8C0C39BC69B44AB6D8A746E
SHA-256:	113E5E2F3912C9271BC8D2BB386DE5F649F9326F1CC308100F493EEC0B90223F
SHA-512:	9C8A8E325D37F63DB367D1899C1F1BCC4243FBA327F53C2C1816C1AD326A7B41F4B5D65622BABC24F5B1D09F0601BD5536109A9912D91295133B27EDAD75515
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://connect.facebook.net/signals/config/141590300270327?v=2.9.33&r=stable

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\141590300270327[1].js	
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

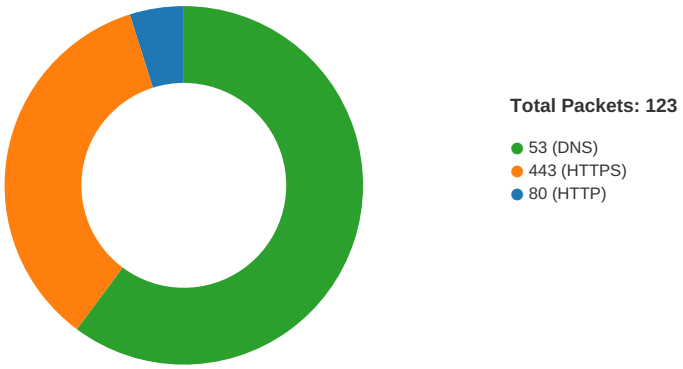
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\John-Danial[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 48x48, frames 3
Category:	downloaded
Size (bytes):	1559
Entropy (8bit):	7.430405746867828
Encrypted:	false
SSDEEP:	48:7vyMsEmQjC7vHwzHYgRdd4mVOY14OhY5/BAR:eMshOC7vQzHDd4mn+OS5/BAR
MD5:	166A96874F5D509B2846DB0A7C443F4C
SHA1:	E804746EF2671FA43E1459BF8AEE00CD37CFFEB7
SHA-256:	4818C0612BA0A4ED8232293DF5D286DBDB05213164926B5C3C5C9210E055B4BB
SHA-512:	62552A4E62D7AB3D6EBC1C31555A7595A5D9701D7E6D728AB4013496C473452052AF1553C663500ED8D85DF4A5A812E854C0965733CA337162A02A5B0613BD41
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://storangegoogleapiddp.agilecrm.com/images/flatfull/John-Danial.jpg
Preview:	......JFIF.....C.....!......"$".$.....C.....0.0.....Xq .>a.x%..!.:. .:...Y...u..m@..PZj..fr.....h..I.Qe...X"...TV.....[.^.4.=..H....X.&....."..."..1.....(..?.x.aG..\.]1...k...5..q.u....}m.7..3Z"._...\.b..Z.F..u..<.....%..]..OI.... ...V.#.M'._/...e.e.d.wU.g.....4r...':....c....:Z....RF1.;..MD....tI1m...9._.C...tU....._vt....RpO.....55..t}..f.%.3JZr1.XZ...I..i.%.N1.+j..s|.&}....U..Y...,7h.M...C..K.7A6!.. Y....)..>V ..6.]...ci8.an"n=.....k...H.X.M.@D....UU7s.B.=u...=G.*Evy.a....).....!1..AQ"B.aq.#2.....?.....d...b...2....;.....g...M..Lc...'C..#X...R,.a.c.C.....w.`..L..qF..4.....@. .N.7..<.3.ZhL.....39.ch....Z...:Ia..w..2F..M..y....i..h.I'.f..<r.j..I....Z..Uf..A..R..:.B....]..!..*.{.`.

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 18:58:57.001307964 CET	49716	80	192.168.2.3	142.250.185.179

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 18:58:57.001894951 CET	49717	80	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:57.049824953 CET	80	49716	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.049916983 CET	49716	80	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:57.050656080 CET	49716	80	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:57.052978992 CET	80	49717	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.053060055 CET	49717	80	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:57.099112988 CET	80	49716	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.215784073 CET	80	49716	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.215876102 CET	49716	80	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:57.221435070 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:57.269937992 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.270153999 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:57.276326895 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:57.326301098 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.336754084 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.336810112 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.336841106 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.336863995 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.337397099 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:57.387299061 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:57.393145084 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:57.393237114 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:57.440445900 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.441848993 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.441973925 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.442862034 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.442895889 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.442981958 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:57.443032980 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:57.444472075 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:57.448889017 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.449075937 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:57.499444008 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.673621893 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.673892021 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.673990011 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.674046040 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:57.674108028 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:57.674117088 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:57.674705982 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:57.681500912 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:57.723140001 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.730159044 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.970086098 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.970149994 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.970179081 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.970371962 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:57.971914053 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.971956015 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.972002029 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:57.972055912 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:57.972115993 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:57.973746061 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.973790884 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.973905087 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:57.973934889 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:57.976309061 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.976358891 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.976428032 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:57.976461887 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:57.979871035 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:57.980226994 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:58.025907040 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:58.068645000 CET	49718	443	192.168.2.3	142.250.185.179

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 18:58:58.076109886 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:58.117492914 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:58.148133039 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:58.148703098 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:58.196639061 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:58.196979046 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:58.283356905 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:58.283410072 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:58.283435106 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:58.283591032 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:58.284058094 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:58.285135984 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:58.285165071 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:58.285275936 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:58.285322905 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:58.287019014 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:58.287055969 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:58.287146091 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:58.287193060 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:58.290616035 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:58.290657997 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:58.290815115 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:58.294091940 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:58.294117928 CET	49721	443	192.168.2.3	13.226.175.122
Feb 22, 2021 18:58:58.294208050 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:58.294243097 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:58.294296026 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:58.295062065 CET	49722	443	192.168.2.3	13.226.175.122
Feb 22, 2021 18:58:58.297642946 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:58.297688007 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:58.297723055 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:58.297756910 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:58.301100969 CET	443	49718	142.250.185.179	192.168.2.3
Feb 22, 2021 18:58:58.301177025 CET	49718	443	192.168.2.3	142.250.185.179
Feb 22, 2021 18:58:58.321513891 CET	443	49718	142.250.185.179	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 18:58:49.218453884 CET	50620	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:58:49.277914047 CET	53	50620	8.8.8.8	192.168.2.3
Feb 22, 2021 18:58:50.425168991 CET	64938	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:58:50.478604078 CET	53	64938	8.8.8.8	192.168.2.3
Feb 22, 2021 18:58:51.382894039 CET	60152	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:58:51.436054945 CET	53	60152	8.8.8.8	192.168.2.3
Feb 22, 2021 18:58:52.132263899 CET	57544	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:58:52.182403088 CET	53	57544	8.8.8.8	192.168.2.3
Feb 22, 2021 18:58:53.568336010 CET	55984	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:58:53.619966984 CET	53	55984	8.8.8.8	192.168.2.3
Feb 22, 2021 18:58:54.374433041 CET	64185	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:58:54.433976889 CET	53	64185	8.8.8.8	192.168.2.3
Feb 22, 2021 18:58:55.694143057 CET	65110	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:58:55.757328033 CET	53	65110	8.8.8.8	192.168.2.3
Feb 22, 2021 18:58:56.922090054 CET	58361	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:58:56.992753983 CET	53	58361	8.8.8.8	192.168.2.3
Feb 22, 2021 18:58:58.093260050 CET	63492	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:58:58.162075043 CET	60831	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:58:58.163455009 CET	53	63492	8.8.8.8	192.168.2.3
Feb 22, 2021 18:58:58.223371029 CET	53	60831	8.8.8.8	192.168.2.3
Feb 22, 2021 18:58:58.297306061 CET	60100	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:58:58.322890043 CET	53195	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:58:58.346033096 CET	53	60100	8.8.8.8	192.168.2.3
Feb 22, 2021 18:58:58.385093927 CET	53	53195	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:00.008235931 CET	50141	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 18:59:00.075457096 CET	53	50141	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:00.717005014 CET	53023	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:00.758415937 CET	49563	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:00.765552044 CET	53	53023	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:00.790321112 CET	51352	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:00.799118042 CET	59349	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:00.809169054 CET	57084	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:00.809900999 CET	53	49563	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:00.829771996 CET	58823	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:00.837590933 CET	57568	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:00.848042965 CET	53	59349	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:00.860475063 CET	53	51352	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:00.870234013 CET	53	57084	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:00.887684107 CET	53	57568	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:00.888385057 CET	53	58823	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:00.895327091 CET	50540	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:00.903312922 CET	54366	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:00.951878071 CET	53	54366	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:00.975912094 CET	53	50540	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:01.448964119 CET	53034	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:01.497642994 CET	53	53034	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:02.051567078 CET	57762	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:02.061393976 CET	55435	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:02.110115051 CET	53	55435	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:02.119381905 CET	53	57762	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:02.153537035 CET	50713	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:02.223258018 CET	53	50713	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:02.376311064 CET	56132	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:02.436624050 CET	53	56132	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:02.448631048 CET	58987	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:02.452238083 CET	56579	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:02.456516027 CET	60633	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:02.460340977 CET	61292	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:02.500215054 CET	53	58987	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:02.501542091 CET	63619	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:02.503703117 CET	53	56579	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:02.507981062 CET	53	60633	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:02.525234938 CET	53	61292	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:02.550132036 CET	53	63619	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:02.660151958 CET	64938	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:02.711515903 CET	53	64938	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:03.325958967 CET	61946	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:03.390690088 CET	53	61946	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:03.398386955 CET	64910	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:03.458482981 CET	53	64910	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:03.470156908 CET	52123	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:03.472902060 CET	56130	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:03.516357899 CET	56338	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:03.518938065 CET	53	52123	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:03.521265984 CET	59420	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:03.524524927 CET	53	56130	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:03.535957098 CET	58784	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:03.542375088 CET	63978	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:03.546838045 CET	62938	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:03.552351952 CET	55708	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:03.567996025 CET	56803	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:03.575637102 CET	53	56338	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:03.579490900 CET	53	59420	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:03.595623016 CET	53	62938	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:03.601191044 CET	53	55708	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:03.601479053 CET	53	58784	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:03.612790108 CET	53	63978	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:03.616615057 CET	53	56803	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:04.324681044 CET	57145	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 18:59:04.328723907 CET	55359	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:04.328783035 CET	58306	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:04.378637075 CET	53	55359	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:04.381496906 CET	53	58306	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:04.409466028 CET	53	57145	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:04.473520994 CET	64124	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:04.522017956 CET	53	64124	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:05.230231047 CET	49361	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:05.281738043 CET	53	49361	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:06.186604023 CET	63150	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:06.244479895 CET	53	63150	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:07.365406990 CET	53279	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:07.419687986 CET	53	53279	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:16.279510021 CET	56881	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:16.339392900 CET	53	56881	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:25.719324112 CET	53642	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:25.772293091 CET	53	53642	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:26.496751070 CET	55667	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:26.545602083 CET	53	55667	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:26.726567984 CET	53642	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:26.778280020 CET	53	53642	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:27.515712976 CET	55667	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:27.574959993 CET	53	55667	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:27.743431091 CET	53642	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:27.795166969 CET	53	53642	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:29.907969952 CET	55667	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:29.956547022 CET	53	55667	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:29.974750996 CET	53642	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:30.026310921 CET	53	53642	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:31.498214006 CET	54833	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:31.560173988 CET	53	54833	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:31.648658991 CET	62476	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:31.700278044 CET	53	62476	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:31.917212963 CET	55667	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:31.966511011 CET	53	55667	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:32.873087883 CET	49705	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:32.923706055 CET	53	49705	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:33.886805058 CET	61477	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:33.984925985 CET	53642	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:34.036432981 CET	53	53642	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:34.113610983 CET	53	61477	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:34.159913063 CET	61633	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:34.208672047 CET	53	61633	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:35.919624090 CET	55667	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:35.969178915 CET	53	55667	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:37.766433954 CET	55949	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:37.818212032 CET	53	55949	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:38.130240917 CET	57601	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:38.179069996 CET	53	57601	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:38.845021963 CET	49342	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:38.897367001 CET	53	49342	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:40.585912943 CET	56253	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:40.637614965 CET	53	56253	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:42.591445923 CET	49667	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:42.641465902 CET	53	49667	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:43.768176079 CET	55439	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:43.825344086 CET	53	55439	8.8.8.8	192.168.2.3
Feb 22, 2021 18:59:47.421511889 CET	57069	53	192.168.2.3	8.8.8.8
Feb 22, 2021 18:59:47.482974052 CET	53	57069	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 18:58:56.922090054 CET	192.168.2.3	8.8.8.8	0xae98	Standard query (0)	storangego ogleapiddp .agilecrm.com	A (IP address)	IN (0x0001)
Feb 22, 2021 18:58:58.162075043 CET	192.168.2.3	8.8.8.8	0x2976	Standard query (0)	doxhze3l6s 7v9.cloudfront.net	A (IP address)	IN (0x0001)
Feb 22, 2021 18:58:58.297306061 CET	192.168.2.3	8.8.8.8	0x7964	Standard query (0)	cdnjs.clou dflare.com	A (IP address)	IN (0x0001)
Feb 22, 2021 18:58:58.322890043 CET	192.168.2.3	8.8.8.8	0xed55	Standard query (0)	d1gwclp1pm zk26.cloud front.net	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:00.717005014 CET	192.168.2.3	8.8.8.8	0x6202	Standard query (0)	cdn.jsdelivr.net	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:00.799118042 CET	192.168.2.3	8.8.8.8	0x41db	Standard query (0)	static.ads-twitter.com	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:00.809169054 CET	192.168.2.3	8.8.8.8	0x22bf	Standard query (0)	s.adroll.com	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:00.829771996 CET	192.168.2.3	8.8.8.8	0x24a7	Standard query (0)	www.clickc ease.com	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:00.895327091 CET	192.168.2.3	8.8.8.8	0xaa52	Standard query (0)	stats2.agi lecrm.com	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:00.903312922 CET	192.168.2.3	8.8.8.8	0xf01e	Standard query (0)	s3.amazona ws.com	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:02.051567078 CET	192.168.2.3	8.8.8.8	0xb2c6	Standard query (0)	googleads. g.doubleclick.net	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:02.061393976 CET	192.168.2.3	8.8.8.8	0xb27d	Standard query (0)	d.adroll.m gr.consensu.org	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:02.153537035 CET	192.168.2.3	8.8.8.8	0xa85d	Standard query (0)	our.agilecrm.com	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:02.376311064 CET	192.168.2.3	8.8.8.8	0xdd40	Standard query (0)	d.adroll.com	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:02.448631048 CET	192.168.2.3	8.8.8.8	0x6432	Standard query (0)	analytics. twitter.com	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:02.452238083 CET	192.168.2.3	8.8.8.8	0xb6e2	Standard query (0)	t.co	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:02.460340977 CET	192.168.2.3	8.8.8.8	0xed45	Standard query (0)	www.google .co.uk	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:02.501542091 CET	192.168.2.3	8.8.8.8	0xa983	Standard query (0)	stats.g.do ubleclick.net	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.325958967 CET	192.168.2.3	8.8.8.8	0x3a2c	Standard query (0)	connect.fa cebook.net	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.398386955 CET	192.168.2.3	8.8.8.8	0x3eae	Standard query (0)	pixel.adve rtising.com	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.470156908 CET	192.168.2.3	8.8.8.8	0x6a68	Standard query (0)	sync.outbr ain.com	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.472902060 CET	192.168.2.3	8.8.8.8	0xb590	Standard query (0)	simage2.pu bmatic.com	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.516357899 CET	192.168.2.3	8.8.8.8	0x4c0f	Standard query (0)	idsync.rlcdn.com	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.521265984 CET	192.168.2.3	8.8.8.8	0xc914	Standard query (0)	dsum-sec.c asalemedia.com	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.535957098 CET	192.168.2.3	8.8.8.8	0xabec	Standard query (0)	cm.g.doubl eclick.net	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.542375088 CET	192.168.2.3	8.8.8.8	0x43e1	Standard query (0)	pixel.rubi conproject.com	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.546838045 CET	192.168.2.3	8.8.8.8	0x78be	Standard query (0)	us-u.openx.net	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.552351952 CET	192.168.2.3	8.8.8.8	0x9ac8	Standard query (0)	x.bidswitch.net	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.567996025 CET	192.168.2.3	8.8.8.8	0x75bb	Standard query (0)	eb2.3lift.com	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:04.324681044 CET	192.168.2.3	8.8.8.8	0x7965	Standard query (0)	sync.taboola.com	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:04.328723907 CET	192.168.2.3	8.8.8.8	0xec11	Standard query (0)	ib.adnxs.com	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:04.328783035 CET	192.168.2.3	8.8.8.8	0xed72	Standard query (0)	ads.yahoo.com	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:04.473520994 CET	192.168.2.3	8.8.8.8	0x8fc8	Standard query (0)	ups.analyt ics.yahoo.com	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:16.279510021 CET	192.168.2.3	8.8.8.8	0x22c6	Standard query (0)	storangego ogleapiddp .agilecrm.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 18:58:56.992753983 CET	8.8.8.8	192.168.2.3	0xae98	No error (0)	storangegoogleapiddp.agilecrm.com	ghs.googlehosted.com		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:58:56.992753983 CET	8.8.8.8	192.168.2.3	0xae98	No error (0)	ghs.googlehosted.com		142.250.185.179	A (IP address)	IN (0x0001)
Feb 22, 2021 18:58:58.223371029 CET	8.8.8.8	192.168.2.3	0x2976	No error (0)	doxhze3l6s7v9.cloudfront.net		13.226.175.122	A (IP address)	IN (0x0001)
Feb 22, 2021 18:58:58.223371029 CET	8.8.8.8	192.168.2.3	0x2976	No error (0)	doxhze3l6s7v9.cloudfront.net		13.226.175.94	A (IP address)	IN (0x0001)
Feb 22, 2021 18:58:58.223371029 CET	8.8.8.8	192.168.2.3	0x2976	No error (0)	doxhze3l6s7v9.cloudfront.net		13.226.175.204	A (IP address)	IN (0x0001)
Feb 22, 2021 18:58:58.223371029 CET	8.8.8.8	192.168.2.3	0x2976	No error (0)	doxhze3l6s7v9.cloudfront.net		13.226.175.101	A (IP address)	IN (0x0001)
Feb 22, 2021 18:58:58.346033096 CET	8.8.8.8	192.168.2.3	0x7964	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Feb 22, 2021 18:58:58.346033096 CET	8.8.8.8	192.168.2.3	0x7964	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Feb 22, 2021 18:58:58.385093927 CET	8.8.8.8	192.168.2.3	0xed55	No error (0)	d1gwclp1pmzk26.cloudfront.net		99.86.162.148	A (IP address)	IN (0x0001)
Feb 22, 2021 18:58:58.385093927 CET	8.8.8.8	192.168.2.3	0xed55	No error (0)	d1gwclp1pmzk26.cloudfront.net		99.86.162.151	A (IP address)	IN (0x0001)
Feb 22, 2021 18:58:58.385093927 CET	8.8.8.8	192.168.2.3	0xed55	No error (0)	d1gwclp1pmzk26.cloudfront.net		99.86.162.127	A (IP address)	IN (0x0001)
Feb 22, 2021 18:58:58.385093927 CET	8.8.8.8	192.168.2.3	0xed55	No error (0)	d1gwclp1pmzk26.cloudfront.net		99.86.162.221	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:00.765552044 CET	8.8.8.8	192.168.2.3	0x6202	No error (0)	cdn.jsdelivr.net	dualstack.f3.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:59:00.848042965 CET	8.8.8.8	192.168.2.3	0x41db	No error (0)	static.ads-twitter.com	platform.twitter.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:59:00.848042965 CET	8.8.8.8	192.168.2.3	0x41db	No error (0)	platform.twitter.map.fastly.net		151.101.12.157	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:00.860475063 CET	8.8.8.8	192.168.2.3	0xcc74	No error (0)	pagead.l.doubleclick.net		172.217.16.130	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:00.870234013 CET	8.8.8.8	192.168.2.3	0x22bf	No error (0)	s.adroll.com	wildcard.adroll.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:59:00.888385057 CET	8.8.8.8	192.168.2.3	0x24a7	No error (0)	www.clickcease.com	www.clickcease.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:59:00.951878071 CET	8.8.8.8	192.168.2.3	0xf01e	No error (0)	s3.amazonaws.com		52.216.76.206	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:00.975912094 CET	8.8.8.8	192.168.2.3	0xaa52	No error (0)	stats2.agilecrm.com	ghs.googlehosted.com		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:59:00.975912094 CET	8.8.8.8	192.168.2.3	0xaa52	No error (0)	ghs.googlehosted.com		142.250.185.179	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:02.110115051 CET	8.8.8.8	192.168.2.3	0xb27d	No error (0)	d.adroll.mgr.consensu.org	d.adroll.com		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:59:02.110115051 CET	8.8.8.8	192.168.2.3	0xb27d	No error (0)	d.adroll.com	adserver-vpc-alb-1-1446435489.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:59:02.110115051 CET	8.8.8.8	192.168.2.3	0xb27d	No error (0)	adserver-vpc-alb-1-1446435489.eu-west-1.elb.amazonaws.com		54.246.184.51	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 18:59:02.110115051 CET	8.8.8.8	192.168.2.3	0xb27d	No error (0)	adserver-vpc-alb-1-1446435489.eu-west-1.elb.amazonaws.com		54.78.251.22	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:02.119381905 CET	8.8.8.8	192.168.2.3	0xb2c6	No error (0)	googleads.g.doubleclick.net	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:59:02.119381905 CET	8.8.8.8	192.168.2.3	0xb2c6	No error (0)	pagead46.l.doubleclick.net		172.217.23.98	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:02.223258018 CET	8.8.8.8	192.168.2.3	0xa85d	No error (0)	our.agilecrm.com	ghs.googlehosted.com		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:59:02.223258018 CET	8.8.8.8	192.168.2.3	0xa85d	No error (0)	ghs.googlehosted.com		142.250.185.179	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:02.436624050 CET	8.8.8.8	192.168.2.3	0xdd40	No error (0)	d.adroll.com	adserver-vpc-alb-3-890571764.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:59:02.436624050 CET	8.8.8.8	192.168.2.3	0xdd40	No error (0)	adserver-vpc-alb-3-890571764.eu-west-1.elb.amazonaws.com		52.209.227.220	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:02.436624050 CET	8.8.8.8	192.168.2.3	0xdd40	No error (0)	adserver-vpc-alb-3-890571764.eu-west-1.elb.amazonaws.com		3.248.28.111	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:02.500215054 CET	8.8.8.8	192.168.2.3	0x6432	No error (0)	analytics.twitter.com	ads.twitter.com		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:59:02.500215054 CET	8.8.8.8	192.168.2.3	0x6432	No error (0)	ads.twitter.com	s.twitter.com		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:59:02.500215054 CET	8.8.8.8	192.168.2.3	0x6432	No error (0)	s.twitter.com		104.244.42.131	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:02.500215054 CET	8.8.8.8	192.168.2.3	0x6432	No error (0)	s.twitter.com		104.244.42.195	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:02.500215054 CET	8.8.8.8	192.168.2.3	0x6432	No error (0)	s.twitter.com		104.244.42.3	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:02.500215054 CET	8.8.8.8	192.168.2.3	0x6432	No error (0)	s.twitter.com		104.244.42.67	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:02.503703117 CET	8.8.8.8	192.168.2.3	0xb6e2	No error (0)	t.co		104.244.42.69	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:02.503703117 CET	8.8.8.8	192.168.2.3	0xb6e2	No error (0)	t.co		104.244.42.5	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:02.503703117 CET	8.8.8.8	192.168.2.3	0xb6e2	No error (0)	t.co		104.244.42.197	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:02.503703117 CET	8.8.8.8	192.168.2.3	0xb6e2	No error (0)	t.co		104.244.42.133	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:02.525234938 CET	8.8.8.8	192.168.2.3	0xed45	No error (0)	www.google.co.uk		142.250.186.35	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:02.550132036 CET	8.8.8.8	192.168.2.3	0xa983	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:59:02.550132036 CET	8.8.8.8	192.168.2.3	0xa983	No error (0)	stats.l.doubleclick.net		173.194.76.155	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:02.550132036 CET	8.8.8.8	192.168.2.3	0xa983	No error (0)	stats.l.doubleclick.net		173.194.76.157	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:02.550132036 CET	8.8.8.8	192.168.2.3	0xa983	No error (0)	stats.l.doubleclick.net		173.194.76.156	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 18:59:02.550132036 CET	8.8.8.8	192.168.2.3	0xa983	No error (0)	stats.l.doubleclick.net		173.194.76.154	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.390690088 CET	8.8.8.8	192.168.2.3	0x3a2c	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:59:03.390690088 CET	8.8.8.8	192.168.2.3	0x3a2c	No error (0)	scontent.xx.fbcdn.net		31.13.92.14	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.458482981 CET	8.8.8.8	192.168.2.3	0x3eae	No error (0)	pixel.advertising.com	prod.ups-adcom.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:59:03.458482981 CET	8.8.8.8	192.168.2.3	0x3eae	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)
Feb 22, 2021 18:59:03.458482981 CET	8.8.8.8	192.168.2.3	0x3eae	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		3.126.63.176	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.458482981 CET	8.8.8.8	192.168.2.3	0x3eae	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		52.59.102.119	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.458482981 CET	8.8.8.8	192.168.2.3	0x3eae	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		35.156.106.231	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.458482981 CET	8.8.8.8	192.168.2.3	0x3eae	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		52.57.10.248	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.458482981 CET	8.8.8.8	192.168.2.3	0x3eae	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		52.59.28.101	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.458482981 CET	8.8.8.8	192.168.2.3	0x3eae	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		35.156.153.71	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.458482981 CET	8.8.8.8	192.168.2.3	0x3eae	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		52.28.254.214	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.458482981 CET	8.8.8.8	192.168.2.3	0x3eae	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		52.28.239.147	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.518938065 CET	8.8.8.8	192.168.2.3	0x6a68	No error (0)	sync.outbrain.com	alldcs.outbrain.org		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:59:03.518938065 CET	8.8.8.8	192.168.2.3	0x6a68	No error (0)	alldcs.outbrain.org	nydc1.outbrain.org		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:59:03.518938065 CET	8.8.8.8	192.168.2.3	0x6a68	No error (0)	nydc1.outbrain.org		64.202.112.127	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.524524927 CET	8.8.8.8	192.168.2.3	0xb590	No error (0)	simage2.pubmatic.com	pug-lhrc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:59:03.524524927 CET	8.8.8.8	192.168.2.3	0xb590	No error (0)	pug-lhrc.pubmatic.com	pug-lhr.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:59:03.524524927 CET	8.8.8.8	192.168.2.3	0xb590	No error (0)	pug-lhr.pubmatic.com		185.64.190.80	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.575637102 CET	8.8.8.8	192.168.2.3	0x4c0f	No error (0)	idsync.rlcdn.com		34.120.207.148	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.579490900 CET	8.8.8.8	192.168.2.3	0xc914	No error (0)	dsum-sec.casalemedia.com	dsum-sec.casalemedia.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:59:03.595623016 CET	8.8.8.8	192.168.2.3	0x78be	No error (0)	us-u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.595623016 CET	8.8.8.8	192.168.2.3	0x78be	No error (0)	us-u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 18:59:03.601191044 CET	8.8.8.8	192.168.2.3	0x9ac8	No error (0)	x.bidswitch.net	alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:59:03.601191044 CET	8.8.8.8	192.168.2.3	0x9ac8	No error (0)	alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com		54.93.211.166	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.601191044 CET	8.8.8.8	192.168.2.3	0x9ac8	No error (0)	alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com		35.157.168.25	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.601191044 CET	8.8.8.8	192.168.2.3	0x9ac8	No error (0)	alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com		52.28.82.26	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.601191044 CET	8.8.8.8	192.168.2.3	0x9ac8	No error (0)	alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com		52.57.167.187	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.601191044 CET	8.8.8.8	192.168.2.3	0x9ac8	No error (0)	alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com		52.57.47.211	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.601191044 CET	8.8.8.8	192.168.2.3	0x9ac8	No error (0)	alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com		18.194.12.4	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.601191044 CET	8.8.8.8	192.168.2.3	0x9ac8	No error (0)	alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com		52.59.128.17	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.601191044 CET	8.8.8.8	192.168.2.3	0x9ac8	No error (0)	alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com		35.158.9.168	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.601479053 CET	8.8.8.8	192.168.2.3	0xabec	No error (0)	cm.g.doubleclick.net	pagead.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:59:03.601479053 CET	8.8.8.8	192.168.2.3	0xabec	No error (0)	pagead.l.doubleclick.net		142.250.74.194	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.612790108 CET	8.8.8.8	192.168.2.3	0x43e1	No error (0)	pixel.rubiconproject.com	pixel.rubiconproject.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:59:03.616615057 CET	8.8.8.8	192.168.2.3	0x75bb	No error (0)	eb2.3lift.com	eu-eb2.3lift.com		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:59:03.616615057 CET	8.8.8.8	192.168.2.3	0x75bb	No error (0)	eu-eb2.3lift.com	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:59:03.616615057 CET	8.8.8.8	192.168.2.3	0x75bb	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		18.158.74.203	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.616615057 CET	8.8.8.8	192.168.2.3	0x75bb	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		35.156.37.164	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.616615057 CET	8.8.8.8	192.168.2.3	0x75bb	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		52.57.162.23	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 18:59:03.616615057 CET	8.8.8.8	192.168.2.3	0x75bb	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		18.184.39.197	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.616615057 CET	8.8.8.8	192.168.2.3	0x75bb	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		52.57.49.235	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.616615057 CET	8.8.8.8	192.168.2.3	0x75bb	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		18.185.82.201	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.616615057 CET	8.8.8.8	192.168.2.3	0x75bb	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		18.157.239.120	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:03.616615057 CET	8.8.8.8	192.168.2.3	0x75bb	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		18.195.223.167	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:04.378637075 CET	8.8.8.8	192.168.2.3	0xec11	No error (0)	ib.adnxs.com	g.geogslb.com		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:59:04.378637075 CET	8.8.8.8	192.168.2.3	0xec11	No error (0)	g.geogslb.com	ib.anycast.adnxs.com		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:59:04.378637075 CET	8.8.8.8	192.168.2.3	0xec11	No error (0)	ib.anycast.adnxs.com		37.252.172.45	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:04.378637075 CET	8.8.8.8	192.168.2.3	0xec11	No error (0)	ib.anycast.adnxs.com		37.252.173.38	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:04.378637075 CET	8.8.8.8	192.168.2.3	0xec11	No error (0)	ib.anycast.adnxs.com		37.252.172.37	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:04.378637075 CET	8.8.8.8	192.168.2.3	0xec11	No error (0)	ib.anycast.adnxs.com		37.252.172.36	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:04.378637075 CET	8.8.8.8	192.168.2.3	0xec11	No error (0)	ib.anycast.adnxs.com		37.252.172.249	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:04.378637075 CET	8.8.8.8	192.168.2.3	0xec11	No error (0)	ib.anycast.adnxs.com		37.252.173.22	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:04.378637075 CET	8.8.8.8	192.168.2.3	0xec11	No error (0)	ib.anycast.adnxs.com		37.252.172.38	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:04.378637075 CET	8.8.8.8	192.168.2.3	0xec11	No error (0)	ib.anycast.adnxs.com		37.252.172.250	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:04.381496906 CET	8.8.8.8	192.168.2.3	0xed72	No error (0)	ads.yahoo.com	edge.gycpi.b.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:59:04.381496906 CET	8.8.8.8	192.168.2.3	0xed72	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.22	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:04.381496906 CET	8.8.8.8	192.168.2.3	0xed72	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.23	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:04.409466028 CET	8.8.8.8	192.168.2.3	0x7965	No error (0)	sync.taboola.com	am-sync.taboola.com		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:59:04.409466028 CET	8.8.8.8	192.168.2.3	0x7965	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
Feb 22, 2021 18:59:04.409466028 CET	8.8.8.8	192.168.2.3	0x7965	No error (0)	am-vip001.taboola.com		141.226.228.48	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:04.522017956 CET	8.8.8.8	192.168.2.3	0x8fc8	No error (0)	ups.analytics.yahoo.com	prod.ups-ats.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:59:04.522017956 CET	8.8.8.8	192.168.2.3	0x8fc8	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)
Feb 22, 2021 18:59:04.522017956 CET	8.8.8.8	192.168.2.3	0x8fc8	No error (0)	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud		18.156.0.31	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:04.522017956 CET	8.8.8.8	192.168.2.3	0x8fc8	No error (0)	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud		3.126.56.137	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:16.339392900 CET	8.8.8.8	192.168.2.3	0x22c6	No error (0)	storangegoogleapiddp.agilecrm.com	ghs.googlehosted.com		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 18:59:16.339392900 CET	8.8.8.8	192.168.2.3	0x22c6	No error (0)	ghs.googlehosted.com		142.250.185.179	A (IP address)	IN (0x0001)
Feb 22, 2021 18:59:34.113610983 CET	8.8.8.8	192.168.2.3	0x690a	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- storangegoogleapiddp.agilecrm.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49716	142.250.185.179	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 18:58:57.050656080 CET	1001	OUT	GET / HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: storangegoogleapiddp.agilecrm.com Connection: Keep-Alive
Feb 22, 2021 18:58:57.215784073 CET	1002	IN	HTTP/1.1 302 Found Location: https://storangegoogleapiddp.agilecrm.com/ X-Cloud-Trace-Context: 85dac3716f9219ee681faa28864d1c2b Date: Mon, 22 Feb 2021 17:58:57 GMT Content-Type: text/html Server: Google Frontend Content-Length: 0

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 22, 2021 18:58:57.336841106 CET	142.250.185.179	443	192.168.2.3	49718	CN=*.agilecrm.com CN=RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Oct 29 01:00:00 CET 2020	Tue Nov 30 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
							Thu Jul 16 14:25:27 CEST 2020	Thu Jun 01 01:59:59 CEST 2023		
							Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 16 14:25:27 CEST 2020	Thu Jun 01 01:59:59 CEST 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Feb 22, 2021 18:58:58.423819065 CET	13.226.175.122	443	192.168.2.3	49721	CN=*.cloudfront.net, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Tue May 26 02:00:00 CEST 2020 Thu Aug 01 14:00:00 CEST 2013 Mon Nov 06 01:00:00 CET 2017	Wed Apr 21 14:00:00 CEST 2021 Tue Aug 01 14:00:00 CEST 2028 Sun Nov 06 00:59:59 CET 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert Global CA G2, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 3948 Parent PID: 792

General

Start time:	18:58:54
Start date:	22/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7acfa0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 5500 Parent PID: 3948

General

Start time:	18:58:55
Start date:	22/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3948 CREDAT:17410 /prefetch:2
Imagebase:	0x820000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly

Copyright null 2021