ID: 384832
Cookbook: browseurl.jbs
Time: 22:12:57
Date: 09/04/2021
Version: 31.0.0 Emerald

Table of Contents

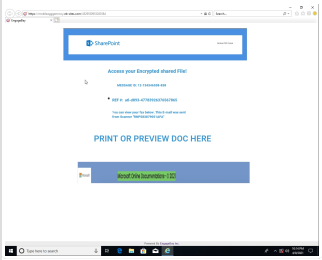
Analysis Report https://mobileagggennncy.eb-sites.com…

Overview

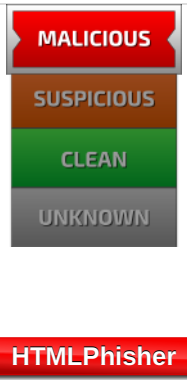
General Information

Sample URL:	http://https://mobileagggennncy.eb-sites.com/4529550953283584
Analysis ID:	384832
Infos:	

Most interesting Screenshot:



Detection



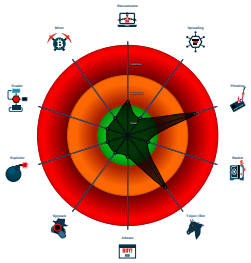
HTMLPhisher

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

Signatures

- Antivirus detection for URL or domain
- Yara detected HtmlPhish10
- Performs DNS queries to domains w…
- Phishing site detected (based on log…
- Found iframes
- HTML body contains low number of …
- HTML title does not match URL
- Invalid T&C link found
- Suspicious form URL found

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 160 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 3160 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:160 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

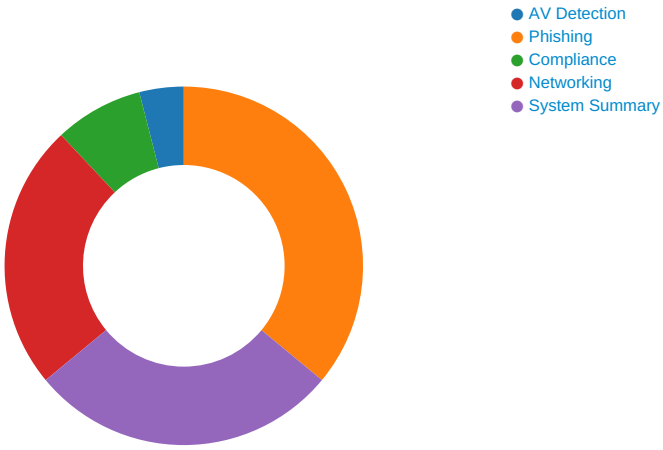
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\gim[1].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ZKSVK37S.htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Phishing:

Yara detected HtmlPhish10

Phishing site detected (based on logo template match)

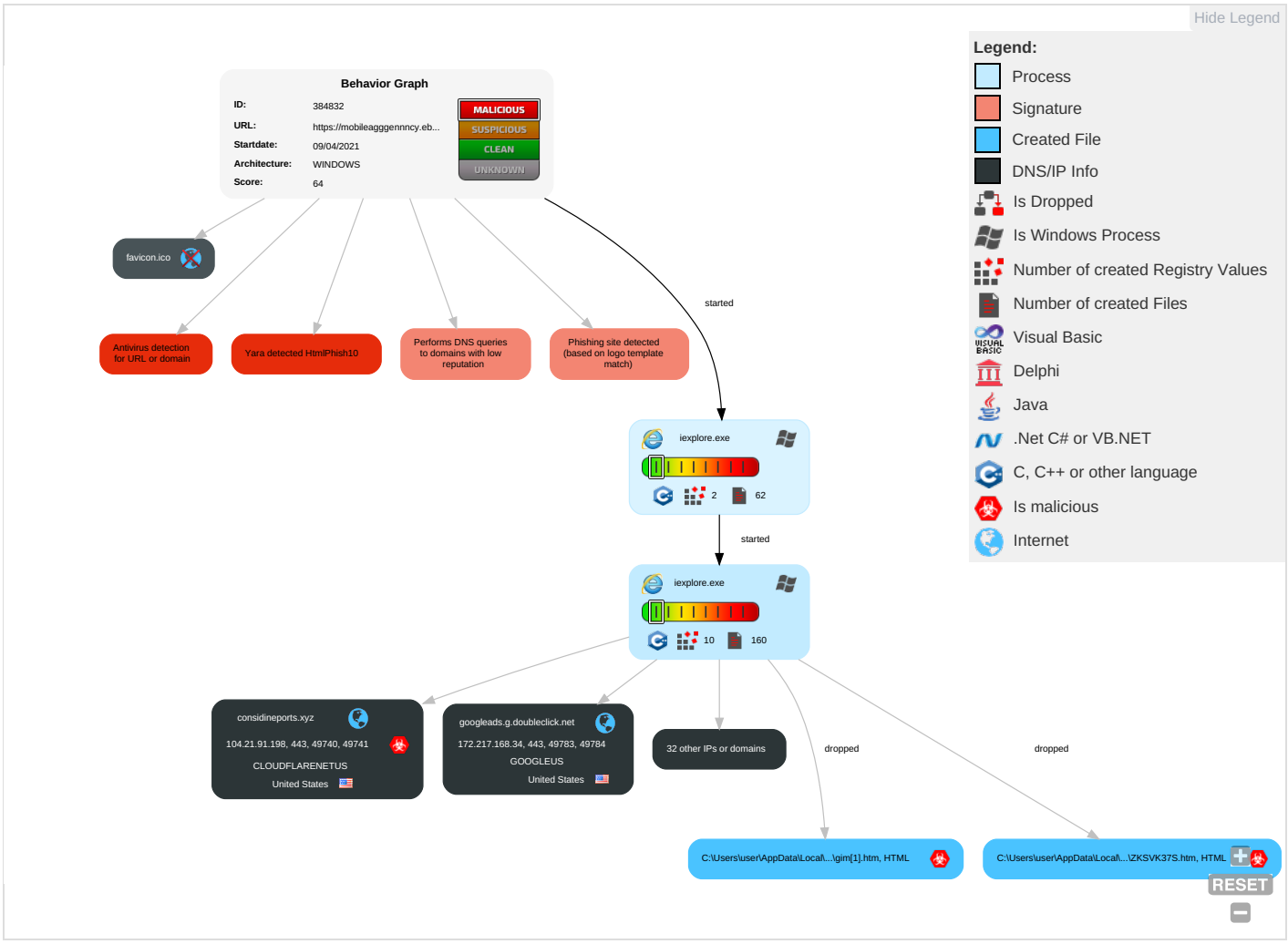
Networking:

Performs DNS queries to domains with low reputation

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 1	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 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups

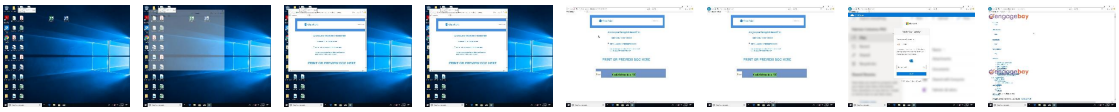
Behavior Graph

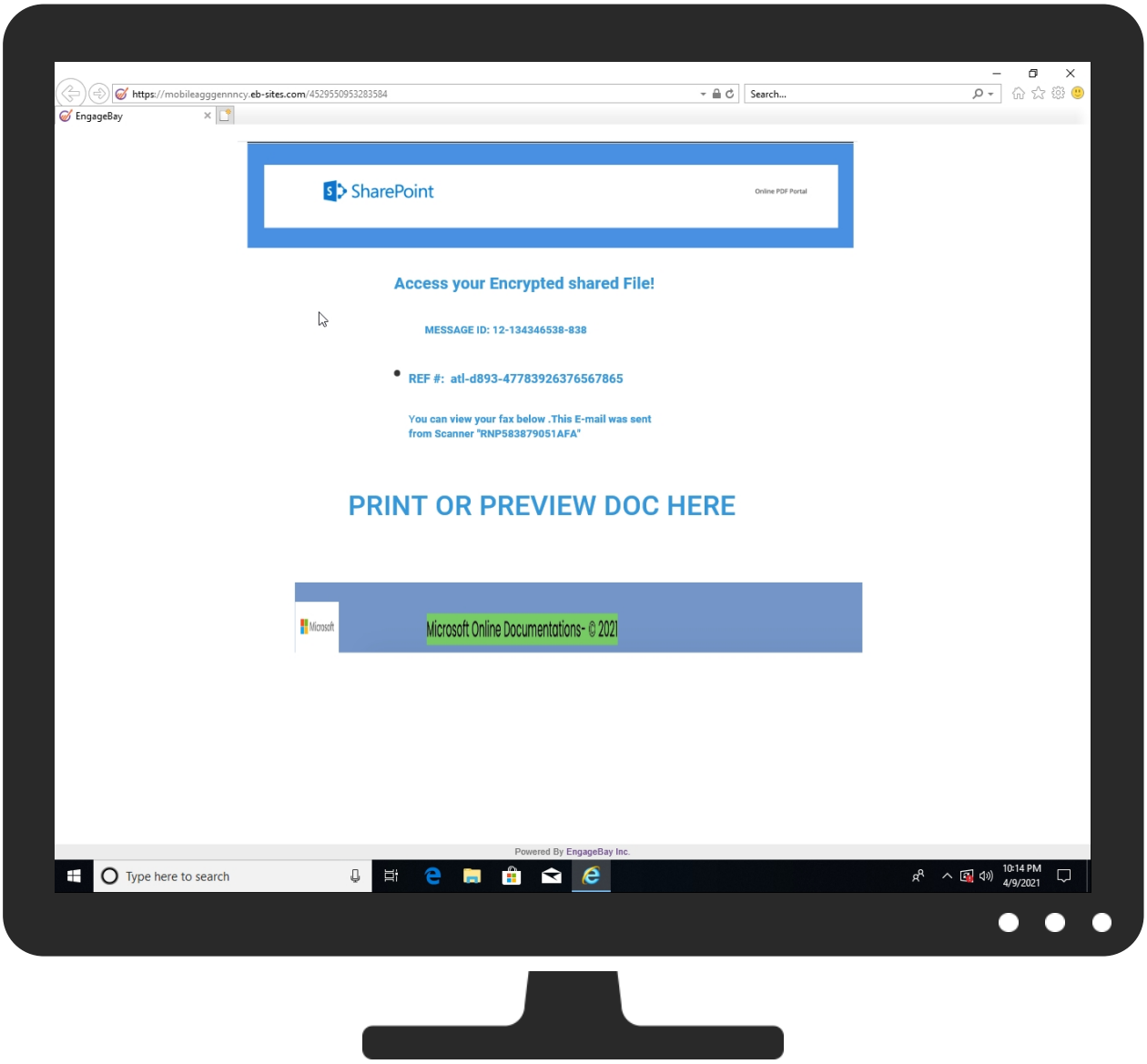


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://mobileagggennncy.eb-sites.com/4529550953283584	0%	Virustotal		Browse
http://https://mobileagggennncy.eb-sites.com/4529550953283584	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://considineports.xyz/gim/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Source	Detection	Scanner	Label	Link
http://https://www.engagebay.com/alternative-to-drip	0%	Avira URL Cloud	safe	
http://https://www.engagebay.com/blog/	0%	Avira URL Cloud	safe	
http://https://www.hotjarconsent.com/sv.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/sv.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/sv.html	0%	URL Reputation	safe	
http://https://cdn5.engagebay.com/img/products-menu/service.svg	0%	Avira URL Cloud	safe	
http://https://www.engagebay.com/infusionsoft-alternative	0%	Avira URL Cloud	safe	
http://https://www.engagebay.com/marketing/ecommerce-marketing-automation	0%	Avira URL Cloud	safe	
http://https://www.engagebay.com/solutions/real-estate-crm-marketing	0%	Avira URL Cloud	safe	
http://https://www.engagebay.com	0%	Avira URL Cloud	safe	
http://https://app.engagebay.com/signup	0%	Avira URL Cloud	safe	
http://https://www.engagebay.com/crm/predictive-lead-scoring	0%	Avira URL Cloud	safe	
http://https://www.engagebay.com/crm/crm-analytics	0%	Avira URL Cloud	safe	
http://https://www.engagebay.com/comparisons	0%	Avira URL Cloud	safe	
http://https://www.engagebay.com/integrations/mandrill-integration	0%	Avira URL Cloud	safe	
http://https://www.engagebay.com/alternative-to-aweber	0%	Avira URL Cloud	safe	
http://https://www.hotjarconsent.com/pl.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/pl.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/pl.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/fr.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/fr.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/fr.html	0%	URL Reputation	safe	
http://https://www.engagebay.com/new/import.php	0%	Avira URL Cloud	safe	
http://https://www.engagebay.com/crm/call-center-crm	0%	Avira URL Cloud	safe	
http://https://www.engagebay.com/marketing/video-marketing-templates	0%	Avira URL Cloud	safe	
http://https://www.engagebay.com/service/free-live-chat-software	0%	Avira URL Cloud	safe	
http://https://www.engagebay.com/crm/online-crm	0%	Avira URL Cloud	safe	
http://https://www.engagebay.com/?utm_source=eb-lps53283584	0%	Avira URL Cloud	safe	
http://https://www.hotjarconsent.com/el.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/el.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/el.html	0%	URL Reputation	safe	
http://https://www.engagebay.com/affiliate-program	0%	Avira URL Cloud	safe	
http://https://www.hotjarconsent.com/zh.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/zh.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/zh.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/fi.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/fi.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/fi.html	0%	URL Reputation	safe	
http://https://www.engagebay.com/integrations/zapier-integration	0%	Avira URL Cloud	safe	
http://https://www.engagebay.com/favicon.ico	0%	Avira URL Cloud	safe	
http://https://www.engagebay.com/integrations/xero-integration	0%	Avira URL Cloud	safe	
http://https://www.engagebay.com/crm/auto-dialer-software	0%	Avira URL Cloud	safe	
http://https://www.engagebay.com/crm/contact-management-software	0%	Avira URL Cloud	safe	
http://https://www.hotjarconsent.com/sq.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/sq.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/sq.html	0%	URL Reputation	safe	
http://https://mobileagggennncy.eb-sites.com/4529550953283584Root	0%	Avira URL Cloud	safe	
http://https://www.engagebay.com/	0%	Avira URL Cloud	safe	
http://https://www.hotjarconsent.com/it.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/it.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/it.html	0%	URL Reputation	safe	
http://daneden.me/animate	0%	URL Reputation	safe	
http://daneden.me/animate	0%	URL Reputation	safe	
http://daneden.me/animate	0%	URL Reputation	safe	
http://https://www.engagebay.com/marketing/push-notifications	0%	Avira URL Cloud	safe	
http://https://www.hotjarconsent.com	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com	0%	URL Reputation	safe	
http://https://www.engagebay.com/customer-journey-to-success	0%	Avira URL Cloud	safe	
http://https://mobileagges.com/4529550953283584	0%	Avira URL Cloud	safe	
http://https://www.engagebay.com/crm/b2b-crm	0%	Avira URL Cloud	safe	
http://https://www.engagebay.com/insightly-alternative	0%	Avira URL Cloud	safe	
http://https://www.hotjarconsent.com/pt_br.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/pt_br.html	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://www.hotjarconsent.com/pt_br.html	0%	URL Reputation	safe	
http://https://www.engagebay.com/marketing/email-templates	0%	Avira URL Cloud	safe	
http://https://cdn5.engagebay.com/img/products-menu/marketing.svg	0%	Avira URL Cloud	safe	
http://https://www.engagebay.com/affordable-hubspot-alternative	0%	Avira URL Cloud	safe	
http://https://www.engagebay.com/crm/sales-tracking-software	0%	Avira URL Cloud	safe	
http://https://www.engagebay.com/integrations	0%	Avira URL Cloud	safe	
http://https://www.engagebay.com/crm/crm-metrics	0%	Avira URL Cloud	safe	
http://https://www.engagebay.com/blog/all-in-one-marketing-suite-for-just-1-dollar-day/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
stackpath.bootstrapcdn.com	104.18.10.207	true	false		high
considineports.xyz	104.21.91.198	true	true		unknown
vc-live-cf.hotjar.io	13.32.25.78	true	false		unknown
stats.l.doubleclick.net	74.125.143.154	true	false		high
maxcdn.bootstrapcdn.com	104.18.10.207	true	false		high
mobileagggennncy.eb-sites.com	143.110.228.35	true	false		unknown
vars.hotjar.com	99.86.3.62	true	false		high
scontent.xx.fbcdn.net	157.240.17.15	true	false		high
snippet.growsumo.com	104.18.2.70	true	false		high
in-live.live.eks.hotjar.com	18.203.1.140	true	false		high
script.hotjar.com	13.32.25.17	true	false		high
googleads.g.doubleclick.net	172.217.168.34	true	false		high
cdnjs.cloudflare.com	104.16.18.94	true	false		high
d3w29h23ietttc.cloudfront.net	13.32.25.93	true	false		high
www.engagebay.com	18.236.57.96	true	false		unknown
d2p078bqz5urf7.cloudfront.net	13.35.253.54	true	false		high
cdn5.engagebay.com	13.32.25.22	true	false		unknown
tracking.g2crowd.com	104.18.26.190	true	false		high
www.google.ch	216.58.215.227	true	false		high
ghs.googlehosted.com	172.217.168.51	true	false		unknown
q.quora.com	3.230.50.184	true	false		high
static-cdn.hotjar.com	13.32.25.20	true	false		high
in.hotjar.com	unknown	unknown	false		high
favicon.ico	unknown	unknown	false		unknown
stats.g.doubleclick.net	unknown	unknown	false		high
vc.hotjar.io	unknown	unknown	false		unknown
cdn2.eb-pages.com	unknown	unknown	false		unknown
code.jquery.com	unknown	unknown	false		high
static.hotjar.com	unknown	unknown	false		high
platform.linkedin.com	unknown	unknown	false		high
www.linkedin.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
static-exp1.licdn.com	unknown	unknown	false		high
app.engagebay.com	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://mobileagggennncy.eb-sites.com/4529550953283584	true		unknown
http://https://www.engagebay.com/?utm_source=eb-lps	true		unknown

URLs from Memory and Binaries

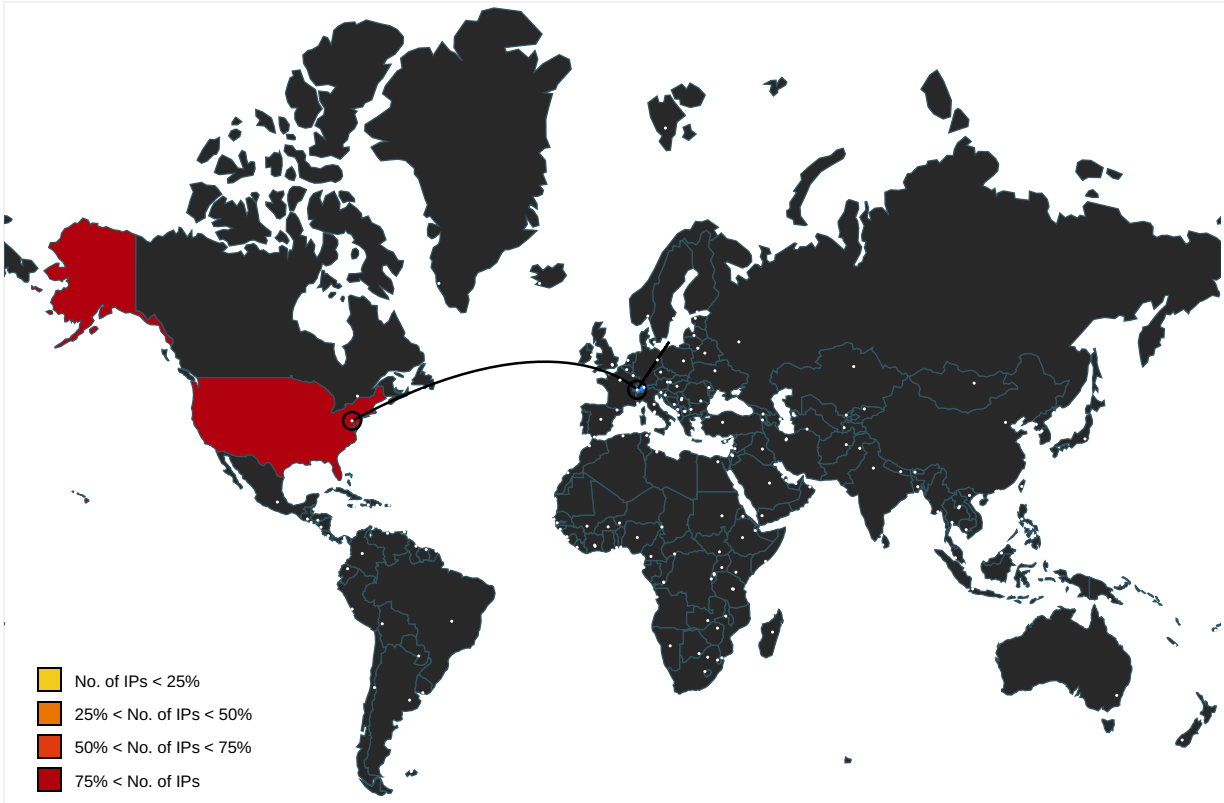
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/Modernizr/Modernizr/blob/master/modernizr.js	head[1].js.2.dr	false		high
http://https://in.linkedin.com/company/engagebay-inc	ZKSVK37S.htm.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.engagebay.com/alternative-to-drip	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://domain.com/file.js	head[1].js.2.dr	false		high
http://https://www.engagebay.com/blog/	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.hotjarconsent.com/sv.html	modules.d11c6f20b1e00021f55d[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.linkedin.com	in[1].js.2.dr	false		high
http://https://cdn5.engagebay.com/img/products-menu/service.svg	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.engagebay.com/infusionsoft-alternative	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://photoswipe.com	bundle.min[1].js.2.dr	false		high
http://https://code.jquery.com/jquery-3.2.1.slim.min.js	gim[1].htm.2.dr	false		high
http://https://www.linkedin.com/cws/member/public_profile	in[1].js.2.dr	false		high
http://www.zytrax.com/tech/web/mobile_ids.html	head[1].js.2.dr	false		high
http://https://zapier.com/apps/engagebay-marketing/integrations/quickbooks	ZKSVK37S.htm.2.dr	false		high
http://https://d2p078bqz5urf7.cloudfront.net/cloud/assets/img/featured-check.svg);	ZKSVK37S.htm.2.dr	false		high
http://https://github.com/headjs/headjs/issues/270	head[1].js.2.dr	false		high
http://https://www.linkedin.com/biz/api/recommendation/count?type=PDCT&id=	in[1].js.2.dr	false		high
http://https://www.engagebay.com/marketing/ecommerce-marketing-automation	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://q.quora.com/_/ad/	gtm[1].js.2.dr	false		high
http://https://www.engagebay.com/solutions/real-estate-crm-marketing	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://bugs.jquery.com/ticket/12282#comment:15	head[1].js.2.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.5.3/js/bootstrap.bundle.min.js	4529550953283584[1].htm.2.dr	false		high
http://https://github.com/twbs/bootstrap/graphs/contributors)	bootstrap.min[1].js.2.dr, bootstrap.bundle.min[1].js.2.dr	false		high
http://https://www.engagebay.com	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://scrollmagic.io	bundle.min[1].js.2.dr	false		high
http://https://app.engagebay.com/signup	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/cujojs/curl	head[1].js.2.dr	false		high
http://https://www.engagebay.com/?utm_source=eb-lps	4529550953283584[1].htm.2.dr, ~DF667DE1B8134EFA5C.TMP.1.dr	false		unknown
http://https://d2p078bqz5urf7.cloudfront.net/cloud/assets/img/logo/fav/ab-16x16.ico5:	imagestore.dat.2.dr	false		high
http://https://stats.g.doubleclick.net/j/collect	analytics[1].js.2.dr	false		high
http://https://www.engagebay.com/crm/predictive-lead-scoring	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js	gim[1].htm.2.dr	false		high
http://https://www.engagebay.com/crm/crm-analytics	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.linkedin.com/uas/oauth2/authorize	in[1].js.2.dr	false		high
http://https://www.engagebay.com/comparisons	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://d2p078bqz5urf7.cloudfront.net/cloud/landingpage-builder/page/page.css?84-9.43432727340016823	4529550953283584[1].htm.2.dr	false		high
http://https://www.engagebay.com/integrations/mandrill-integration	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.engagebay.com/alternative-to-aweber	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.hotjarconsent.com/pl.html	modules.d11c6f20b1e00021f55d[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.hotjarconsent.com/fr.html	modules.d11c6f20b1e00021f55d[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zytrax.com/tech/web/browser_ids.htm	head[1].js.2.dr	false		high
http://https://www.engagebay.com/new/import.php	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.engagebay.com/crm/call-center-crm	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.idangero.us/swiper/	swiper.min[1].css.2.dr	false		high
http://https://www.engagebay.com/marketing/video-marketing-templates	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.engagebay.com/service/free-live-chat-software	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://platform.linkedin.com/xdoor/extensions/Login.js	in[1].js.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://schema.org	ZKSVK37S.htm.2.dr	false		high
http://https://www.engagebay.com/crm/online-crm	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://platform.linkedin.com/in.js	ZKSVK37S.htm.2.dr	false		high
http://https://www.engagebay.com/?utm_source=eb-lps53283584	~DF667DE1B8134EFA5C.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.hotjarconsent.com/el.html	modules.d11c6f20b1e00021f55d[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.linkedin.com/biz/	in[1].js.2.dr	false		high
http://https://www.engagebay.com/affiliate-program	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://d2p078bqz5urf7.cloudfront.net/cloud/landingpage-builder/page/bootstrap.min.css	4529550953283584[1].htm.2.dr	false		high
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	bootstrap.min[1].js.2.dr, bootstrap.min[1].css.2.dr	false		high
http://https://www.twitter.com/engagebay	ZKSVK37S.htm.2.dr	false		high
http://caniuse.com/#feat=css-gradients	head[1].js.2.dr	false		high
http://www.idangero.us/	swiper.min[1].css.2.dr	false		high
http://https://www.hotjarconsent.com/zh.html	modules.d11c6f20b1e00021f55d[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.hotjar.com	box-5e3cec51ed8e99df6977c199d27812d7[1].htm.2.dr	false		high
http://https://www.hotjarconsent.com/fi.html	modules.d11c6f20b1e00021f55d[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.engagebay.com/integrations/zapier-integration	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.engagebay.com/favicon.ico	imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.engagebay.com/integrations/xero-integration	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://d2p078bqz5urf7.cloudfront.net/jsapi	ehform[1].js.2.dr	false		high
http://https://api.linkedin.com/xdoor/widgets/api/proxy.html	in[1].js.2.dr	false		high
http://https://www.linkedin.com/cws/share	in[1].js.2.dr	false		high
http://https://www.linkedin.com/cws/cap/recruiter_member	in[1].js.2.dr	false		high
http://https://www.engagebay.com/crm/auto-dialer-software	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://d2p078bqz5urf7.cloudfront.net/cloud/prod/assets/lib/font-family/roboto.css	4529550953283584[1].htm.2.dr	false		high
http://https://www.engagebay.com/crm/contact-management-software	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.hotjarconsent.com/sq.html	modules.d11c6f20b1e00021f55d[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://mobileagggennncy.eb-sites.com/4529550953283584Root	{87227E5C-99BB-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://platform.linkedin.com/xdoor/extensions/Wizard.js	in[1].js.2.dr	false		high
http://https://www.engagebay.com/	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.hotjarconsent.com/it.html	modules.d11c6f20b1e00021f55d[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://d2p078bqz5urf7.cloudfront.net/cloud/landingpage-builder/page/page-actions.js?=84-9.434327273	4529550953283584[1].htm.2.dr	false		high
http://daneden.me/animate	animate[1].css.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.engagebay.com/marketing/push-notifications	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.hotjarconsent.com	modules.d11c6f20b1e00021f55d[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.engagebay.com/customer-journey-to-success	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://mobileagges.com/4529550953283584	{87227E5C-99BB-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.engagebay.com/crm/b2b-crm	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.linkedin.com/cws/sfdc/company	in[1].js.2.dr	false		high
http://https://www.engagebay.com/insightly-alternative	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.hotjarconsent.com/pt_br.html	modules.d11c6f20b1e00021f55d[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.linkedin.com/cws/sfdc/signal	in[1].js.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.engagebay.com/marketing/email-templates	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn5.engagebay.com/img/products-menu/marketing.svg	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.engagebay.com/affordable-hubspot-alternative	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://github.com/cferdinandi/smooth-scroll	bundle.min[1].js.2.dr	false		high
http://https://www.engagebay.com/crm/sales-tracking-software	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://mobileagggennncy.eb-sites.com/4529550953283584	{87227E5C-99BB-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		unknown
http://https://www.engagebay.com/integrations	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://d2p078bqz5urf7.cloudfront.net/cloud/assets/livechat/chatfile.png	app[1].js.2.dr	false		high
http://https://www.engagebay.com/crm/crm-metrics	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.engagebay.com/blog/all-in-one-marketing-suite-for-just-1-dollar-day/	ZKSVK37S.htm.2.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.18.10.207	stackpath.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
18.203.1.140	in-live.live.eks.hotjar.com	United States		16509	AMAZON-02US	false
13.35.253.54	d2p078bqz5urf7.cloudfront.net	United States		16509	AMAZON-02US	false
143.110.228.35	mobileagggennncy.eb-sites.com	United States		30376	COLLEGE-OF-ST-SCHOLASTICAUS	false
3.230.50.184	q.quora.com	United States		14618	AMAZON-AESUS	false
18.236.57.96	www.engagebay.com	United States		16509	AMAZON-02US	false
157.240.17.15	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
99.86.3.62	vars.hotjar.com	United States		16509	AMAZON-02US	false
13.32.25.22	cdn5.engagebay.com	United States		7018	ATT-INTERNET4US	false
13.32.25.20	static-cdn.hotjar.com	United States		7018	ATT-INTERNET4US	false
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
74.125.143.154	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
104.18.26.190	tracking.g2crowd.com	United States		13335	CLOUDFLARENETUS	false
172.217.168.51	ghs.googlehosted.com	United States		15169	GOOGLEUS	false
104.18.2.70	snippet.growsumo.com	United States		13335	CLOUDFLARENETUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.32.25.17	script.hotjar.com	United States		7018	ATT-INTERNET4US	false
172.217.168.34	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
13.32.25.78	vc-live-cf.hotjar.io	United States		7018	ATT-INTERNET4US	false
104.21.91.198	considineports.xyz	United States		13335	CLOUDFLARENETUS	true
13.32.25.93	d3w29h23ietttc.cloudfront.net	United States		7018	ATT-INTERNET4US	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	384832
Start date:	09.04.2021
Start time:	22:12:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://mobileagggennncy.eb-sites.com/45295509 53283584
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:	6
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.phis.troj.win@3/128@27/21
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://considineports.xyz/gim/ • Browsing link: https://www.engagebay.com/?utm_source=eb-lps

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 13.64.90.137, 40.88.32.150, 2.18.101.230, 52.147.198.201, 172.217.168.10, 216.58.215.227, 69.16.175.42, 69.16.175.10, 216.58.215.234, 20.50.102.62, 23.10.249.35, 23.10.249.9, 95.100.54.203, 216.58.215.232, 172.217.168.78, 204.79.197.200, 13.107.21.200, 172.217.168.66, 13.107.42.14, 172.217.168.4, 152.199.19.161, 13.107.246.19, 13.107.213.19, 104.43.193.48, 13.88.21.125, 23.0.174.200, 23.0.174.185 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, cds.s5x3j6q5.hwcdn.net, arc.msn.com.nsatc.net, standard.t-0009.t-msedge.net, fs-wildcard.microsoft.com.edgekey.net, e11290.dspg.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, l-0005.l-msedge.net, audownload.windowsupdate.nsatc.net, www.google.com, watson.telemetry.microsoft.com, li-prod-static.azureedge.net, au-bg-shim.trafficmanager.net, www.google-analytics.com, fonts.googleapis.com, fs.microsoft.com, ajax.googleapis.com, dual-a-0001.a-msedge.net, od.linkedin.edgesuite.net, skypedataprdcolcus15.cloudapp.net, 2-01-2c3e-0055.cdx.cedexis.net, t-0009.t-msedge.net, blobcollector.events.data.trafficmanager.net, li-prod-static.afd.azureedge.net, a1916.dscg2.akamai.net, cs9.wpc.v0cdn.net, au.download.windowsupdate.com.edgesuite.net, www.googleadservices.com, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, 2-01-2c3e-003d.cdx.cedexis.net, iecvlist.microsoft.com, go.microsoft.com, www.googletagmanager.com, dual.t-0009.t-msedge.net, Edge-Prod-ZRH.ctrl.t-0009.t-msedge.net, bat.bing.com, arc.trafficmanager.net, prod.fs.microsoft.com.akadns.net, www-linkedin-com.l-0005.l-msedge.net, skypedataprdcolwus17.cloudapp.net, www-google-analytics.l.google.com, fonts.gstatic.com, ie9comview.vo.msecnd.net, www-googletagmanager.l.google.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, star-azureedge-prod.trafficmanager.net, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus17.cloudapp.net, bat-bing-com.a-0001.a-msedge.net, go.microsoft.com.edgekey.net, skypedataprdcolwus15.cloudapp.net • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\1WR86ORS\www.linkedin[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FE D
Malicious:	false
Reputation:	low
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\MWPL12YV\www.engagebay[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):	2126
Entropy (8bit):	5.068978223628608
Encrypted:	false
SSDEEP:	48:LoQK0PNQKo1Qxo1Q/KQQc4Qxo1Q/KQQc4Qxo1Q/KQQc4QcQLmPUuQxo1Q/KQQc45:UQfFQz1Qi1Q/KQQc4Qi1Q/KQQc4Qi1QU
MD5:	B9CCC8544E63B5926612791DF6CFCE9A
SHA1:	4D393853BFD170E292F906F3E73AA3CE91EDF0E3
SHA-256:	F4F8F0FBD4232AC555034AB799F12A0FBC186F6B32A5D67155E432B84FEC8F81
SHA-512:	77BD11799365E8A98942DFE5A10252FD7458B5DDDCB3CD71A627A1A258E89D37B5629AE7DAED8D373AB351F70F9182D370D9BAD5E1140375B1FF30A97B18DB D
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="modernizr" value="modernizr" ltime="1522151904" htime="30879176" /></root><root></root><root><item name="_hjLocalStorageTest" value="1" ltime="1525121904" htime="30879176" /></root><root></root><root><item name="_hjid" value="3d7edf08-c5b3-4181-88fc-66b584b84211" ltime="1525271904" htime="30879176" /></root><root><item name="_hjid" value="3d7edf08-c5b3-4181-88fc-66b584b84211" ltime="1525271904" htime="30879176" /><item name="_uetsid" value="9990314099bb11ebacf3ffb54ed96433" ltime="1531911904" htime="30879176" /><item name="_uetsid_exp" value="Sun, 11 Apr 2021 05:14:17 GMT" ltime="15 31911904" htime="30879176" /></root><root><item name="_hjid" value="3d7edf08-c5b3-4181-88fc-66b584b84211" ltime="1525271904" htime="30879176" /><item name="_uetsid" value="9990314099bb11ebacf3ffb54ed96433" ltime="1531911904" htime="30879176" /><item name="_uetsid_exp" value="Sun, 11 Apr 2021 05:14:17 GMT" ltime="1531911904" htime="30879176" /></root><root><item name="_hjid" val

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\SMFUI6ZJ\mobileagggennncy.eb-sites[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	146
Entropy (8bit):	5.05304897319283

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\SMFUI6ZJ\mobileagggennncy.eb-sites[1].xml	
Encrypted:	false
SSDEEP:	3:D90aK1ryRtFwstECAC6l0QAqLVbL26AvnS9kBX23uXyqIAqSQcLLFbaKb:JFK1rUFD6jAqwBokBXeuCqlQItb
MD5:	3C706366000D91CC89CB0E02842FDE8F
SHA1:	063C437ED9A8F8FD9C764EEEB061D0276C9DB116
SHA-256:	621D6E8106E9A758AE94F7BEA8F3D7056136B0E61591C7B0B0DD369A1057138F
SHA-512:	F1717610E75570A7506ABB90C35DE7515A8E7C108209447333083FD9DE51B97182B5E9D179DF83415E6FF72E279921422FFFB4A816A9481937CBF535FB0FB149
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="Engagehub_Data" value="{"app_visitor_id":5056178670272512}" ltime="1271521904" htime="30879176" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{87227E5A-99BB-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8593950797098568
Encrypted:	false
SSDEEP:	48:lwRGcprY7GwpL1G/ap81GIpcurCGvnZpvurZGo3qp9ur2Go4lpmurkGWBX9urdGW:rnZYVZR23WevtekfexlMeqeLetfeOcX
MD5:	1A2438D22B6C188282C630487A6CEFC6
SHA1:	45A77DA410C0BF4E989A234153E26D08E950111C
SHA-256:	B1BA53BC9571E69E0A78BA52D8408BBFB2AC1F44DFECC206705246418CE1DB45
SHA-512:	9228B7D8B5373084F2EC4F2151F91EB992406858F268004F474A510E8E338FEF46EC17E22316165F8D2128E9D8D2A148903F54ABB7B33A0BA1C8DCED14F57EB5
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\{87227E5C-99BB-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	53182
Entropy (8bit):	2.0813576018723943
Encrypted:	false
SSDEEP:	192:rhZFQ96rk+jx2RWwMUF1X1G1fDmb1msTjDGDMfQWyfxPPdmERdTRvJlNlCOi:rn6ow4gAFc1Q1fM1mg0v9Z4EX9JDlK
MD5:	1B779EC17B82CEAA5B770F833139D041
SHA1:	CE32CEECFD774F77B78D8562384AE73C2C6B184A
SHA-256:	80B1212C5E36091AA33EA85012EB08734D949068CC344AE0259BE489AE6FD9BD
SHA-512:	F5FD234025B3CCBBA7CC3442841B122086B76BCB86749FFEF2747F26182D71E2BB743A55A7FB30D8EF2EA92A0F12D4F53815DE374DCBDEFBF033C13166D480D 2
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\{87227E5D-99BB-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.565756869987779
Encrypted:	false
SSDEEP:	48:lwQGcprRGwpa4G4pQMGrapbSHGQpKhG7HpRNTGIpG:rUZLQo6KBSxAQTrA
MD5:	A90D494258E74A1E65A6056BCA7865AD
SHA1:	E79F18C26BDF8E89DFC9B36022CF62966BB290BA
SHA-256:	31D5746BB2B9E53A106F26312809F86A99D66601498C55C6C43202E9F8766187
SHA-512:	30CFB568950B535A0BE8061963FBBB1FA3BCD36C8AF5F938A2A03BEE376C44E7FBE38CEDDA19516A6BE1DA747DBA47D06E69176A40C5ADC656D0E0BB915C1 D1A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{87227E5D-99BB-11EB-90E4-ECF4BB862DED}.dat	
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):	310177
Entropy (8bit):	3.256841289416492
Encrypted:	false
SSDEEP:	1536:s7aVgWOWNM9FXh7lTixyAw4ncj8P8WZ9HNusdgGy8p1FF:s7aPOEM9FXh0xtwNjA8WZ9HNusNbFF
MD5:	873B2A441313D879DAA8B3E138259B94
SHA1:	941C4AE8F2D038B112B2B67D69322B3B6216BE9E
SHA-256:	D226C1E32E45B820D3297E7FFC87564D0C79E067DC39DBB691334C8778FD12B9
SHA-512:	DDCC617581FD456C719EBF3CC6F2E05A48596D87E3387E9DFDF5E10F632BEA157EA96CFC1EC7639DC6AC1E5D71B752D15716708D839C23D3A6EF0C9EA46BE8C
Malicious:	false
Reputation:	low
Preview:	L.h.t.t.p.s.:././.d.2.p.0.7.8.b.q.z.5.u.r.f.7...c.l.o.u.d.f.r.o.n.t...n.e.t./.c.l.o.u.d./.a.s.s.e.t.s./.i.m.g./.l.o.g.o./.f.a.v./.a.b.-.1.6.x.1.6...i.c.o.~..... .h.....(..... ....9h..9h..9h..9h`.8f..8e..9g..9h..9h:.9h..9h.....9h..9i..9hC.8f..9g.?{.|C...;o.9g.9h.9h..9h..9h..9h.....9h..9hL.9h..B..jK..E[.6b..=_.9g/.9h..9h.9h..9h..9h.....9h'.9h.:m.E[.1d..0d.?3c.3c..0d.A.....9hj.9h.9h..9h..9h.....9g..=t.RU.-f.B3c..3c.3c.B3c..3c..1d...*6..9h..9h.9h%.9h.....8f.~B..5b..3c.3c.^3c..3c.~3c.a3c..3c.....9gC.9h.9h].9h.....9h.;m.1d.3c..3c.W3c.3c..3c.S3c.3c..1d.^.7b..9h.9h..9h..9h..9h..9g.$i..3c..3c..3c.,3c..3c..3c.53c..3c..F[.=.8f..9h..9h..9h..9h.9h.....2c.23c.G3c..3c.=3c.o3c..3c.A3c..2d.~B.K.8eI.9g..9h..9h..9h.9h3.9h..9h.3c..3c..3c../e...q..2c.s3c..3c.mJ..NW.....9h4.9h..9h..9h..9h..9h.....5\.....eM..3c.3c..3c.L3c..3c...9h..9ha.9h.9h..9h>.9h..9h..9h..9h..9hu.8f.XS.@2c..3c..3c.#3c...9h..9h..9h]

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\256x256[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 256 x 256, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	2630
Entropy (8bit):	7.597751252234089
Encrypted:	false
SSDEEP:	48:0zcB/r6mLdc/DWX++MRZv55WJvXZOAiohK33cdJLwGpdqDiRM+Z:0zo/r0/6MRZ30PPhKHcdSGpoDQZ
MD5:	E39A5D5C5BA81573D6755E89968770B4
SHA1:	6F462A7FB46C204F57C064DFF2413919A6357D28
SHA-256:	966BD92374537A737014313DE6A759835C8FF3BFB8AA78B7AA9FE49A65A6775E
SHA-512:	DB1E92968EAA7B86D19CFB3365C0DCDBB1CAB9F155BFFD3809F7E151A3AFCA4113FE7C119C849550808A9F952EB22FDB2E80E231BAFFCDB98237FEE65EAAD75F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn5.engagebay.com/images/256x256.png
Preview:	.PNG.....IHDR.....k.XT....PLTEh9..Laj:..c4.N[.c3.c3h9...!i....tRNSh....`..kI....IDATx.... ..'.....$$H....T. * ].....e.....(/....u..eY....7.....W..".z.....O....%.B.....x.z>.|.....&.....O..%....-...D... .....<..|q..N.O. ].@^'.@DD....o.B.<...~...R....P...@ ..)/....(.n.....-.o."(d.0 ....R..A4...`.....m$.....;3..X..~...:....."...'.....]...3.6...8.=N..._s'.X.f..).N...F.....`.|...j..=...0.....g..y....P...(h....+....A....'2....C.....60.8...@.....I...w..I.....r 6..&..r.Q.A..9u.....m@*.....}... .`..M..S."+.=.F.R...L.Z&.....kT..zF.n. ..0.6..f...M.1..>5.._.@..y...g... . ..1./....P... ...H.....M.B..O.Z#N.>....L?;?.!...&.....>p6@.....(.....0..7|.7@....{..N@}.@:.....!....t...F.....z3.W.*...I..P..D-..~...1".....Li.q...!0y...0.....D.e.m..0J.....{.\../.|.`..v>.....`:..O.....f.O...0.~....._P..*....~.....@_.....;.\....j%.._..r...`.....h.....`.t.'....d..;..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\T1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 640 x 118, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	16150
Entropy (8bit):	7.9651870912045775
Encrypted:	false
SSDEEP:	384:Iq2RNypi1Q/JuL8YuNZfWD9P/2VXo9UOfdw/FxiZNN:12jypii/YIPuZP/2VXoqOfyzQNN
MD5:	BD65D4B80B616A5F477758A83D90E2B4
SHA1:	768A2B61D67572537E2BF607E3DD70FCA22FDB12
SHA-256:	A19FA01108C2EBB6AB3071E01E8282E68E74487D610FBD375F2BC436AA6A8CB7
SHA-512:	0AE0E70ACE3E9A50457875839D061C20AF241E7A763F5E2F582A113503DC0DEF1C5F82385DCD70479305290BFD38FC5EE56EEA0B612A35CBA4F4D4878A256BAC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/T1.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\T1[1].png	

Preview:

.PNG........IHDR.......v.....oG.<....PLTE...&3e...3;^...!&Q...<U.!&Q......-/O...!&Q...<U....!&Q...-0P...!&Q...!&P...9R.!'Q %P..............+.N &O %O &P.$P!&Q=V. $P......!&P<T. $P.
........!&Q...?R.!&S...!&Q..............!&P...... %O!&Q %P<U.......=W.<U.<V.:T.;U.<U.<U.... &P......<U.;U.... %P;V.......... %P!&Q... %P............VUU...<U....!&Q %P %
Q...SRR!&QTSS=W. %P %P...<V. %P %P>Z.... %P &Q...<U.<U.<U.<T.TRRWVVWVVVUU...TSS $PUTTVUUWUU...UUU......VUUXWW...<U.UUU.......?Z.UTT......VTT
>X.UTT<V.WVV>X.=W....ONN............UTT..............wvv...gggjhh........."'Q"'R=V.......!%P...$)T......WVV......XWW>X.=W....@[....UTT.........(,W.......#N....2X...'/`...LNk...SUq
........58]\[[<?b........fg{/<w+6l......DFg4G.;S.7K.]^xqr.......zz.{|.:P.wvvll.2A.gff......``_...nmm.......w......tRNS....... ........R.X.....@.$.g ....`*.T..K..*7...(....H.^4.p.3~ws.....5.g....Z.<.y:
.. ...b.....eL".0.pF..jZ..A...GR=:....T0k..~_2(..M....F.].......9....v..qC....g...B...;0IDATx..._h.q.....C6..8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\T2[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 2048 x 544, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	20812
Entropy (8bit):	7.818976244358117
Encrypted:	false
SSDEEP:	384:vZJ9HoG8R2q5yNLHIVBpX46aJGFX66E/AzQ8pbaKM5tHx5yKN:vZvoDAKyByBpX46rF65eaptR0KN
MD5:	9B22D3C490E9AB379656B65C3CDFA55D
SHA1:	C83585C440F315D22BC456C7F7602D5ABA9D0035
SHA-256:	F1DD52020EAC20F76CA2C88A78DF0984ED93E9AF6D23ADF25CE640D154B7F307
SHA-512:	78EA4E2CF1ADA284700E8717EC504286694C2A99CD776D4807DC2B24942D3B4A55B4BFD93042934E06882814CA90502322D12D764428A566B8A902C21C70919E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/T2.png

Preview:

.PNG........IHDR....... .....&.yz....PLTE...333333443B.D332442J.JJ.JI.K443J.J442444J.J332441333332J.KJ.JI.KJ.JH.I332120332333J.KJ.JJ.JJ.JK.LJ.JJ.J443222I.J44233
2I.JK.LK.L443J.JJ.KJ.KK.L332I.J441J.K443443332I.JH.I443I.JI.JI.J332442I.JI.J443333H.H443J.KJ.J442J.K332J.KJ.KJ.J554J.K332332J.J333443442332I.JJ.K33233
2L.MI.JK.L332J.KJ.K332442J.KI.K332J.KI.JJ.K332K.LJ.K551333K.L000J.K443665887O.PN.OP.QK.LJ.KN.OL.MM.NM.NP.QP.RL.MT.U..b>...otRNS......>.JB......W'.N=..
...B......q.# ..*.......Q%G..y73....wld8.1..k_....eR..]..s......E.L.Z,......} .U.T....H...O.IDATx...`..@.........TUUUUUUUUUUUUUUUU
UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU.=8........m.UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU
UUUUa..Y...0...M!./Ut..,lDTH....b1D.-..,...._l.[dY.b.z........|.............................Eqsu.p..T....{N.Q.9...5...+i.....Y.r2,.B.1f..1.Vi.?.O.......8e...P.C..]...._wJ...4m......^...M.C.C=.....XnW
...M......c...?|

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\T3[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1250 x 764, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	31345
Entropy (8bit):	7.9406198550287
Encrypted:	false
SSDEEP:	768:TbxJXsyBEfiZmpD7aSb4SkMW50RIkQ8XYlz3glNAuejlZJM0lm6:TdJXJBe57/0SzZYl0PAu4lZzm6
MD5:	93D4EFF829C00BDE208F5B4C5233AD87
SHA1:	077F459B13334AA887142316D9877E03E80596EF
SHA-256:	7C8DDD36B2A9478BC8448E6EAE400B228ED60FB902C071C9C3A2FD0D18AAC874
SHA-512:	E0A5DF7AD6103B4EF66039A31E428BED58508619AA5F01CC50DBD6A5ADD4182A828ADDC196512F0922795BD2DB93A03ABA378C9985102C82B124C3FC670A7A9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/T3.png

Preview:

.PNG........IHDR.............zT.....PLTE...XXZXXZ...XXZ...XXZ**+%&#c.B...?L.GIG++,WWY\\^XXZaac__baacVVXaacXXZ[[].u.^^a...``bXXZc.B``b``bU^c...YY[88:.HZSc``c::;X
XZYY[$#$.H?L.667?L..I\dWc.B**+.HdL.--.WWY?M.XXZVVXXXZXX[.Lj.G<H.XXZ.I&&'CQ.fM.^^`YY[c.B[[^../""#YY[...fM.112]]```beL.``b"'?L.d.B?L....XXZ]]_lQ.DS.``b
..A>K.__bXXZXXZ334^^a//0a`c\.>:F.].>``bYY[.C``b...YY[]]___a?L.d.Cto{XXZ.L_Gy//0.Lc.B.E.H=J..M>J....e.D.GBP.]]_AO.b.A.EAO.dK.:F...L.Kd.CcK.fM.e.CfL.[~=...c.B.LeL
.fM.99:.H.....M.B..A...<<=:F..C.Be.C...\Fv.I:F...B.bu....LCQ.;;<.y^...XXZ.......HeL.?L.c.B...\\^]TTZVWe[q.qe8q~......oy.BhrIck....."{.O_d...#....q<myS[_...``b.x.(|.VY\bbd
3t...Z.AaG~...;....\.CCP....jP.TZ.4B....Z.7C................m.Ws\..z....5Z.i.FAI.........h.F....k.......k.I........ytv.Y....+.....tRNS.@.........@./|.......Fa..:........,G.......@#@'..!...[......I..l..L5\e..
[5.A.=..W..S. ..~Zq.p.c-..v...B....0...Q!.Q..]..q.o..P..o...^...S...q.../q.j.p>.5.....2.....b..Z..v{IDATx.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\T4[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, 1655x400, frames 3
Category:	downloaded
Size (bytes):	42751
Entropy (8bit):	7.819989746960434
Encrypted:	false
SSDEEP:	768:58Kjm1+Zi9JIdy0/RrAMkiPuCTt22DIQ8v2DTID/zG2oSDL2UkB1WVIQp8ztjpD+:2l1+ZiUdykRrA9iPugCQU7D6Y324i8gW
MD5:	6AF5D09D4655ECDBBC123BEC308A2392
SHA1:	6181D852EFAD896216D59F1383CE7B7233BB52E8
SHA-256:	BEE91EAE390A7B480D7E21A0780F633D782504F9DA706B338025C9D158446238
SHA-512:	40AB519B203DE88F8CED6DA228AAD5A343A842489294E24FCC7364FD3C50FFC671F375C5356970AAD01AC0009E326ECD3E608789A6F40A61A332761CF964EC9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\T4[1].jpg

IE Cache URL:	http://https://www.engagebay.com/images/T4.jpg

Preview:

......JFIF............C.....................#....*%,+)%((.4B8.1?2((:N:?DGJKJ-7QWQHVBIJG...C......."..''G0(0GGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGG
GGGGGGGGGGGGGGGGGG........w..MW^z...}....'M>9.>......^.:m....]6.:....F.......................
....1v.bTj....<1.r0.......,.....xu...7nt..uY.>{s.......mh.3.....`...
.~...H59..:.......x...o;k...G.u......SZ...*...[j.n.......gY3>.Vl9?x.<....Fq.6>....... ...N.Go...(S.s.
Z.u..3!K..Y.fl.....0../AU...0..m.Ob...2..|NwmX`...[....TN.y..y.......E....Okt.(..........

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\T5[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 241 x 75, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	3089
Entropy (8bit):	7.860538988840208
Encrypted:	false
SSDEEP:	96:zumBnNHbOmvLLKvqNoIwo8EbPIx1/4miqyYnCnaJ:amZNHbrPyIwo3QBizYn4aJ
MD5:	CD806F0E3C484251FA29C12544F06EC2
SHA1:	9F788042F68739AC4253B2D8744FD53A9A601E9D
SHA-256:	80E1437A8DC4782A7DD392DC1C9E1589B4DF3D0D454CA7C02EEFB4908E984BDD
SHA-512:	EEAFC2D3EB03E832D2A4CB936EEEF29C68FDD4419AF2F2A4FA2DE7AD31209141AE188E7014EB75F98DC41EC9E65FD01957CAFCE415FEDEF3025B466AD5CB BBF5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/T5.png

Preview:

.PNG........IHDR.......K......D.(....PLTE........8..
....-u{....YtRNS.......K..q''..,.t.&.. .C......._]Q.<..Q.X71..j+..d<4...}F..9...{iA..'.J.yu1.....p..sY...YIDATx...1..0....l...l.R.).z.''V.....H.`O.A.......
....B....h....q...}}..C.|..C...+...<.b.....XSr...c..i.{v 2.9n.&../.|...h.?.X]..@....+.A.!m.....H.@4.'.-H+WD....Hk6.gGco.........K.>.{...........oc...W.}...........r....g..re.}7.w=...f...2........P#''
j..._!..=`.:..q...G...+.G.h...6ej....;.....*.!.8....[....\.-H..*..!R...Y..4].........:...k_}Ap.C!!..FQ.....k.dK.p..G.=...T.../....p.G.kG.b...4.......0|1......!...uE.k>5....X?...JY/.........j.W..z.........;@.L.0
..m...aj.$....*,MK..e...B.(..6...........+....l.%''0E.W.m.*..#._y..3.X_E......S6...50..@.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\T6[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 741 x 209, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	11006
Entropy (8bit):	7.939656191124424
Encrypted:	false
SSDEEP:	192:4dSy9kZjjIVyH8MOSv8FlyFRH9TMK85CF0hulrsotyu9TNXhcFrelJHbBwT:4dP9kuycM3v7RHdH0hyrZMuVlhccdwT
MD5:	53A0E48AC4E2E35BA7D7B6EEC3DBE0D3
SHA1:	14A2E379D1A44058B0E34A88E68DAD75A82FAFBD
SHA-256:	BDD3E92439411EAFBCA743B800AE4500DFCF2A1F6994EC722657B78F087E0A69
SHA-512:	DA43D881700798C938AC7B4B345425976EEC6853EAF44FFB8EA2AF05D6CE05B8E500FD9E409C8EFFBA053AC68535B551AAF4C2820CB4AE291A50427CC82C00 3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/T6.png

Preview:

.PNG........IHDR............\.<^....PLTE...KKMKKMKKMKKMKKMKKMKKMKKMKKMKKMKKMKKMKKMKKMKKMKKM{.M{.M..<M.HG.OP.KE.SF.SN.GN.G..<J.LE.SL.HH.N..=n.C
...E.SM.HU.GE.Sc.E..@..S.H..?E.S.....=..<...E.S`.E|.A.....;E.SE.SE.SN.HE.Sv.Hw.B..;M.Hg.D..r.A{.b..<..n.Bh.Dg.D...q.Bu.C..;c.E..;}.B|.Bs.A..<...<..<..;.....}}.xL.HM.O....
..KKML.H{.ME.S.....>..?..>..?z.@|.@..<x.Aw.A..>u.A..<s.A..<r.B..Z..bN.H..z.._V.Gp.B..f..=i.E..\t.C..~n.B..X..FY.Fq.Dm.C..;..s..c..VR.G_.Fd.Ek.Dk.C..I\.F{.Cv.C..?....v..p.
.}.B..;...m..h..Q..A..>..j..Mb.E..Dm.Dh.C..B..=.....V..Jx.C..<.....=.............|..m..\P.Hp.D...d.._..V..OP.O..MV.LZ.Kf.E.....U..Q..L..Ig.F..?.....u..SK.Q_.H..E..>.......Sa.F^.F.....y..p..l..
[..Nz.E.........r.r^.]..>........}.....at.^}.J..HW.H..B.........e.bq.K..D...........r..m..`.q.....\tRNS.@....`.. 0..pP..... @.P@@0... ....``0.....pSC......p`P@.....`........0...........p@0 ...%..'Z
IDATx....m.0..Q...a......C...j.^..)................@Z..Y#b(..-.xQ9).{.......rR.^.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\T7[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 225 x 170, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	5602
Entropy (8bit):	7.899368211101467
Encrypted:	false
SSDEEP:	96:LDNoM6qen5GWXj8JDssOGcW6JoBgC46CHEAhk4OlR6IRILJc5vq10VFG:LJbc5LT8MGkoBgCktSLvhRItK/VY
MD5:	BED2623A1F408BBA8502EAEF84C811B6
SHA1:	60F0B673AE0D9275C9CC0DB48140F09DF8E0BE36
SHA-256:	9EB0B5FE69F56BA152AB2A6A778439A0EE48CFDF64C5758DB70BDA9898891247
SHA-512:	D36FFBB0806A2933ED7D8A43CCAA798E505A0A43B0044803A2DB279028FE49829E420CC4BD7468E50CE6FC72E0CD0FBFF26F50630BBE5DCC308CD8AFA1A604 4D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\T7[1].png	
IE Cache URL:	http://https://www.engagebay.com/images/T7.png
Preview:	.PNG.....IHDR.....l.....PLTE....+L.)I.Qr...../..6..2..&.(G.$@..-..+.Qr..'..0.Qr....)I.>_.Qr.+L.!;.Qr.Qr..$.Qr.Qr.%A....Qr.Qr.,L.-M.#=N5V.Qr....Qr.)I. 8..)..!.Qr.Qr.Qr. Qr..8.Qr.Pq.(H.'F.Qr.'E.Qr..5..2.Qr....Qr.. .Qr. 8.%C.Qr..6..$.Gh.Qr.Qr.'E.Qr.*I)/O.Qr.Qr.Qr.(G -M.'D.%B.(G.Qr.Qr.Qr.Qr.!;../.Qr.Qrt<\.Qr..)..#.Qr.Qr.!:.Qr.....!.'E.'E..!.Qr..$.. . .... .(F.)H.Qr.Qr.Qr. 8."=.Qr../.Qr.Rs.. ....Qr.-P.Qr.Qr.QrY7X..7..3.Qr.Qr....,N.+L.$@.'E=3SC4T..7.Qr..3.Qr..'..2.Qrd8Y.Qr.Pq.Qr.Qr.,L.Qr.";."=. 981Q.Qr.Qr.#>.Qr..2. :.Qr .Qr.Qr.Qr.Qr.,N2/P. :.Qr..$.-Mk9Z.Qr.?^.Qri9Zi?^..3..3.;Y.Qr.@_.+K//PB3S.(F.'CE3T..,K4U.)Ev<\\7X..7.=[.Qr.?`.'E!-M&.O!-MK4Ui9ZM5Ub8X.Bc.@a.Mm.,L.+L(.N ..Q'.N=2R20Q.?`.Bcgu.X6W.,L.Lk.,L....Mm. 8.C^U7X.>X.Qr.*I.,N.+K./S.$D.1V.-O..Q.-P.)I."B.'G.0U./T.&F.2Y.)I.Ux.*J.)K.(G..:.6`..@C.#.....tRNS....2.$.;.X..kd.....vb..... ....7...bT?.....YTP....J.....qH#.....zvrhD@5.....YLJ*&.....sn_?.....xOD7.....kQD;'.....jh_V2/*'.....^>4-)VTL410

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\T8[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 320 x 54, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	6165
Entropy (8bit):	7.931276860079077
Encrypted:	false
SSDEEP:	96:Gv2YE7TcmCPyvc2l24VLiFntij5jJAUnk8QnCeueIVKM3CJxJv/Dedi7KR:GvtEE3mcwKXiVjJDk8+cePJX/DJQ
MD5:	3F693419687F83122AA70C55912C44C3
SHA1:	104909366BBF5D57F72D5B0D93FE737CA721A88A
SHA-256:	D12E026F4D5A0237D38C93026D34403345DC412FEA391CBB69D46C4F37D641E2
SHA-512:	2F3D14A710D8A150EF23106BC906E30DBE7E622CF0CB22F06D8B7BB2BF3E9523D50A8E4CFAB109102285AA3F378611FB3E0E8385E2D91B88AA30FBFBE4518A1A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/T8.png
Preview:	.PNG.....IHDR...@...6.....B.....PLTE.....6P[.....3OZ.....!.....@...0MY..#.....&;.....5..-.CP....)JV!FR.....`jr.....-KW.....*=I.....-...-LX)HT .AM.....*=.,,..y}..DQ.....ty..6D.#8.....GYb.4E. 1..*MXb#FR..0.....&HT.....AN.?M...Itz2NY5KW.1B..'..%...../FS.!....M]f.;J.....u{.pw|.....gpv.JV.EQ.=J.....Zg. Wc.Q].7G.:F.....[go.`l.NY.CO.=L. 6..2.....w~.bls^glS`h.CQ!:H.7A.....~..Ydj.T`IV]@S];Q\.@K...{...cqBPX.GS.3@..4|..emrR]eQ[bBV`)CP$?L...Tck.]h.2>..... ..q..gs.iqDR[>MV,.....|..w..kxI\e8NY.-=...Xv..px.cq V`8HR..:...&.....#...s..Yh.BN1BL../^..$...T_.NZ.MW.....s...k|.JV=KT.....0.....V`.2A..*..#.....=..Z.....j.....x../y.3 mtZns.dpIfj.bj.....9..{..rLR.....IDATx..i\.G..g.....j..B.%..1....m..C...\.."..`.-"..PQ.E.J..[.jk.....}3..6..._..Q7.3..3.}3.....0...x..g..<j.d.-.fp....9....0r[.wn...`... P..y..-.Op.G.....)g.....q..45.V

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\automations[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	21423
Entropy (8bit):	4.231385163760046
Encrypted:	false
SSDEEP:	384:eT++Fcb3VGGVrGixjhVjg1OSp1O/9464r8tgB1WegKgzjIAvNYqUYQQAjU4Z+5mB:oeGaGixtowjoWeVgzjx8Rv
MD5:	D77F130361E4275326003BE19C3E8381
SHA1:	74864701FB79AB5A6BC2D2A573C8A64321C8D618
SHA-256:	94EB7CC84CA838B41BCC00426D3D9CA54BFF9DE053F0BFA05EF5C86844F8A6EC
SHA-512:	C31F46D7CF3B9383FE85966C4254662C7A2BA2655D0BD956F3BECF6FD654AB2E78C2FB3AC64236C45861C6315C88EA9D7D101C305D2CF1174271F4C30049B41
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/automations.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 21.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="FilledOutline" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px"... y="0px" viewBox="0 0 70 70" style="enable-background:new 0 0 70 70;" xml:space="preserve">..<style type="text/css">....st0{fill:#E6E7E8;}....st1{fill:#6DC9F7;}....st2{fill:#D4FBFF;}....st3{fill:#FFFFFF;}....st4{fill:#0089EF;}....st5{fill:#FA759E;}.. ..st6{fill:#3A2C60;}....st7{fill:#FFD7E5;}..</style>..<g>...<g>....<path class="st0" d="M63.8,7.9H10.1c-2.5,0-4.4,2-4.5,4.5v36.9c0,2.5,2,4.4,4.5,4.5h20.5l-1,6.7h-5.2c-1,0-1.8,0.8-1.8,1.8v0.1.....c0,1,0.8,1.8,1.8,1.8h25.1c1,0,1.8-0.8,1.8-1.8v-0.1c0-1-0.8-1.8-1.8-1.8h-5.2l-1-6.7h20.5c2.5,0,4.4-2,4.5-4.5V12.4.....C68.2,9.9,66.2,8,63.8,7.9z"/>.... <path class="st1" d="M7.8,6.3h53.7c2.2,0,3.9,1.7,3.9,3.9v36.9c0,2.2-1.7,3.9-3.9,3.9H7.8c-2.2,0-3.9-1.7-3.9-3.9V10.2.....C3.9,8,5.7,6.3,7.8,6.3z

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\bootstrap.bundle.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	84152
Entropy (8bit):	5.1609825846750415
Encrypted:	false
SSDEEP:	768:du/iPy7+zZHVPVBNpwV7BTUB6/YLF/fB+4ed4MMAja+t+QnXLb1+uaR+orWieOJ6:deiayUYLZ83dPD3GAP6f2jX+i/Q2
MD5:	7F389F5D2622CE2090ECA7C36BCB90BC
SHA1:	AB27031159724E2421F6FF5C70F48E657ABE9D39
SHA-256:	8D7089253DCA29C9CD8D9DEB7EC69B0A3D445F88F6A26478C719BE1F90ADCB01
SHA-512:	89C7978E36E6076AF0A17F7729AE870073FE07BE88635CF4A3787E3753DE0ED452B3279EB54DFFD10289A86C8F25C5FADF3CAC35E860805C0C0BF6E2EDDBCCA
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\bootstrap.bundle.min[1].js	
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/4.5.3/js/bootstrap.bundle.min.js
Preview:	/*!. * Bootstrap v4.5.3 (https://getbootstrap.com/). * Copyright 2011-2020 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors). * Licensed under MIT (https://github.com/twbs/bootstrap/blob/main/LICENSE). */.!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquery")):"function"==typeof define&&define.amd?define(["exports","jquery"],e):e((t="undefined"!=typeof globalThis?globalThis:t||self).bootstrap={},t.jQuery)}(this,(function(t,e){"use strict";function n(t){return t&&"object"==typeof t&&"default"in t?t:{default:t}}var i=n(e);function o(t,e){for(var n=0;n<e.length;n++){var i=e[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(t,i.key,i)}}function r(t,e,n){return e&&o(t.prototype,e),n&&o(t,n),t}function a(){return(a=Object.assign||function(t){for(var e=1;e<arguments.length;e++){var n=arguments[e];for(var i in n)Object.prototype.hasOwnProperty.call(n,i)&&(t[i]=n[i])}retu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\bootstrap.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	144877
Entropy (8bit):	5.049937202697915
Encrypted:	false
SSDEEP:	1536:GcoqwrUPyDHU7c7TcDEBi82NcuSELL4d/+oENM6HN26Q:VoPgPard2oENM6HN26Q
MD5:	450FC463B8B1A349DF717056FBB3E078
SHA1:	895125A4522A3B10EE7ADA06EE6503587CBF95C5
SHA-256:	2C0F3DCFE93D7E380C290FE4AB838ED8CADFF1596D62697F5444BE460D1F876D
SHA-512:	93BF1ED5F6D8B34F53413A86EFD4A925D578C97ABC757EA871F3F46F340745E4126C48219D2E8040713605B64A9ECF7AD986AA8102F5EA5ECF9228801D962F5D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css
Preview:	/*!. * Bootstrap v4.0.0 (https://getbootstrap.com). * Copyright 2011-2018 The Bootstrap Authors. * Copyright 2011-2018 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */:root{--blue:#007bff;--indigo:#6610f2;--purple:#6f42c1;--pink:#e83e8c;--red:#dc3545;--orange:#fd7e14;--yellow:#ffc107;--green:#28a745;--teal:#20c997;--cyan:#17a2b8;--white:#fff;--gray:#6c757d;--gray-dark:#343a40;--primary:#007bff;--secondary:#6c757d;--success:#28a745;--info:#17a2b8;--warning:#ffc107;--danger:#dc3545;--light:#f8f9fa;--dark:#343a40;--breakpoint-xs:0;--breakpoint-sm:576px;--breakpoint-md:768px;--breakpoint-lg:992px;--breakpoint-xl:1200px;--font-family-sans-serif:-apple-system,BlinkMacSystemFont,"Segoe UI",Roboto,"Helvetica Neue",Arial,sans-serif,"Apple Color Emoji","Segoe UI Emoji","Segoe UI Symbol";--font-family-monospace:SFMono-Regular,Menlo,Monaco,Consolas,"Liberation Mono","Courier New",monospace}*,::after,::before{box-sizing:border-box}html{font-family:sans

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\calling[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	4539
Entropy (8bit):	4.471701450653081
Encrypted:	false
SSDEEP:	96:s+foFC5DV5IIy7CPggntyDOfvmk4p6EE3uaDgBJwqy:doFC5DAHmggIDOV4pRE34In
MD5:	B8D565E63D6C7C1272E2F1663CB9B8BD
SHA1:	8E2EBAAA90BA0C60438A65AC83B9788B5D5E2AA6
SHA-256:	857BEBA0A971C2DC0256EBE400D2DC68FBD85AB20D555C0161C2332C23C00487
SHA-512:	EB4FA33E3E91824718B2481628D7028F79130E805AB14E2D492F00B06BDA88714925A00DCC31EA054D9B09F0B40F7D852F8E5DBEEC1A1FD20A93947D4E9BCDC8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/calling.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 21.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 70 70" style="enable-background:new 0 0 70 70;" xml:space="preserve">..<style type="text/css">....st0{fill:#E6E7E8;}....st1{fill:#FA759E;}....st2{fill:#FFFFFF;}....st3{fill:#0089EF;}....st4{fill:#3A2C60;}..</style>..<g>...<path class="st0" d="M64.1,37c-0.3-1.8-1.2-3.4-2.6-4.6c0-0.1,0-0.1,0-0.2c0-14.8-12-26.8-26.8-26.8S7.9,17.4,7.9,32.2....C7.9,47,19.9,59,34.7,59c0.5,0,1,0,1.5,0c0.7,0.9,1.6,1.7,2.6,2.3c0.1,0.7-0.2,1.4-0.8,1.8c-0.3,0.2-0.6,0.3-0.9,0.3....c0-0.2,0-0.4-0.1-0.6c-0.3-1.2-1-2.1-1.9-2.3c-0.8-0.2-1.5,0.2-1.9,0.9c-0.3,0.8,0,1.7,0.7,2.2c0.6,0.4,1.3,0.7,2.1,0.8....c-0.1,0.4-0.3,0.8-0.7,1.1c-0.5,0.3-1.2,0.4-1.7,0.2c-1-0.2-1.9-0.9-2.4-1.8c-0.1-0.3-0.4-0.4-0.7-0.3c-0.3,0.1-0.4,0.4-0.3,0.7....c0.6,1.2,1.7,2,3.1,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\capterra-46[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 126 x 120, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	8267
Entropy (8bit):	7.935403730376425
Encrypted:	false
SSDEEP:	192:4IpHh6q5f4BDVaC680VprT4adBQh3Qx7VUUMTV0tjZIp:l4w2bSUr3Qxtpap
MD5:	BF0E0C84097A0D2A7982B7272C03FC96
SHA1:	3C344DB564DB593D27E4A137E62B8E598B0A10AD
SHA-256:	F4D360B8B1DCF6689B29EB0C3D30B09ED7B70E9D35925955325F42F467B95160
SHA-512:	11630C500009DFA6F00CDD94AAD19B11517DBAEA56F611AD1A15E1128421DB66EF88F882AD4595ED6698DFCDE04FDA6FCABB91B6188F55BC0F8A9DEF715DC80

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\capterra-46[1].png	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/capterra-46.png
Preview:	.PNG.....IHDR...~...x.....4zF.....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-c138 79.159824, 2016/09/14-01:09:01 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns :xmp="http://ns.adobe.com/xap/1.0/" xmpMM:DocumentID="xmp.did:87B578B41C5F11EBA0A58A91143E0A5C" xmpMM:InstanceID="xmp.iid:87B578B31C5F11EBA0 A58A91143E0A5C" xmp:CreatorTool="Adobe Photoshop CC 2017 (Windows)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:EACBAECB1C5E11EBB77BF52F8F 84DA9B" stRef:documentID="xmp.did:EACBAECC1C5E11EBB77BF52F8F84DA9B"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.m.w....IDATx..].|T...}.ld#.da'..".wD..u.P.m.ZE.]|...^}.V_...X..7..UQ.(....H da...u.w.7w&3.d2....=...df.{.....9.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\comapany-management[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	5849
Entropy (8bit):	4.607384615713871
Encrypted:	false
SSDEEP:	96:s+foQLSlfAP9VZtDKcE6R3xHI1Tei5mlqhuBjUjV7sHnSXctvy+5gLP4s8NWyt7X:doQ4fAP9VZtDKiRBHkTnxOecgUVWC
MD5:	052813943480B59A9936F27D00C16734
SHA1:	8233A1624805F4AE618EAF4B9557E05F6F1C9F63
SHA-256:	F01205D8B2F04A10B0C4B4FDE15674C1603599B207B563BE3B98D134C255F149
SHA-512:	90F68099DFAA4B0919FC875F437C99B5528E5805A3CBEBC929F3C8F3B326E91339D7F676AEEA3CD912ADCC29536E0FFFF9B6C09357C475FE86C63AC7753B6E1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/comapany-management.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 21.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 70 70" style="enable-background:new 0 0 70 70;" xml:space="preserve">..<style type="text/css">....st0{fill:#E6E7E8;}....st1{fill:#6DC9F7;}....st2{fill:#D4FBFF;}....st3{fill:#FFFFFF;}....st4{fill:#0089EF;}....st5{fill:#FA759E;}....st6{fill:#3A2C60;}..</style>..<path class="st0" d="M64.5,7.1H8.4c-2.5,0-4.6,2.1-4.6,4.6v38.1c0,2.5,2.1,4.6,4.6,4.6h21.2l-1,7h-5.3c-1,0-1.8,0.8-1.8,1.8...c0,0,0,0,0,0v0.1c0,1,0.8,1.8,1.8,1.8h25.9c1,0,1.8-0.8,1.8-1.8v-0.1c0-1-0.8-1.8-1.8-1.8h-5.3l-1-7h21.8c2.2,0,4-1.8,4-4V11.2...C68.5,8.9,66.7,7.1,64.5,7.1z"/>..<path class="st1" d="M6.1,5.4h55.5c2.2,0,4,1.8,4,4v38.1c0,2.2-1.8,4-4,4H6.1c-2.2,0-4-1.8-4-4V9.4C2.1,7.2,3.9,5.4,6.1,5.4z"/>..<path class="st2" d="M61.6,5.4H6.1c-2.2,0-4,1.8-4,4v34.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\contact-management[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	4588
Entropy (8bit):	4.781748297485202
Encrypted:	false
SSDEEP:	96:s+foTjblqluAh3L2ukkEf64uakJMditWrYOMF:doTm3L2ukkEf6XWbG
MD5:	B8F846982BD9633C74DD66C1A97554EB
SHA1:	464C844677DCDB2CD85DF498BC1C5CAF4999B234
SHA-256:	898E025C3EC76CB15FA6C905A623DD11F7A9107C798435DA3961D7073865B692
SHA-512:	B02204B721EAE213B288B6E10B50FD2493198BAC37FAF41F4053995F1B6CCE232179E4B3911C0B932C5740607B1B2B0624071A1A5D9A48525A1412D51E8F8D98
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/contact-management.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 21.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 70 70" style="enable-background:new 0 0 70 70;" xml:space="preserve">..<style type="text/css">....st0{fill:#E6E7E8;}....st1{fill:#D4FBFF;}....st2{fill:#0089EF;}....st3{fill:#6DC9F7;}....st4{fill:#FFD7E5;}....st5{fill:#FA759E;}....st6{fill:#FFFFFF;}....st7{fill:#3A2C60;}..</style>..<g>...<path class="st0" d="M56.9,27.5c5.5-4.7,6.1-13,1.4-18.4S45.3,3,39.8,7.7s-6.1,13-1.4,18.4c0.4,0.5,0.9,0.9,1.4,1.4....c-1.2,0.4-2.4,1-3.4,1.7c-2-6.9-9.3-10.9-16.2-8.9s-10.9,9.3-8.9,16.2c0.7,2.4,2.1,4.6,4.6,2c-5.8,2-9.6,7.4-9.6,13.5V66....c0,0.9,0.7,1.7,1.7,1.7h33c0.9,0,1.7-0.7,1.7-1.7v-9.7c0-1.3-0.2-2.7-0.6-4h23.4c0.9,0,1.7-0.7,1.7-1.7V41....C66.5,34.9,62.6,29.5,56.9,27.5L56.9,27.5z"/>...<path class="st1" d="M53.5,25.5c-4.4,3.2-10.4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	911
Entropy (8bit):	5.180032150665888
Encrypted:	false
SSDEEP:	24:5AOYNZGL78AOYsZn9AOYXZG38AOYUTZGR88AOYN7ZG7K:eOWwLjOLUOgwXOxTw+OCwG
MD5:	6559984CF35A95A1F3567F4903E47716
SHA1:	6651235A71D4F95AACBA18BBADBC5E7B08017A3D
SHA-256:	5874DEC01627A418A8167969C6B2715778231B523B028CC6F769C764A98ACEAA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\css[1].css	
SHA-512:	FAF0ED047ABEB1FAB00688C3586CA457C93B21ADAC29C57228490912BE5ED25BA2DD100652A31F701F3F1CA4B6E435F628CA5765142C8DE9463BCAD4D27A16E1
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Poppins';. font-style: normal;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/poppins/v15/pxiByp8kv8JHgFVrLDz8Z1xlEw.woff) format('woff');.}.@font-face {. font-family: 'Poppins';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/poppins/v15/pxiEyp8kv8JHgFVrJJfedA.woff) format('woff');.}.@font-face {. font-family: 'Poppins';. font-style: normal;. font-weight: 500;. src: url(https://fonts.gstatic.com/s/poppins/v15/pxiByp8kv8JHgFVrLGT9Z1xlEw.woff) format('woff');.}.@font-face {. font-family: 'Poppins';. font-style: normal;. font-weight: 600;. src: url(https://fonts.gstatic.com/s/poppins/v15/pxiByp8kv8JHgFVrLEj6Z1xlEw.woff) format('woff');.}.@font-face {. font-family: 'Poppins';. font-style: normal;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/poppins/v15/pxiByp8kv8JHgFVrLCz7Z1xlEw.woff) format('woff');.}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\deal-management[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	9105
Entropy (8bit):	4.367760086560026
Encrypted:	false
SSDEEP:	192:doo3lwmpepZv6cn6HjBGCxojK0DdWHW8XjKb4Yaz9GY/cv:dhipZPIjBp+jdWHBXeb4P0v
MD5:	8EB8916CA65EC3DCEC0CAF25743BC92D
SHA1:	94D18C3A0905C5B3896B7BF75EDB8DC88027EC29
SHA-256:	43864CA54A47CCF679FCB84BD85A5E7E56A7E1CE3D08C1964A11703529A223C6
SHA-512:	D0FF0A95AB8BECBC7FD1A1924DD9C28EA52FE2130319251EFB7CB1C0E0FBC73C6FF6A360C92A871C41408F1CFDD59830AA2D70E37C39A75992B25110C739879
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/deal-management.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 21.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 70 70" style="enable-background:new 0 0 70 70;" xml:space="preserve">..<style type="text/css">....st0{fill:#FA759E;}....st1{fill:#3A2C60;}....st2{fill:#0089EF;}....st3{fill:#87796F;}....st4{fill:#6DC9F7;}....st5{fill:#FFFFFF;}....st6{fill:#FCE8CB;}..</style>..<g>...<path class="st0" d="M6.4,5.7L3.8,3.1l0,16.5l0,4.3l0,11.7l5,5.1l0.1,0.1l16.4-16.4L6.4,5.7z"/>...<path class="st1" d="M25.8,24.1L7,5.4L4.3,2.8C4.2,2.7,4,2.7,3.9,2.7C3.7,2.8,3.6,3,3.6,3.1l0,16.5c0,0.2,0.2,0.4,0.4,0.4....c0.2,0,0.4-0.2,0.4-0.4l0-15.5L6.4,6l18.5,18.4L9.1,40.2l-4.6-4.7l0-11.5c0-0.2-0.2-0.4-0.4-0.4c-0.2,0-0.4,0.2-0.4,0.4l0,11.7....c0,0.1,0,0.2,0.1,0.3l5,5.1l0.1,0.1c0.1,0.1,0.2,0.1,0.3,0.1c0.1,0,0.2,0,0.3-0.1l16.4-16.4c0.1-0.1,0.1-0.2,0.1-0.3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ehform[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):	651
Entropy (8bit):	5.208980753751723
Encrypted:	false
SSDEEP:	12:AAASI2N7Vr4A6qKIVZuHnm0mqEN+DRWULEVQO/KSpOZzbRAre6PQASb:6l+vU2uHm0oURWUoVQOShb+re6HK
MD5:	D7F798CDEFFB827BD6AECCB1D2FDF9B4
SHA1:	350DC1C89F250EE00FBA4B9646D04ABDC2E8D3DC
SHA-256:	6C0C4A916D8E100DD65071ACFE381949C6A6D74A356369F7948B60FE787922E7
SHA-512:	F8FD2D4754A71C50D823C12EA32FC113BD478CF69354B68070641F9528A3A9D8A4C43345E74CDB3D56F22ABF32FEDD15874C0C79DD2E84EA8F543A8352D0A8(
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://d2p078bqz5urf7.cloudfront.net/jsapi/ehform.js
Preview:	function engagehub_load_cloud_static_file(){try{var d=window.navigator&&window.navigator.appVersion.split("MSIE");if(parseFloat(d[1])){d=parseFloat(d[1])}var a="https://d2p078bqz5urf7.cloudfront.net/jsapi";var b=document.createElement("script");b.type="text/javascript";b.async=true;b.src=a+"/min/v214.js"+((d&&d==10)?"?t="+new Date().getTime():"");document.getElementsByTagName("body")[0].appendChild(b)}catch(c){}}(function(){if(typeof Engagebay_JS_Settings!="undefined"){console.warn("Engagebay script is already loaded. It seems like you are including the Engagebay script more than once. Ignoring.");return}engagehub_load_cloud_static_file()})();

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\email-broadcast[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	6778
Entropy (8bit):	4.399712030800259
Encrypted:	false
SSDEEP:	96:s+foCLZUZKhlEXllW9Tf7rvGP6HiqwWz0vexM0KFpoDbPDVEbFpkSxDISEgoubg0:doCLZUg/KSfiCMPWxJSqb2RpkutZes5
MD5:	B431CB8C5709DB935E09754C542AF630
SHA1:	471F8A99B838350BF513310BA401473A3DA56C0D
SHA-256:	EAB6D3DF7C67C6DD788A46E93E155EF5C488B38AF71058888BEC0D8D79982771
SHA-512:	5E0F5EEE32D7DAACFE1FF857A6A5A114CA1539AA4E3365F5199901E8EA3B439724B14C109B44073F4B832746EFE322C51DF395CC18B56DC7670E2B5AB57A3E3A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\email-broadcast[1].svg	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/email-broadcast.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 21.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 70 70" style="enable-background:new 0 0 70 70;" xml:space="preserve">..<style type="text/css">....st0{fill:#0089EF;}....st1{fill:#3A2C60;}....st2{fill:#FA759E;}....st3{fill:#FFD7E5;}....st4{fill:#6DC9F7;}..</style>..<path class="st0" d="M42.4,11.9l-4.6-3.8c-1.8-1.5-4.8-1.5-6.6,0l-4.6,3.8l-2.2,1.8l-3.1,2.6c0,0-14,11.7-15.6,13l20.9,17.3l4.6,3.8...c1.8,1.5,4.8,1.5,6.6,0l4.6-3.8l20.9-17.3C63.1,29.1,42.4,11.9,42.4,11.9z"/>..<path class="st1" d="M63.6,29c-0.2-0.1-17.4-14.5-20.9-17.4l-4.6-3.8c-2-1.6-5.1-1.6-7.1,0L21.2,16c0,0-14,11.7-15.6,13...c-0.1,0.1-0.1,0.2-0.1,0.3c0,0.1,0.1,0.2,0.1,0.3L31,50.7c1,0.8,2.3,1.2,3.5,1.2c1.3,0,2.6-0.4,3.5-1.2l25.4-21.1...c0.1-0.1,0.1-0.2,0.1-0.3C63.7,29.1,63.7,29,63.6,29z M37.6,50.1c-1.7,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\email-sequences[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	2590
Entropy (8bit):	5.111365160066199
Encrypted:	false
SSDEEP:	48:c4AQfES8bCmMmxtoT4J+lJG2+t6MtlIWJem+jsLkji9QmsnMg8ZOu:sQfomVmBvJVY6snMJ
MD5:	7A30AADD9A927068961921A4E178AD18
SHA1:	627AD619CDC2F8EE0FA81B5918150F57B3F7B4AA
SHA-256:	ADFF6DC16C4AC174B637FABD8207145BD403263C7F214CB04731D98B1FE1523F
SHA-512:	920069BFBA5F834EBB11DAD0EAE2E457508CE5BA3B7614170097A9F0988D58EAD6122154843E0E1802F6E88FD850259073579063CFEFF3CF734BCBF2D067D0B3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/email-sequences.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 21.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Capa_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 70 70" style="enable-background:new 0 0 70 70;" xml:space="preserve">..<style type="text/css">....st0{fill:#E6E7E8;}....st1{fill:#0089EF;}....st2{fill:#6DC9F7;}....st3{fill:#FA759E;}....st4{fill:#3A2C60;}....st5{fill:#FFD7E5;}....st6{fill:#FFDBED;}..</style>..<g>...<g>....<path class="st0" d="M67.5,25.1c0-6-4.9-10.9-10.9-10.9c-4.6,0-8.6,2.9-10.2,7H7.3c-1.7,0-3,1.4-3,3V58c0,1.7,1.4,3,3,3h53.5.....c1.7,0,3-1.4,3-3V33.3C66.1,31.4,67.5,28.4,67.5,25.1L67.5,25.1z"/>....<g>.....<g>.....<path class="st1" d="M60.8,57.2H7.3c-1.7,0-3-1.4-3-3V20.5c0-1.7,1.4-3,3-3h53.5c1.7,0,3,1.4,3,3v33.6.....C63.8,55.8,62.4,57.2,60.8,57.2z"/>.....<g>.....<path class="st2" d="M63.8,20.5v12.8C61.9,35,59.4,36,56.7,36c-6,0-10.9-4.9-10.9-10

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\email-template-builder[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	5545
Entropy (8bit):	4.836652651610519
Encrypted:	false
SSDEEP:	96:s+foQh09D2bumYXSXIRsrU+E+zZmd8vh2bjNBH9Q7HB5+2+B+Zq+H+ubH+p:doQe2bumYiXwsg+DeM2FBa7HmlgZxeu4
MD5:	8BACC9AC447A9F535B385A19FE353ECF
SHA1:	8D32C62CF3FE58BD89AC9EF6F93AB1A9C4A16E31
SHA-256:	FAFC2A58FA323A94D205DF1B211B2B30EBA17F1D94AA55CC9749AC1765660430
SHA-512:	3A4CFC0100ED731246BC6C9BAB28D807E58147292759028F578E0F99A75468349EEE7DA3319181AFBF1773911B9DBABE8AD7545A846280529BCB68FE4084A9FA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/email-template-builder.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 21.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 70 70" style="enable-background:new 0 0 70 70;" xml:space="preserve">..<style type="text/css">....st0{fill:#E6E7E8;}....st1{fill:#6DC9F7;}....st2{fill:#D4FBFF;}....st3{fill:#FFFFFF;}....st4{fill:#0089EF;}....st5{fill:#FA759E;}....st6{fill:#3A2C60;}....st7{fill:#E8EDF2;}....st8{fill:#C5D3DD;}....st9{fill:#0ED2B3;}....st10{fill:#FEDF30;}....st11{fill:#01C0FA;}..</style>..<g>...<path class="st0" d="M63,9H9.3c-2.5,0-4.4,2-4.5,4.5v36.9c0,2.5,2,4.4,4.5,4.5h20.5l-1,6.7h-5.2c-1,0-1.8,0.8-1.8,1.8v0.1....c0,1,0.8,1.8,1.8,1.8h25.1c1,0,1.8-0.8,1.8-1.8v-0.1c0-1-0.8-1.8-1.8-1.8h-5.2l-1-6.7H63c2.5,0,4.4-2,4.5-4.5V13.5....C67.4,11,65.4,9.1,63,9z"/>...<path class="st1" d="M7,7.4h53.7c2.2,0,3.9,1.7,3.9,3.9v36.9c0,2.2-1.7,3.9-3.9,3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\forms[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	4922
Entropy (8bit):	4.760399797958382
Encrypted:	false
SSDEEP:	96:s+foQzESFq5J6zUWs28w+7du9FtxTtpe06VFqDaj8/OkbsTZdAUKOnLd5Yhq:doQoP6z3WYz56iaj8syNSB9
MD5:	A0E8AED4141829C1B30F3C8DF6C835D2
SHA1:	CAE8EB40C7E9F2D245900615921887D06803F272
SHA-256:	98573037590301E7944C0D7E1E59483A5782170909E456D1461705E038C49F07
SHA-512:	748706F7100600B8AA6B0591BCCCC70B29AA5152AF451BC80BAADC8C7A58FC7F92C1FBC5E4D9BCA986F582E9D903A66A49B4E8A8FD4424FCE00373EFA1B855F1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\forms[1].svg	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/forms.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 21.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 70 70" style="enable-background:new 0 0 70 70;" xml:space="preserve">..<style type="text/css">....st0{fill:#E6E7E8;}....st1{fill:#6DC9F7;}....st2{fill:#D4FBFF;}....st3{fill:#FFFFFF;}....st4{fill:#0089EF;}....st5{fill:#FA759E;}....st6{fill:#FFD7E5;}....st7{fill:#3A2C60;}..</style>..<path class="st0" d="M67.9,24.7l-2.5-2.5v-5.9c0-2.4-1.9-4.3-4.3-4.3H47.1l-5.4-5.4c0,0,0,0-0.1,0c0,0-0.1,0-0.1-0.1...c-0.1,0-0.1,0-0.2-0.1c0,0,0,0,0,0H18.2c-0.8,0-1.4,0.6-1.4,1.4l0,0V12H9.8c-2.4,0-4.3,1.9-4.3,4.3v35.3c0,2.4,1.9,4.3,4.3,4.3h19.6...l-1,6.4h-4.9c-0.9,0-1.7,0.8-1.7,1.7V64c0,0.9,0.8,1.7,1.7,1.7c0,0,0,0,0,0h24c0.9,0,1.7-0.8,1.7-1.7v-0.1c0-0.9-0.8-1.7-1.7-1.7...c0,0,0,0,0,0h-4.9l-1-6.4h19.6c2.4,0,4.3-1.9,4.3-4.3V30.2l2.6-2.6c0.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\g2crowd-46[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 126 x 120, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	9035
Entropy (8bit):	7.94851943340266
Encrypted:	false
SSDEEP:	192:Dyj6JMnH5Lt2D6Ko5TNhyrK+5voarxhUywhcG9GJgxIzxEOq:Dyj6KH5LED67DhPKvx03hcG9tl5q
MD5:	0F5F9D4069215D4844B998551B3815BC
SHA1:	C5FB24E58E7D24BCCCCA908E5B9939D4A39ED7B2
SHA-256:	D799057CAB2DA492784C1D08E89A0E50D1A5085F337A92E3D99081907F90552D
SHA-512:	64FAF976F8EE40F21090927E4B2A6E662F7E65245D8512CE1EBDF89C7E30490E09B4EE181CEEA02D4D1A01E26689D9D1C397CB92507939BEBA1A31970BCEF9A1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/g2crowd-46.png
Preview:	.PNG.....IHDR...~...x.....4zF.....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-c138 79.159824, 2016/09/14-01:09:01 "> <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 2017 (Windows)" xmpMM:InstanceID="xmp.iid:F34519B21D0E11EBB2B0D53EF5AEB5AC" xmpMM:DocumentID="xmp.did:F34519B31D0E11EBB2B0D53EF5AEB5AC"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:F34519B01D0E11EBB2B0D53EF5AEB5AC" stRef:documentID="xmp.did:F34519B11D0E11EBB2B0D53EF5AEB5AC"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>zqq.....IDATx..].|.....F..)I *E.... H..R..~.....R...,O...~<.i....R.PD.....E.H.LO...w...@HO..^~.dw.....3BUU..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\getapp-47[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 126 x 120, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	12822
Entropy (8bit):	7.966411077639622
Encrypted:	false
SSDEEP:	192:TgVXp5vlTWBdjdEEFEsyhha9A3g4/ibKYMwo72InsKn29kbG8MZ253A/FZ7P+B:6XHvlW/dzEs6wJYi+gfInsK2QU0RaZqB
MD5:	41E6432D06B5D72712D079B8A3204050
SHA1:	4FB4F7C6993B698DBFD608AD328A27CEEF9F45F8
SHA-256:	515EE55C689B7A9A6656EC88AC81EE3D5C72ED38E424E7154AF46BB8BF0D07A2
SHA-512:	D4D897C64C9A639CC8ED52DCEC1FEA56490551CC16B58C97610FDD879AD7EA26D5681B4D814FD2595AEF6344A775FFF969D8913912C78E668760FC217D54AD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/getapp-47.png
Preview:	.PNG.....IHDR...~...x.....4zF.....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-c138 79.159824, 2016/09/14-01:09:01 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:DocumentID="xmp.did:5E9BBECB1D0F11EBA35FDD3B94A67EE4" xmpMM:InstanceID="xmp.iid:5E9BBECA1D0F11EBA35FDD3B94A67EE4" xmp:CreatorTool="Adobe Photoshop CC 2017 (Windows)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:45AD9CBF1C5C11EBAF8DEB957FA5C63A" stRef:documentID="xmp.did:45AD9CC01C5C11EBAF8DEB957FA5C63A"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>(..T....IDATx..].x.W.>...F\ ./...k...."-V4....I.$.....Pj@.....%$h.I n..y..,K.O../.<aG...c.{G.V.I...5.~...7=..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\help-desk[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	7423
Entropy (8bit):	4.394913339442646
Encrypted:	false
SSDEEP:	192:domIb/TxKY5UU8EAK5IxhftbBvmfbYvi3rnaiVQYA7a:dnIb7IxEAK5Ixhrvmf5rnaw
MD5:	F987FA0FF4AE98D2AEF1E8060894CAD2
SHA1:	35E1CFDA95CC2F6AAE5A59D97FC2C11A6780E57C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\help-desk[1].svg	
SHA-256:	AD344390DB83AB37B01C1EECE95369B82FFB5E3E3EAAEBDE50F9802356EB099F
SHA-512:	C5EB5473D3F8A073AB1288ED7E8724E080DE98569F54DB86D2B965139F5B1A149BD7BFBAADCC2B5C4EA5AA4A2D9E0D1FBD022DA1848A0E0EF026B14CE0FBA 2DD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/help-desk.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 21.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 70 70" style="enable-background:new 0 0 70 70;" xml:space="preserve">..<style type="text/css">....st0{fill:#E6E7E8;}....st1{fill:#0089EF;}....st2{fill:#6DC9F7;}....st3{fill:#FFFFFF;}....st4{fill:#FA759E;}....st5{fill:#FFD7E5;}....st6{ fill:#3A2C60;}..</style>..<g>...<path class="st0" d="M62,9.2H50.1c-0.3,0-0.6,0.2-0.6,0.6v10.7H27.4v-3.8c0-1.8-1.5-3.3-3.3-3.3H7.4c-1.8,0-3.3,1.5-3.3,3.3v9.7....c0,1.8,1.5 ,3.3,3.3,3.3h5.5v3.6c0,0.2,0.1,0.4,0.3,0.5c0.1,0,0.1,0,0.2,0c0.1,0,0.3,0,0.4-0.1l1.8-1.6v4c-4.3,0.3-7.5,4-7.2,8.3....c0.1,1.8,0.8,3.4,2,4.8c-3,0.8-5,3.5-5,6.5v5.6C5.4,62. 3,6.1,63,7,63h55c3.4,0,6.2-2.8,6.2-6.2V15.3C68.2,11.9,65.4,9.2,62,9.2z"/>...<path class="st1" d="M59.8,18.7H24.6v5.3c0,1.5-1.2,2.8-2.8,2.8H16l-2.1,1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\index-bg[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1440 x 286, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	172512
Entropy (8bit):	7.987788863670359
Encrypted:	false
SSDEEP:	3072:N5t3HDBkB8rLcLavIvDeMBY2tLVBQ82GyqDUBLFdt7936rKRco:Nv3HDSBU0RvDemVtc8XQxbf31uo
MD5:	BBF9CD031055746B47C0204D4CC63D04
SHA1:	4E3D2A8999A5A439DF7D90917426ED89326A3597
SHA-256:	CD861D2E7864A593466E921C2C187AF6504EE840F06D2B52836D8AA6FB1F15C7
SHA-512:	11C8295C37308C7BE1D090AC4011D527B8EC83EB37313AA7665143DD3858E897BD88BE7C0DE4FFF7724461E030B0C36492AF65679D167C08B924FA045F858398
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/index-bg.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-c138 79.159824, 2016/09/14-01:09:01 "> <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 2017 (Windows)" xmpMM:InstanceID="xmp.iid:9D1BCF3D1AC211EBBB0BBA3D49365089" xmpMM:DocumentID="xmp.did:9D1BCF3E1AC211EBBB0BBA3D49365089"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:9D1BCF3B1AC211EBBB0BBA3D49365089" stRef:documentID="xmp.did:9D1BCF3C1AC211EBBB0BBA3D49365089"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.P.k...PIDATx..rcI.-...Z.....R.=.3.o.....L.t..JQ)...r+.~&.u....~.`$A...!.O....8.....p8.....p8....1m....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery-3.2.1.slim.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	69597
Entropy (8bit):	5.369216080582935
Encrypted:	false
SSDEEP:	1536:qNhEyjjTikEJO4edXXe9J578go6MWX2xkjVe4c4j2ll2Ac7pK3F71QDU8CuT:Exc2yjq4j2uYnQDU8CuT
MD5:	5F48FC77CAC90C4778FA24EC9C57F37D
SHA1:	9E89D1515BC4C371B86F4CB1002FD8E377C1829F
SHA-256:	9365920887B11B33A3DC4BA28A0F93951F200341263E3B9CEFD384798E4BE398
SHA-512:	CAB8C4AFA1D8E3A8B7856EE29AE92566D44CEEAD70C8D533F2C98A976D77D0E1D314719B5C6A473789D8C6B21EBB4B89A6B0EC2E1C9C618FB1437EBC77D3A 269
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://code.jquery.com/jquery-3.2.1.slim.min.js
Preview:	/*! jQuery v3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_evalUrl,-event/ajax,-effects,-effects/Tween,-effects/animatedSelector | (c) JS Foundation and other contributors | jquery.org/license */!function(a,b){"use strict";"object"==typeof module &&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_e

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\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):	85578
Entropy (8bit):	5.366055229017455
Encrypted:	false
SSDEEP:	1536:EYE1JVoiB9JqZdXXe2pD3PgoIiulrUndZ6a4tfOR7WpfWBZ2BJda4w9W3qG9a986:v4J+OlfOhWppCW6G9a98Hr2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery.min[1].js	
MD5:	2F6B11A7E914718E0290410E85366FE9
SHA1:	69BB69E25CA7D5EF0935317584E6153F3FD9A88C
SHA-256:	05B85D96F41FFF14D8F608DAD03AB71E2C1017C2DA0914D7C59291BAD7A54F8E
SHA-512:	0D40BCCAA59FEDECF7243D63B33C42592541D0330FEFC78EC81A4C6B9689922D5B211011CA4BE23AE22621CCE4C658F52A1552C92D7AC3615241EB640F8514B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js
Preview:	/*! jQuery v2.2.4 | (c) jQuery Foundation | jquery.org/license */!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProperty,l={},m="2.2.4",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:e.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a){return n.each(this,a)},map:function(a){return this.pushStack(n.map(this,function(b,c){return a.call

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\landing-pages[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	7552
Entropy (8bit):	4.758372599124537
Encrypted:	false
SSDEEP:	192:doQ/NumYiX/mxJXM4N3B0wlVR6HYU+afWavawyaA5sS2C0:dpUmHX/mxJc4N3uFR6HYU+afWavawyaP
MD5:	84A8AD252F9958742FD8CF69932AFFE1
SHA1:	7B6E99513CD0141BF92084EC00F809F6E2A72727
SHA-256:	67F53748F67E587C234779029F6B10F100FA823CA917114372797EAAED48D4DC
SHA-512:	D1B54EF23CA30F2954A82F0D77FCFAA9E7D53CEE730AB5A6B7BD930EF168144257197BBF432243F29C7437B997597CFCD1C8A542FE5342B29522447D4E3C069
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/landing-pages.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 21.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 70 70" style="enable-background:new 0 0 70 70;" xml:space="preserve">..<style type="text/css">....st0{fill:#E6E7E8;}....st1{fill:#6DC9F7;}....st2{fill:#D4FBFF;}....st3{fill:#FFFFFF;}....st4{fill:#0089EF;}....st5{fill:#FA759E;}....st6{fill:#3A2C60;}....st7{fill:#FF7D95;}....st8{fill:#CBF4FB;}....st9{fill:#D0F2D2;}....st10{fill:#A0E5A5;}..</style>..<g>...<path class="st0" d="M63,9H9.3c-2.5,0-4.4,2-4.5,4.5v36.9c0,2.5,2,4.4,4.5,4.5h20.5l-1,6.7h-5.2c-1,0-1.8,0.8-1.8,1.8v0.1....c0,1,0.8,1.8,1.8,1.8h25.1c1,0,1.8-0.8,1.8-1.8v-0.1c0-1-0.8-1.8-1.8-1.8h-5.2l-1-6.7H63c2.5,0,4.4-2,4.5-4.5V13.5....C67.4,11,65.4,9.1,63,9z"/>...<path class="st1" d="M7,7.4h53.7c2.2,0,3.9,1.7,3.9,3.9v36.9c0,2.2-1.7,3.9-3.9,3.9H7c-2.2,0-3.9-1.7-3.9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\leadgrabbers[1].json	
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):	2242
Entropy (8bit):	5.103788838054876
Encrypted:	false
SSDEEP:	48:2cc3PmHRYjq+FdF3tfmQEutf62CexUIQZlQDQ6SuIpBXU:2ccfw2F1FtzCeBDQnZo
MD5:	0A68E4779703CBBC3794E0F8B22EB9EB
SHA1:	0461B544EBE0D365ABE7F2F5759B68B192D0691D
SHA-256:	F05194179059EEFC22BF8A7384F97BE205D9712024468B936EFDFE0D0A97C652
SHA-512:	B9597F1F221FC4F0EDDC6D31607358971A0EB20CCE1185909190E56223902DBAB6EC7929CCB6419E6EAEB75DBD21BE75A6B97BC4A64102EFB549917F8035EC5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://app.engagebay.com/jsapi/rest/leadgrabbers?apiKey=260ad2gtu21qgp99vcfa1vkhmo
Preview:	[{"created_time":0,"updated_time":0,"is_popup_callout":true,"isEnableEmail":true,"is_recaptcha_enabled":false,"disable":false,"rules":[],"or_rules":[],"webRules":[],"webAutomations":[],"addCountryAsTag":false,"addCityAsTag":false,"userIds":[],"version":"v1","formStats":{"totalVisitors":0,"uniqueVisitors":0,"totalContacts":0,"refreshContacts":false,"mobile":0,"desktop":0,"created_time":0,"updated_time":0},"pushContactToURL":true,"spamDetected":false,"email_domain_settings":{"free_service_domains":false},"formOwner":{"id":5652407104045056,"domain_id":6014394531053568,"email":"nicole@mobileagency.com","password":"a490293055c84b2c530e7f14a5d391a3","password_decrypted":"","name":"Nicole Frida","created_time":1617901360,"updated_time":1617996394,"is_admin":true,"is_verified":true,"is_owner":true,"job_title":"","role":"other","phone_number":"+1800-458-4320 ","language":"en","time_zone":"Africa/Algiers","time_format":"24","loggedin_time":1617972937,"logging_in":false,"bcc_email":"fgfceahbaeaef

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\lilahbulock-4[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 520 x 460, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	194091
Entropy (8bit):	**7.991953546522532**

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\lilahbulock-4[1].png	
Encrypted:	**true**
SSDEEP:	3072:nI7vK3uWDOpioWqGV1fOBmJoZgWnCyzliXVmZ9vwCqE1xLXLS7kOGc3xxoZ0+FKg:swDoWqGV1laZrQKpwCqE7jLSQe33O+v4
MD5:	7B3DD494033416C973E80521B085C590
SHA1:	F07B97CCF56A448699496E963119DA17F9D8BC1E
SHA-256:	0C01E33DEED757631C0498B810D683EA6B7B25CF11511771C26406785F9357B8
SHA-512:	D3220FFE8258AF24158BFC0CCB5E7B73C053FF0CCE89FF4B59AD554A27EA45C0361FCADA72F136370D1F5CB59B26F4BCB4AC4F75DEEF98C65FE3F9B11FA59 11
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/lilahbulock-4.png
Preview:	.PNG.....IHDR.....mP\....tEXtSoftware.Adobe ImageReadyq.e<...niTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c138 79.159824, 2016/09/14-01:09:01 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:271a6474-c4c2-bd4d-95b3-de2544db1b77" xmpMM:DocumentID="xmp.did:64D3C6A71A9F11EB9D82B43902815010" xmpMM:InstanceID="xmp.iid:64D3C6A61A9F11EB9D82B43902815010" xmp:CreatorTool="Adobe Photoshop CC 2017 (Windows)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:0088215E1A9C11EB86B5F4A814094F0E" stRef:documentID="xmp.did:0088215F1A9C11EB86B5F4A814094F0E"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.[.q...SIDATx....T....wz....R....D.i..O.h.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\live-chat[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	2673
Entropy (8bit):	5.017914360878234
Encrypted:	false
SSDEEP:	48:c4A+fES861YNpn1ilpKG0Erjb2FDLxNQWAzxzp94yN7ZAWmaG:s+foJNVGJjb2F/xNqlNWyN7ZAWmaG
MD5:	CD76F5A6B9BC20039333BA83877A67CD
SHA1:	9931C02B4B7A473EDBBA74D60FC3D8B680EF64D8
SHA-256:	0251D6517C0DE7101A66973F43A98CFBCF945610150C84D68BA1BB07DAB21811
SHA-512:	71ACE59C4A0BCADBE9BEA5AF8E6F1B7EC3DE5FED80A8E6A20C728947C89ECD070EED5B6F40573C5063090846AAB4878BE79C0075068A875A4B253B116D7876 50
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/live-chat.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 21.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 70 70" style="enable-background:new 0 0 70 70;" xml:space="preserve">..<style type="text/css">....st0{fill:#E6E7E8;}....st1{fill:#FA759E;}....st2{fill:#FFFFFF;}....st3{fill:#0089EF;}....st4{fill:#3A2C60;}....st5{fill:none;}....st6{fill:none;stroke:#FFFFFF;stroke-miterlimit:10;}..</style>..<g>...<path class="st0" d="M60.5,18.7h-1.8v-5.4c0-4-3.2-7.2-7.2-7.2H11.8c-4,0-7.2,3.2-7.2,7.2v23c0,4,3.2,7.2,7.2,7.2h1.8v5.4....c0,4,3.2,7.2,7.2,7.2h13.8L45.7,66c0.2,0.2,0.6,0.2,0.8,0c0.1-0.1,0.1-0.2,0.1-0.4v-9.4h13.8c4,0,7.2-3.2,7.2-7.2v-23....C67.7,21.9,64.4,18.7,60.5,18.7z"/>...<path class="st1" d="M18.5,17h39.7c3.7,0,6.6,3,6.6,6.6c0,0,0,0,0v23c0,3.7-3,6.6-6.6,6.6c0,0,0,0,0,0H43.9v10l-11.3-10h-14....c-3.7,0-6.6-3-6.6-6.6c0,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\milestone-tracking[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	4449
Entropy (8bit):	4.61320211891341
Encrypted:	false
SSDEEP:	96:s+foc8tljOEiDaczqJshuqw1wyzlbCtjXw0Zgt7QV:doS8HRYAgV
MD5:	D403DBE3705A5464B0BA061B175F3CC8
SHA1:	0795CBE2E4FB501768161C519D19B8366AEFFC32
SHA-256:	E10F0893760492AA271FA24B3933FC9C5781471846400E86B09CA07470D1ABD3
SHA-512:	391B98E5CB384CAB50BD02FFA657D2EC1C44632B7449D92C4F189DB402B986A539CF532051CD0F384C3A94023E28298D79EB4864D40AC5BDB49D5882900419D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/milestone-tracking.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 21.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 70 70" style="enable-background:new 0 0 70 70;" xml:space="preserve">..<style type="text/css">....st0{fill:#E6E7E8;}....st1{fill:#D4FBFF;}....st2{fill:#0089EF;}....st3{fill:#3A2C60;}....st4{fill:#FA759E;}....st5{fill:#2196F3;}..</style>..<path class="st0" d="M64.2,36.1C64.1,21.9,53.6,10,39.6,8.2l0.1-0.1c0.9-0.7,1.1-2,0.3-3c-0.7-0.9-2-1.1-3-0.3l0,0l-4.3,3.4...c-0.4,0.3-0.7,0.8-0.8,1.3C19.6,11.4,10.2,21.7,9.3,34.3c-0.8,0.2-1.4,0.9-1.4,1.8C8,50.3,18.7,62.3,32.8,64l0,0...c-0.9,0.7-1.1,2-0.3,3s2,1.1,3,0.3l4.3-3.4c0.4-0.3,0.7-0.8,0.8-1.4C52.7,60.4,62,50.2,62.8,37.8C63.6,37.6,64.2,36.9,64.2,36.1z"/>..<circle class="st1" cx="33.9" cy="34" r="26.3"/>..<path class="st2" d="M36.2,6.5l1.1-0.9C38,5,38.1,4,37.5,3.4C37,2.7,36,2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\min_v6[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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\min_v6[1].css	
Size (bytes):	2116
Entropy (8bit):	4.986653900154579
Encrypted:	false
SSDEEP:	24:T2DAPg2n1/kKUuf+5TVUeeEMID/5v9XQf9flgWOBXYhsOg0Nt0XO2D07ya/hAcld:CD7MHbHmJ9XQFcGbM2h1
MD5:	0001A59FB5DC223B9327003735A359B4
SHA1:	2E83DDF2239116E46CE84D5CB3BCFFC4152CD87E
SHA-256:	668C4EA01B5AD8F78A731AB245C4E23994EFB33D0A6F525D5B0F42828B2E2591
SHA-512:	D4439604390C6CEAAC1F585C3336A998C458C5AC3FC8F635A70914FFBAE935F6E40C3FDF06B4037380F4EBC7A521ADD2CD0B7B61B4F50F5CE5A5E17A3A0ABE EA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://d2p078bqz5urf7.cloudfront.net/jsapi/css/iframe/min_v6.css
Preview:	.engagebay-popup-iframe{border:0;position:fixed;height:100px;width:auto;min-width:410px;max-width:100%;max-height:100%;display:inline;z-index:16777271}@media screen and (max-width:480px){.engagebay-popup-iframe{min-width:300px}}.engagebay-popup-iframe.popupbox{top:0;bottom:0;left:0;right:0;height:100%!important;width:100%!important}.engagebay-popup-iframe.fullform{background-color:#32303b}.engagebay-popup-iframe.slide-left,.engagebay-popup-iframe.slide-right{bottom:5px;top:auto}.engagebay-popup-iframe.dropdown{position:fixed;top:0;left:0;right:0;bottom:auto;width:100%!important}.engagebay-popup-iframe.slide-left{left:5px;right:auto}.engagebay-popup-iframe.slide-right{left:auto;right:5px}.engagebay-popup-iframe.engage-fadeInUp{-webkit-animation:fadeInUp .4s;-moz-animation:fadeInUp .4s;-o-animation:fadeInUp .4s;animation:fadeInUp .4s;animation-timing-function:linear}@-webkit-keyframes fadeInUp{0%{opacity:0;-webkit-transform:translateY(0)}1%{-webkit-transform:translateY(20px)}100%{opacity

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\oppointment-calendar[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	5593
Entropy (8bit):	4.690554308662805
Encrypted:	false
SSDEEP:	96:sQfoaAxY+YZYEYbYIYIYi1acHdadVv7LPySNteNvKNDTO7PPsPPOE0Clave:5oaAxDadeRrytV/ySNANvKN0PPsPPOUC
MD5:	08235146FFE7DBA63FDE21F2720DF8C1
SHA1:	7B705DF50BCC35CBA48409C7580BE493434D8256
SHA-256:	379FB96FA3D3C9C035722480D8CB34A2BE09B83CABC0BE8C39C761990B8CE3D5
SHA-512:	0F51C9B82A6F0C1DF07066D469B52927DF37797159F71A2B0205994426B668E519AB4F900378CE167EF90EECE3687D7D45872F53CEF20720F2CDAA51CBF3BF3F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/oppointment-calendar.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 21.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Capa_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 70 70" style="enable-background:new 0 0 70 70;" xml:space="preserve">..<style type="text/css">....st0{fill:#FFFFFF;}....st1{fill:#6DC9F7;}....st2{fill:#0089EF;}....st3{fill:#A5DDFF;}....st4{fill:#FA759E;}....st5{fill:#3A2C60;}..</style>..<path class="st0" d="M58,58.3v3.1c0,1.9,1.5,3.4,3.4,3.4l0,0c1.9,0,3.4-1.5,3.4-3.4v-46c0-2.7-2.2-4.8-4.8-4.8h-9.4H17.8h-3.6...c-2.7,0-4.8,2.2-4.8,4.8v42.9H58z"/>..<path class="st1" d="M58,61.4v-3.1l0,0H5.2v3.1c0,1.9,1.5,3.4,3.4,3.4h52.8l0,0C59.5,64.8,58,63.3,58,61.4z"/>..<path class="st2" d="M64.7,20.6H9.4v-5.2c0-2.7,2.2-4.8,4.8-4.8h45.7c2.7,0,4.8,2.2,4.8,4.8V20.6z"/>..<g>...<path class="st3" d="M31.4,48.8L31.4,48.8c-1.9,0-3.4-1.5-3.4-3.4l0,0c0-1.9,1.5-3.4,3.4-3.4l0,0c1.9,0,3.4,1.5

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\popper.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	19188
Entropy (8bit):	5.212814407014048
Encrypted:	false
SSDEEP:	384:+CbuG4xGNoDic2UjKPafxwC5b/4xQviOJU7QzxzivDdE3pcGdjkd/9jt3B+Kb964:zb4xGmiJfaf7gxQvVU7eziv+cSjknZ3f
MD5:	70D3FDA195602FE8B75E0097EED74DDE
SHA1:	C3B977AA4B8DFB69D651E07015031D385DED964B
SHA-256:	A52F7AA54D7BCAAFA056EE0A050262DFC5694AE28DEE8B4CAC3429AF37FF0D66
SHA-512:	51AFFB5A8CFD2F93B473007F6987B19A0A1A0FB970DDD59EF45BD77A355D82ABBBD60468837A09823496411E797F05B1F962AE93C725ED4C00D514BA40269D1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js
Preview:	/*. Copyright (C) Federico Zivolo 2017. Distributed under the MIT License (license terms are at http://opensource.org/licenses/MIT).. */(function(e,t){'object'==typeof exports&&'undefined'!=typeof module?module.exports=t():'function'==typeof define&&define.amd?define(t):e.Popper=t()})(this,function(){'use strict';function e(e){return e&&'[object Function]'==={}.toString.call(e)}function t(e,t){if(1!==e.nodeType)return[];var o=getComputedStyle(e,null);return t?o[t]:o}function o(e){return'HTML'===e.nodeName?e:e.parentNode||e.host}function n(e){if(!e)return document.body;switch(e.nodeName){case'HTML':case'BODY':return e.ownerDocument.body;case'#document':return e.body;}var i=t(e),r=i.overflow,p=i.overflowX,s=i.overflowY;return /(auto|scroll)/.test(r+s+p)?e:n(o(e))}function r(e){var o=e&&e.offsetParent,i=o&&o.nodeName;return i&&'BODY'!==i&&'HTML'!==i?-1!==['TD','TABLE'].indexOf(o.nodeName)&&'static'===t(o,'position')?r(o):o:e?e.ownerDocument.documentElement:document.documentElement}functio

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\products[1].svg	
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	5005
Entropy (8bit):	4.768067202450823
Encrypted:	false
SSDEEP:	96:s+foQKpnqHAUN/hMKNzZ9J2l5/GMR9jN6GpnnxMfE2boQytWG+8n3Xq5NNJdB:doQSqHLN/GKNUlJRC6niboP3Xq5/Jb
MD5:	3D700636847AB504CD624FA323CECF08
SHA1:	38AE4146A76F4DAB8C15CA176E3491831F679634
SHA-256:	BB148FFF89F8FA0BD196E6C156E8512CC38525F5E3AE568DD79DBD7DF167C6F7
SHA-512:	4FF37FA746A9A095C9651A44AFD0FEB859336B96A0906EA8B0BB27EACA9CC3F4FD8DCF69AA053C53E467E185F87CAD8C77F61F8E35005284FE0B87128E15A12D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/products.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 21.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 70 70" style="enable-background:new 0 0 70 70;" xml:space="preserve">..<style type="text/css">....st0{fill:#E6E7E8;}....st1{fill:#6DC9F7;}....st2{fill:#D4FBFF;}....st3{fill:#FFFFFF;}....st4{fill:#0089EF;}....st5{fill:#FA759E;}....st6{fill:#FFD7E5;}....st7{fill:#3A2C60;}..</style>..<g>...<path class="st0" d="M65.1,15.7c0-2.3-1.9-4.2-4.2-4.2h-13c-3.5-3.4-8.2-5.1-13-4.9c-4.5,0.2-8.6,2-11.6,4.9h-13....c-2.3,0-4.2,1.9-4.2,4.2v34.8c0,2.3,1.9,4.2,4.2,4.2h19.3l-0.9,6.3h-4.8c-0.9,0-1.7,0.8-1.7,1.7c0,0.9,0.8,1.7,1.7,1.7h23.5....c0.9,0,1.7-0.8,1.7-1.7s-0.8-1.7-1.7-1.7h-4.8l-0.9-6.3h19.3c2.3,0,4.2-1.9,4.2-4.2L65.1,15.7L65.1,15.7z"/>...<g>....<path class="st1" d="M8.1,52.1h50.7c2,0,3.7-1.6,3.7-3.7V13.6c0-2-1.6-3.7-3.7-3.7H8.1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\proposals[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	2879
Entropy (8bit):	4.972982710934913
Encrypted:	false
SSDEEP:	48:c4A+fES8bGM5As1QyMSscgluLcOvoj3U6v0w+L/SZ35lpvnqx7xny9o+oAUPCMQD:s+foiJsXMcgllOvN6vK+ZzpvnI7VyLoA
MD5:	3825385B9396AD109B8A19FA44666EB2
SHA1:	84CE72BA04DCCB1E3CBE14B1A1FAFA7F28FC2831
SHA-256:	F4B5E96D4036F0753950A2EFBDCEBBCA07E207102CCCB719F51DF85FDA6BB5D4
SHA-512:	304356D4AE81ED425175A1F35130DA58EF636EF97180C9F2265C42179095F15E9387CE12B3D1729B90ECFB80C39995CCB0F0BEAF430856BE363753C3EF8F8C58
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/proposals.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 21.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 70 70" style="enable-background:new 0 0 70 70;" xml:space="preserve">..<style type="text/css">....st0{fill:#E6E7E8;}....st1{fill:#0089EF;}....st2{fill:#FFFFFF;}....st3{fill:#FA759E;}....st4{fill:#6DC9F7;}....st5{fill:#3A2C60;}..</style>..<g>...<path class="st0" d="M59.3,52.5c3-3.2,2.8-8.3-0.5-11.3c-1.3-1.2-3.1-2-4.9-2.1V21.5c0-0.2-0.1-0.3-0.2-0.4L38.4,5.8....c-0.1-0.1-0.3-0.2-0.4-0.2H9.6c-0.9,0-1.7,0.8-1.7,1.7v57.5c0,0.9,0.8,1.7,1.7,1.7h53.1c0.9,0,1.7-0.8,1.7-1.7v-5.7....C64.4,56,62.3,53.3,59.3,52.5L59.3,52.5z"/>...<path class="st1" d="M51.1,19.3L35.8,4H7.3C6.7,4,6.2,4.5,6.2,5.1v57.5c0,0.6,0.5,1.1,1.1,1.1h42.6c0.6,0,1.1-0.5,1.1-1.1....L51.1,19.3L51.1,19.3z"/>...<g>....<path class="st2" d="M35.8,4H7.3C6.7,4,6.2,4.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\push-notifications[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	5070
Entropy (8bit):	4.580881359163553
Encrypted:	false
SSDEEP:	96:s+fomCqPshIRtODAmpClWSNewmD9ceDyApDFd004/EG148UOkZQWHK0tGHvTYLg:domCqPEIRwkmpCIIR5gn/jW0pKGLYE
MD5:	1E6E20150CFA21B0EFB026716438A017
SHA1:	3904D553DC5EB1B682D5EC6DDF358CE43F074850
SHA-256:	96E2F6BA1F7901927B42D5B352BFFF0A840AF95E98A241D68C92F25B08331C01
SHA-512:	D7B590A134747DB5F82D81A7608C2FB177A5E5CF6281B2F1F7585A5ACC9141D097876709BE5E4D287F2E1AAA0AFA436CDDBD5FDA7F0D1B2B7637A777303AAEB6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/push-notifications.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 21.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 70 70" style="enable-background:new 0 0 70 70;" xml:space="preserve">..<style type="text/css">....st0{fill:#E6E7E8;}....st1{fill:#0089EF;}....st2{fill:#6DC9F7;}....st3{fill:#FFD7E5;}....st4{fill:#FFFFFF;}....st5{fill:#3A2C60;}....st6{fill:#FA759E;}....st7{fill:#F6F3FF;}..</style>..<path class="st0" d="M62.7,42.7c-0.6-0.1-1.3,0.1-1.8,0.4c-0.1-1.5-1.3-2.8-2.8-3c-1.1-0.1-2.2,0.4-2.9,1.4c-1-1.4-2.9-1.8-4.3-0.9...c-0.1,0.1-0.1,0.1-0.2,0.2v-1.6c6-11.5,1.6-25.6-9.9-31.6S15.1,6.1,9.1,17.5S7.5,43.2,19,49.1c6.2,3.2,13.5,3.5,19.9,0.8v3.9...c0,7.4,6,13.3,13.3,13.3,13.3s13.3-6,13.3-13.3V46C65.7,44.3,64.4,42.9,62.7,42.7L62.7,42.7z"/>..<circle class="st1" cx="27.7" cy="26.2" r="22.9"/>..<circle class="st2" cx="27.7" cy="26.2" r="18.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\segmentation[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	10976
Entropy (8bit):	4.3535612272928415
Encrypted:	false
SSDEEP:	192:doQH4neLX7JuxEvwxq/rFOIX1b7bRh0ZKoSa8mhoHnT/:dpcGc4slXdfX9a8mhoHT/
MD5:	1878D12814037896AF2A07EECFCC773C
SHA1:	DFF93070B23742301AEE8F7D2BD29838D65372C9
SHA-256:	64C5976B2E541EBBAE8AA6730DDC282C4007D5658F00D5F4A0E7D4923CFAE2FB
SHA-512:	D37E577A04F6EF1F688DD585FC61EA92EDFAD20508251C6794CBA2CB5A5C90374715AA7404A10287F7CFB51331E486B1158366797DE9226505577A85EEAA5FF5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/segmentation.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 21.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 70 70" style="enable-background:new 0 0 70 70;" xml:space="preserve">..<style type="text/css">....st0{fill:#E6E7E8;}....st1{fill:#6DC9F7;}....st2{fill:#FFD7E5;}....st3{fill:#FFFFFF;}....st4{fill:#FA759E;}....st5{fill:#3A2C60;}..</style>..<circle class="st0" cx="36.1" cy="36.1" r="17.1"/>..<path class="st0" d="M34.4,11.1v4.4c0,0.9,0.7,1.7,1.7,1.7s1.7-0.7,1.7-1.7v-4.4c0.7,0.6,1.6,0.5,2.3-0.1c0.6-0.6,0.6-1.7,0-2.3...l-2.8-2.8c-0.7-0.6-1.7-0.6-2.3,0l-2.8,2.8c-0.6,0.6-0.6,1.7,0,2.3C32.8,11.6,33.8,11.6,34.4,11.1L34.4,11.1z"/>..<path class="st0" d="M37.7,61.1v-4.4c0-0.9-0.7-1.7-1.7-1.7s-1.7,0.7-1.7,1.7v4.4c-0.7-0.6-1.6-0.5-2.3,0.1...c-0.6,0.6-0.6,1.7,0,2.3l2.8,2.8c0.6,0.6,1.7,0.6,2.3,0c0,0,0,0,0,0l2.8-2.8c0.6-0.6,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\site-messages[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	2491
Entropy (8bit):	5.0521988110368765
Encrypted:	false
SSDEEP:	48:c4A+fES86n1+BevH3PldLIkp8I8KSFb6QydRBc8ezHUlqMlLRCU:s+fo24MNBLyYRJeoIv0U
MD5:	E11EEA4BE9174535E2068C6C8916F6F4
SHA1:	36830A936E65842EDA41D51BBB9CAF02F2C6F4B2
SHA-256:	EEFF9069DB1C8CBF81C65C26C6185682ADB4E338504C7CAAD960E32FAFF8AB85
SHA-512:	A54F71D5F9EBC3DDE231E1EE4815227BA913032833AE05E83032511B627A0D6FB44217FD4A26D7C6A32F00A12C921678BF12607C6926CB75B5E90E3088FA2434
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/site-messages.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 21.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 70 70" style="enable-background:new 0 0 70 70;" xml:space="preserve">..<style type="text/css">....st0{fill:#E6E7E8;}....st1{fill:#FA759E;}....st2{fill:#FFFFFF;}....st3{fill:#6DC9F7;}....st4{fill:#3A2C60;}..</style>..<path class="st0" d="M63.5,31.8H41.2c-2.5,0-4.5,2-4.5,4.5v12.9c0,2.5,2,4.5,4.5,4.5h7.3v4.8c0,0.4,0.3,0.8,0.8,0.8...c0.2,0,0.4-0.1,0.5-0.2l6.1-5.4h7.6c2.5,0,4.5-2,4.5-4.5V36.3C68, 33.8,66,31.8,63.5,31.8z"/>..<path class="st0" d="M36.2,37.8V24.8c0-2.5-2-4.5-4.5-4.5H9.4c-2.5,0-4.5,2-4.5,4.5v12.9c0,2.5,2,4.5,4.5,4.5H17l6.1,5.4...c0.3,0.3,0.8,0.3,1.1-0.1c0.1-0.1,0.2-0.3,0.2-0.5v-4.8h7.3C34.2,42.2,36.2,40.2,36.2,37.8z"/>..<path class="st1" d="M60.4,29.5H38.1c-2.1,0-3.7,1.7-3.7,3.7c0,0,0,0,0,0v12.9c0,2.1,1.7,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\sms-broadcast[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3122
Entropy (8bit):	4.76616231188095
Encrypted:	false
SSDEEP:	48:c4A+fES86AxlXSXoOmThXKgWlQSTKVMIb7ELh45qzYeEbD3ctuAM/IrG92jFz:s+fo+z2aT0ODdYqzf6guAM/IrK2h
MD5:	506A28ED609BA580B52E616B89EC0E2F
SHA1:	0A44CFA6F7EC72617C8C8C754C68DE9C9361156C
SHA-256:	3478C6A1A05AE12B24F294E439EFC6406F95733429F286A737D9B6FC633DBC52
SHA-512:	3050F54ABBC41E26C70EABA9FE94AF673B93F889F1EB987267E1B680A5CEAAFEC8B536CD5CCC7F7753523D6BD4BE8E4C85045A3A3D30A56BD1D1EC4AAD13203E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/sms-broadcast.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 21.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 70 70" style="enable-background:new 0 0 70 70;" xml:space="preserve">..<style type="text/css">....st0{fill:#E6E7E8;}....st1{fill:#FA759E;}....st2{fill:#FFFFFF;}....st3{fill:#0089EF;}....st4{fill:#3A2C60;}..</style>..<path class="st0" d="M60,19h-1.8v-5.3c0-3.9-3.2-7-7-7h-39c-3.9,0-7,3.2-7,7v22.6c0,3.9,3.2,7,7,7H14v5.3c0,3.9,3.2,7,7,7h13.6...l10.9,9.7c0.2,0.2,0.6,0.2,0.8,0c0.1-0.1,0.1-0.2,0.1-0.4v-9.2H60c3.9,0,7-3.2,7-7V26.1C67,22.2,63.9,19,60,19z"/>..<path class="st1" d="M18.8,17.4h39c3.6,0,6.5,2.9,6.5,6.5c0,0,0,0,0,0v22.6c0,3.6-2.9,6.5-6.5,6.5c0,0,0,0,0,0H43.7v9.8l-11.1-9.8...H18.8c-3.6,0-6.5-2.9-6.5-6.5c0,0,0,0,0,0V23.9C12.3,20.3,15.3,17.4,18.8,17.4z"/>..<path class="st2" d="M57.8,17.4h-1.7c3.6,0,6.5,2.9,6.5,6.5

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\social-posts-scheduling[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	4309
Entropy (8bit):	5.146109541586964
Encrypted:	false
SSDEEP:	48:c4AQfES8QfSyJYwf578JF63KltsEG74VTPTkmWwJxJgitRIli/4BXs3lK/4j7v0l:sQfoQvJYm6sJw1BINE/9mwA6dp
MD5:	49CB329371E9CD0D316701F78E667C16
SHA1:	2EEA0E39D51E018FE683CE03411D963247561CD5
SHA-256:	C8AC026A3665A57E5AC962AFD88664B07BCBF8842C6EC319BF1E7015C080C03F
SHA-512:	18F5E4C496A61115FA9C6F85E3ED33CF8F92470464BFCE8A435F0882DABE64A1D2F83B3B869E25637E2A6389988C19849B2E76CDF11B682163176BE3389808EB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/social-posts-scheduling.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 21.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Capa_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 70 70" style="enable-background:new 0 0 70 70;" xml:space="preserve">..<style type="text/css">....st0{fill:#E6E7E8;}....st1{fill:#6DC9F7;}....st2{fill:#3A2C60;}....st3{fill:#FFFFFF;}....st4{fill:#FA759E;}....st5{fill:#0089EF;}.. </style>..<circle class="st0" cx="35" cy="35" r="31.7"/>..<rect x="4.3" y="4.3" class="st1" width="41.9" height="57.6"/>..<path class="st2" d="M45.2,61.9h-40c-0.6,0-0.9-0.4-0.9-1V5.3c0-0.6,0.4-1,0.9-1h40c0.6,0,0.9,0.4,0.9,1V61...C46.2,61.5,45.7,61.9,45.2,61.9z M5.3,60.9h39.9V5.3H5.3V60.9z"/>..<rect x="8.3" y="8.3" class="st3" width="34" height="49.7"/>..<g>...<polygon class="st4" points="14.8,40.1 12.1,37.5 13.3,36.3 14.8,37.9 18.4,34.4 19.5,35.5 ."/>...<polygon class="st2" points="14.8,51.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\social-suite[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	16391
Entropy (8bit):	4.358419700219709
Encrypted:	false
SSDEEP:	384:dpv3CPQ2cwPNq8rbTC+62LYzxMlMKYzM5Y7mFGOEcaAi4zO+K:TmcOZm+6CYzxMlMKYKEOjaz
MD5:	2DF39EF2F5ACCD63CA2A4482D1545C03
SHA1:	4ABB93122327C9BD2A4DB7BFD47D28E17E113958
SHA-256:	D814C1010C55AEB4BE1A3735C3F362347A94CEB459F80943A85E9BE7D65A2873
SHA-512:	0FCDB8C6D897A08755B855C856E2A151E13258C168143C187CACB9DB44BE71C97DBA544DF162EA36ACE91CD7181FBD2D254BE31B62F16CCA6A0B662350CC46D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/social-suite.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 21.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 70 70" style="enable-background:new 0 0 70 70;" xml:space="preserve">..<style type="text/css">....st0{fill:#E6E7E8;}....st1{fill:#6DC9F7;}....st2{fill:#FFD7E5;}....st3{fill:#FFFFFF;}....st4{fill:#FA759E;}....st5{fill:#3A2C60;}....st6{fill:#D4FBFF;}....st7{fill:#0089EF;}....st8{fill:#FCEBF9;}....st9{fill:#90D8F9;}..</style>..<circle class="st0" cx="36.1" cy="36.1" r="17.1"/>..<path class="st0" d="M34.4 ,11.1v4.4c0,0.9,0.7,1.7,1.7,1.7s1.7-0.7,1.7-1.7v-4.4c0.7,0.6,1.6,0.5,2.3-0.1c0.6-0.6,0.6-1.7,0-2.3...l-2.8-2.8c-0.7-0.6-1.7-0.6-2.3,0l-2.8,2.8c-0.6,0.6-0.6,1.7,0,2.3C32.8 ,11.6,33.8,11.6,34.4,11.1L34.4,11.1z"/>..<path class="st0" d="M37.7,61.1v-4.4c0-0.9-0.7-1.7-1.7-1.7c-0.9,0-1.7,0.7-1.7,1.7v4.4c-0.7-0.6-1.6-0.5-2.3,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\sticky-bars[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3787
Entropy (8bit):	4.920460852237317
Encrypted:	false
SSDEEP:	96:s+foQL7lfBP9Ia6fi5mlCi0tvWi5pUb2JgzRe1gyk9rNqFT:doQ9fBP9Ia68sOUbDRxtUT
MD5:	DC6919F7E886C2226076E0CDA5B96147
SHA1:	0C547FF384BECD5769DB67E269650E7C01AD1137
SHA-256:	18E1AE3A649B11C45A5A01040BF996D28FEB5F3768F9F96567EAE3189E12C549
SHA-512:	5A94403389B49CF4E9DEE864393C494BB7B4E6FE26019B6B9D9A1A5450D70381D0DF55F304CCFF8694872940C1DE3F68A507A86DDE5A1C12A44CD04930651A9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/sticky-bars.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 21.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 70 70" style="enable-background:new 0 0 70 70;" xml:space="preserve">..<style type="text/css">....st0{fill:#E6E7E8;}....st1{fill:#6DC9F7;}....st2{fill:#D4FBFF;}....st3{fill:#FFFFFF;}....st4{fill:#0089EF;}....st5{fill:#FA759E;}....st6{fill:#3A2C60;}..</style>..<path class="st0" d="M64.5,7.1H8.4c-2.5,0-4.6,2.1-4.6,4.6v38.1c0,2.5,2.1,4.6,4.6,4.6h21.2l-1,7h-5.3c-1,0-1.8,0.8-1.8,1.8l0,0v0.1...c0,1,0.8,1.8, 1.8,1.8h25.9c1,0,1.8-0.8,1.8-1.8v-0.1c0-1-0.8-1.8-1.8-1.8h-5.3l-1-7h21.8c2.2,0,4-1.8,4-4V11.2...C68.5,8.9,66.7,7.1,64.5,7.1z"/>..<path class="st1" d="M6.1,5.4h55.5c2.2,0, 4,1.8,4,4v38.1c0,2.2-1.8,4-4,4H6.1c-2.2,0-4-1.8-4-4V9.4C2.1,7.2,3.9,5.4,6.1,5.4z"/>..<path class="st2" d="M61.6,5.4H6.1c-2.2,0-4,1.8-4,4v34.3h63.6V9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\task-management[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	7802
Entropy (8bit):	4.511282101523211
Encrypted:	false
SSDEEP:	192:5okGZy36tuZymNNOKFNaul/mNO6g8U+LxwYbJ:5XGZy3lYmnOKFNNGmNO/8U8wYbJ
MD5:	C42CF185EC63E6E36490480D2438E25A
SHA1:	7081BE184D9C68129BE52B9EF6D13184A5869085
SHA-256:	8661ED32D35E37905FD4CBD72B23CBC265D41E91B6C8E04926470C8D79CA5F0D
SHA-512:	4664909636A158BB53D93AB7DEF76ADC9CEBE6D857302C37A5648026FD7CA1CB3266843CA6C034C78AB16F83F09D2F5E4A4F7CCF7C4332540F3EB226C097C0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/task-management.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 21.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Capa_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 70 70" style="enable-background:new 0 0 70 70;" xml:space="preserve">..<style type="text/css">....st0{fill:#E0E4E8;}....st1{fill:#0089EF;}....st2{fill:#3A2C60;}....st3{fill:#FFFFFF;}....st4{fill:#FA759E;}....st5{fill:#183651;}....st6{fill:#6DC9F7;}..</style>..<path class="st0" d="M24.5,45.5c-9.6-9.6-9.6-25.3,0-34.9s25.3-9.6,34.9,0s9.6,25.3,0,34.9S34.1,55.1,24.5,45.5z"/>..<path class="st1" d="M33.9,40.9l-4.8-4.8L6.4,55.3C3.7,57.6,3.6,61.6,6,64c2.5,2.5,6.4,2.3,8.7-0.4L33.9,40.9z"/>..<g>...<path class="st2" d="M10.3,66.7L10.3,66.7c-1.9,0-3.6-0.7-4.9-2c-2.9-2.9-2.7-7.5,0.4-10.2l22.7-19.1c0.4-0.3,1-0.3,1.3,0,1....l4.8,4.8c0.4,0.4,0.4,1,0.1,1.3L15.5,64.2C14.2,65.8,12.2,66.7,10.3,66.7z M29.1,37.5L7.1,56c-2.3,1.9-2.4,5.3-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\911384212383388[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	246518
Entropy (8bit):	5.467422541475686
Encrypted:	false
SSDEEP:	6144:Rk1HWCSntDV/H4K3V/H486EPjQHWuH3Hpo:f6El
MD5:	A4B38042EA6ACE06DE774822C0346D88
SHA1:	6B179A042BAFFD8274549E3EAC2B3B567D0DC961
SHA-256:	881F531E943E1496414116389246A0815362C561C555CD4B3CB1B8D17B8499A4
SHA-512:	F309384992431EB6311A69011D7E83AD4AB61E624644CDA5913B9AD55791A04965AC544DAF58B14ECD939EA86CC55C4F86975B549E01EE9EB08D8C698CC3C4E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://connect.facebook.net/signals/config/911384212383388?v=2.9.33&r=stable
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\FollowCompany[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	1630
Entropy (8bit):	5.1957508424564764
Encrypted:	false
SSDEEP:	24:hvsvD4HClxGliZalfPxpfbUrdFiRm16oC2XbzhDmqRbUJVVo9bukqGIFFz4lUQwQ:w4Hrcx1+dFiRm1Z7DmqhUJDolukq14l1
MD5:	472A699A8847E1EF87B45DFF6868F7C1
SHA1:	2FA81EBAD1028352EB6EE3F058833F50027AC398
SHA-256:	73FDCDC4063F0C09E3F16E1A3FA2C0DCBE4C037DEA7737F9BC12A634DF311C24
SHA-512:	C03AD6256DA5B764F8B31B4032C2C4A02F6DDE50D30A80B3D1A6FE74001EE31B6F44511747C685ECF3B94B68D0F8EC319BBD92F8DA07395B74884F0990E6727
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.. . .. <html>. <head>. <meta charset="UTF-8">. <link rel="stylesheet" href="https://static-exp1.licdn.com/sc/h/dijojhtrim9upz6fkl56xvl3m">. <script src="https://platform.linkedin.com/xdoor/scripts/in.js#mode=sdk" type="application/javascript"></script>. </head>.. <body>. . . <svg viewbox="-12 -10 60 60" x="0" y="0" preserveaspectratio="xMinYMin meet" class="logo">. <rect width="28" height="28" x="5" y="5" class="fill-white"></rect>. <g class="fill-blue">. <path d="M34.5,3H5.6C4.2,3,3,4.1,3,5.4v29.1C3,35.9,4.2,37,5.6,37h29C35.9,37,37,35.9,37,34.6V5.4C37,4.1,35.9,3,34.5,3zM13,32H8V16h5V32zM10.5,13.9c-1.9,0-3.4-1.5-3.4-3.4c0-1.9,1.5-3.4,3.4-3.4s3.4,1.5,3.4,3.4C13.9,12.4,12.4,13.9,10.5,13.9zM32,32h-5v-7.9c0-2.4-1-4-2.6-4c-2.3,0-3.4,2.1-3.4,4.6V32h-5V16h5v2.1c0.8-1.4,2.2-2.5,4.7-2.5c4.7,0,6.3,1.7,6.3,5.4V32z"></path>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ZKSVK37S.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ZKSVK37S.htm	
File Type:	HTML document, UTF-8 Unicode text
Category:	downloaded
Size (bytes):	125505
Entropy (8bit):	4.787911437420829
Encrypted:	false
SSDEEP:	1536:oViJolW/ywU1ImJEw+6MKYrzSLmsIyZA7A7L/sRDP9ZhqIDdi:YiJolW/+1ImJu6Xl7L/QDPrhZM
MD5:	A52A71CB51013769DD203F025EE7FEFF
SHA1:	3C1E8C2694D5B23F86780C92FCD71722696FC977
SHA-256:	723E75C27846FFF4B8CB3082F72A36646D5F0670B0C084B11848DA15E2385827
SHA-512:	ECBD613D686C3C2B289160F6CF3A98DF9D276AF7C1C3FF7DEC62D5920048B53081E174B0B11D5766832DC02C9F4B83D7000F5453C7210F45096755C993C3A1B
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ZKSVK37S.htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/?utm_source=eb-lps
Preview:	<!DOCTYPE html>..<html xmlns="http://www.w3.org/1999/xhtml" xmlns:og="http://ogp.me/ns#" xmlns:fb="https://www.facebook.com/2008/fbml">..<head lang="en">... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">..<meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">..<title>All-in-One CRM - Marketing, Sales & Support Software | EngageBay</title>..<meta name="description" content="EngageBay is an affordable all-in-one CRM with marketing, sales & support solution for growing businesses to engage and convert web visitors to happy customers">... <link rel="shortcut icon" href="images/favicon.ico" />-->.. <meta property="og:title" content="All-in-One CRM - Marketing, Sales & Support Software | EngageBay" />..<meta property="og:url" content="https://www.engagebay.com" />..<meta property="og:image" content="https://cdn5.engagebay.com/images/engagebay-hero-image.png" />..<meta property="og:description" content="EngageBay is an affordable all-in-one

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ajax-loading[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 32 x 32
Category:	downloaded
Size (bytes):	4176
Entropy (8bit):	7.391571732170233
Encrypted:	false
SSDEEP:	96:3774Cj4XcWiszAQvsNUlBOu3P7qjHoc95lJ6lWNaZSB:L/WiszT0UlB77055zlWNnB
MD5:	E4234472AFB925DDB203AD99CB2EC0B0
SHA1:	385550A74827324C3CD787275290E96311DFC8FB
SHA-256:	4DC14FE5DF68D2AE899E237FAF9264D6DF02605DD655368CB856CD6CE75C7573
SHA-512:	BCD2A1DB766D79742BD61C5620B7C3503CE1C0C7E19AA9451A6F1A15733C00CE09DF4E01C82906B9C4483363D8574BA6DEDAEBBF378BDA01D9A190DDB1A88BD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn5.engagebay.com/images/ajax-loading.gif
Preview:	GIF89a . .....lllDDDNNN.....LLL.....666.....zzz<<<(((,,,...vvv...'''''...VVV.... .....&&&.....>>>...ttt.....000.....BBB..... .....ZZZ$$$...~~~rrr.....|||...hhhjjj.....```.....xxx.....XXX222.....***bbb^^^...ppp.....!..NETSCAPE2.0.....!..Created with ajaxload.info.!.....,... . .....).....).4.)...3....*.5..A..9@.....+..&.....<..... .....)KFN....!.....%.....''..!'.....,..D.....#..6...`xU....-T.....A. d .....1. ...._.r`...A.....Q.'.L.p H`A....Q0BKA....1.....F..`...c.pdld.....(.`b.....R.p"...a.=xa!./{..6...B...?6.%b..Ru$`..2$....6dC..E.c!F(C.A.S.%hE.....@.. ...$'rbP..I.)D.v.....(....wFj..2...3>X.p@..cF<.:.I...T.....#.JD'.7...-.MK...%&...`...@.!.....,... . .....TT).....I((K/.....4F....F.....K....I.....AFL..FA.....(.XMDF..%....$..:(NI.....<....<(0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\animate[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	81068
Entropy (8bit):	4.941624360117711
Encrypted:	false
SSDEEP:	768:KHuauafqftulucfwfk+1fHf7SpS/fjfsY9:8fqfofwfk+1fHfJfjfsY9
MD5:	79A80CC63E5E2BF1771C65B98688015A
SHA1:	64EC59C7C18C4AF6D80F82E97BA2C01CA4861D55
SHA-256:	E3AD9E38CE001A10EF4D6B21EFA7CEAB890F4EADD1FA4D47E6DEF54098DE336E
SHA-512:	3A68BC6AD6F25D242E0ED0021EC050FDA183264EC9A8851D4B9FBD71D7AE2E082DF2FCA33E27F858121FC13E82958F7A3BECA45BCA0B5B6AAD2AB9902A48AC71
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn5.engagebay.com/css/animate.css?v=1.4.60
Preview:	@import url('https://fonts.googleapis.com/css?family=Poppins:300,400,500,600,700');.@charset "UTF-8";../*!. * animate.css -http://daneden.me/animate. * Version - 3.5.1. * Licensed under the MIT license - http://opensource.org/licenses/MIT. *. * Copyright (c) 2016 Daniel Eden. */...animated {. -webkit-animation-duration: 1s;. animation-duration: 1s;. -webkit-animation-fill-mode: both;. animation-fill-mode: both;.}...animated.infinite {. -webkit-animation-iteration-count: infinite;. animation-iteration-count: infinite;.}...animated.hinge {. -webkit-animation-duration: 2s;. animation-duration: 2s;.}...animated.flipOutX,..animated.flipOutY,..animated.bounceIn,..animated.bounceOut {. -webkit-animation-duration: .75s;. animation-duration: .75s;.}..@-webkit-keyframes bounce {. from, 20%, 53%, 80%, to {. -webkit-animation-timing-function: cubic-bezier(0.215, 0.610, 0.355, 1.000);. animation-timing-function: cubic-bezier(0.215, 0.610, 0.355, 1.000);. -webkit-transform: trans

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bootstrap.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	154615
Entropy (8bit):	5.060705991714609
Encrypted:	false
SSDEEP:	1536:L/xImaGIcCQYYDnDEBi83NcuSEk/5kXruKiq3SYiLENM6HN26n:L/RZzoi3q3SYiLENM6HN26n
MD5:	F64D3837A895BE24BE21E6B11E1664F4
SHA1:	E6C5CB0A491D9B8D97E03CD6F5A1937BB02D8014
SHA-256:	A36B91284CC33D2E26FEBA77675A1D587684C541455E347F3BB1AC2529657AC9
SHA-512:	2396210074AF9EDB9F48AED8074EB5B0E3749C2A2945260AFC441047C197319B35BFC46375DBF3896D9959B692D76E1A32D6CC5BB855488AD0EC0CC62D99648
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://d2p078bqz5urf7.cloudfront.net/cloud/landingpage-builder/page/bootstrap.min.css
Preview:	/*!.. * Bootstrap v4.3.1 (https://getbootstrap.com/).. * Copyright 2011-2019 The Bootstrap Authors.. * Copyright 2011-2019 Twitter, Inc... * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE).. */::after,::before{box-sizing:border-box}html{font-family:sans-serif;line-height:1.15;-webkit-text-size-adjust:100%;-webkit-tap-highlight-color:transparent}article,aside,figcaption,figure,footer,header,hgroup,main,nav,section{display:block}body{}}[tabindex="-1"]:focus{outline:0!important}hr{box-sizing:content-box;height:0;overflow:visible}h1,h2,h3,h4,h5,h6{margin-top:0;margin-bottom:.5rem}p{margin-top:0;margin-bottom:0}abbr[data-original-title],abbr[title]{text-decoration:underline;-webkit-text-decoration:underline dotted;text-decoration:underline dotted;cursor:help;border-bottom:0;-webkit-text-decoration-skip-ink:none;text-decoration-skip-ink:none}address{margin-bottom:1rem;font-style:normal;line-height:inherit}dl,ol,ul{margin-top:0;margin-bottom:1rem}ol ol,ol ul,ul ol,u

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\chunk-vendors[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):	280872
Entropy (8bit):	5.424859265226465
Encrypted:	false
SSDEEP:	3072:AeX89ALKo+wrd6mW1MiOFQuSsfmKC6S45A7dKdcA+sXjB8QP+EXYcsv3:Ab9ALKoa5MnV3AJKdcjGjB8QGRv3
MD5:	9035EB115D3E5BF9ABED815E9396E37E
SHA1:	9501EE8DF191F3ABAE50E3D0AEF541F777DABB7E
SHA-256:	2C78983DDC7A65312AAD866227654928E1FE90EE87D9F8FCC84DB4CCDF444983
SHA-512:	18555341D88396EC798CFE45AE09435391F129C1F6A849851012143D42477D3A29B34BEE897DF2095BDEE59D10ED1AC3219C4B3897B43730DD695426C36FA2FC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://d2p078bqz5urf7.cloudfront.net//livechat/5-1/js/chunk-vendors.js
Preview:	(window["webpackJsonp"]=window["webpackJsonp"]||[]).push([["chunk-vendors"],{"044b":function(t,e){./*!. * Determine if an object is a Buffer. *. * @author Feross Aboukhadijeh <https://feross.org>. * @license MIT. */.t.exports=function(t){return null!=t&&null!=t.constructor&&"function"===typeof t.constructor.isBuffer&&t.constructor.isBuffer(t)},"0a06":function(t,e,n){"use strict";var r=n("2444"),o=n("c532"),i=n("f6b4"),s=n("5270");function a(t){this.defaults=t,this.interceptors={request:new i,response:new i}}a.prototype.request=function(t){"string"===typeof t&&(t=o.merge({url:arguments[0]},arguments[1])),t=o.merge(r,{method:"get"},this.defaults,t),t.method=t.method.toLowerCase();var e=[s,void 0],n=Promise.resolve(t);this.interceptors.request.forEach((function(t){e.unshift(t.fulfilled,t.rejected)})),this.interceptors.response.forEach((function(t){e.push(t.fulfilled,t.rejected)}));while(e.length)n=n.then(e.shift(),e.shift());return n},o.forEach(["delete","get","head","options"],(funct

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\commons[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	4234
Entropy (8bit):	4.915711819486833
Encrypted:	false
SSDEEP:	48:U1tkogYcBpzUXQ+5DGrfjzOYztStjTY2l+ORMCHaZPUs2/GdAZeKQfObdqDZIw0S:U1OjyKjjfwiqGycAkWoZt7
MD5:	7E58D8C57DD337D51C801F2DE145B33A
SHA1:	59CCED5D51BE1996FC1123033D187D755DF3C8A8
SHA-256:	222283BD442533DF373E971DD801D07E58E2FBD7C0702C79078EBABBD8BAB3A5
SHA-512:	5B71293E70333395FA1D62D995E91CCDD74E540883114D5CE1DFF702291A56B8CD6F347D5E2F192EE1E79C120118ABE691A42F9E28D7258822C76E850E1735AE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://d2p078bqz5urf7.cloudfront.net/cloud/landingpage-builder/page/commons.css?84-9.434327273400168234
Preview:	body {.. font-family: 'Varela', sans-serif !important;.. background-color: #f6f8f9;.. color: #43506a;.. letter-spacing: 0.01em;.. font-size: 12px;..}.....carousel .carousel-control-prev .chevron, .carousel .carousel-control-next .chevron{...font-size: 23px;.. color: #fff;..}.....carousel .carousel-control-prev:hover .chevron, .carousel .carousel-control-next:hover .chevron{.. z-index: .8;..}.....carousel .carousel-indicators li:hover{... z-index: 1;..}.....carousel .carousel-inner.default .carousel-item{...text-align: center;..}.....carousel .carousel-inner.thumbnail_left .carousel-item, .carousel .carousel-inner.thumbnail_top .carousel-item{...padding-top: 15px;..}.....carousel .carousel-inner.default .carousal-thumbnail{...width: auto !important;...height: 100% !important;...max-width: 100%;..}.....carousel .carousel-inner.default .carousel-description{.. .position: absolute;.. right: 15%;.. bottom: 20px;.. left: 15%;.. z-index: 10;.. padding-top: 2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\featured-check[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	2809
Entropy (8bit):	2.1701756413603173
Encrypted:	false
SSDEEP:	12:t4KdhKM0G1HVbpOo4IC2cDPuYZNueuyJNna+AKsJKAzpHViidcF4+/HULI+U:t4ChKM0G1nTWuioXyJNrsJKg0SJU
MD5:	B3B960029108AACB76345E53100D843F
SHA1:	88357F24828AAF8453FF75187A39A68584C6A6E8
SHA-256:	8508971426A0748CFAFE9B33C7BB6F6FF97CFEBDFEEE75131B8DC67E71057F33
SHA-512:	99A09F1563451F53D49A9E8E1821BEC4B3AC134C917BD9D27F259A0A03EF4BB9251D10CF0016BE27CF4707F3C1A7B17BFB79017D53604E4C44CC965C94C276E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://d2p078bqz5urf7.cloudfront.net/cloud/assets/img/featured-check.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="15.562" height="11.656" viewBox="0 0 15.562 11.656">. <metadata><?xpacket begin="." id="W5M0MpCehiHzre SzNTczkc9d"?>.<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="htt p://www.w3.org/1999/02/22-rdf-syntax-ns#">. <rdf:Description rdf:about=""/>. </rdf:RDF>.</x:xmpmeta>. . . . . .

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\font-awesome.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	31000
Entropy (8bit):	4.746143404849733
Encrypted:	false
SSDEEP:	384:wHu5yWeTUKW+KlkJ5de2UYDyVfwYUas2l8yQ/8dwmaU8G:wwlr+Klk3Yi+fwYUf2l8yQ/e9vf
MD5:	269550530CC127B6AA5A35925A7DE6CE
SHA1:	512C7D79033E3028A9BE61B540CF1A6870C896F8
SHA-256:	799AEB25CC0373FDEE0E1B1DB7AD6C2F6A0E058DFADAA3379689F583213190BD
SHA-512:	49F4E24E55FA924FAA8AD7DEBE5FFB2E26D439E25696DF6B6F20E7F766B50EA58EC3DBD61B6305A1ACACD2C80E6E659ACCEE4140F885B9C9E71008E9001FB F4B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://stackpath.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css
Preview:	/*!. * Font Awesome 4.7.0 by @davegandy - http://fontawesome.io - @fontawesome. * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License). */@font-face{font-family:'FontAwesome';src:url('../fonts/fontawesome-webfont.eot?v=4.7.0');src:url('../fonts/fontawesome-webfont.eot?#iefix&v=4.7.0') format('embedded-opentype'),url('../fonts/fontawesome-webfont.woff2?v=4.7.0') format('woff2'),url('../fonts/fontawesome-webfont.woff?v=4.7.0') format('woff'),url('../fonts/fontawesome-web font.ttf?v=4.7.0') format('truetype'),url('../fonts/fontawesome-webfont.svg?v=4.7.0#fontawesomeregular') format('svg');font-weight:normal;font-style:normal}.fa{display:inline-block;font:normal normal normal 14px/1 FontAwesome;font-size:inherit;text-rendering:auto;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale}.fa-lg{ font-size:1.33333333em;line-height:.75em;vertical-align:-15%}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-fw{width:1.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\growsumo.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	4823
Entropy (8bit):	5.333741183743766
Encrypted:	false
SSDEEP:	96:wq2bJz7dej+xsRlUabgiW6rEBSYY0nfEuPm9/xoP9VQ7MYqH1t7qD6h62/rEqE:wvNz70+xwl8WrEBjnfRm92F/Ys7woEf
MD5:	26446285D706A92CFA802A528B86B9BC
SHA1:	0D3AFFE067754872EF9A95582270E3C778A23A28
SHA-256:	9B7A2B3D5EC3249E7DAFAFB15148B44230102AB875C525AC1EBC0A2C58AE2D0C
SHA-512:	C1E57D9B4914E87B6CE109C057F3C0725925C9B4CD26C5DE81D9187466ED31F2A4575EBF261714AA83680784C3E4D92FA72F52FC0EF871FB91E9255D2BE13CE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://snippet.growsumo.com/growsumo.min.js
Preview:	!function(){"use strict";function o(o){return"string"!=typeof o?"":decodeURIComponent(atob(o).split("").map((function(o){return"%"+("00"+o.charCodeAt(0).toString(16)).sli ce(-2)})).join(""))}var n,t=(function(o,n){var t;t=function(){function o(){for(var o=0,n={};o<arguments.length;o++){var t=arguments[o];for(var e in t)n[e]=t[e]}return n}function n(o){return o.replace(/(%[0-9A-Z]{2})+/g,decodeURIComponent)}return function t(e){function r(){}function a(n,t,a){if("undefined"!=typeof document){"number"==typeo f(a=o({path:"/"},r.defaults,a)).expires&&(a.expires=new Date(1*new Date+864e5*a.expires)),a.expires=a.expires?a.expires.toUTCString():"";try{var i=JSON.stringify(t);/^[\{\ []/.test(i)&&(t=i)}catch(o){}t=e.write?e.write(t,n):encodeURIComponent(String(t)).replace(/%(23|24|26|2B|3A|3C|3E|3D|2F|3F|40|5B|5D|5E|60|7B|7D|7C)/g,decodeURI Component),n=encodeURIComponent(String(n)).replace(/%(23|24|26|2B|5E|60|7C)/g,decodeURIComponent).replace(/[\(\)]/g,escape);var u="";for(var s in a)a[s]&&(u+=";

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\iframe[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1280
Entropy (8bit):	5.044373612229707
Encrypted:	false
SSDEEP:	24:dx0x15u/n6j9SRQfoLQwvRdRQflzpKB28BioDZMMXYTxVn:Hi14iSuQ8MHutF028DaMX4xVn
MD5:	116E28F03C0E6DDA20174E08F1A49685
SHA1:	1D23C80D0102F33C8E08B48E764C6BC8BAE97E7C
SHA-256:	4401CB5A593CBA0A74412658BAB8F87A2976E49183C8343FCC209CA99AE9EF2F
SHA-512:	8A8C1D18E075BB711176CAFFC03116592FC77EFEDEE42B4C613F0E422DC3FE0D9C6C21935F1E0D0065DDDDDD904D8584F43322DD4F4A377829B8B97BB8C9C D4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://d2p078bqz5urf7.cloudfront.net/cloud/landingpage-builder/page/iframe.js?=84-9.434327273400168234
Preview:	function loadHTMLTypeContentInFrame(iframe) {.....try {....if(Number($(iframe).attr("data-retry")) >= 2).....return;...} catch (e) {...}.....try {.....var content = $(iframe). attr("data-srcdoc");....if(!content).....return;...../// Parse and check....try {.....var parser = new DOMParser();.....var doc = parser.parseFromString(content, "text/html");... ..$(doc.documentElement).find('body').find('.engage-bay-source-form form').attr("onsubmit", "window.parent.EhForm.submit_form(event,this)");.....content =doc.do cumentElement.outerHTML.....var formId = $(doc.documentElement).find('body').find('.engage-bay-source-form form').attr('data-id');.....if(formId){.....$(iframe).add Class('engage-bay-source-form');.....$(iframe).attr('data-id', formId);.....}....} catch (e) {....}...../// console.info('content', content);.....var dstDoc = iframe.contentDocument \|\| iframe.contentWindow.document;....dstDoc.write(content);....dstDoc.close();.....$(iframe).removeAttr("data-srcdoc");

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\in[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):	185838
Entropy (8bit):	5.449028457561 91
Encrypted:	false
SSDEEP:	3072:MvNu7fo+FZhlUX2EmnDe5IkRn2Bxqntoc:g+FZm2EmnDe5IkRn2BxYb
MD5:	A2459BCE2BD8C09CE0ED34CBA5606F1E
SHA1:	375C1A6E2210A2FE75DCE803AD3A9D832E819520
SHA-256:	5E28055AE167278115C69E3285DCA9E5BB62F1B723A40F9108F91953F98B4960
SHA-512:	2145E89F19CEF817CC5451FF5CEF08852E06088DAB794A41D33045A46FA09D92AF06F027D3BD34F839E88EAD0380441121B097388D85825BDFA6BF1C174F5854
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://platform.linkedin.com/in.js
Preview:	/* xdoor-frontend: v0.2.6 (Mon, 1 Feb 2021 21:02:04 GMT) */.(function() {..var PAYLOAD = {"ENV":{"widget":{"alumni_url":"https://www.linkedin.com/cws/alumni","f ollowmember_url":"https://www.linkedin.com/cws/followmember","settings_url":"https://www.linkedin.com/cws/settings","share_url":"https://www.linkedin.com/cws/sh are","share_counter_url":"https://www.linkedin.com/countserv/count/share","company_url":"https://www.linkedin.com/cws/company/profile","member_profile_url":"htt ps://www.linkedin.com/cws/member/public_profile","full_member_profile_url":"https://www.linkedin.com/cws/member/full_profile","referral_center_url":"https://www.linkedin. com/cws/referral","apply_url":"https://www.linkedin.com/cws/job/apply","mail_url":"https://www.linkedin.com/cws/mail","apply_counter_url":"https://www.linkedin.com/counts erv/count/job-apply","company_insider_url":"https://www.linkedin.com/cws/company/insider","sfdc_member_url":"https://www.linkedin.com/cws/sfdc/member","sfdc_com pany_url":"https://w

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\jquery.mCustomScrollbar.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):	42838
Entropy (8bit):	5.142619900446187
Encrypted:	false
SSDEEP:	768:pHtyRbNWmYd7Z9t6vw7R01rnk6BcxL+zhRNxA5l2ng7ytcKaWDxQ:pHtyRsmYd7Z9t6+R9
MD5:	6D2F565FE99884AFB7E2B814447FF80C
SHA1:	49E78F1286F383135FACF507F46FABAC4B5EC1DB
SHA-256:	0DE9AC1F9FDD435533248ACEB3F29914CFDB8F804EB505749F801635A48B2CA2
SHA-512:	7D94B6A677D6F76F5C11D35EAF768FB39BA4F8929A04A1CEF12D425122388A66666F7EB0A40607AADB1ED307C6DAE88D08DB64280526DAD75A9414ACFC17F0 4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn5.engagebay.com/css/jquery.mCustomScrollbar.min.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\jquery.mCustomScrollbar.min[1].css	
Preview:	.mCustomScrollbar{-ms-touch-action:pinch-zoom;touch-action:pinch-zoom}.mCustomScrollbar.mCS_no_scrollbar,.mCustomScrollbar.mCS_touch_action{-ms-touch-action:auto;touch-action:auto}.mCustomScrollBox{position:relative;overflow:visible;height:100%;max-width:100%;outline:0;direction:ltr}.mCSB_container{overflow:visible;width:auto;height:auto}.mCSB_inside>.mCSB_container{margin-right:0}.mCSB_container.mCS_no_scrollbar_y.mCS_y_hidden{margin-right:0}.mCS-dir-rtl>.mCSB_inside>.mCSB_container{margin-right:0;margin-left:30px}.mCS-dir-rtl>.mCSB_inside>.mCSB_container.mCS_no_scrollbar_y.mCS_y_hidden{margin-left:0}.mCSB_scrollTools{position:absolute;width:16px;height:auto;left:auto;top:0;right:0;bottom:0;opacity:.75;filter:"alpha(opacity=75)";-ms-filter:"alpha(opacity=75)"}.mCSB_outside+.mCSB_scrollTools{right:-26px}.mCS-dir-rtl>.mCSB_inside>.mCSB_scrollTools,.mCS-dir-rtl>.mCSB_outside+.mCSB_scrollTools{right:auto;left:0}.mCS-dir-rtl>.mCSB_outside+.mCSB_scrollTools{left:-26px}.mCSB_scrollTools .mCS

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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):	171089
Entropy (8bit):	5.367970232927022
Encrypted:	false
SSDEEP:	3072:jxcq0hrLZwpsYbmzORDU8Cuo+414Jiz6fh6lTqya98HrZ:KHBLZjYqORDU8Cu1O4kyQQya98HrZ
MD5:	DDDD143C668B51DD5C19F4CC5CC68F5B
SHA1:	05C641FB96F8D118BAE4D4D7BDAF14CCE5CBFA5B
SHA-256:	A426AB2F85A2EABB334AA9E40378465958DAA48AAA9F4863D208AF72780994BE
SHA-512:	6355576A5E2ED401199E87CFDAAE3FEFBF491D1770A6B210131ED1680D01C7D8210EC2DDE7F00888DD17AA0BD8ACA4D0364F8523C5688B967F1CE59CB338EA0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/jquery/3.1.1/jquery.min.js
Preview:	/*! jQuery v3.1.1 | (c) jQuery Foundation | jquery.org/license */!function(a,b){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.1.1",r=function(a,b){return new r.fn.init(a,b)},s=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,t=/^-ms-/,u=/-([a-z])/g,v=function(a,b){return b.toUpperCase()};r.fn=r.prototype={jquery:q,constructor:r,length:0,toArray:function(){return f.call(this)},get:function(a){return null==a?f.call(this):a<0?this[a+this.length]:this[a]},pushStack:function(a){var b=r.merge(this.con

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\leadgrabbers[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	373905
Entropy (8bit):	5.215223589793861
Encrypted:	false
SSDEEP:	1536:l0LnALJ6LqYcs/d9LnALJ6LqYcs//2x1LnALJ6LqYcs/6q+cLnALJ6LqYcs/ngiX:lwvxB2xpUCWuQU
MD5:	E22E8BCAD1CF853D910E8291C97021E8
SHA1:	E70C93B9B1A8EC9DC72556AC6AD189E408AB8435
SHA-256:	27C2F8DA86250A0E4566DAAEFA686C2286A8BB893E1B855B2CABB3D5BE9EF8A3
SHA-512:	A61B86D15EA4325E2E521D235775A1D933B8DD0975876F53E7AF7291C411E9D540A0ACECE881402C8C041502D0A287DBFB181547843F09CCCD7D625D708B5BE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://app.engagebay.com/jsapi/rest/leadgrabbers?apiKey=ktb76s1540fl2hnhbqnrtd2npb
Preview:	[{"id":4538242625961984,"name":"Get on a call","alias_name":"get on a call","owner_id":5769015641243648,"created_time":1581589129,"autoResponder":{"send_autoresponse_email":false,"autoresponder_email_subject":"{{Subscriber.firstname}}, thanks for your subscription","autoresponder_email_content":"<!DOCTYPE html>\n<html>\n<head>\n</head>\n<body>\n \n Hello {{Subscriber.firstname}}, \n Thanks for signing up to our newsletter. We will send you weekly updates. Hope you will enjoy it! \n</body>\n</html>","from_email":"4893098786160640","autorespond_bcc":"","autorespond_cc":"","autorespond_reply_to":""},"updated_time":1581594413,"form_html":"<form class=\"form form-style-form7 form-size-550px has-title-image\" onsubmit=\"window.parent.EhForm.submit_form(event,this)\" style=\"\n \n background-color:#fffff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\logo[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	33412
Entropy (8bit):	3.8357567409710938
Encrypted:	false
SSDEEP:	384:5jv5Jo01970ZwVE0+4/ofo1bF1jcVWRuJaED/3FswKszvImRaZ4g4rzpB+gPW7ex:5jnH/P5U8ApD/3FKHsZW7eAn+yjq5t
MD5:	74FD6E18050C04B669B09A2A7B309543
SHA1:	455F0F888A63DA34155C2D2FFD02E85A962751A6
SHA-256:	43E12CCB1BC2B82CF2E220A8802B90BF2DF9BA98A036278A5B16E78B8ABBE406
SHA-512:	1136A656643175D1A1C7FF018A818A6C80D8BA3C8C303B75A4578024C137BA5D3402A923774E889864BE72E4A8073745CBAC065CBD20DFA34F4CD562C1F8BA5
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\logo[1].svg	
Reputation:	low
IE Cache URL:	http://https://cdn5.engagebay.com/logo.svg
Preview:	<svg id="svg" version="1.1" width="400" height="60.38104543234002" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" style="display: block;"><g id="svgg"><path id="path0" d="M28.644 7.741 C 28.953 7.883,29.403 7.991,29.644 7.981 C 30.022 7.964,30.002 7.943,29.500 7.829 C 29.179 7.756,28.729 7.648,28.500 7.589 C 28.230 7.519,28.281 7.573,28.644 7.741 M20.794 7.951 C 21.001 7.991,21.301 7.990,21.460 7.948 C 21.620 7.906,21.450 7.874,21.083 7.875 C 20.717 7.877,20.586 7.911,20.794 7.951 M7.389 31.167 C 7.389 31.854,7.419 32.135,7.455 31.792 C 7.491 31.448,7.491 30.885,7.455 30.542 C 7.419 30.198,7.389 30.479,7.389 31.167 M48.825 33.287 C 48.779 33.675,48.806 33.928,48.883 33.850 C 48.961 33.773,48.998 33.456,48.966 33.146 C 48.910 32.597,48.906 32.601,48.825 33.287 M42.879 33.667 C 42.879 34.079,42.911 34.248,42.951 34.042 C 42.991 33.835,42.991 33.498,42.951 33.292 C 42.911 33.085,42.879 33.254,42.879 33.667 M3.179 39.962 C 3.282 40.258,3.434 40.543,3.518 40.5

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\page-actions[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	3381
Entropy (8bit):	5.050091219850445
Encrypted:	false
SSDEEP:	48:8GgHvGCGNoe3M8WdetCNT5kK3948/QeMdjED6CjkC/e4eXo0Y+DsmnjxCd8JCWlj:P9u544izXV286l6ZRYRk8HCKJSh4pW
MD5:	62E9E627C1322AB990194EB6BDFD5499
SHA1:	448B8FD27CF3E19E92374CEF0045A08BC2C26B3E
SHA-256:	FAE77A813E81D7829692F1C70D6F9E2CEBFAACE0941A85CDC7E142204840C635
SHA-512:	3605E978599D6FE6E85CD2C3E55E9E20C6399F788015367DE1CFD98DE1F23B47190E4E5D7A5BCA4CA3757A5FA6A6F45EC64B25767B333914A8B37E97D6A7DE2C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://d2p078bqz5urf7.cloudfront.net/cloud/landingpage-builder/page/page-actions.js?=84-9.434327273400168234
Preview:	$('.engagebay-lp-button').....on(.....'click',.....function(e) {.....e.preventDefault();.....var buttonAction = $(this).attr('data-actionType');.....var buttonActionValue = $(this).attr('data-actionValue');.....if (!buttonAction || !buttonActionValue).....return;.....switch (buttonAction) {.....case "open_url_in_new_tab":.....var pattern = /^((http|https|ftp):\/\/)/;.....if (!pattern.test(buttonActionValue)) {.....buttonActionValue = "http://" + buttonActionValue;.....}.....window.open(buttonActionValue, '_blank').focus();.....return;.....case "open_url_in_same_tab":.....if (window.parent.location.....&& window.parent.location.href.....indexOf('/landingpage-builder/preview/preview.jsp') > 0).....window.parent.location = buttonActionValue;.....else{.....var pattern = /^((http|https|ftp):\/\/)/;.....if (!pattern.test(buttonActionValue)) {.....buttonActionValue = "http://" + buttonActionV

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\page[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1520
Entropy (8bit):	5.090582382913269
Encrypted:	false
SSDEEP:	24:na6zmCdzf0xEBjvWfFVXm87nyIctbdQkerJy+y8LEKv008QuWIGQSEMcqQo6yh0P:nzfdYqdoFVXm8dObdqN18QVeIh/XivRX
MD5:	71374AEE1A3FD085641B64402B0FA5CE
SHA1:	86FA69E69AE2BECCF082FD67766C46648B4861C9
SHA-256:	D3D99606E7E22717A6225968F11A608D5DF2FFB37488D4DDAE8B139D157337C7
SHA-512:	F63808FA1DD4B29A2B66AE022CFB38B2367B9FAE181CFE04D58C04E88359AAF0F679CE47410A2E1AD324BE92AA6ADE3554C8CCFCFAE78A6118617C0FE05D26A1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://d2p078bqz5urf7.cloudfront.net/cloud/landingpage-builder/page/page.css?84-9.434327273400168234
Preview:	body{.. margin: 0;.. text-align: left;.. font-size: 1rem;.. /* font-family: -apple-system, BlinkMacSystemFont, "Segoe UI", Roboto, "Helvetica Neue", Arial, "Noto Sans", sans-serif, "Apple Color Emoji", "Segoe UI Emoji", "Segoe UI Symbol", "Noto Color Emoji";.. font-size: 1rem;.. font-weight: 400;.. line-height: 1.5;.. color: #212529;.. background-color: #fff; */.. ..}....body .container{...padding-left: 0;...padding-right: 0;..}.....no-border {...border: none;..}.....section-background-video {...display: block;.. position: absolute;.. right: 0;.. .bottom: 0;.. .width: 100%; .. .height: 100%;.. .boder:none;..}....button{...box-shadow: none !important;..}..button:hover{...box-shadow: none !important;...opacity: 0.9;..}....@media only screen and (min-width:601px) {....has-mobile-view .desktop-view {....display: block;...}....has-mobile-view .mobile-view{....display: none;...}.....}.....video-modal iframe{...min-height: 400px;..}.....video-modal video{...height: 400px;.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\pixel[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	2.7374910194847146
Encrypted:	false
SSDEEP:	3:CU9yltxlHh/:m/
MD5:	DF3E567D6F16D040326C7A0EA29A4F41
SHA1:	EA7DF583983133B62712B5E73BFFBCD45CC53736
SHA-256:	548F2D6F4D0D820C6C5FFBEFFCBD7F0E73193E2932EEFE542ACCC84762DEEC87

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\pixel[1].gif	
SHA-512:	B2CA25A3311DC42942E046EB1A27038B71D689925B7D6B3EBB4D7CD2C7B9A0C7DE3D10175790AC060DC3F8ACF3C1708C336626BE06879097F4D0ECAA7F56701
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://q.quora.com/_/ad/3eac0d5d116c4d1896518c0538c256d9/pixel?tag=ViewContent&i=gtm&u=https%3A%2F%2Fwww.engagebay.com%2F%3Futm_source%3Deb-lps
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\roboto[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	202
Entropy (8bit):	4.934838261225945
Encrypted:	false
SSDEEP:	6:6THRSa2q9VemJBglZYtN85DeSvMM1lKDoA/:6TUaZe+BglZ4HMKDD
MD5:	775CD75CE56F94D14325B4C781973549
SHA1:	D876A8786FC35410F3079D057B1E953B3DC662E1
SHA-256:	A1AD98928C3F060D83E612380CEC67893929AAA4C8BD9EDF4A8AF49891C1DC7A
SHA-512:	0483F53DB961318F3084DF74020400EF99CE78696493F095BC337DEFC70E1D37436228831EC2C019184F87A1FF9D6ECBC31845C327136E06401312A561D9DD9D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://d2p078bqz5urf7.cloudfront.net/cloud/prod/assets/lib/font-family/roboto.css
Preview:	@import url('https://fonts.googleapis.com/css?family=Roboto:100,100i,300,300i,400,400i,500,500i,700,700i,900,900i&display=swap'); ..body, .font-family-roboto { ..font-family: 'Roboto', sans-serif; ..}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\swiper.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	16721
Entropy (8bit):	5.195211078057414
Encrypted:	false
SSDEEP:	96:3M6Y6g0ewBTC944pL9FmLqXCi9mPmc6imGlidxXHmXgyXIvQkfPlJV8pqnf7fafC:cD0GpaNliHHmXgyXyzSHF68EB0SwW
MD5:	889597CBE2BAB6270452E3B291E68002
SHA1:	A21F4E790097C2604942E48F91C8D62CD4D0F42E
SHA-256:	62FB7652C4BDCD7421CEB287B29F52B36BF4F5B85BBAC8E3E4409081FDDF15B0
SHA-512:	E9B426B68F357B9FC751567EEAFFD82021C12A09C3D04B5F8BB963F02A6207C68633BD840D05E9A3DDBC5A35537BD726AC37477571624EAFB6B3D59CF4DE7B3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn5.engagebay.com/css/swiper.min.css
Preview:	/**.. * Swiper 3.3.1.. * Most modern mobile touch slider and framework with hardware accelerated transitions.. * .. * http://www.idangero.us/swiper/.. * .. * Copyright 2016, Vladimir Kharlampidi.. * The iDangero.us.. * http://www.idangero.us/.. * .. * Licensed under MIT.. * .. * Released on: February 7, 2016.. */...swiper-container{margin:0 auto;position:relative;overflow:hidden;z-index:3}.swiper-container.overflow-visible{overflow: visible}.swiper-container-no-flexbox .swiper-slide{float:left}.swiper-container-vertical>.swiper-wrapper{-webkit-box-orient:vertical;-moz-box-orient:vertical;-ms-flex-direction:column;-webkit-flex-direction:column;flex-direction:column}.swiper-wrapper{position:relative;width:100%;height:100%;z-index:1;display:-webkit-box;display:-moz-box;display:-ms-flexbox;display:-webkit-flex;display:flex;-webkit-transition-property:-webkit-transform;-moz-transition-property:-moz-transform;-o-transition-property:-o-transform;-ms-transition-property:-ms-transform;transitio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\tracking-code[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	1327
Entropy (8bit):	5.361051951607773
Encrypted:	false
SSDEEP:	24:oXVlDJhNc2UEcVNOoRWR9Gge5VkOKLkfm22QiRWbtVfBO0OY+IHERWysljZctUH:oXVlDzOxjw6gKWV7Fwx9B/mIHEwhIoUH
MD5:	FCBA0F665CE0A04E86CB150E09615FE9
SHA1:	658FF52C6AF02C05CDAAD907F26FD50DD869445B
SHA-256:	8AF8E9F419E2815A99EE8D436E45D60EDDE4AADF966A17C727D7A0D96E7DB814
SHA-512:	27F6E316601C10029F57454108C0E2DAB52AE06A30DF742A6BABDE6ED6124EDAD4DC625294DD4A659A68288C84AAD2B1B9B4A8D774AC159F9AA19275AD11750
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn5.engagebay.com/3pp/tracking-code.js?v=0.0.05

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\tracking-code[1].js	
Preview:	$(function () {. "use strict";.});../* Facebook Pixel Code */.!function(f,b,e,v,n,t,s).{if(f.fbq)return;n=f.fbq=function(){n.callMethod?.n.callMethod.apply(n,arguments):n.queue .push(arguments)};.if(!f._fbq)f._fbq=n;n.push=n;n.loaded=!0;n.version='2.0';.n.queue=[];t=b.createElement(e);t.async=!0;.t.src=v;s=b.getElementsByTagName(e)[0]; .s.parentNode.insertBefore(t,s)}(window, document,'script',.'https://connect.facebook.net/en_US/fbevents.js');.fbq('init', '911384212383388');.fbq('track', 'PageView');./* End Facebook Pixel Code */..(function(h,o,t,j,a,r){. h.hj=h.hj||function(){(h.hj.q=h.hj.q||[]).push(arguments)};. h._hjSettings={hjid:1657477,hjsv:6};. a=o.getElem entsByTagName('head')[0];. r=o.createElement('script');r.async=1;. r.src=t+h._hjSettings.hjid+j+h._hjSettings.hjsv;. a.appendChild(r);. })(window,document ,'https://static.hotjar.com/c/hotjar-','.js?sv=');..(function (w, d, s, l, i) {. w[l] = w[l] || []; w[l].push({. 'gtm.start':. new

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 3351 x 1679, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	452896
Entropy (8bit):	7.872716308954457
Encrypted:	false
SSDEEP:	6144:bI8EZ9DLcIWd4wmppq1ombiGIC5zz+mcCpuyKQjsxxbHEqKLFPwBL/Q77:kT3VpOeE4rlLbktwov
MD5:	C7F488705C8708B654074FC4B9DAB1F9
SHA1:	7A475F1D3CDCE930BAB967E4EF96F25505CA0384
SHA-256:	CDFF0A47D3BB27E0015ED5332BB2614A5CC8FF8879B9469B531F18FB9DBC9822
SHA-512:	CE1AD081D548DA89AAC04B3C25DCE3AC086E71E749D0797EC5501B1E3925026371548CC405117AADBA5B65A53AF1FF5A0CA7238B121D8A28CB9AB8A49869700
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://considineports.xyz/gim/1.png
Preview:	.PNG.....IHDR.....[8.....sRGB.....gAMA.....a.....pHYs.....e...!tEXtCreation Time.2020:10:26 18:10:40.+.8...xIDATx^....H..}..m.....\"\P....2...p...?,...T....."3.c. .....p8...VDT....._.....?...L....._...O.....Q..>@0.V....A....M.4M.....x..~f*.~&.....(..z`Cl..i..i..i..i..i..i..i..i..i..i...~B.....D.sh..`..@.....r...%.\./..KE.K....]!....V..... ...z.i..i._....rc*./..[./5.....X..O..n..i..i..i..i..i..i..i..i..i..i..i..i._...XSH..:..[D...."..."...w.w|.._".....E.#|..9.$d.+...A..E&.B.... ..E.A.g.4M.4.<...b.2_..\D...E..Sa.S.,4M.4M.4M.4M.4M.4M .4M.4M.4M.4M.4./.?....q ..s.&"Om...../.....r..4.RQ|..._./.Y.T..._...r.....5|..~|.(..i..i._....re..[H.l.,...Q.....)..4F.,./.....p=._....y.?.)....Z~...Z.|.....Y.4M.4M.4M.4M.4M.4M.4M..F...DV? z.....t|.(.d.....e }.H...._.....e"|..._...../...}../.....E....!1....i...M.....KFZ.&..Er.W-DDS{.5.ppa..|._.f.....><x.|..Sn.v..l._.....Uxx..l?s.=..y.4M.4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\A-B-for-landing-pages-and-emails[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	4409
Entropy (8bit):	4.792510807081154
Encrypted:	false
SSDEEP:	96:s+fo/811dfW59NkQvMJTY5UAU6AUvWHd4dwtbWprn8OK7H60+W0vzG:do/81mbNkTSNGI+FW67aNBK
MD5:	FAA281054779D622F9BFC36580B125E5
SHA1:	113440405A9DC4AA9CBF08A2BC0A9AE75712A0B6
SHA-256:	F6632DCA5F55D171E3480AA692F7FA0F8C83672C92ADDE161240C7F2EC7DBB21
SHA-512:	451437B86A73B60557B497830508A4430BB50CF4C28809D07B00BBFCE263334FA144AF4ACDF73A5DC8EC4ECE289F090319A08FE7C84BB92E813E8256BBC3AFAC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/A-B-for-landing-pages-and-emails.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 21.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 70 70" style="enable-background:new 0 0 70 70;" xml:space="preserve">..<style type="text/css">....st0{fill:#E6E7E8;}....st1{fill:#0089EF;}....st2{fill:#FFFFFF;}....st3{fill:#D4FBFF;}....st4{fill:#6DC9F7;}....st5{fill:#FA759E;}....st6{ fill:#3A2C60;}..</style>..<g>...<path class="st0" d="M67.4,57.7h-5.1v-33c0-2.2-1.8-3.9-3.9-3.9h-2.8V9.6c0-0.9-0.8-1.7-1.7-1.7H16.3c-0.9,0-1.7,0.8-1.7,1.7v11.2....h-2.8c-2 .2,0-3.9,1.8-3.9,3.9v33H2.8c-0.3,0-0.6,0.3-0.6,0.6v2.2c0,2.2,1.8,3.9,3.9,3.9h57.9c2.2,0,3.9-1.8,3.9-3.9v-2.2....C68,57.9,67.8,57.7,67.4,57.7L67.4,57.7z"/>...<g>....<g>..... <path class="st1" d="M57.3,18.1h-3.4v25.2c0,0.6-0.5,1.1-1.1,1.1H38.5L34,50.7l-4.5-6.3H15.2c-0.6,0-1.1-0.5-1.1-1.1V18.1h-3.4.....c-1.9,0-3.4,1.5-3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Screen_Shot_2021_04_08_at_6[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1912 x 308, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	46365
Entropy (8bit):	7.591085470611775
Encrypted:	false
SSDEEP:	768:0bgjCHx3Kqzs80j2sI44KUMRB3DuS969B0J4fX1e13MKj1Fize:0bgypKqzJ0jLIEhp8z02/1e1Vj1J
MD5:	BB72768C09454F285DD70F26EC18108B
SHA1:	297F725E70F5D2880CF34A3EF7BFCEAFEDD40EFA
SHA-256:	9E2F9E43E295FF18F4F670A5F44E6653D9FA83F71EB06321714014435514B008
SHA-512:	18EF19FDDC168D33110C4F11C19F2C5C5E99DE2B464D880F78765C7EB7666FC30158C37280439700194272CB030DD8E16F84DAD3C88F8B241430385B0A5869EC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn2.eb-pages.com/uploads/6014394531053568/Screen_Shot_2021_04_08_at_6.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Screen_Shot_2021_04_08_at_6[1].png	
Preview:	.PNG.....IHDR...x...4.....NiCCPICC Profile..H....\SW.....$..D@F.K.M..!...2.Q.I a..T...u.(....Xl..R'j.Eq[.RT*.X..w3.~.....~....=..sN..]..u....5..HV.H..gO..d.z.....0.C T...q...._...h.....J!.H"...RX.....2.\Q.....v...j.l...B..9O..j..r..&%..y/.d.@...@....%.<.G..d..H*..A..".D.c .)*..fh..s>../>sF|..y#..E#...R^(.....KQ.jx.G.h.EL.:gX.[.3b.L..'.O.l...T....R%..T.=j!T.`... ..H.....r..0>N...F.!.....Stc.....:.u..I....quc....j.S..T...-..?..e.$%.2...Z"M.....XY.....lK%..a..*I..=d.X.....e.*..t..".p.X.D..qM.$%F[.l.P....r.X.M..#VN...E$....u.e..|.....$..~ya...'....z[...d.X|\1\. Z.x..81E.'../...../.q.."...`..3@>.v...._.(.....].....k2(..C....pM...@.....r5.%....."....o.f.ld.4.+.H.6...Z.....:....4.a.l.%1..A.!F.]ps<.....5.6/....G..=.....p..E.=]Z..,.....e..i.#.....;.ps....y.x(...jy .....M.#.|Rs....RFQ.(...w.....3RU.H....>....c?..b..3....v.k.l...]..yd...YC.%i.).~...O..S]I.G.G..{].(..V.7C>G!....p....2..1l/./O.....6...y? ....*.....t.5..f._:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Screen_Shot_2021_04_09_at_1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1874 x 156, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	47881
Entropy (8bit):	7.910481602643038
Encrypted:	false
SSDEEP:	768:Cbg3uG0i+iKPPkEwG31nebQ9+Maz2u621kpuEjJgJPaRrl3OZIk:Cbg+oQEEwG3MQVaB6WkpfWkp3O6k
MD5:	0DA1B0859153453BEDC493A1C8A67EE1
SHA1:	19FADDB900282B9B0D6D36F9258383EB9FBDCCF3
SHA-256:	D33E7757AB5941BE2895103191340168B155A56DB3CF1128E10412110942BB4C
SHA-512:	6C82940044BE77940ACF2F54D543A4A219C6F0B9DAE7C7AF73AFF004CFC8123EF12D877B6863E49493A57FB76567C29C24DD459BFB8EA3F9C73995537E0E663
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn2.eb-pages.com/uploads/6014394531053568/Screen_Shot_2021_04_09_at_1.png
Preview:	.PNG.....IHDR...R.....NiCCPICC Profile..H....\SW.....$..D@F.K.M..!...2.Q.I a..T...u.(....Xl..R'j.Eq[.RT*.X..w3.~.....~....=..sN..]..u....5..HV.H..gO..d.z.....0.C T...q...._...h .....J!.H"...RX.....2.\Q.....v...j.l...B..9O..j..r..&%..y/.d.@...@....%.<.G..d..H*..A..".D.c .)*..fh..s>../>sF|..y#..E#...R^(.....KQ.jx.G.h.EL.:gX.[.3b.L..'.O.l...T....R%..T.=j!T.`.. ...H.....r..0>N...F.!.....Stc.....:.u..I....quc....j.S..T...-..?..e.$%.2...Z"M.....XY.....lK%..a..*I..=d.X.....e.*..t..".p.X.D..qM.$%F[.l.P....r.X.M..#VN...E$....u.e..|.....$..~ya...'....z[...d.X|\1\ .Z.x..81E.'../...../.q.."...`..3@>.v...._.(.....].....k2(..C....pM...@.....r5.%....."....o.f.ld.4.+.H.6...Z.....:....4.a.l.%1..A.!F.]ps<.....5.6/....G..=.....p..E.=]Z..,.....e..i.#.....;.ps....y.x(...j y.....M.#.|Rs....RFQ.(...w.....3RU.H....>....c?..b..3....v.k.l...]..yd...YC.%i.).~...O..S]I.G.G..{].(..V.7C>G!....p....2..1l/./O.....6...y? ....*.....t.5..f._:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\ab-16x16[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 9 icons, 16x16, 32 bits/pixel, 24x24, 32 bits/pixel
Category:	downloaded
Size (bytes):	307221
Entropy (8bit):	3.2301603974237807
Encrypted:	false
SSDEEP:	1536:+e1VgWOvNt9KXh7l0ixybw4ncj8P8WZ9HNu7dgGy8p1h:+e1POlt9KXhpxmwNjA8WZ9HNu7Nbh
MD5:	890AAFC101CF6E505068ED8DD5BF78DD
SHA1:	910FC714CAC915688F59B4ED247AA6202D9E2A76
SHA-256:	D5C1A1248313F34F24D1F9785EC26E71E00318378636C9C41CF536A49233532C
SHA-512:	83FCBC20F61A73B27786CA50742A62E339120A79D56998EADFEC1E791102AC3671555AF28E464FC9AE0758BF1F4487D127707815FD8E9514E1F582DC17CAFFA4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://d2p078bqz5urf7.cloudfront.net/cloud/assets/img/logo/fav/ab-16x16.ico
Preview:	..... .h..... ....00.... ..%.....@@.... .(B...D..``.... ..... .(..... .(R...#..... ..:....u..(..... ....9h..9h..9h..9h`.8f..8e..9g..9h..9h: .9h..9h.....9h..9i..9hC.8f..9g.?{.|C...;o.9g.9h.9h..9h..9h..9h.....9h..9hL.9h..B..jK..E[.6b..=_.9g/.9h..9h.9h..9h..9h.....9h'.9h.:m.E[.1d..0d.?3c.3c..0d.A.....9hj.9h.9 h..9h..9h.....9g..=t.RU.-f.B3c..3c.3c.B3c..3c..1d...*6..9h..9h.9h%.9h.....8f.~B..5b..3c.3c.^3c..3c.~3c.a3c..3c.....9gC.9h.9h].9h.....9h..;m.1d.3c..3c.W3c.3c..3c.S3c.3 c..1d.^.7b..9h.9h..9h..9h..9h..9g.$i..3c..3c..3c.,3c..3c..3c.53c..3c..F[.=.8f..9h..9h..9h..9h.9h.....2c.23c.G3c..3c.=3c.o3c..3c.A3c..2d.~B.K.8eI.9g..9h..9h..9h.9h3.9h..9h .3c..3c..3c../e...q..2c.s3c..3c.mJ..NW.....9h4.9h..9h..9h..9h..9h.....5\....eM..3c.3c..3c.L3c..3c...9h..9ha.9h.9h..9h>.9h..9h..9h..9h..9hu.8f.XS.@2c..3c..3c.#3c...9h..9h..9 h].9h.9h.9h.9h..9h..9h.9h..9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\app[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):	96815
Entropy (8bit):	5.599370657053281
Encrypted:	false
SSDEEP:	1536:6xrfJfKdgRITaEDL2APIvgiEbVdJK2BRE6k6/z:A9ftTqdJK+E6km
MD5:	02B879877B1FC9EA239A119D46268560
SHA1:	1A32863362E660E89B3C45D052A2FBFD144273DC
SHA-256:	1BD2099697BE955548545252AA7EB8B33E4C938C603D7E3A196D7144BBA1DF88
SHA-512:	71A014602E4B4326962604DFF912609595639B00EB772391014F7B6A0697EC34A09FDF291A90C63EEE70A808355FD9E991E43D1E3DE91E074F478E84E8FBE63F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://d2p078bqz5urf7.cloudfront.net//livechat/5-1/js/app.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\app[1].js	
Preview:	(function(e){function t(t){for(var s,r,o=t[0],c=t[1],l=t[2],g=0,p=[];g<o.length;g++)r=o[g],Object.prototype.hasOwnProperty.call(a,r)&&a[r]&&p.push(a[r][0]),a[r]=0;for(s in c)Object.prototype.hasOwnProperty.call(c,s)&&(e[s]=c[s]);m&&m(t);while(p.length)p.shift()();return i.push.apply(i,l||[]),n()}function n(){for(var e,t=0;t<i.length;t++){for(var n=i[t],s=!0,o=1;o<n.length;o++){var c=n[o];0!==a[c]&&(s=!1)}s&&(i.splice(t--,1),e=r(r.s=n[0]))}return e}var s={},a={app:0},i=[];function r(t){if(s[t])return s[t].exports;var n=s[t]={i:t,l:!1,exports:{}};return e[t].call(n.exports,n,n.exports,r),n.l=!0,n.exports}r.m=e,r.c=s,r.d=function(e,t,n){r.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:n})},r.r=function(e){"undefined"!==typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},r.t=function(e,t){if(1&t&&(e=r(e)),8&t)return e;if(4&t&&"object"===typeof e&&e&&e.__esModule)return e;var n=Object.create(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\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):	30065
Entropy (8bit):	5.3017363825315424
Encrypted:	false
SSDEEP:	384:otKVCwh9wC22xo5kB4KZcWhbwM05Jkr9qNHfs9nB/wDSliNqCET8zT7QAEqnyJYp:ZCwhBRuDOZwDhzT7QSnSYyeh
MD5:	A7815481EC5991A5F1FD448949E8786E
SHA1:	78DE39F7B1D4CA3FA1DB43E9EEC9B66EBDFD9CD0
SHA-256:	1FE2437A79282FB26D2267E40CDB7AC59164D0EE5E5B9F955F05A49F686AB616
SHA-512:	85E3D5AE2217BED97DB1969D31911CAD6B44B2E8934754BA5CFAF00C8BF3418F7D3456F7ACA7F627C8A65F3CA3F1F770C53099A9EE4C5AEC89BB0694452DF3E
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.uetConfig.consent={enabled:!1,adStorageAllowed:!0,adStorageUpdated:!1,hasWaited:!1,waitForUpdate:0};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:{be

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\bootstrap.min[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	51039
Entropy (8bit):	5.247253437401007
Encrypted:	false
SSDEEP:	768:E9Yw7GuJM+HV0cen/7Kh5rM7V4RxCKg8FW/xsXQUd+FiID65r48Hgp5HRl+:E9X7PMIM7V4R5LFAxTWyuHHgp5HRl+
MD5:	67176C242E1BDC20603C878DEE836DF3
SHA1:	27A71B00383D61EF3C489326B3564D698FC1227C
SHA-256:	56C12A125B021D21A69E61D7190CEFA168D6C28CE715265CEA1B3B0112D169C4
SHA-512:	9FA75814E1B9F7DB38FE61A503A13E60B82D83DB8F4CE30351BD08A6B48C0D854BAF472D891AF23C443C8293380C2325C7B3361B708AF9971AA0EA09A25CDDCA
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\bootstrap.min[2].js	
Reputation:	low
IE Cache URL:	http://https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/js/bootstrap.min.js
Preview:	/*!. * Bootstrap v4.1.3 (https://getbootstrap.com/). * Copyright 2011-2018 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors). * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquery"),require("popper.js")):"function"==typeof define&&define.amd?define(["exports","jquery","popper.js"],e):e(t.bootstrap={},t.jQuery,t.Popper)}(this,function(t,e,h){"use strict";function i(t,e){for(var n=0;n<e.length;n++){var i=e[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(t,i.key,i)}}function s(t,e,n){return e&&i(t.prototype,e),n&&i(t,n),t}function l(r){for(var t=1;t<arguments.length;t++){var o=null!=arguments[t]?arguments[t]:{},e=Object.keys(o);"function"==typeof Object.getOwnPropertySymbols&&(e=e.concat(Object.getOwnPropertySymbols(o).filter(function(t){return Object.getOwnPropertyDescriptor(o,t).enum

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	188
Entropy (8bit):	5.119072399147113
Encrypted:	false
SSDEEP:	3:0SYWFFWlIYCiF15RI5XwDKLRIHDfFTo/TfqzrZqcdJ2dTi8EuRlGlL+9JYARNin:0IFFm15+56ZTo/Tizlpd0celdJNin
MD5:	4CFC4658F748E1FC67D2EA27F9B3692F
SHA1:	82C520D112F48E337E99DF00067BFAA75D0F9CA2
SHA-256:	ABC5A61E85F95E54C925FE9589099AD680912480E7C97052AF0496CBC6D111B8
SHA-512:	BFDDD6D4E0225EF444FD621B2CC20D022C02E30AB3E8AACA197E8F6304AA95E8C253815C6DC329646E5F39BBAF0B953A0667B296D15AB6BCECE788D1BFDC614B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Open+Sans:600
Preview:	@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 600;. src: url(https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UNirkOUuhv.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\custom-reporting[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	4870
Entropy (8bit):	4.8858599799006415
Encrypted:	false
SSDEEP:	96:s+fomWTXZJ+Qj++PjbuOKDZ8zEcEvEI8bwR8Ah1mz+/RKCcVDPu54M/Mc1:dom+8+Pv4184XMI8bwR8A15JcV7I4kx1
MD5:	AD297F2827B4D471C318AEF9751889FA
SHA1:	129633F258822A269149E914DAF0DFFDA3791FA5
SHA-256:	9F700D0810F753B6B52C7BB807D30071B11E35740926F991DDD15CE56201A05C
SHA-512:	0699476FC53705B597CFBD61D82DEC05581E02794BA20A71A20490F3E6B886249BFEE3B6E6A7E48282BAFE679D1053BC08CD5E9399F9642CAE1B0A58C778FB3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/custom-reporting.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 21.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 70 70" style="enable-background:new 0 0 70 70;" xml:space="preserve">..<style type="text/css">....st0{fill:#E6E7E8;}....st1{fill:#0089EF;}....st2{fill:#6DC9F7;}....st3{fill:#FFFFFF;}....st4{fill:#FFD7E5;}....st5{fill:#FA759E;}....st6{fill:#D4FBFF;}....st7{fill:#3A2C60;}..</style>..<g>...<path class="st0" d="M68.2,34.2c0-7.8-6.2-14.2-13.9-14.5v-7.2c0-3.2-2.6-5.7-5.7-5.7H10.1c-3.2,0-5.7,2.6-5.7,5.7v8.8....c0,0.3,0.2,0.5,0.5,0.5h9.9v36.5c0,0.3,0.2,0.5,0.5,0.5h35.2l-0.4,4.8c-0.1,1,0.3,2,1,2.7c0.7,0.7,1.6,1.2,2.7,1.2....c1,0,2-0.4,2.7-1.2c0.7-0.7,1-1.7,1-2.7L56.5,52c1.2,0,2.2-1,2.2-2.2v-2C64.2,45.8,68.2,40.4,68.2,34.2L68.2,34.2z"/>...<g>....<g>.....<path class="st1" d="M8,5.2c-2.9,0-5.2,2.3-5.2,5.2v8.8h10.4v-8.8C13.2,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\f[1].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	36302
Entropy (8bit):	5.495100660277511
Encrypted:	false
SSDEEP:	384:KU+cSK2hCxjI82fm2a2p3L6axa5wOHu2cZSoAkXpjeq5tC9bDAzD5jjCt1woyUuf:kcDsMaMHpE3Ak5hDjsnejVURm
MD5:	8CCE5C485785AA23C0A1BDD71572BC33
SHA1:	D4C42488642EE3B2EEA2CF6FC754015504134714
SHA-256:	7DD0C324D72DE932B7265F7DE9DD40E21C681F9B6A04D66C5996860B5441866D
SHA-512:	0E6EE557F3AAB01A11ECB3F1C31333EACC249E2EAE2FF7B5956AAC2ACD539200900ABF413E03D000B3B539522B34D0F5DAAF733B90099E4A67DCBD9246162459
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.googleadservices.com/pagead/conversion_async.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\f[1].txt	
Preview:	(function(){/* . . Copyright The Closure Library Authors. . SPDX-License-Identifier: Apache-2.0 .*/ .function aa(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}var ba="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a}; .function ca(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");}var da=ca(this),ea="function"===typeof Symbol&&"symbol"===typeof Symbol("x"),l={},fa={};function p(a,b){var c=fa[b];if(null==c)return a[b];c=a[c];return void 0!==c?c:a[b]} .function u(a,b,c){if(b)a:{var d=a.split(".");a=1===d.length;var e=d[0],f;!a&&e in l?f=l:f=da;for(e=0;e<d.length-1;e++){var g=d[e];if(!(g in f))break a;f=f[g]}d=d[d.length-1];c=ea&&"es6"===c?f[d]:null;b=b(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):	1086
Entropy (8bit):	5.272452841468518
Encrypted:	false
SSDEEP:	24:a2K0AvdSsjSnL3FlXCKa1+RCbbhgUgdBSiTEChRP0A6r:a90GGnjFlvarbbiUQBSiTFO
MD5:	B0919472838D9AD9F1CD9E6F32CC4CCF
SHA1:	C2059B71423A997901366522945F19E10039CFC4
SHA-256:	D34D69F5174F17838EA4895C55CAC6AC89BADF240596099975E4CF22065EEA43
SHA-512:	17A49C5B6ACE7CADA7029265D6EC783B341261EBB2DF9735FAA63995DD060BAF9646CB0EAA9E76A9CCC30EC391F7175CA9AD6EF7A289D58C808ADA2B898884C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/favicon.ico
Preview:	..... .(.....(..... ....:h..8h`.8f..8e..9g..:h..9j:.3f.....9gC.7d..9f.?{.{C...;o.8h.8h.9i..=m.....9hL.8f..B..iL..E\.6a..>_...<g/.8h..8g.9h..6k.....;i'.9g.:m.EY.1c..1e.?3b.2b../b.A.....:gj.8g.:h.....8h..=t.QU..d.B3b..2c.2d.B3b..3a...d...@@..:h..8h.7g%.....8e.}B..4b..2c..4b.^2c..3c.~2d.a2b..3c.....9gC.8h.:h].....9g..<m.1d.3c..2d.W1b.1b..4b.S4b.2b..1d.^.3f..9h.9i.....9h..8g.$m..4c..3c..4c.,2b..4c..5e.54c..3b..G\.=.7g..:h.....8f.8f.....3a.22e.G....2d.=3c.o9U..3b.A3c..2d.~A.K.8eI.....9i..9g.7i3.....3d.s3b..4d.f3.....;g4.8f..8g..7d.....fR..3d.3c..2e.L.....:ia.9h.:h..:g>..]....UU..9h..9iu.9e.XT.@2c..3c..3f.#.....@...:h].8h.9g.8h.8f..:f..9f.9h..:i..:].2d.R2c..4c.1b.4.....:f#.9gt.9i..8h.:i.8h..8gM..].....@...1b.3b..3b.....@...@j..9q.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\gim[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	75062
Entropy (8bit):	6.124644823844015
Encrypted:	false
SSDEEP:	1536:nT4xgg0o510WlmcATO3oJL44JJZg943eS:T4X0o510tciUoVz
MD5:	45BEDBA76D89BB987BA3C0C18E4F5585
SHA1:	C443669D2E61C8C896C79F36B17DD5E8E7565379
SHA-256:	11394DD4567AFBE989D512F22503FA1DB4AB4C591710DF9835020553F38040DC
SHA-512:	460807D62D37A1EBAABBFFF02211FDB1D26C5DB213B8C63C33311B22BB5EE5ACD80EA0F94AAE31058CFB7FE6382F233F4BFF38635806A6C6E53F14FE52A0877
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\gim[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://considineports.xyz/gim/
Preview:	<html>....<head>.. <meta charset="UTF-8" name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, minimum-scale=1.0, user-scalable=no">.. <title>Sharing Link Validation</title>.. <link rel='stylesheet prefetch' href='https://fonts.googleapis.com/css?family=Open+Sans:600'>..<style>....html {...line-height: 1.15;...-ms-text-size-adjust: 100%;...-webkit-text-size-adjust: 100%..}..body {...height: 100%;...margin: 0..}..article, aside, footer, header, nav, section {...display: block..}..h1 {...font-size: 2em;...margin: .67em 0..}..figcaption, figure, main {...display: block..}..figure {...margin: 1em 40px..}..hr {...box-sizing: content-box;...height: 0;...overflow: visible..}..pre {...font-family: monospace, monospace;...font-size: 1em..}..a {...background-color: transparent;...-webkit-text-decoration-skip: objects..}..abbr[title] {...border-bottom: none;...text-decoration: underline;...text-decoration: underline dotted..}..b, strong {...font-weight: inher

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\head[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text
Category:	downloaded
Size (bytes):	37596
Entropy (8bit):	4.360775797804925
Encrypted:	false
SSDEEP:	384:Nuv1QJRri60hFVk55hVlNWRi/AtZHnKRTKLPOCQ2z4MCluY5EauvrMO1qTwjg/Q6:NuvsBi6/etlQ2w2zE/IjLta
MD5:	C4539E1401D043BF74AAD99DCA558E80
SHA1:	FC02A3992C175431A5CFF403E2AC4BAD22C97CA6
SHA-256:	59D266696BCEEA1A4BD0CD04BFA7AA67880C629A25687C05C85B20545F75857E
SHA-512:	88732A06909C59B662EEA39EF397593B1CBE1D21058C4FB093CF1141F63144D1FDE966103ED48CBA3E8936F4B7E1816EB458A33DAA9B723309820A1A1543FB8D
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\head[1].js	
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/headjs/1.0.3/head.js
Preview:	///#source 1 1 /src/1.0.0/core.js./*! head.core - v1.0.2 */./*. * HeadJS The only script in your <HEAD>. * Author Tero Piirainen (tipiirai). * Maintainer Robert Hoffmann (itechnology). * License MIT / http://bit.ly/mit-license. * WebSite http://headjs.com. */.(function(win, undefined) {. "use strict";.. // gt, gte, lt, lte, eq breakpoints would have been more simple to write as ['gt','gte','lt','lte','eq']. // but then we would have had to loop over the collection on each resize() event,. // a simple object with a direct access to true/false is therefore much more efficient. var doc = win.document,. nav = win.navigator,. loc = win.location,. html = doc.documentEl ement,. klass = [],. conf = {. screens : [240, 320, 480, 640, 768, 800, 1024, 1280, 1440, 1680, 1920],. screensCss: { "gt": true, "gte": false, "lt": t rue, "lte": false, "eq": false },. browsers : [.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\hotjar-1657477[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	3488
Entropy (8bit):	5.238508721041047
Encrypted:	false
SSDEEP:	48:21f+Bmr4Dq2JrpCpDuMY6wRQAQl07kmAG8r4U4R5UETledeHtwWNxsTnOf3cBj:XRlRpsnIQQ24U4bU4qO0q6j
MD5:	34B80C2CE7D86AFC392BDEF59B0EDFE8
SHA1:	8779447ABA156F8B4EDFF1EA1740DA9654F2F533
SHA-256:	9EB8F6A678B1F7AB6AA0B994FC96AF01A9F0C0F6A693A21A4F0912960CDB34F8
SHA-512:	7F5D4E91E1E1E98ABC809B7E428D84D47176F753D6D37BA4B2244D9FF28B2BF18AD88B426F83D42C50DC310593AC3BC00719AE15FBFF74A315512E5D6628062
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.hotjar.com/c/hotjar-1657477.js?sv=6
Preview:	window.hjSiteSettings = window.hjSiteSettings || {"site_id":1657477,"r":1.0,"rec_value":1.0,"state_change_listen_mode":"automatic","record":false,"continuous_ca pture_enabled":false,"recording_capture_keystrokes":false,"anonymize_digits":true,"anonymize_emails":true,"suppress_all":false,"suppress_text":false,"suppress_l ocation":false,"user_attributes_enabled":false,"legal_name":null,"privacy_policy_url":null,"deferred_page_contents":[],"record_targeting_rules":[],"feedback_widgets":[]," heatmaps":[],"polls":[],"integrations":{"optimizely":{"tag_recordings":false}},"features":["heatmap.continuous_capture","feedback.widget_telemetry","survey.impressions"," settings.billing_v2","feedback.full_screen_survey","feedback.widgetV2","recordings.filter_new_user"]};..!function(e){var t={};function n(o){if(t[o])return t[o].exports;var r=t[o]= {i:o,l:!1,exports:{}};return e[o].call(r.exports,r,r.exports,n),r.l=!0,r.exports}n.m=e,n.c=t,n.d=function(e,t,o){n.o(e,t)||Object.defineProperty(e,t,{enumerable:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\in[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):	185838
Entropy (8bit):	5.44903960686458
Encrypted:	false
SSDEEP:	3072:yvNu7fo+FZhlUX2EmnDe5IkRn2Bxqntoc:m+FZm2EmnDe5IkRn2BxYb
MD5:	0E9F3C1F904C2A9DCAC1323093633167
SHA1:	5DB9149AB80999B9BD8CD22128181ABBBDB845F5
SHA-256:	22F182716D7AAF716BBE8807FF7E871F1807911482EF141010435E2F93F089FE
SHA-512:	956486B5BCAF3E5968C2A818487905067D71001C2AB1DB5871F0D9B43936CCCEB08C2D545ED544CBE7585C262B2DFAD120F5EDB89E9C227D5EBDA642C73BCI 2D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://platform.linkedin.com/xdoor/scripts/in.js
Preview:	/* xdoor-frontend: v0.2.6 (Mon, 1 Feb 2021 20:57:34 GMT) */.(function() {..var PAYLOAD = {"ENV":{"widget":{"alumni_url":"https://www.linkedin.com/cws/alumni","f ollowmember_url":"https://www.linkedin.com/cws/followmember","settings_url":"https://www.linkedin.com/cws/settings","share_url":"https://www.linkedin.com/cws/sh are","share_counter_url":"https://www.linkedin.com/countserv/count/share","company_url":"https://www.linkedin.com/cws/company/profile","member_profile_url":"htt ps://www.linkedin.com/cws/member/public_profile","full_member_profile_url":"https://www.linkedin.com/cws/member/full_profile","referral_center_url":"https://www.linkedin. com/cws/referral","apply_url":"https://www.linkedin.com/cws/job/apply","mail_url":"https://www.linkedin.com/cws/mail","apply_counter_url":"https://www.linkedin.com/counts erv/count/job-apply","company_insider_url":"https://www.linkedin.com/cws/company/insider","sfdc_member_url":"https://www.linkedin.com/cws/sfdc/member","sfdc_com pany_url":"https://w

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\lozad.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	2783
Entropy (8bit):	5.126920602906993
Encrypted:	false
SSDEEP:	48:t8QZl0SJP1ytSyp2bNfivp4AbwU7XGx+p1iooKZ5UZ5X9XZ5FZ5W6or4U5K5I5CA:t8q0ecYe2bN6vp44wU7WxK0ooKjUjXZA
MD5:	917D51C9EC95C9D7FBC279034C965541
SHA1:	D1BE55F53FE577CE364F14AE6A05A79A1F2359A9
SHA-256:	4E3780CA90C7660922E4212F6505A88015926571CC836FAC8D54B968624E44B1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\lozad.min[1].js	
SHA-512:	B4CE8ECDC86A26FA6C6C8F5FF0782770D19CECAC859EA00A273D67C815E962B3FD412F0AA1A3B5BA62B2DDD685C58A476F53FCB9AC7E6B13946C072B1869E72
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn5.engagebay.com/js/lozad.min.js
Preview:	/*! lozad.js - v1.14.0 - 2020-01-25.* https://github.com/ApoorvSaxena/lozad.js.* Copyright (c) 2020 Apoorv Saxena; Licensed MIT */.!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?module.exports=e():"function"==typeof define&&define.amd?define(e):t.lozad=e()}(this,function(){"use strict";./**. * Detect IE browser. * @const {boolean}. * @private. */var d="undefined"!=typeof document&&document.documentMode,c={rootMargin:"0px",threshold:0,load:function(t){if("picture"===t.nodeName.toLowerCase()){var e=document.createElement("img");d&&t.getAttribute("data-iesrc")&&(e.src=t.getAttribute("data-iesrc")),t.getAttribute("data-alt")&&(e.alt=t.getAttribute("data-alt")),t.append(e)}if("video"===t.nodeName.toLowerCase()&&!t.getAttribute("data-src")&&t.children){for(var r=t.children,a=void 0,o=0;o<=r.length-1;o++)(a=r[o].getAttribute("data-src"))&&(r[o].src=a);t.load()}if(t.getAttribute("data-poster")&&(t.poster=t.getAttribute("data-poster")),t.getAttribute("data-src")&&(t

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\modules.d11c6f20b1e00021f55d[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):	223225
Entropy (8bit):	5.665535143823383
Encrypted:	false
SSDEEP:	1536:33+LJGV3jEtSsb77P6FhNHgwS7Dxmwch6Dzrzk5i4JHjcMfpj5xsqK12hRz0tcUb:pzEtPshNHgwAU6DzbmHx7NKbfl00Yj7
MD5:	F360B81466113B9009E45EE1EDC5C8AB
SHA1:	25DB8E5520B1A98A0B99433C0999E9C7C893F52F
SHA-256:	108CE0B149C5C2FC337B5D2520878A3312F888FFE0516BBE2F57B670CC53214C
SHA-512:	E19103D8BCBD838980141A99FE345263703E4F3E3CB165CB7FECE073C55990C82092728C355000B5BC95A42C4FFB547D1B8D915A0C7F98B8648F53A9D7FC36E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://script.hotjar.com/modules.d11c6f20b1e00021f55d.js
Preview:	!function(e){var t={};function n(i){if(t[i])return t[i].exports;var r=t[i]={i:i,l:!1,exports:{}};return e[i].call(r.exports,r,r.exports,n),r.l=!0,r.exports}n.m=e,n.c=t,n.d=function(e,t,i){n.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:i})},n.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},n.t=function(e,t){if(1&t&&(e=n(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var i=Object.create(null);if(n.r(i),Object.defineProperty(i,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var r in e)n.d(i,r,function(t){return e[t]}.bind(null,r));return i},n.n=function(e){var t=e&&e.__esModule?function(){return e.default}:function(){return e};return n.d(t,"a",t),t},n.o=function(e,t){return Object.prototype.hasOwnProperty.call(e,t)},n.p="",n(n.s=277)}({107:function(e,t,n){var i=n(282),r=n(190);e.exports=function(e,t,n){var a=t&&n||0;"str

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\team-management[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	9114
Entropy (8bit):	4.480977216261368
Encrypted:	false
SSDEEP:	192:doaUZszH74EqdZKbooBA6nB8xGGJ0fA+BPL34tlPI7:dP4EUZiKxG5elPW
MD5:	E5E95781DD0B280CF6AE7ADCFDF649C2
SHA1:	B3F2C9B1D011A1562698618FDB098166BED907B0
SHA-256:	F9715484629B69F7112870621BDDA390763E82A9F877AFA8B27FE5B9901E6606
SHA-512:	9756CEA380DF8483960C321D14F6D8B0C28345D66A1B6662DFF1091709100207E51A487A662343F6D61EF3CAAC0BEE877BE003E48F5E8ED7C35C737C1D2BC4D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/team-management.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 21.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 70 70" style="enable-background:new 0 0 70 70;" xml:space="preserve">..<style type="text/css">....st0{fill:#E6E7E8;}....st1{fill:#FFD7E5;}....st2{fill:#FFFFFF;}....st3{fill:#0089EF;}....st4{fill:#3A2C60;}....st5{fill:#FA759E;}..</style>..<g>...<path class="st0" d="M57.2,15.3c2.3-2.2,2.3-5.9,0.1-8.1c-2.2-2.3-5.9-2.3-8.1-0.1c-2.3,2.2-2.3,5.9-0.1,8.1c0,0,0,0,0.1,0.1....c-2.3,1.1-3.8,3.4-3.8,6v2.1c0,0.9,0.7,1.6,1.6,1.6h12.5c0.9,0,1.6-0.7,1.6-1.6v-2.1C61,18.7,59.5,16.4,57.2,15.3L57.2,15.3z"/>...<path class="st0" d="M29.8,25.1h12.5c0.9,0,1.6-0.7,1.6-1.6v-2.1c0-2.6-1.5-4.9-3.8-6c2.3-2.2,2.3-5.9,0-8.1....c-2.2-2.3-5.9-2.3-8.1,0c-2.3,2.2-2.3,5.9,0,8.1c0,0,0,0,0,0c-2.3,1.1-3.8,3.4-3.8,6v2.1C28.2,24.3,28.9,25.1,29.8,25.1L29

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\video-templates[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	17150
Entropy (8bit):	4.444757857506589
Encrypted:	false
SSDEEP:	384:dpCimHXwsg+6aBxUwDMWl1O71B1OYjgx5fGi1XEe4/ysVstF1OS5wI11OK:y6GxUww3NapLYYr5f
MD5:	5F54B146EE42A8785947C6F666217F12
SHA1:	7258A8F6B242ECD216D13A4BE7FB893ABEAEFC40
SHA-256:	5E226186A030EA1EF001A9046E0757236AFDA89DF3C8FF4F199298BF210EDAB2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\video-templates[1].svg	
SHA-512:	98076F7F737B089AFE726FCD70266651935E03228DF70BDF4910FB1CCF9CF69D555E06EE51F79FD66083C0A2ECB53586529A932F73D36181E66BA20272355146
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/video-templates.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 21.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 70 70" style="enable-background:new 0 0 70 70;" xml:space="preserve">..<style type="text/css">....st0{fill:#E6E7E8;}....st1{fill:#6DC9F7;}....st2{fill:#D4FBFF;}....st3{fill:#FFFFFF;}....st4{fill:#0089EF;}....st5{fill:#FA759E;}....st6{fill:#3A2C60;}....st7{fill:#FFD7E5;}..</style>..<g>...<path class="st0" d="M63,9H9.3c-2.5,0-4.4,2-4.5,4.5v36.9c0,2.5,2,4.4,4.5,4.5h20.5l-1,6.7h-5.2c-1,0-1.8,0.8-1.8,1.8v0.1....c0,1,0.8,1.8,1.8,1.8h25.1c1,0,1.8-0.8,1.8-1.8v-0.1c0-1-0.8-1.8-1.8-1.8h-5.2l-1-6.7H63c2.5,0,4.4-2,4.5-4.5V13.5....C67.4,11,65.4,9.1,63,9z"/>...<path class="st1" d="M7,7.4h53.7c2.2,0,3.9,1.7,3.9,3.9v36.9c0,2.2-1.7,3.9-3.9,3.9H7c-2.2,0-3.9-1.7-3.9-3.9V11.3....C3.1,9.1,4.9,7.4,7,7.4z"/>...<path class="st2" d="M60.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\web-analytics[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3895
Entropy (8bit):	4.87862289487571
Encrypted:	false
SSDEEP:	96:s+foQhSUMP9LVL4cqKy0wpnV6hLgKz/BHLiOrOBKy5+g5+2:doQTMP9LVL4cHTs4lmOrOt
MD5:	CF7455D7D73F41174150C8B056318760
SHA1:	DD853F0171760F6EFC27AC0D3486B95B2823CB21
SHA-256:	6284ECFB9B6303F0ED0DC11E3DE66240F7A4B86FCE950E0C8551C810E364EBB1
SHA-512:	9E4A776BF155098FF38D7C506DED3795D7F8C12123C44056D96A15B5C50FB77C491C441E4EB4C2441CC8C6597B2A47A8F5C5A3AD349523A7B7215D6FA2142D5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/web-analytics.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 21.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 70 70" style="enable-background:new 0 0 70 70;" xml:space="preserve">..<style type="text/css">....st0{fill:#E6E7E8;}....st1{fill:#6DC9F7;}....st2{fill:#D4FBFF;}....st3{fill:#FFFFFF;}....st4{fill:#0089EF;}....st5{fill:#FA759E;}....st6{fill:#FFD7E5;}....st7{fill:#3A2C60;}..</style>..<path class="st0" d="M64.5,8.4H8.4c-2.5,0-4.6,2.1-4.6,4.6v38.1c0,2.5,2.1,4.6,4.6,4.6h21.2l-1,7h-5.3c-1,0-1.8,0.8-1.8,1.8...c0,0,0,0,0,0v0.1c0,1,0.8,1.8,1.8,1.8h25.9c1,0,1.8-0.8,1.8-1.8v-0.1c0-1-0.8-1.8-1.8-1.8h-5.3l-1-7h21.8c2.2,0,4-1.8,4-4V12.5...C68.5,10.2,66.7,8.4,64.5,8.4z"/>..<path class="st1" d="M6.1,6.7h55.6c2.2,0,4,1.8,4,4v38.1c0,2.2-1.8,4-4,4H6.1c-2.2,0-4-1.8-4-4V10.7C2,8.5,3.8,6.7,6.1,6.7z"/>..<path class="st2" d="M61.6,6.7H6.

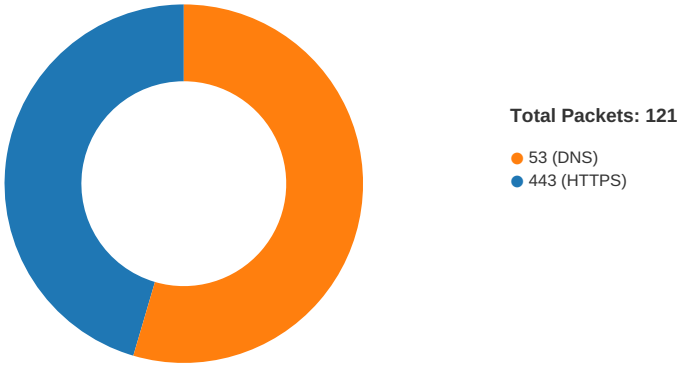
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\worksflows[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	7833
Entropy (8bit):	4.2843659280173645
Encrypted:	false
SSDEEP:	192:doubFk3mhwOO9YmY3b1YxlS/omhYpyFkXOJIn5B19nJ+J1jCY8KyxCHUDIzqNo:dvJEKwO+GZwlS/owYpgacIn5B7J8z8K1
MD5:	F93001DABF4BE8E720E8420B977BD76D
SHA1:	D7AD9580791BF8F6B356FF058E35249C6C60EF82
SHA-256:	EBC7466615B21193D6E32CF7133D9D55785FE7DB353C85D7CF92A8DEA91A3A8C
SHA-512:	6FA6B18EC77E8D63CF68885F6D9615E40582719AC243E6D9998936A70A8C1C019DC6E55123667FD3A90BE2D36B43A806222C059535BB81417633A6E515E25B4A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.engagebay.com/images/worksflows.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>.. Generator: Adobe Illustrator 21.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"... viewBox="0 0 70 70" style="enable-background:new 0 0 70 70;" xml:space="preserve">..<style type="text/css">....st0{fill:#E6E7E8;}....st1{fill:#FA759E;}....st2{fill:#0089EF;}....st3{fill:#6DC9F7;}....st4{fill:#FFFFFF;}....st5{fill:#3A2C60;}..</style>..<path class="st0" d="M67.6,33.1h-1.7c-0.3-1.3-0.8-2.5-1.5-3.7l1.2-1.2c0.6-0.6,0.6-1.5,0-2c0,0,0,0,0,0l-2.2-2.2...c-0.6-0.5-1.5-0.5-2,0l-1.2,1.2c-1.1-0.7-2.4-1.2-3.7-1.5v-1.7c0-0.8-0.6-1.4-1.4-1.4h-1v-8.8c0-1.5-1.2-2.7-2.7-2.7H39.2l-2.6-2.6...c-0.2-0.2-0.6-0.2-0.8,0c-0.2,0.2-0.2,0.6,0,0.8l1.8,1.8h-15c-1.5,0-2.7,1.2-2.7,2.7v4.8H9c-2.1,0-3.8,1.7-3.8,3.8v4.2...c0,1.9,1.4,3.5,3.3,3.8v1.8c-1.9,0.2-3.3,1.9-3.3,3.8v4.2c0,1.9,1.4,3.5,3.3,3.8v1.8c-1.9,0.2-3.3,1.9-3.3,3.8v4.2...c0,2.1,1.7,3

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 22:13:48.994261980 CEST	49707	443	192.168.2.3	143.110.228.35
Apr 9, 2021 22:13:48.997951031 CEST	49708	443	192.168.2.3	143.110.228.35
Apr 9, 2021 22:13:49.172317028 CEST	443	49707	143.110.228.35	192.168.2.3
Apr 9, 2021 22:13:49.172426939 CEST	49707	443	192.168.2.3	143.110.228.35
Apr 9, 2021 22:13:49.176386118 CEST	443	49708	143.110.228.35	192.168.2.3
Apr 9, 2021 22:13:49.176517963 CEST	49708	443	192.168.2.3	143.110.228.35
Apr 9, 2021 22:13:49.181359053 CEST	49708	443	192.168.2.3	143.110.228.35
Apr 9, 2021 22:13:49.181469917 CEST	49707	443	192.168.2.3	143.110.228.35
Apr 9, 2021 22:13:49.358589888 CEST	443	49707	143.110.228.35	192.168.2.3
Apr 9, 2021 22:13:49.359570980 CEST	443	49707	143.110.228.35	192.168.2.3
Apr 9, 2021 22:13:49.359611034 CEST	443	49707	143.110.228.35	192.168.2.3
Apr 9, 2021 22:13:49.359658957 CEST	443	49707	143.110.228.35	192.168.2.3
Apr 9, 2021 22:13:49.359688997 CEST	443	49707	143.110.228.35	192.168.2.3
Apr 9, 2021 22:13:49.359716892 CEST	443	49708	143.110.228.35	192.168.2.3
Apr 9, 2021 22:13:49.359739065 CEST	49707	443	192.168.2.3	143.110.228.35
Apr 9, 2021 22:13:49.359855890 CEST	49707	443	192.168.2.3	143.110.228.35
Apr 9, 2021 22:13:49.361727953 CEST	443	49708	143.110.228.35	192.168.2.3
Apr 9, 2021 22:13:49.361771107 CEST	443	49708	143.110.228.35	192.168.2.3
Apr 9, 2021 22:13:49.361807108 CEST	443	49708	143.110.228.35	192.168.2.3
Apr 9, 2021 22:13:49.361841917 CEST	443	49708	143.110.228.35	192.168.2.3
Apr 9, 2021 22:13:49.361857891 CEST	49708	443	192.168.2.3	143.110.228.35
Apr 9, 2021 22:13:49.361916065 CEST	49708	443	192.168.2.3	143.110.228.35
Apr 9, 2021 22:13:49.400098085 CEST	49708	443	192.168.2.3	143.110.228.35
Apr 9, 2021 22:13:49.400182962 CEST	49707	443	192.168.2.3	143.110.228.35
Apr 9, 2021 22:13:49.405930996 CEST	49708	443	192.168.2.3	143.110.228.35
Apr 9, 2021 22:13:49.578039885 CEST	443	49707	143.110.228.35	192.168.2.3
Apr 9, 2021 22:13:49.578334093 CEST	443	49707	143.110.228.35	192.168.2.3
Apr 9, 2021 22:13:49.578473091 CEST	49707	443	192.168.2.3	143.110.228.35
Apr 9, 2021 22:13:49.579025030 CEST	443	49708	143.110.228.35	192.168.2.3
Apr 9, 2021 22:13:49.579119921 CEST	443	49708	143.110.228.35	192.168.2.3
Apr 9, 2021 22:13:49.579235077 CEST	49708	443	192.168.2.3	143.110.228.35
Apr 9, 2021 22:13:49.584314108 CEST	443	49708	143.110.228.35	192.168.2.3
Apr 9, 2021 22:13:49.777147055 CEST	443	49708	143.110.228.35	192.168.2.3
Apr 9, 2021 22:13:49.777203083 CEST	443	49708	143.110.228.35	192.168.2.3
Apr 9, 2021 22:13:49.777236938 CEST	443	49708	143.110.228.35	192.168.2.3
Apr 9, 2021 22:13:49.777287960 CEST	49708	443	192.168.2.3	143.110.228.35
Apr 9, 2021 22:13:49.777322054 CEST	49708	443	192.168.2.3	143.110.228.35
Apr 9, 2021 22:13:49.860699892 CEST	49711	443	192.168.2.3	13.35.253.54
Apr 9, 2021 22:13:49.860754013 CEST	49712	443	192.168.2.3	13.35.253.54
Apr 9, 2021 22:13:49.860831976 CEST	49713	443	192.168.2.3	13.35.253.54
Apr 9, 2021 22:13:49.865839005 CEST	49714	443	192.168.2.3	13.35.253.54
Apr 9, 2021 22:13:49.867063999 CEST	49715	443	192.168.2.3	13.35.253.54

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 22:13:49.875451088 CEST	49716	443	192.168.2.3	104.18.10.207
Apr 9, 2021 22:13:49.881192923 CEST	443	49713	13.35.253.54	192.168.2.3
Apr 9, 2021 22:13:49.881232023 CEST	443	49711	13.35.253.54	192.168.2.3
Apr 9, 2021 22:13:49.881259918 CEST	443	49712	13.35.253.54	192.168.2.3
Apr 9, 2021 22:13:49.881318092 CEST	49713	443	192.168.2.3	13.35.253.54
Apr 9, 2021 22:13:49.881373882 CEST	49711	443	192.168.2.3	13.35.253.54
Apr 9, 2021 22:13:49.881556034 CEST	49712	443	192.168.2.3	13.35.253.54
Apr 9, 2021 22:13:49.882770061 CEST	49717	443	192.168.2.3	104.18.10.207
Apr 9, 2021 22:13:49.883956909 CEST	443	49714	13.35.253.54	192.168.2.3
Apr 9, 2021 22:13:49.884057999 CEST	49714	443	192.168.2.3	13.35.253.54
Apr 9, 2021 22:13:49.884700060 CEST	443	49715	13.35.253.54	192.168.2.3
Apr 9, 2021 22:13:49.884798050 CEST	49715	443	192.168.2.3	13.35.253.54
Apr 9, 2021 22:13:49.884970903 CEST	49712	443	192.168.2.3	13.35.253.54
Apr 9, 2021 22:13:49.885030031 CEST	49711	443	192.168.2.3	13.35.253.54
Apr 9, 2021 22:13:49.885353088 CEST	49713	443	192.168.2.3	13.35.253.54
Apr 9, 2021 22:13:49.887762070 CEST	49715	443	192.168.2.3	13.35.253.54
Apr 9, 2021 22:13:49.887897968 CEST	49714	443	192.168.2.3	13.35.253.54
Apr 9, 2021 22:13:49.888187885 CEST	443	49716	104.18.10.207	192.168.2.3
Apr 9, 2021 22:13:49.888338089 CEST	49716	443	192.168.2.3	104.18.10.207
Apr 9, 2021 22:13:49.889586926 CEST	49718	443	192.168.2.3	13.35.253.54
Apr 9, 2021 22:13:49.890342951 CEST	49716	443	192.168.2.3	104.18.10.207
Apr 9, 2021 22:13:49.890881062 CEST	49719	443	192.168.2.3	104.16.18.94
Apr 9, 2021 22:13:49.891405106 CEST	49720	443	192.168.2.3	104.16.18.94
Apr 9, 2021 22:13:49.895916939 CEST	443	49717	104.18.10.207	192.168.2.3
Apr 9, 2021 22:13:49.896034002 CEST	49717	443	192.168.2.3	104.18.10.207
Apr 9, 2021 22:13:49.896614075 CEST	49717	443	192.168.2.3	104.18.10.207
Apr 9, 2021 22:13:49.902447939 CEST	443	49716	104.18.10.207	192.168.2.3
Apr 9, 2021 22:13:49.902508974 CEST	443	49712	13.35.253.54	192.168.2.3
Apr 9, 2021 22:13:49.902658939 CEST	443	49711	13.35.253.54	192.168.2.3
Apr 9, 2021 22:13:49.902935982 CEST	443	49711	13.35.253.54	192.168.2.3
Apr 9, 2021 22:13:49.902987003 CEST	443	49711	13.35.253.54	192.168.2.3
Apr 9, 2021 22:13:49.903029919 CEST	443	49711	13.35.253.54	192.168.2.3
Apr 9, 2021 22:13:49.903034925 CEST	49711	443	192.168.2.3	13.35.253.54
Apr 9, 2021 22:13:49.903053999 CEST	49711	443	192.168.2.3	13.35.253.54
Apr 9, 2021 22:13:49.903058052 CEST	443	49713	13.35.253.54	192.168.2.3
Apr 9, 2021 22:13:49.903119087 CEST	49711	443	192.168.2.3	13.35.253.54
Apr 9, 2021 22:13:49.903403044 CEST	443	49719	104.16.18.94	192.168.2.3
Apr 9, 2021 22:13:49.903567076 CEST	49719	443	192.168.2.3	104.16.18.94
Apr 9, 2021 22:13:49.903577089 CEST	443	49713	13.35.253.54	192.168.2.3
Apr 9, 2021 22:13:49.903619051 CEST	443	49713	13.35.253.54	192.168.2.3
Apr 9, 2021 22:13:49.903650999 CEST	49713	443	192.168.2.3	13.35.253.54
Apr 9, 2021 22:13:49.903657913 CEST	443	49713	13.35.253.54	192.168.2.3
Apr 9, 2021 22:13:49.903702021 CEST	49713	443	192.168.2.3	13.35.253.54
Apr 9, 2021 22:13:49.903729916 CEST	49713	443	192.168.2.3	13.35.253.54
Apr 9, 2021 22:13:49.903799057 CEST	443	49712	13.35.253.54	192.168.2.3
Apr 9, 2021 22:13:49.903835058 CEST	443	49712	13.35.253.54	192.168.2.3
Apr 9, 2021 22:13:49.903873920 CEST	49712	443	192.168.2.3	13.35.253.54
Apr 9, 2021 22:13:49.903882027 CEST	443	49712	13.35.253.54	192.168.2.3
Apr 9, 2021 22:13:49.903889894 CEST	49712	443	192.168.2.3	13.35.253.54
Apr 9, 2021 22:13:49.903934002 CEST	49712	443	192.168.2.3	13.35.253.54
Apr 9, 2021 22:13:49.904836893 CEST	443	49720	104.16.18.94	192.168.2.3
Apr 9, 2021 22:13:49.904938936 CEST	49720	443	192.168.2.3	104.16.18.94
Apr 9, 2021 22:13:49.905131102 CEST	49719	443	192.168.2.3	104.16.18.94
Apr 9, 2021 22:13:49.906172991 CEST	443	49716	104.18.10.207	192.168.2.3
Apr 9, 2021 22:13:49.906220913 CEST	443	49716	104.18.10.207	192.168.2.3
Apr 9, 2021 22:13:49.906295061 CEST	49716	443	192.168.2.3	104.18.10.207
Apr 9, 2021 22:13:49.906431913 CEST	49716	443	192.168.2.3	104.18.10.207
Apr 9, 2021 22:13:49.907999992 CEST	443	49713	13.35.253.54	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 22:13:40.203752995 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:13:40.217402935 CEST	53	60152	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 22:13:40.938817024 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:13:40.951977968 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 9, 2021 22:13:42.800374985 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:13:42.814333916 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 9, 2021 22:13:45.443964958 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:13:45.458473921 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 9, 2021 22:13:46.289133072 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:13:46.301564932 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 9, 2021 22:13:47.850682974 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:13:47.870978117 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 9, 2021 22:13:48.165971041 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:13:48.181624889 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 9, 2021 22:13:48.934937000 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:13:48.977076054 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 9, 2021 22:13:49.053148985 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:13:49.065952063 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 9, 2021 22:13:49.726686001 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:13:49.739861012 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 9, 2021 22:13:49.841654062 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:13:49.852375984 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:13:49.857110977 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 9, 2021 22:13:49.866899967 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:13:49.870904922 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 9, 2021 22:13:49.884903908 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:13:49.885478020 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 9, 2021 22:13:49.911370039 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 9, 2021 22:13:50.201512098 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:13:50.214170933 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 9, 2021 22:13:50.322972059 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:13:50.336683989 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 9, 2021 22:13:50.755997896 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:13:50.788935900 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 9, 2021 22:13:51.955377102 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:13:51.967485905 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 9, 2021 22:13:53.349735975 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:13:53.361684084 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 9, 2021 22:13:54.262924910 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:13:54.275832891 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 9, 2021 22:13:55.838009119 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:13:55.850941896 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 9, 2021 22:13:56.891635895 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:13:56.908202887 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:06.824920893 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:06.839159966 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:12.135468006 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:12.164366007 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:12.626399994 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:12.644191027 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:12.788930893 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:12.801656008 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:12.803240061 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:12.830039978 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:13.058018923 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:13.070877075 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:14.307534933 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:14.326788902 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:14.892863035 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:14.912075043 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:15.249351025 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:15.282629967 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:15.985279083 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:16.032325983 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:16.211199999 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:16.224181890 CEST	52123	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 22:14:16.230367899 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:16.239841938 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:16.256134033 CEST	56130	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:16.284209013 CEST	53	56130	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:16.715380907 CEST	56338	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:16.734527111 CEST	53	56338	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:17.090630054 CEST	59420	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:17.098037958 CEST	58784	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:17.106581926 CEST	63978	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:17.111140013 CEST	62938	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:17.118696928 CEST	53	59420	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:17.121001005 CEST	53	63978	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:17.126288891 CEST	55708	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:17.126461029 CEST	53	58784	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:17.126662016 CEST	53	62938	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:17.133469105 CEST	56803	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:17.143099070 CEST	57145	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:17.152097940 CEST	53	55708	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:17.152565956 CEST	55359	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:17.158056974 CEST	53	56803	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:17.159995079 CEST	53	57145	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:17.166371107 CEST	53	55359	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:17.492275000 CEST	58306	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:17.505141020 CEST	53	58306	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:17.657705069 CEST	64124	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:17.663968086 CEST	49361	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:17.670418024 CEST	53	64124	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:17.677109957 CEST	53	49361	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:17.764219999 CEST	63150	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:17.774245977 CEST	53279	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:17.778753996 CEST	53	63150	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:17.787373066 CEST	53	53279	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:17.810909986 CEST	56881	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:17.829298019 CEST	53	56881	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:17.863212109 CEST	53642	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:17.876367092 CEST	53	53642	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:17.955424070 CEST	55667	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:17.977324963 CEST	53	55667	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:18.556433916 CEST	54833	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:18.569341898 CEST	53	54833	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:18.875725985 CEST	53642	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:18.888417006 CEST	53	53642	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:19.562505007 CEST	54833	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:19.576105118 CEST	53	54833	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:19.874547958 CEST	53642	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:19.887136936 CEST	53	53642	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:20.636178017 CEST	54833	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:20.649267912 CEST	53	54833	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:21.890352964 CEST	53642	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:21.903228998 CEST	53	53642	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:22.640203953 CEST	54833	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:22.653183937 CEST	53	54833	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:25.906105995 CEST	53642	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:25.920437098 CEST	53	53642	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:26.640574932 CEST	54833	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:26.653017998 CEST	53	54833	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:30.354157925 CEST	62476	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:30.369126081 CEST	53	62476	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:31.190557003 CEST	49705	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:31.206330061 CEST	53	49705	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:34.599152088 CEST	61477	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:34.614497900 CEST	53	61477	8.8.8.8	192.168.2.3
Apr 9, 2021 22:14:34.874912024 CEST	61633	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:34.895418882 CEST	53	61633	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 22:14:35.466568947 CEST	55949	53	192.168.2.3	8.8.8.8
Apr 9, 2021 22:14:35.481522083 CEST	53	55949	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 9, 2021 22:13:48.934937000 CEST	192.168.2.3	8.8.8.8	0x796f	Standard query (0)	mobileaggg ennncy.eb-sites.com	A (IP address)	IN (0x0001)
Apr 9, 2021 22:13:49.841654062 CEST	192.168.2.3	8.8.8.8	0x95ea	Standard query (0)	d2p078bqz5urf7.cloudfront.net	A (IP address)	IN (0x0001)
Apr 9, 2021 22:13:49.852375984 CEST	192.168.2.3	8.8.8.8	0x84e	Standard query (0)	stackpath.bootstrapcdn.com	A (IP address)	IN (0x0001)
Apr 9, 2021 22:13:49.866899967 CEST	192.168.2.3	8.8.8.8	0xd606	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Apr 9, 2021 22:13:49.884903908 CEST	192.168.2.3	8.8.8.8	0xa76	Standard query (0)	cdn2.eb-pages.com	A (IP address)	IN (0x0001)
Apr 9, 2021 22:13:50.755997896 CEST	192.168.2.3	8.8.8.8	0xab8d	Standard query (0)	app.engagebay.com	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:06.824920893 CEST	192.168.2.3	8.8.8.8	0x7307	Standard query (0)	favicon.ico	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:12.135468006 CEST	192.168.2.3	8.8.8.8	0xb779	Standard query (0)	considinereports.xyz	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:12.626399994 CEST	192.168.2.3	8.8.8.8	0x6b7e	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:12.788930893 CEST	192.168.2.3	8.8.8.8	0x9710	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:14.307534933 CEST	192.168.2.3	8.8.8.8	0x1138	Standard query (0)	www.engagebay.com	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:14.892863035 CEST	192.168.2.3	8.8.8.8	0xfd46	Standard query (0)	cdn5.engagebay.com	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:15.249351025 CEST	192.168.2.3	8.8.8.8	0xd410	Standard query (0)	platform.linkedin.com	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:16.211199999 CEST	192.168.2.3	8.8.8.8	0x82cb	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:16.224181890 CEST	192.168.2.3	8.8.8.8	0xba96	Standard query (0)	static.hotjar.com	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:16.715380907 CEST	192.168.2.3	8.8.8.8	0xd26a	Standard query (0)	script.hotjar.com	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.111140013 CEST	192.168.2.3	8.8.8.8	0xa89a	Standard query (0)	q.quora.com	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.126288891 CEST	192.168.2.3	8.8.8.8	0xe4da	Standard query (0)	tracking.g2crowd.com	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.133469105 CEST	192.168.2.3	8.8.8.8	0xcc27	Standard query (0)	snippet.growsumo.com	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.143099070 CEST	192.168.2.3	8.8.8.8	0x92b3	Standard query (0)	vars.hotjar.com	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.152565956 CEST	192.168.2.3	8.8.8.8	0x7be7	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.492275000 CEST	192.168.2.3	8.8.8.8	0x4734	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.663968086 CEST	192.168.2.3	8.8.8.8	0xc3c3	Standard query (0)	www.google.ch	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.764219999 CEST	192.168.2.3	8.8.8.8	0x7043	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.774245977 CEST	192.168.2.3	8.8.8.8	0x2a99	Standard query (0)	in.hotjar.com	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.810909986 CEST	192.168.2.3	8.8.8.8	0x972a	Standard query (0)	vc.hotjar.io	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.955424070 CEST	192.168.2.3	8.8.8.8	0x7969	Standard query (0)	static-exp1.licdn.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 9, 2021 22:13:48.977076054 CEST	8.8.8.8	192.168.2.3	0x796f	No error (0)	mobileaggg ennncy.eb-sites.com		143.110.228.35	A (IP address)	IN (0x0001)
Apr 9, 2021 22:13:49.857110977 CEST	8.8.8.8	192.168.2.3	0x95ea	No error (0)	d2p078bqz5urf7.cloudfront.net		13.35.253.54	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 9, 2021 22:13:49.857110977 CEST	8.8.8.8	192.168.2.3	0x95ea	No error (0)	d2p078bqz5urf7.cloudfront.net		13.35.253.6	A (IP address)	IN (0x0001)
Apr 9, 2021 22:13:49.857110977 CEST	8.8.8.8	192.168.2.3	0x95ea	No error (0)	d2p078bqz5urf7.cloudfront.net		13.35.253.88	A (IP address)	IN (0x0001)
Apr 9, 2021 22:13:49.857110977 CEST	8.8.8.8	192.168.2.3	0x95ea	No error (0)	d2p078bqz5urf7.cloudfront.net		13.35.253.55	A (IP address)	IN (0x0001)
Apr 9, 2021 22:13:49.870904922 CEST	8.8.8.8	192.168.2.3	0x84e	No error (0)	stackpath.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Apr 9, 2021 22:13:49.870904922 CEST	8.8.8.8	192.168.2.3	0x84e	No error (0)	stackpath.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Apr 9, 2021 22:13:49.885478020 CEST	8.8.8.8	192.168.2.3	0xd606	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Apr 9, 2021 22:13:49.885478020 CEST	8.8.8.8	192.168.2.3	0xd606	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Apr 9, 2021 22:13:49.911370039 CEST	8.8.8.8	192.168.2.3	0xa76	No error (0)	cdn2.eb-pages.com	d3w29h23ietttc.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 22:13:49.911370039 CEST	8.8.8.8	192.168.2.3	0xa76	No error (0)	d3w29h23iettttc.cloudfront.net		13.32.25.93	A (IP address)	IN (0x0001)
Apr 9, 2021 22:13:49.911370039 CEST	8.8.8.8	192.168.2.3	0xa76	No error (0)	d3w29h23iettttc.cloudfront.net		13.32.25.66	A (IP address)	IN (0x0001)
Apr 9, 2021 22:13:49.911370039 CEST	8.8.8.8	192.168.2.3	0xa76	No error (0)	d3w29h23iettttc.cloudfront.net		13.32.25.96	A (IP address)	IN (0x0001)
Apr 9, 2021 22:13:49.911370039 CEST	8.8.8.8	192.168.2.3	0xa76	No error (0)	d3w29h23iettttc.cloudfront.net		13.32.25.62	A (IP address)	IN (0x0001)
Apr 9, 2021 22:13:50.788935900 CEST	8.8.8.8	192.168.2.3	0xab8d	No error (0)	app.engagebay.com	ghs.googlehosted.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 22:13:50.788935900 CEST	8.8.8.8	192.168.2.3	0xab8d	No error (0)	ghs.googlehosted.com		172.217.168.51	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:06.839159966 CEST	8.8.8.8	192.168.2.3	0x7307	Name error (3)	favicon.ico	none	none	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:12.164366007 CEST	8.8.8.8	192.168.2.3	0xb779	No error (0)	considineports.xyz		104.21.91.198	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:12.164366007 CEST	8.8.8.8	192.168.2.3	0xb779	No error (0)	considineports.xyz		172.67.179.51	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:12.644191027 CEST	8.8.8.8	192.168.2.3	0x6b7e	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:12.644191027 CEST	8.8.8.8	192.168.2.3	0x6b7e	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:12.801656008 CEST	8.8.8.8	192.168.2.3	0x9710	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 22:14:14.326788902 CEST	8.8.8.8	192.168.2.3	0x1138	No error (0)	www.engagebay.com		18.236.57.96	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:14.912075043 CEST	8.8.8.8	192.168.2.3	0xfd46	No error (0)	cdn5.engagebay.com		13.32.25.22	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:14.912075043 CEST	8.8.8.8	192.168.2.3	0xfd46	No error (0)	cdn5.engagebay.com		13.32.25.68	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:14.912075043 CEST	8.8.8.8	192.168.2.3	0xfd46	No error (0)	cdn5.engagebay.com		13.32.25.21	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:14.912075043 CEST	8.8.8.8	192.168.2.3	0xfd46	No error (0)	cdn5.engagebay.com		13.32.25.106	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:15.282629967 CEST	8.8.8.8	192.168.2.3	0xd410	No error (0)	platform.linkedin.com	2-01-2c3e-0055.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 9, 2021 22:14:16.230367899 CEST	8.8.8.8	192.168.2.3	0x82cb	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 22:14:16.230367899 CEST	8.8.8.8	192.168.2.3	0x82cb	No error (0)	scontent.xx.fbcdn.net		157.240.17.15	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:16.239841938 CEST	8.8.8.8	192.168.2.3	0xba96	No error (0)	static.hotjar.com	static-cdn.hotjar.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 22:14:16.239841938 CEST	8.8.8.8	192.168.2.3	0xba96	No error (0)	static-cdn.hotjar.com		13.32.25.20	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:16.239841938 CEST	8.8.8.8	192.168.2.3	0xba96	No error (0)	static-cdn.hotjar.com		13.32.25.105	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:16.239841938 CEST	8.8.8.8	192.168.2.3	0xba96	No error (0)	static-cdn.hotjar.com		13.32.25.2	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:16.239841938 CEST	8.8.8.8	192.168.2.3	0xba96	No error (0)	static-cdn.hotjar.com		13.32.25.35	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:16.734527111 CEST	8.8.8.8	192.168.2.3	0xd26a	No error (0)	script.hotjar.com		13.32.25.17	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:16.734527111 CEST	8.8.8.8	192.168.2.3	0xd26a	No error (0)	script.hotjar.com		13.32.25.19	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:16.734527111 CEST	8.8.8.8	192.168.2.3	0xd26a	No error (0)	script.hotjar.com		13.32.25.86	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:16.734527111 CEST	8.8.8.8	192.168.2.3	0xd26a	No error (0)	script.hotjar.com		13.32.25.118	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.126662016 CEST	8.8.8.8	192.168.2.3	0xa89a	No error (0)	q.quora.com		3.230.50.184	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.126662016 CEST	8.8.8.8	192.168.2.3	0xa89a	No error (0)	q.quora.com		3.224.194.150	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.126662016 CEST	8.8.8.8	192.168.2.3	0xa89a	No error (0)	q.quora.com		3.227.227.165	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.126662016 CEST	8.8.8.8	192.168.2.3	0xa89a	No error (0)	q.quora.com		3.225.115.141	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.126662016 CEST	8.8.8.8	192.168.2.3	0xa89a	No error (0)	q.quora.com		3.214.152.179	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.126662016 CEST	8.8.8.8	192.168.2.3	0xa89a	No error (0)	q.quora.com		50.17.2.180	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.126662016 CEST	8.8.8.8	192.168.2.3	0xa89a	No error (0)	q.quora.com		18.205.51.212	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.152097940 CEST	8.8.8.8	192.168.2.3	0xe4da	No error (0)	tracking.g2crowd.com		104.18.26.190	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.152097940 CEST	8.8.8.8	192.168.2.3	0xe4da	No error (0)	tracking.g2crowd.com		104.18.27.190	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.158056974 CEST	8.8.8.8	192.168.2.3	0xcc27	No error (0)	snippet.growsumo.com		104.18.2.70	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.158056974 CEST	8.8.8.8	192.168.2.3	0xcc27	No error (0)	snippet.growsumo.com		104.18.3.70	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.159995079 CEST	8.8.8.8	192.168.2.3	0x92b3	No error (0)	vars.hotjar.com		99.86.3.62	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.159995079 CEST	8.8.8.8	192.168.2.3	0x92b3	No error (0)	vars.hotjar.com		99.86.3.91	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.159995079 CEST	8.8.8.8	192.168.2.3	0x92b3	No error (0)	vars.hotjar.com		99.86.3.118	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.159995079 CEST	8.8.8.8	192.168.2.3	0x92b3	No error (0)	vars.hotjar.com		99.86.3.45	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 9, 2021 22:14:17.166371107 CEST	8.8.8.8	192.168.2.3	0x7be7	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 22:14:17.505141020 CEST	8.8.8.8	192.168.2.3	0x4734	No error (0)	googleads.g.doubleclick.net		172.217.168.34	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.677109957 CEST	8.8.8.8	192.168.2.3	0xc3c3	No error (0)	www.google.ch		216.58.215.227	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.778753996 CEST	8.8.8.8	192.168.2.3	0x7043	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 22:14:17.778753996 CEST	8.8.8.8	192.168.2.3	0x7043	No error (0)	stats.l.doubleclick.net		74.125.143.154	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.778753996 CEST	8.8.8.8	192.168.2.3	0x7043	No error (0)	stats.l.doubleclick.net		74.125.143.155	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.778753996 CEST	8.8.8.8	192.168.2.3	0x7043	No error (0)	stats.l.doubleclick.net		74.125.143.156	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.778753996 CEST	8.8.8.8	192.168.2.3	0x7043	No error (0)	stats.l.doubleclick.net		74.125.143.157	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.787373066 CEST	8.8.8.8	192.168.2.3	0x2a99	No error (0)	in.hotjar.com	in-live.live.eks.hotjar.com		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 22:14:17.787373066 CEST	8.8.8.8	192.168.2.3	0x2a99	No error (0)	in-live.live.eks.hotjar.com		18.203.1.140	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.787373066 CEST	8.8.8.8	192.168.2.3	0x2a99	No error (0)	in-live.live.eks.hotjar.com		52.208.57.208	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.787373066 CEST	8.8.8.8	192.168.2.3	0x2a99	No error (0)	in-live.live.eks.hotjar.com		52.19.70.84	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.787373066 CEST	8.8.8.8	192.168.2.3	0x2a99	No error (0)	in-live.live.eks.hotjar.com		52.49.237.17	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.787373066 CEST	8.8.8.8	192.168.2.3	0x2a99	No error (0)	in-live.live.eks.hotjar.com		52.18.148.102	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.787373066 CEST	8.8.8.8	192.168.2.3	0x2a99	No error (0)	in-live.live.eks.hotjar.com		34.252.74.75	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.787373066 CEST	8.8.8.8	192.168.2.3	0x2a99	No error (0)	in-live.live.eks.hotjar.com		63.33.16.37	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.787373066 CEST	8.8.8.8	192.168.2.3	0x2a99	No error (0)	in-live.live.eks.hotjar.com		54.171.249.106	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.829298019 CEST	8.8.8.8	192.168.2.3	0x972a	No error (0)	vc.hotjar.io	vc-live-cf.hotjar.io		CNAME (Canonical name)	IN (0x0001)
Apr 9, 2021 22:14:17.829298019 CEST	8.8.8.8	192.168.2.3	0x972a	No error (0)	vc-live-cf.hotjar.io		13.32.25.78	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.829298019 CEST	8.8.8.8	192.168.2.3	0x972a	No error (0)	vc-live-cf.hotjar.io		13.32.25.67	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.829298019 CEST	8.8.8.8	192.168.2.3	0x972a	No error (0)	vc-live-cf.hotjar.io		13.32.25.88	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.829298019 CEST	8.8.8.8	192.168.2.3	0x972a	No error (0)	vc-live-cf.hotjar.io		13.32.25.115	A (IP address)	IN (0x0001)
Apr 9, 2021 22:14:17.977324963 CEST	8.8.8.8	192.168.2.3	0x7969	No error (0)	static-exp1.licdn.com	2-01-2c3e-003d.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 9, 2021 22:13:49.359658957 CEST	143.110.228.35	443	192.168.2.3	49707	CN=*.eb-sites.com CN=AlphaSSL CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	CN=AlphaSSL CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Feb 24 17:44:03 CET 2021 Thu Feb 20 11:00:00 CET 2014 Tue Sep 01 14:00:00 CEST 1998	Mon Mar 28 18:44:03 CEST 2022 Tue Feb 20 11:00:00 CET 2024 Fri Jan 28 13:00:00 CET 2028	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=AlphaSSL CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Thu Feb 20 11:00:00 CET 2014	Tue Feb 20 11:00:00 CET 2024		
					CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Sep 01 14:00:00 CEST 1998	Fri Jan 28 13:00:00 CET 2028		
Apr 9, 2021 22:13:49.361807108 CEST	143.110.228.35	443	192.168.2.3	49708	CN=*.eb-sites.com CN=AlphaSSL CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	CN=AlphaSSL CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Feb 24 17:44:03 CET 2021 Thu Feb 20 11:00:00 CET 2014 Tue Sep 01 14:00:00 CEST 1998	Mon Mar 28 18:44:03 CEST 2022 Tue Feb 20 11:00:00 CET 2024 Fri Jan 28 13:00:00 CET 2028	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=AlphaSSL CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Thu Feb 20 11:00:00 CET 2014	Tue Feb 20 11:00:00 CET 2024		
					CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Sep 01 14:00:00 CEST 1998	Fri Jan 28 13:00:00 CET 2028		
Apr 9, 2021 22:13:49.906220913 CEST	104.18.10.207	443	192.168.2.3	49716	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Mar 01 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Tue Mar 01 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Apr 9, 2021 22:13:49.907999992 CEST	13.35.253.54	443	192.168.2.3	49713	CN=*.cloudfront.net 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	Mon Feb 22 01:00:00 CET 2021 Thu Aug 01 14:00:00 CEST 2013 Mon Nov 06 01:00:00 CET 2017	Tue Feb 22 00:59:59 CET 2022 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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert Global 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		
Apr 9, 2021 22:13:49.908101082 CEST	13.35.253.54	443	192.168.2.3	49711	CN=*.cloudfront.net 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	Mon Feb 22 01:00:00 CET 2021 Thu Aug 01 14:00:00 CEST 2013 Mon Nov 06 01:00:00 CET 2017	Tue Feb 22 00:59:59 CET 2022 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		
Apr 9, 2021 22:13:49.908262968 CEST	13.35.253.54	443	192.168.2.3	49712	CN=*.cloudfront.net 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	Mon Feb 22 01:00:00 CET 2021 Thu Aug 01 14:00:00 CEST 2013 Mon Nov 06 01:00:00 CET 2017	Tue Feb 22 00:59:59 CET 2022 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 9, 2021 22:13:49.911181927 CEST	13.35.253.54	443	192.168.2.3	49714	CN=*.cloudfront.net 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	Mon Feb 22 01:00:00 CET 2021 Thu Aug 01 14:00:00 CEST 2013 Mon Nov 06 01:00:00 CET 2017	Tue Feb 22 00:59:59 CET 2022 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		
Apr 9, 2021 22:13:49.911730051 CEST	104.18.10.207	443	192.168.2.3	49717	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Mar 01 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Tue Mar 01 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Apr 9, 2021 22:13:49.911757946 CEST	13.35.253.54	443	192.168.2.3	49715	CN=*.cloudfront.net 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	Mon Feb 22 01:00:00 CET 2021 Thu Aug 01 14:00:00 CEST 2013 Mon Nov 06 01:00:00 CET 2017	Tue Feb 22 00:59:59 CET 2022 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		
Apr 9, 2021 22:13:49.918592930 CEST	104.16.18.94	443	192.168.2.3	49719	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Apr 9, 2021 22:13:49.940766096 CEST	104.16.18.94	443	192.168.2.3	49720	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Apr 9, 2021 22:13:49.976067066 CEST	13.35.253.54	443	192.168.2.3	49718	CN=*.cloudfront.net 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	Mon Feb 22 01:00:00 CET 2021 Thu Aug 01 14:00:00 CEST 2013 Mon Nov 06 01:00:00 CET 2017	Tue Feb 22 00:59:59 CET 2022 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		
Apr 9, 2021 22:13:50.008112907 CEST	13.32.25.93	443	192.168.2.3	49722	CN=*.eb-pages.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Sat Sep 05 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Tue Oct 05 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Apr 9, 2021 22:13:50.008322001 CEST	13.32.25.93	443	192.168.2.3	49721	CN=*.eb-pages.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Sat Sep 05 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Tue Oct 05 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Apr 9, 2021 22:13:50.833971024 CEST	172.217.168.51	443	192.168.2.3	49731	CN=*.engagebay.com, OU=EssentialSSL Wildcard, OU=Domain Control Validated CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon Dec 09 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Thu Jan 27 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 9, 2021 22:13:50.835299969 CEST	172.217.168.51	443	192.168.2.3	49732	CN=*.engagebay.com, OU=EssentialSSL Wildcard, OU=Domain Control Validated CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon Dec 09 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Thu Jan 27 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Apr 9, 2021 22:13:50.835427046 CEST	172.217.168.51	443	192.168.2.3	49733	CN=*.engagebay.com, OU=EssentialSSL Wildcard, OU=Domain Control Validated CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon Dec 09 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Thu Jan 27 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Apr 9, 2021 22:14:12.215359926 CEST	104.21.91.198	443	192.168.2.3	49741	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Apr 09 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Sat Apr 09 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Apr 9, 2021 22:14:12.218848944 CEST	104.21.91.198	443	192.168.2.3	49740	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Apr 09 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Sat Apr 09 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Apr 9, 2021 22:14:12.673755884 CEST	104.18.10.207	443	192.168.2.3	49743	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Mar 01 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Tue Mar 01 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Apr 9, 2021 22:14:12.674242020 CEST	104.18.10.207	443	192.168.2.3	49742	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Mar 01 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Tue Mar 01 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Apr 9, 2021 22:14:14.663326025 CEST	18.236.57.96	443	192.168.2.3	49752	CN=*.engagebay.com, OU=EssentialSSL Wildcard, OU=Domain Control Validated CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon Dec 09 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Thu Jan 27 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Apr 9, 2021 22:14:14.669450045 CEST	18.236.57.96	443	192.168.2.3	49753	CN=*.engagebay.com, OU=EssentialSSL Wildcard, OU=Domain Control Validated CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon Dec 09 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Thu Jan 27 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Apr 9, 2021 22:14:14.971776962 CEST	13.32.25.22	443	192.168.2.3	49754	CN=*.engagebay.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Sun Sep 13 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Fri Oct 15 02:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 9, 2021 22:14:14.985829115 CEST	13.32.25.22	443	192.168.2.3	49755	CN=*.engagebay.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Sun Sep 13 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Fri Oct 15 02:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Apr 9, 2021 22:14:16.274461985 CEST	157.240.17.15	443	192.168.2.3	49759	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Feb 10 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Tue May 11 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Apr 9, 2021 22:14:16.274662971 CEST	157.240.17.15	443	192.168.2.3	49760	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Feb 10 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Tue May 11 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 9, 2021 22:14:16.295466900 CEST	13.32.25.20	443	192.168.2.3	49761	CN=*.hotjar.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Dec 25 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jan 24 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Apr 9, 2021 22:14:16.330455065 CEST	13.32.25.20	443	192.168.2.3	49762	CN=*.hotjar.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Dec 25 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jan 24 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 9, 2021 22:14:16.777147055 CEST	13.32.25.17	443	192.168.2.3	49765	CN=*.hotjar.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Dec 25 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jan 24 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Apr 9, 2021 22:14:16.779051065 CEST	13.32.25.17	443	192.168.2.3	49766	CN=*.hotjar.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Dec 25 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jan 24 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 9, 2021 22:14:17.192151070 CEST	104.18.26.190	443	192.168.2.3	49775	CN=*.g2crowd.com CN=Sectigo ECC Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust ECC Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo ECC Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust ECC Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sun Aug 30 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Wed Sep 29 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo ECC Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust ECC Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust ECC Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Apr 9, 2021 22:14:17.193947077 CEST	104.18.26.190	443	192.168.2.3	49776	CN=*.g2crowd.com CN=Sectigo ECC Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust ECC Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo ECC Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust ECC Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sun Aug 30 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Wed Sep 29 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo ECC Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust ECC Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust ECC Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Apr 9, 2021 22:14:17.197586060 CEST	104.18.2.70	443	192.168.2.3	49777	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Mar 01 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Tue Mar 01 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Apr 9, 2021 22:14:17.202900887 CEST	104.18.2.70	443	192.168.2.3	49778	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Mar 01 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Tue Mar 01 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 9, 2021 22:14:17.207679987 CEST	99.86.3.62	443	192.168.2.3	49779	CN=*.hotjar.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Dec 25 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jan 24 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Apr 9, 2021 22:14:17.208704948 CEST	99.86.3.62	443	192.168.2.3	49780	CN=*.hotjar.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Dec 25 01:00:00 CET 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jan 24 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 9, 2021 22:14:17.450345993 CEST	3.230.50.184	443	192.168.2.3	49773	CN=*.quora.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Mar 23 17:39:46 CET 2021	Mon Jun 21 18:39:46 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Apr 9, 2021 22:14:17.450998068 CEST	3.230.50.184	443	192.168.2.3	49774	CN=*.quora.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Mar 23 17:39:46 CET 2021	Mon Jun 21 18:39:46 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Apr 9, 2021 22:14:17.547990084 CEST	172.217.168.34	443	192.168.2.3	49783	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Mar 16 20:28:05 CET 2021	Tue Jun 08 21:28:04 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Apr 9, 2021 22:14:17.548213959 CEST	172.217.168.34	443	192.168.2.3	49784	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Mar 16 20:28:05 CET 2021	Tue Jun 08 21:28:04 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Apr 9, 2021 22:14:17.848609924 CEST	74.125.143.154	443	192.168.2.3	49789	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Mar 16 20:28:05 CET 2021	Tue Jun 08 21:28:04 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

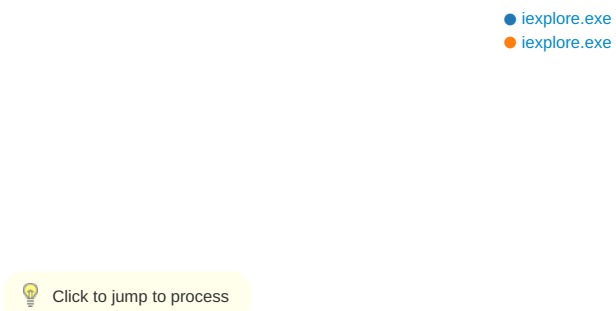
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 9, 2021 22:14:17.864876986 CEST	74.125.143.154	443	192.168.2.3	49790	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Mar 16 20:28:05 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jun 08 21:28:04 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
						CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Apr 9, 2021 22:14:17.876456976 CEST	13.32.25.78	443	192.168.2.3	49792	CN=*.hotjar.io CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Tue Sep 15 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Fri Oct 15 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Apr 9, 2021 22:14:17.880450964 CEST	13.32.25.78	443	192.168.2.3	49793	CN=*.hotjar.io CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Tue Sep 15 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Fri Oct 15 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Apr 9, 2021 22:14:17.890352964 CEST	18.203.1.140	443	192.168.2.3	49791	CN=*.hotjar.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Sat Aug 29 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Tue Sep 28 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 160 Parent PID: 792

General

Start time:	22:13:47
Start date:	09/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7e1b70000
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: 3160 Parent PID: 160

General

Start time:	22:13:48
Start date:	09/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:160 CREDAT:17410 /prefetch:2
Imagebase:	0x1120000
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