ID: 375557
Cookbook: browseurl.jbs
Time: 03:16:05
Date: 25/03/2021
Version: 31.0.0 Emerald

Table of Contents

Copyright Joe Security LLC 2021

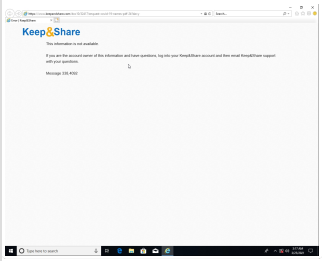
Analysis Report https://www.keepandshare.com/doc10/...

Overview

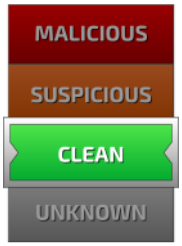
General Information

Sample URL:	http://https://www.keepandshare.com/doc10/32417/enquest-covid-19-names-pdf-2k?da=y
Analysis ID:	375557
Infos:	

Most interesting Screenshot:



Detection

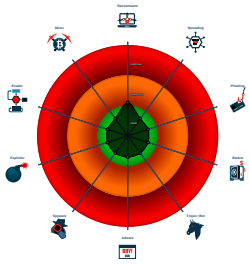


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 4692 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5288 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4692 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

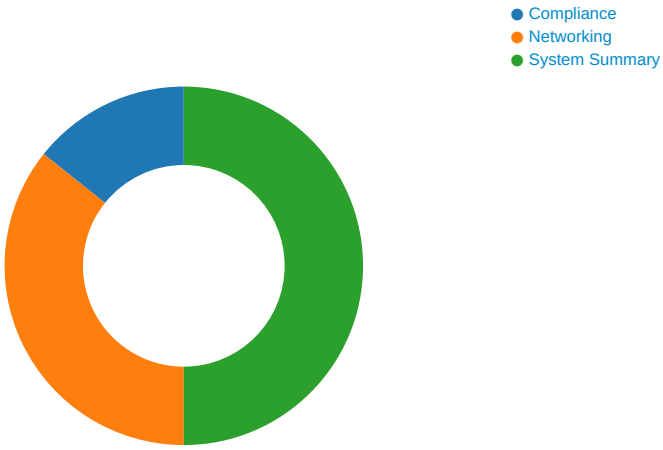
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

Copyright Joe Security LLC 2021



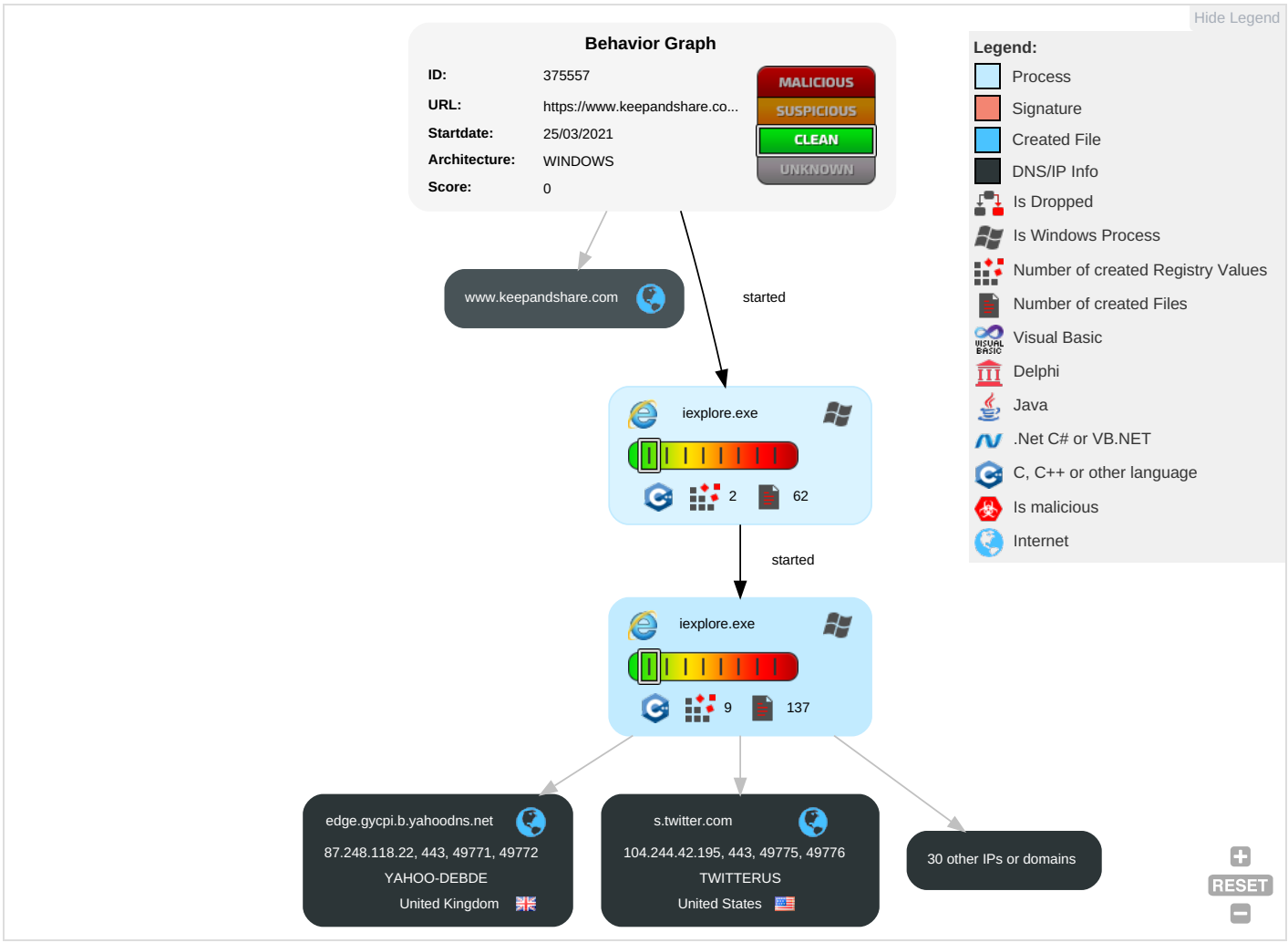
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

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

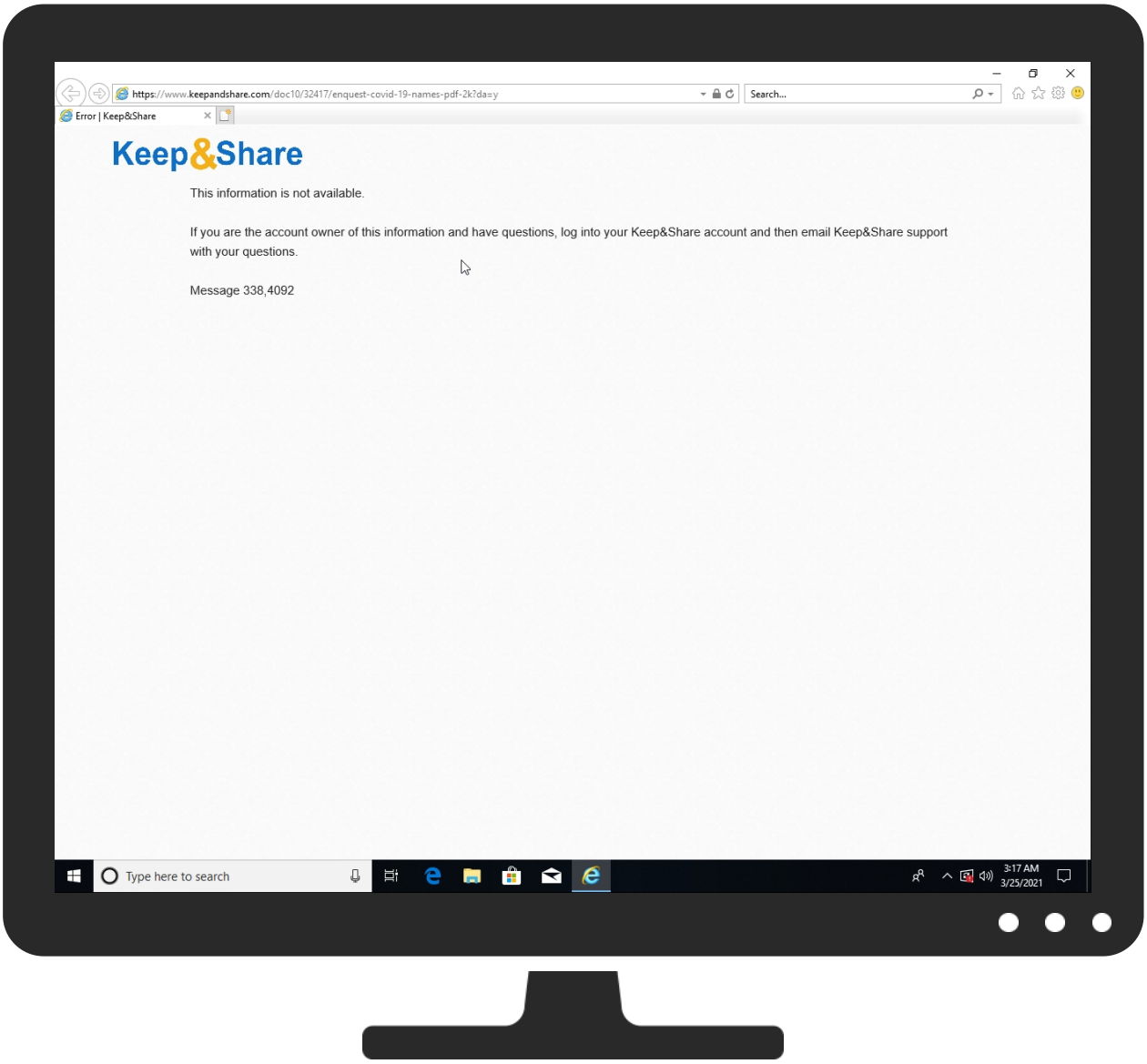
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://www.keepandshare.com/doc10/32417/enquest-covid-19-names-pdf-2k?da=y	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://keepn.com/graphics/lpgraphics/core_pages/index/hero_image.min_v2018.png	0%	Avira URL Cloud	safe	
http://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://fontawesome.iohttp://fontawesome.iohttp://fontawesome.io/license/http://fontawesome.io/licens	0%	Avira URL Cloud	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.keepare.com/oc10/32417/enquest-covid-19-names-pdf-2k?da=yRoot	0%	Avira URL Cloud	safe	
http://www.iloveflipbooks.com/	0%	Avira URL Cloud	safe	
http://https://www.keepare.com/htm/contact_us.phpRoot	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
star-mini.c10r.facebook.com	31.13.86.36	true	false		high
g.global-ssl.fastly.net	151.101.0.65	true	false		unknown
www.keepn.com	64.62.174.128	true	false		unknown
us-u.openx.net	34.98.64.218	true	false		high
stats.l.doubleclick.net	66.102.1.155	true	false		high
s.twitter.com	104.244.42.195	true	false		high
rec.mouseflowaps.netdna-cdn.com	23.111.9.38	true	false		high
prod-eu-pixel-collector-vpc-145135437.eu-west-1.elb.amazonaws.com	52.215.255.105	true	false		high
www.keepandshare.com	64.71.144.43	true	false		high
scontent.xx.fbcdn.net	157.240.17.15	true	false		high
googleads.g.doubleclick.net	172.217.168.34	true	false		high
keepn.com	66.160.183.118	true	false		unknown
cm.g.doubleclick.net	172.217.168.66	true	false		high
ads-bid.l.doubleclick.net	74.125.133.154	true	false		high
widget.trustpilot.com	52.84.138.122	true	false		high
www.google.ch	216.58.215.227	true	false		high
ib.anycast.adnxs.com	37.252.173.62	true	false		high
edge.gycpi.b.yahoodns.net	87.248.118.22	true	false		unknown
www.facebook.com	unknown	unknown	false		high
cdn.mouseflow.com	unknown	unknown	false		high
bid.g.doubleclick.net	unknown	unknown	false		high
pixel.rubiconproject.com	unknown	unknown	false		high
secure.adnxs.com	unknown	unknown	false		high
pixel-geo.prfct.co	unknown	unknown	false		unknown
connect.facebook.net	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
analytics.twitter.com	unknown	unknown	false		high
ads.yahoo.com	unknown	unknown	false		high
tag.marinsm.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.keepandshare.com/htm/contact_us.php	false		high
http://https://www.keepandshare.com/doc10/32417/enquest-covid-19-names-pdf-2k?da=y	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontawesome.io	fontawesome-webfont[1].eot.2.dr, master_external-20180124_1031.min[1].css.2.dr	false		high
http://https://www.keepandshare.com/doc10/32417/enquest-covid-19-names-pdf-2k?da=y	{368AFD0C-8D53-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://developer.keepandshare.com/	WV1W1JAQ.htm.2.dr, contact_us[1].htm.2.dr	false		high

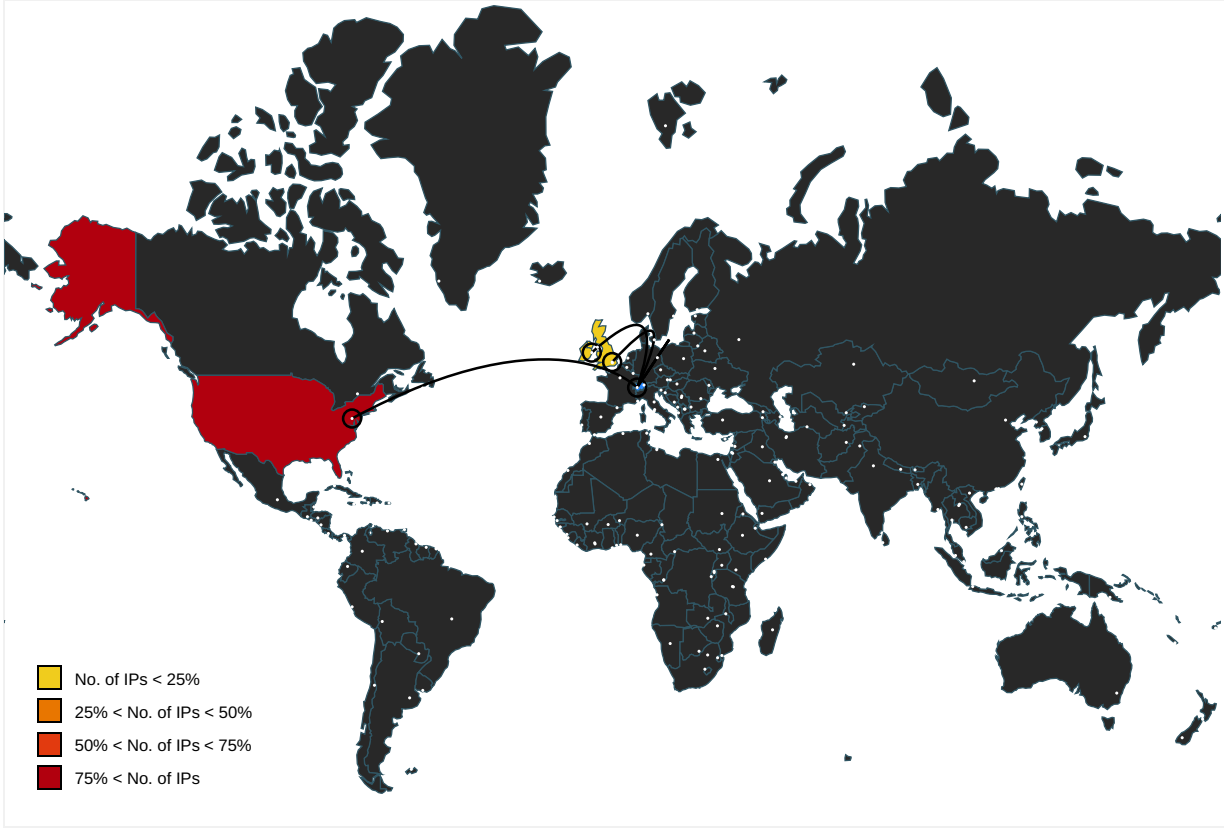
Copyright Joe Security LLC 2021

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://keepn.com/graphics/lpgraphics/core_pages/index/hero_image.min_v2018.png	WV1W1JAQ.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://jquery.org/license	prototype-1.7.3.min[1].js.2.dr	false		high
http://https://support.keepandshare.com	contact_us[1].htm.2.dr	false		high
http://sizzlejs.com/	prototype-1.7.3.min[1].js.2.dr	false		high
http://https://www.trustpilot.com/reviews/5e37e73c3c93ae04c0d91817	539ad60defb9600b94d7df2c[1].json.2.dr	false		high
http://https://www.trustpilot.com/reviews/5f5da04502e8570acc36cb0c	539ad60defb9600b94d7df2c[1].json.2.dr	false		high
http://https://www.keepandshare.com/business/registration_pre.php?form=free_trial	WV1W1JAQ.htm.2.dr	false		high
http://https://www.trustpilot.com/reviews/5ebc367f25e5d209b8ea0577	539adbd6dec7e10e686debee[1].json.2.dr	false		high
http://https://www.keepandshare.com/business/registration_pre.php	WV1W1JAQ.htm.2.dr	false		high
http://https://www.keepandshare.com/htm/contact_us.php	{368AFD0C-8D53-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://www.trustpilot.com/reviews/5e1c7f21c845450bec365306	539ad60defb9600b94d7df2c[1].json.2.dr	false		high
http://https://www.keepandshare.com/htm/message/request_consultation.php	WV1W1JAQ.htm.2.dr, contact_us[1].htm.2.dr	false		high
http://https://www.keepandshare.com	539ad60defb9600b94d7df2c[1].json.2.dr	false		high
http://https://www.keepandshare.com/htm/calendar_self_booking.php	WV1W1JAQ.htm.2.dr	false		high
http://https://www.trustpilot.com/reviews/5e79154e3c93ae0964699854	539adbd6dec7e10e686debee[1].json.2.dr	false		high
http://https://www.keepandshare.com/m/index.php	WV1W1JAQ.htm.2.dr	false		high
http://https://www.trustpilot.com/reviews/5e3bc02d3c93ae04c0db84c4	539ad60defb9600b94d7df2c[1].json.2.dr	false		high
http://https://www.trustpilot.com/review/keepandshare.com	WV1W1JAQ.htm.2.dr, 539adbd6dec7e10e686debee[1].json.2.dr, contact_us[1].htm.2.dr, 539ad60defb9600b94d7df2c[1].json.2.dr	false		high
http://https://www.trustpilot.com/reviews/5ed1613025e5d20a88a2d9c4	539adbd6dec7e10e686debee[1].json.2.dr	false		high
http://www.keepandshare.com/business/support_email/support_email_form.php?type=support	contact_us[1].htm.2.dr	false		high
http://https://www.trustpilot.com/reviews/5eab597c086b64095444c602	539ad60defb9600b94d7df2c[1].json.2.dr	false		high
http://https://connect.facebook.net/en_US/fbevents.js	registration[1].htm.2.dr	false		high
http://https://www.keepandshare.com/business/registration.php?form=free_trial&ifr=y&lp=	{368AFD0C-8D53-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://getbootstrap.com)	bootstrap.min[1].js.2.dr	false	• Avira URL Cloud: safe	low
http://https://www.trustpilot.com/reviews/5e723d163c93ae0964667056	539adbd6dec7e10e686debee[1].json.2.dr, 539ad60defb9600b94d7df2c[1].json.2.dr	false		high
http://https://www.trustpilot.com/reviews/5f095b1e3f06f202a45aef4b	539adbd6dec7e10e686debee[1].json.2.dr	false		high
http://https://www.keepandshare.com/	{368AFD0C-8D53-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://www.keepandshare.com/favicon.ico~	imagestore.dat.2.dr	false		high
http://https://www.trustpilot.com/reviews/5ed6a55825e5d20a88a5da9c	539ad60defb9600b94d7df2c[1].json.2.dr	false		high
http://https://www.trustpilot.com/reviews/5f3eabd402e85708c8d534de	539adbd6dec7e10e686debee[1].json.2.dr	false		high
http://https://www.trustpilot.com/reviews/5e1ca337c8454503e830ec5c	539ad60defb9600b94d7df2c[1].json.2.dr	false		high
http://https://stats.g.doubleclick.net/j/collect	analytics[1].js.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.keepandshare.com/doc10/32417/enquest-covid-19-names-pdf-2k?da=yRoot	{368AFD0C-8D53-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://www.keepandshare.com/doc10/32417/enquest-covid-19-names-pdf-2k?da=y$Error	{368AFD0C-8D53-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://www.trustpilot.com/reviews/5eaafe03086b640954447d45	539adbd6dec7e10e686debee[1].json.2.dr	false		high
http://https://www.trustpilot.com/reviews/5f3164531a5a690788a5c826	539adbd6dec7e10e686debee[1].json.2.dr	false		high
http://https://support.keepandshare.com/a/solutions/categories/92413	contact_us[1].htm.2.dr	false		high
http://https://www.trustpilot.com/reviews/5f738521798e6f0960230d13	539adbd6dec7e10e686debee[1].json.2.dr	false		high
http://https://www.trustpilot.com/evaluate/keepandshare.com	5406e65db0d04a09e042d5fc[2].json.2.dr, 539adbd6dec7e10e686debee[1].json.2.dr, 539ad60defb9600b94d7df2c[1].json.2.dr	false		high
http://https://widget.trustpilot.com/trustboxes/539adbd6dec7e10e686debee/index.html?businessunitId=5654e51c	{368AFD0C-8D53-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://www.apache.org/licenses/LICENSE-2.0	KFOlCnqEu92Fr1MmYUtfBBc9[1].ttf.2.dr, KFOmCnqEu92Fr1Mu4mxP[1].ttf.2.dr, KFOlCnqEu92Fr1MmEU9fBBc9[1].ttf.2.dr	false		high
http://https://widget.trustpilot.com/trustboxes/539ad60defb9600b94d7df2c/index.html?businessunitId=5654e51c	{368AFD0C-8D53-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://www.trustpilot.com/evaluate/embed/keepandshare.com	5406e65db0d04a09e042d5fc[2].json.2.dr, 539adbd6dec7e10e686debee[1].json.2.dr, 539ad60defb9600b94d7df2c[1].json.2.dr	false		high
http://https://www.trustpilot.com/reviews/5f281ed21a5a6907a4798d53	539ad60defb9600b94d7df2c[1].json.2.dr	false		high
http://https://support.keepandshare.com/	WV1W1JAQ.htm.2.dr	false		high
http://https://www.trustpilot.com/reviews/5e25fd103c93ae0b249339a3	539ad60defb9600b94d7df2c[1].json.2.dr	false		high
http://https://www.trustpilot.com/reviews/5ee827277dd7530828c1edf1	539adbd6dec7e10e686debee[1].json.2.dr	false		high
http://fontawesome.iohttp://fontawesome.iohttp://fontawesome.io/license/http://fontawesome.io/licens	fontawesome-webfont[1].eot.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.trustpilot.com/reviews/5ed4399625e5d20a88a4228a	539adbd6dec7e10e686debee[1].json.2.dr, 539ad60defb9600b94d7df2c[1].json.2.dr	false		high
http://https://www.keepandshare.com/business/support_email/support_email_form.php	WV1W1JAQ.htm.2.dr	false		high
http://https://www.keepandshare.com/htm/contact_us.php-covid-19-names-pdf-2k?da=y	~DFF9C80A2350DB77A3.TMP.1.dr	false		high
http://https://www.trustpilot.com/reviews/5e6acbbe3c93ae0964631243	539adbd6dec7e10e686debee[1].json.2.dr	false		high
http://https://www.trustpilot.com/reviews/5f6df3f1798e6f09601fe872	539adbd6dec7e10e686debee[1].json.2.dr, 539ad60defb9600b94d7df2c[1].json.2.dr	false		high
http://https://www.trustpilot.com/reviews/5e8abc41086b6409bc7df9cd	539adbd6dec7e10e686debee[1].json.2.dr	false		high
http://https://www.trustpilot.com/reviews/5f9708295e693f06f872130c	539adbd6dec7e10e686debee[1].json.2.dr	false		high
http://www.keepandshare.com/global/lp/js/matchMedia/0.1.1/matchMedia.js	WV1W1JAQ.htm.2.dr	false		high
http://www.keepandshare.com/business/support_email/support_email_form.php	contact_us[1].htm.2.dr	false		high
http://https://www.keepandshare.com/htm/contact_us.php2Contact	~DFF9C80A2350DB77A3.TMP.1.dr	false		high
http://https://www.trustpilot.com/reviews/5fdba86d755dc107e0c6b8fa	539ad60defb9600b94d7df2c[1].json.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.trustpilot.com/reviews/5f9da8a95e693f06f87692bd	539adbd6dec7e10e686debee[1].json.2.dr, 539ad60defb9600b94d7df2c[1].json.2.dr	false		high
http://https://cct.google/taggy/agent.js	js[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontawesome.io/license	master_external-20180124_1031.min[1].css.2.dr	false		high
http://https://www.trustpilot.com/reviews/5f456f5e02e85708c8d8c2f3	539adbd6dec7e10e686debee[1].json.2.dr	false		high
http://fontawesome.io/license/	fontawesome-webfont[1].eot.2.dr	false		high
http://https://www.trustpilot.com/reviews/5f3237631a5a690788a638cf	539adbd6dec7e10e686debee[1].json.2.dr, 539ad60defb9600b94d7df2c[1].json.2.dr	false		high
http://https://bid.g.doubleclick.net/xbbe/pixel?d=KAE	{368AFD0C-8D53-11EB-90E4-ECF4BB862DED}.dat.1.dr, f[1].txt.2.dr	false		high
http://https://www.keepandshare.com/oc10/32417/enquest-covid-19-names-pdf-2k?da=y	~DFF9C80A2350DB77A3.TMP.1.dr	false		high
http://https://www.keepandshare.com/xOnline	{368AFD0C-8D53-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://widget.trustpilot.com/trustboxes/5406e65db0d04a09e042d5fc/index.html?businessunitId=5654e51c	{368AFD0C-8D53-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://www.google.%/ads/ga-audiences	analytics[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://www.keepare.com/oc10/32417/enquest-covid-19-names-pdf-2k?da=yRoot	{368AFD0C-8D53-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.keepandshare.com/favicon.ico	imagestore.dat.2.dr	false		high
http://https://www.keepandshare.com/index_signin.php	WV1W1JAQ.htm.2.dr	false		high
http://https://www.trustpilot.com/reviews/5f58d91702e85707dcef1486	539ad60defb9600b94d7df2c[1].json.2.dr	false		high
http://www.iloveflipbooks.com/	WV1W1JAQ.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	master_external-20180124_1031.min[1].css.2.dr	false		high
http://https://www.trustpilot.com/reviews/5eb584b525e5d209b8e58d15	539adbd6dec7e10e686debee[1].json.2.dr	false		high
http://https://www.trustpilot.com/reviews/5dfa9f08c845450b74324784	539ad60defb9600b94d7df2c[1].json.2.dr	false		high
http://https://www.trustpilot.com/reviews/5f3678039cc22a073c979286	539ad60defb9600b94d7df2c[1].json.2.dr	false		high
http://https://www.keepare.com/htm/contact_us.phpRoot	{368AFD0C-8D53-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.google.ch/pagead/1p-user-list/1067089813/?random	f[1].txt0.2.dr, f[2].txt.2.dr	false		high
http://https://www.trustpilot.com/reviews/5e56d2593c93ae0bc40aec17	539ad60defb9600b94d7df2c[1].json.2.dr	false		high
http://scripts.sil.org/OFL	K6ngFdK5haaaRGBV8waDwA[1].ttf.2.dr, nHiQo1BypvYzt95zlPq1TvesZW2xOQ-xsNqO47m55DA[1].ttf.2.dr	false		high
http://https://www.trustpilot.com/reviews/5df630f7c845450b742f8871	539ad60defb9600b94d7df2c[1].json.2.dr	false		high
http://https://www.trustpilot.com/reviews/5fc995ca5e693f07049f3a8b	539adbd6dec7e10e686debee[1].json.2.dr	false		high
http://https://widget.trustpilot.com/bootstrap/v5/tp.widget.bootstrap.min.js	tp.widget.sync.bootstrap.min[1].js.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.215.255.105	prod-eu-pixel-collector-vpc-145135437.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
52.84.138.122	widget.trustpilot.com	United States		16509	AMAZON-02US	false
74.125.133.154	ads-bid.l.doubleclick.net	United States		15169	GOOGLEUS	false
23.111.9.38	rec.mouseflowaps.netdna-cdn.com	United States		33438	HIGHWINDS2US	false
66.160.183.118	keepn.com	United States		54288	SOLIDTOOLSINCUS	false
151.101.0.65	g.global-ssl.fastly.net	United States		54113	FASTLYUS	false
157.240.17.15	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
66.102.1.155	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
64.62.174.128	www.keepn.com	United States		6939	HURRICANEUS	false
172.217.168.66	cm.g.doubleclick.net	United States		15169	GOOGLEUS	false
31.13.86.36	star-mini.c10r.facebook.com	Ireland		32934	FACEBOOKUS	false
64.71.144.43	www.keepandshare.com	United States		6939	HURRICANEUS	false
216.58.215.227	www.google.ch	United States		15169	GOOGLEUS	false
87.248.118.22	edge.gycpi.b.yahoodns.net	United Kingdom		203220	YAHOO-DEBDE	false
104.244.42.195	s.twitter.com	United States		13414	TWITTERUS	false
172.217.168.34	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
37.252.173.62	ib.anycast.adnxs.com	European Union		29990	ASN-APPNEXUS	false
34.98.64.218	us-u.openx.net	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	375557
Start date:	25.03.2021
Start time:	03:16:05
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 18s

Copyright Joe Security LLC 2021

Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://www.keepandshare.com/doc10/32417/enquest-covid-19-names-pdf-2k?da=y
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	7
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@3/96@20/18
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://www.keepandshare.com/
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.42.151.234, 104.43.193.48, 104.83.120.32, 172.217.168.78, 172.217.168.35, 216.58.215.226, 204.79.197.200, 13.107.21.200, 216.58.215.228, 172.217.168.3, 69.173.144.139, 69.173.144.138, 69.173.144.165, 152.199.19.161, 23.54.113.104, 20.50.102.62 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, www.googleadservices.com, arc.msn.com.nsatc.net, pixel.rubiconproject.net.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, bat.bing.com, www.google.com, arc.trafficmanager.net, watson.telemetry.microsoft.com, www.gstatic.com, prod.fs.microsoft.com.akadns.net, www.google-analytics.com, fs.microsoft.com, www-google-analytics.l.google.com, fonts.gstatic.com, dual-a-0001.a-msedge.net, ie9comview.vo.msecnd.net, e1723.g.akamaiedge.net, skypedataprdcolcus15.cloudapp.net, bat-bing-com.a-0001.a-msedge.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • VT rate limit hit for: https://www.keepandshare.com/doc10/32417/enquest-covid-19-names-pdf-2k?da=y

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\IQKAPMW1\www.keepandshare[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):	1246
Entropy (8bit):	4.915468209426338
Encrypted:	false
SSDEEP:	24:WUKa4QQxJmiQQxDtMQxOlF9WMQx/UKa4vQxJmogYQxDtMQxOlF9WMQx/UKa4vQxP:LKaNQxJm3QxDyQxOf9HQxMKaGQxJmBYH
MD5:	FA2433EF4996CE9638E2B62CECA42B05
SHA1:	5AB14C39FC4BF1299B13F652B0C775755B9162F5
SHA-256:	0B1F72FE1B4431CAE2491CC8E80C73A7D2F6F29E58489E21A1028A6EA016A728
SHA-512:	B5BCBCA784B426D20BCFCDC663FF783934B4A7EC010A41C603EC98E3B9D8226A90FFF42A15C0A1A576EB3D017EB30E71B1068E1300908C257AC6B6638050525C
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="_uetsid" value="447914108d5311ebbfe15d83c3ce850d" ltime="104254000" htime="30876000" /><item name="_uetsid_exp" value="Fri, 26 Mar 2021 10:17:13 GMT" ltime="104254000" htime="30876000" /><item name="_uetvid" value="44796b008d5311ebbcbc9fd7191ee237" ltime="104294000" htime="30876000" /><item name="_uetvid_exp" value="Sat, 10 Apr 2021 16:17:13 GMT" ltime="104294000" htime="30876000" /></root><root><item name="_uetsid" value="447914108d5311ebbfe15d83c3ce850d" ltime="122154000" htime="30876000" /><item name="_uetsid_exp" value="Fri, 26 Mar 2021 10:17:15 GMT" ltime="122194000" htime="30876000" /><item name="_uetvid" value="44796b008d5311ebbcbc9fd7191ee237" ltime="104294000" htime="30876000" /><item name="_uetvid_exp" value="Sat, 10 Apr 2021 16:17:13 GMT" ltime="104294000" htime="30876000" /></root><root><item name="_uetsid" value="447914108d5311ebbfe15d83c3ce850d" ltime="122154000" htime="30876000" /><item name="_uetsid_exp" value="Fri, 26 Mar 2021 10:17:15 GM

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\X1FQLEDM\www.google[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	111
Entropy (8bit):	4.877882089176732
Encrypted:	false
SSDEEP:	3:D90aK1ryRtFwsW+pEeAqSfqnJz9t2i/CqSQT/tuFKb:JFK1rUFy+pEeAqVn/szQT/tukb
MD5:	DE7F37AFEDDC3C118912C462308816C8
SHA1:	0CBD621B736E902235386F528FF3FA2E93849681
SHA-256:	5D5C5610F295D191EAA3260BE599EB9B7E073717132D6C966163EE102F1BBA0E
SHA-512:	CF520B5264285A28ED037AFEB64A681F42B5A432CEFB891988B6CE7A5CE56F1DE252260107E8E497D591B3DB2E7AFFFE8E449D0C9CCB5E6923A7CBDCDCA1C9E2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\X1FQLEDM\www.google[1].xml	
Preview:	<root></root><root><item name="rc::a" value="MWx4czd4MW43NXR5bQ==" ltime="114574000" htime="30876000" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{368AFD0A-8D53-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8540266255753297
Encrypted:	false
SSDEEP:	96:rNLZHGZ1P2oMWkg9tkAfk8tMkjTkZkQfkkMX:rxZmZF2VWlthfvtMoyNfbMX
MD5:	4BCD4517C17B60D7C7063E8C3D4D9777
SHA1:	C849DA0489927C18701C929D9A5FA1060F35FB75
SHA-256:	90BFD6BF1E79DB2FC6A529E05D6AFAD27C0F9862F238AFEA9976A662138014CD
SHA-512:	381B7A013B6B8A1CD1EA37D0089598EF00A3970210747607813D5158585BB2158BC7A62C486565349D5E25D92D332E8CA96FBF4AC57A629DB56E92323C9AA35B
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\{368AFD0C-8D53-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	62284
Entropy (8bit):	2.769425616477201
Encrypted:	false
SSDEEP:	384:rgsyulQEhyAlA5DFPhYiG9JdBy9dyLe7h751ojsoKY+KF2ofN8j8Fnd9gTBgJST:o/oK8FfVvu
MD5:	842C0AAD93C70E5BDB73E618DF0EEDAC
SHA1:	26F14D5BC682F9820F078FCBA0D99902324153AF
SHA-256:	A25748C3D7811B24ED3DEAC7987416212F4F523A96F11507E98994130A7E41B7
SHA-512:	5F621F2503E09B7C7A5D88426EA618356247BDFB09A80852980276525CF6D6CE47955C8A1A69F6D571C0F8BA36D50AB002880EFBC596510170D4FC48E513AA33
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\{368AFD0D-8D53-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5639847122990622
Encrypted:	false
SSDEEP:	48:IwBGcprQGwpaJG4pQFGrapbSvGQpKxG7HpRMTGIpG:r3Z4QL61BS5AgTYA
MD5:	D2C461905177E9FBC8C966B2DA12A916
SHA1:	EFDF0C7C6D63BE672CAF8F1EDF5374214214E325
SHA-256:	2FD56D1E176FB955AA033FD8A84056DC3FD369B8B036D9CEEF8F7DB1DF13F61E
SHA-512:	6A4B1350F30CD9D5F892DD50BDFC744C33FEE71ABFC0003DC4918780105A58E5CCF50F08269B7C0E3FBA5384D40EBBE294D2E999BFE38D4AF1914D4C3684EC F
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Size (bytes):	15452
Entropy (8bit):	4.1296805393431715
Encrypted:	false
SSDEEP:	96:/Fq+j72Qs4fRKx5JU0/4fme+4+ffQewYxsin/CM/afZRuYGza/fAou9WAjLLhzaL:Nq+axIO4faFxn6FDGCfARLkrxxxF
MD5:	03DC62965602C7FD102DA217147670BC
SHA1:	E6B8A7B4BF251FE009EA9621921D228E031E1E66
SHA-256:	1F0CD6B84E7B81039B6E9EB892F14B1C706B0045B7E2EA08AAB121F42D524A3B
SHA-512:	1DFC79077DF025FB1549DF1FB7F2963393B3D2EBC1A3177C176C327040FDF33753C313075311CBE4226942BEC3854C75907ABBB6C98B75CFACC5B6641E82C82
Malicious:	false
Reputation:	low
Preview:	(.h.t.t.p.s.:././.w.w.w...k.e.e.p.a.n.d.s.h.a.r.e...c.o.m./.f.a.v.i.c.o.n...i.c.o.~..... .h.....(..... ....y.s.y...y...y...y...y...y...y...y...y...y...y...y...y...y...y...y.s.y...y.. .y...y...x...{...~...~...z...x...x...z...{...y...y...y...y...y...{...._.G...3...4...J.....V...l.`...Z....|...y...y...y...y..p.w.....*.....1.....S..x...y...y....".-.....e..... .d.....!. ..r.u..}...y...y...y...x....8. ...!.....8..x...z..]..... '.....3..x...y...y...y...y....!.-.....u.p..y..t.r..... ...,.....i....y...y...y...y...y...p.w.....%...V...%.....f.....V.K.....\..y...y...y...y...y...y...{..t.q. &.....2.....$..y...z...y...y...y...y...y...y...x...~..9.....U....~...y...y...y...y...y...y...y...x..v.n.....+...~..c.D.....i....y...y...y...y...y...y...y...y..Q.....`....w....P.....G....z.. .y...y...y...y...y...y...y...y..l.}.....4...p.w.E.....g....y...y...y...y...y...y...y...y...~..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\5406e65db0d04a09e042d5fc[1].json	
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):	984
Entropy (8bit):	4.990360405989179
Encrypted:	false
SSDEEP:	24:Ya77cyxEFuM77cyxEFuL28bwVQwOaIW/G9teaoKouIgTZIt:YaXhEF/XhEFHiW/PatXlgTZ4
MD5:	03E888BCD26307CA75DD120D41D8FAE3
SHA1:	5E1534A03FC655A8DAAC526C3F7B6604C0CCCA16
SHA-256:	10D34C681282F9D4AF9CAD648B0D33438E66E64BEE236B95D96AABD50A3E9A05
SHA-512:	EF3F4B351143D2ECE1C726F50029F761F92993A7B45CF171055217A6875D7B3EF1EF215632EAD3BC56576D785AE70763FB9C58BF2D2091E871D9CDD651DA453(
Malicious:	false
Reputation:	low
Preview:	{"businessUnit":{"stars":4.5,"trustScore":4.7,"displayName":"Keep&Share","numberOfReviews":{"total":1975,"oneStar":10,"twoStars":16,"threeStars":77,"fourStars": 314,"fiveStars":1558},"websiteUrl":"https://www.keepandshare.com"},"businessEntity":{"stars":4.5,"trustScore":4.7,"displayName":"Keep&Share","numberOfReviews":{ "total":1975,"oneStar":10,"twoStars":16,"threeStars":77,"fourStars":314,"fiveStars":1558},"websiteUrl":"https://www.keepandshare.com"},"reviews":null,"links":{"profileUrl ":"https://www.trustpilot.com/review/keepandshare.com","evaluateUrl":"https://www.trustpilot.com/evaluate/keepandshare.com","evaluateEmbedUrl":"https://www.trus tpilot.com/evaluate/embed/keepandshare.com","consumerWebPageUrl":null},"starsString":"Excellent","translations":{"customerssay":"Our customers say","outofreviews":" [RATING] out of 5 based on [NOREVIEWS] reviews","firstreviewer":"Be the first to review us on"},"settings":{"customStylesAllowed":tr ue}}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\5406e65db0d04a09e042d5fc[2].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):	984
Entropy (8bit):	4.990360405989179
Encrypted:	false
SSDEEP:	24:Ya77cyxEFuM77cyxEFuL28bwVQwOaIW/G9teaoKouIgTZIt:YaXhEF/XhEFHiW/PatXlgTZ4
MD5:	03E888BCD26307CA75DD120D41D8FAE3
SHA1:	5E1534A03FC655A8DAAC526C3F7B6604C0CCCA16
SHA-256:	10D34C681282F9D4AF9CAD648B0D33438E66E64BEE236B95D96AABD50A3E9A05
SHA-512:	EF3F4B351143D2ECE1C726F50029F761F92993A7B45CF171055217A6875D7B3EF1EF215632EAD3BC56576D785AE70763FB9C58BF2D2091E871D9CDD651DA453(
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://widget.trustpilot.com/trustbox-data/5406e65db0d04a09e042d5fc?businessUnitId=5654e51c0000ff000585ead7&locale=en-US
Preview:	{"businessUnit":{"stars":4.5,"trustScore":4.7,"displayName":"Keep&Share","numberOfReviews":{"total":1975,"oneStar":10,"twoStars":16,"threeStars":77,"fourStars": 314,"fiveStars":1558},"websiteUrl":"https://www.keepandshare.com"},"businessEntity":{"stars":4.5,"trustScore":4.7,"displayName":"Keep&Share","numberOfReviews":{ "total":1975,"oneStar":10,"twoStars":16,"threeStars":77,"fourStars":314,"fiveStars":1558},"websiteUrl":"https://www.keepandshare.com"},"reviews":null,"links":{"profileUrl ":"https://www.trustpilot.com/review/keepandshare.com","evaluateUrl":"https://www.trustpilot.com/evaluate/keepandshare.com","evaluateEmbedUrl":"https://www.trus tpilot.com/evaluate/embed/keepandshare.com","consumerWebPageUrl":null},"starsString":"Excellent","translations":{"customerssay":"Our customers say","outofreviews":" [RATING] out of 5 based on [NOREVIEWS] reviews","firstreviewer":"Be the first to review us on"},"settings":{"customStylesAllowed":tr ue}}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\59f77fc955540b22fa000038[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	17259
Entropy (8bit):	5.51486251654515

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\59f77fc955540b22fa000038[1].js	
Encrypted:	false
SSDEEP:	384:hO5oEsFliKxdlh2dcdUdd79h99QD37qVqdaa18oS3tEnevbKjtdX62+N1fvTHrkT:hO5oEsFl1xdlh2dcdUdd79h99QDrqVqZ
MD5:	2504BB49A6034A5241D2C111A23767AD
SHA1:	158ED19173F8973C3FF998CC0F35A083AAFD2E1C
SHA-256:	F6E42E6DD0C039907B0D9BCC72C813A62F2AF201B9B6C459868E29D49E14028B
SHA-512:	7B7A6DF4094E80A9311A7246B573C67760A9E1FA9B4DEF19D34617C5DFEB8C7A7E51D0CED294E455E4A6354D38A6D5700D1F3867A98C4BD98A2A75E637A2CA F
Malicious:	false
Reputation:	low
Preview:	window._pa = window._pa || {};._pa.rtbHostname = "pixel-geo.prfct.co";._pa.segments = [{"name":"All visitors","id":10567892,"regex":".*"},{"name":"Visited \"calendar_grou p\"","id":10614800,"regex":"/htm/calendars/calendar_group\\.php.*/?([?#].*)*$"},{"name":"Signed up for Free Basic","id":10614832,"regex":"/business/registration_complete_ setup\\.php\\?form=email.*/?([?#].*)*$"},{"name":"Signed up Free Trial","id":10614842,"regex":"/business/registration_complete_setup\\.php\\?form=free_trial.*/?([?#].*)*$"}, {"name":"Subscription conversion","id":10614853,"regex":"/business/avangate/transaction_completed\\.php.*/?([?#].*)*$"},{"name":"ALWAYS EXCLUDE: Visited log in page","id":10614875,"regex":"/index_signin\\.php.*/?([?#].*)*$"},{"name":"Free Address Book","id":10878541,"regex":"/htm/free_online_address_books\\.php.*/?([?#].*)*$"}, {"name":"/htm/calendars/free_calendars/free_calendar.php","id":10886278,"regex":"/htm/calendars/free_calendars/free_calendar\\.php.*/?([?#].*)*$"},{"name":"BA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\73f08661-a058-4e73-90df-bb12917a4ad6_eu[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):	764
Entropy (8bit):	5.230501439496272
Encrypted:	false
SSDEEP:	12:jqK4sIsZpfcHToCtNANiYf1MI/CXOTlladqYgxfXhjBVtHZGoiAhYZcruMMwIkKz:jdLZp0z1vANd5/CXOZlamjPGoi2Y66wU
MD5:	302EE656C975B3A53343F1BBE02A0B53
SHA1:	A9CBD216667A93F56A42C47590ABEB98D4D44A43
SHA-256:	F943EACFC483576EB7CA68A1FC5A4251614669E60FF2DE262C16A2FD5CA9CE12
SHA-512:	FC292F4E4EC838C2C10602EC62901D9CD9CF2924EF03638CD526BF6F4E5456A3470CE3A58560D3AFA16447499858755F3BA15BCCC5AAC973A3E06969EAE5BDI F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.mouseflow.com/projects/73f08661-a058-4e73-90df-bb12917a4ad6_eu.js
Preview:	if(typeof mouseflow==='undefined'&&typeof mouseflowPlayback==='undefined'){(function(_1){function _0(){return undefined}function _6(){return null}function _5(){return fal se}function _7(_2){if(_2&&_2.length){for(var _4=0;_4<_2.length;_4++){this.push(_2[_4])}}};_7.prototype.push=function(_3){if(_3&&typeof _3==='function'){_3(mouse flow)}};_1.setTimeout(function(){if(!_1._mfq)_1._mfq=[];_1._mfq=new _7(_mfq)},1);_1.mouseflow={config:_0,start:_0,stop:_0,newPageView:_0,stopSession:_0,rebindEv entHandlers:_0,getSessionId:_6,getPageViewId:_6,tag:_0,star:_0,setVariable:_0,identify:_0,formSubmitAttempt:_0,formSubmitSuccess:_0,formSubmitFailure:_0,debug:_ 0,isRecording:_5,isReturningUser:_5,activateFeedback:_0,websiteId:null,recordingRate:null,version:null}})(window)}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\KFOlCnqEu92Fr1MmEU9fBBc9[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 18 tables, 1st "GDEF", 8 names, Microsoft, language 0x409, Copyright 2011 Google Inc. All Rights Reserved.Roboto MediumRegularVersion 2.137; 2017Roboto-Me
Category:	downloaded
Size (bytes):	35588
Entropy (8bit):	6.410135551455154
Encrypted:	false
SSDEEP:	768:6yVJgIpAqZsXgDNHOBBPXNOKdhT1N+06XAxGrzmoqpxk0SnuUR:enq805OBBdhT1NP6XAxGryoqp2
MD5:	4D88404F733741EAACFDA2E318840A98
SHA1:	49E0F3D32666AC36205F84AC7457030CA0A9D95F
SHA-256:	B464107219AF95400AF44C949574D9617DE760E100712D4DEC8F51A76C50DDA1
SHA-512:	2E5D3280D5F7E70CA3EA29E7C01F47FEB57FE93FC55FD0EA63641E99E5D699BB4B1F1F686DA25C91BA4F64833F9946070F7546558CBD68249B0D853949FF85C5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc9.ttf
Preview:	..... GDEF.....{....dGPOS.....|<....GSUB7b.....8....OS/2t.#...r....`cmap.....st...Lcvt 1..K..y....\fpgm..$...v.....gasp.....{.....glyf.'.....,..j.hdmx.....r\|....head...r..n....6hhea.....q. ...$hmtx..MO..n@....loca\v@z..l(....maxp.....l.... name..:...z,....post.m.d..{.... prep...)..x|...S...d...(.....o.....9.....EX../... >Y..EX../....>Y.....9.....9.....9..... ...9.....9.....01!!.!.....!.5.!.(.<..6.....}.w...x.^.^..^.....<.....9.....EX../... >Y..EX../....>Y.....+X!...Y..../01.#.!.462...."&.~.....J.JH.H.....9KK97JJ....e...@..... %...EX../..."">Y..../..../...../01..#.3..#.3..#...-#...w.}....}.....`.....EX../... >Y..EX../... >Y..EX../....>Y..EX../....>Y.....9../.....+X!...Y...../.....+X!...Y.....01.#. #.#5!.#5!.3.3.3.3.#.3.#.#.3.#...L.L...:...N.N.N.N..:..L.v.:....f....9....`...`....f.8.9...d.-.&...,..*-...9...EX../... >Y..EX../... >Y..EX.#/.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\KFOlCnqEu92Fr1MmYUtfBBc9[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 18 tables, 1st "GDEF", 8 names, Microsoft, language 0x409, Copyright 2011 Google Inc. All Rights Reserved.Roboto BlackRegularVersion 2.137; 2017Roboto-Bla
Category:	downloaded
Size (bytes):	35208
Entropy (8bit):	6.392518822467014

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\KFOlCnqEu92Fr1MmYUtfBBc9[1].ttf	
Encrypted:	false
SSDEEP:	768:53Dmu13ucOmpIN22bN8o6Ze0XlGV+uM49pSeCu7XniviDffw6mo/quUR:lD13DjSNz0XlG0uL9YeCu7Xn4iTo9o/4
MD5:	4D99B85FA964307056C1410F78F51439
SHA1:	F8E30A1A61011F1EE42435D7E18BA7E21D4EE894
SHA-256:	01027695832F4A3850663C9E798EB03EADFD1462D0B76E7C5AC6465D2D77DBD0
SHA-512:	13D93544B16453FE9AC9FC025C3D4320C1C83A2ECA4CD01132CE5C68B12E150BC7D96341F10CBAA2777526CF72B2CA0CD64458B3DF1875A184BBB907C5E3D71
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmYUtfBBc9.ttf
Preview:	..... GDEF.....z\...dGPOS.....z.....GSUB7b.....OS/2ve#...p....`cmap.....r....Lcvt ...=..xX...Zfpgm..#...ud....gasp.....zP....glyf.....,..i~hdmx.....q ....head...R..l....6hh ea.]....p....$hmtx..<...l....locaK./...j.....maxp.....j.... name..9...x....|post.m.d..z0... prep...C..w ...8...d...(.....P...EX../....>Y..EX../....>Y.....9.....9.....9.....9.....9.....0 1!!.!.....!.5.!.(.<..6.....}.w...x.^.^..^....g.....<.....9.....EX../....>Y..EX../....>Y.....+X!...Y..../01.!.!.462..."&....+.g..k.kk.k.....J__.__.....^.....&.....9...../.....9../. .....01..#.3..#.3.+..._+...v.S.8..S.8.....z..... !..9.....EX../....>Y..EX../....>Y..EX../....>Y..EX../....>Y.....9../.....+X!...Y...../.....+X!...Y.....01.#.#.#5 3.#53.3.3.3.3.!.3.!.#.3.#.d.C.C.,,..E.D.E.E...,...C.@.,....f.....`...`.....f.Q.....S.&.Q...-.r.+./..9...EX../....>Y..EX.!/..!.>Y..!...9.....!..9.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\KFOmCnqEu92Fr1Mu4mxP[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 18 tables, 1st "GDEF", 8 names, Microsoft, language 0x409, Copyright 2011 Google Inc. All Rights Reserved.RobotoRegularVersion 2.137; 2017Roboto-Regularht
Category:	downloaded
Size (bytes):	35408
Entropy (8bit):	6.412277939913633
Encrypted:	false
SSDEEP:	768:PX4i+tezjtQYgu30G0xL9nQbuEL7LQo9SBxQbptqKmomjJlvh:PJ2z3G0xpUusLEBKptqNomjV
MD5:	372D0CC3288FE8E97DF49742BAEFCE90
SHA1:	754D9EAA4A009C42E8D6D40C632A1DAD6D44EC21
SHA-256:	466989FD178CA6ED13641893B7003E5D6EC36E42C2A816DEE71F87B775EA097F
SHA-512:	8447BC59795B16877974CD77C52729F6FF08A1E741F68FF445C087ECC09C8C4822B83E8907D156A00BE81CB2C0259081926E758C12B3AEA023AC574E4A6C9885
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxP.ttf
Preview:	..... GDEF.....{`...dGPOS...h..{.....GSUB7b.....OS/2tq#...q....`cmap.....s....Lcvt +.....yl...Tfpgmw.`...vd....gasp.....{T....glyf.....,..j.hdmx.....r ....head.j.z..m....6hh ea.....q....$hmtx..Vl..m.....loca?.#...k.....maxp.....k.... name.U9...y....tpost.m.d..{4... prep.f....x ...l...d...(.....q.....9.....EX../....>Y..EX../....>Y.....9.....9.....9.. ....9.....9.....9.....01!!.!.....!.5.!.(.<..6.....}.w...x.^.^..^.....{.....0...EX../....>Y..EX../....>Y.....+X!...Y.....901.#.3.462..."&.[....7l88l7.....-==Z;;.....#......./.....9 ../.....01..#.3..#.3...o.....o...x.....w.....EX../....>Y..EX../....>Y..EX../....>Y..EX../....>Y.....9|../.....+X!...Y...../.....+X!...Y.....01.!.#.#5!.!5!.3.!.3.3.# .3.#.#.!.!....P.P...E....R.R..R.R..E..P....E.....f....b....`...`.....f.#.b....n.0.....+.i...EX../....>Y..EX."/..">Y.."...9.....+X!.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\analytics[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	47332
Entropy (8bit):	5.518633523108405
Encrypted:	false
SSDEEP:	768:UyC36rcBLbfsl5XqYoyPndHTkoWY3SoavVVy2WiCgYUD0FEw0stZb:UyDAZfY5hVdHTwY3Soljw0sD
MD5:	6A10EB2BB5C90414980729F4F96FFBDA
SHA1:	8BBBD5948255549E4B691B614AA3177DEA9AF1B7
SHA-256:	0F3BE44690AE9914AE3E47B7752E1BDEA316F09938E9094F99E0DE19CCD8987A
SHA-512:	5A505CBAAEEAB8961AA0DE94767F76A09B6F03E60EB0C72954B85EC0392EE1CE383D2088939A314D3175AB24B7A69390C841CFE0237C1D1C40966B43F22AE929
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google-analytics.com/analytics.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var n=this||self,p=function(a,b){a=a.split(".");var c=n;a[0]in c||"undefined"==typeof c.execScript||c.execScript("var "+a[0]);for(var d;a.length&&(d=a.shift());)a.length||void 0===b?c=c[d]&&c[d]!==Object.prototype[d]?c[d]:c[d]={}:c[d]=b};var q=function(a,b){for(var c in b)b.hasOwnProperty(c)&&(a[c]=b[c])},r=function(a){for(var b in a)if(a.hasOwnProperty(b))return!0;return!1};var t=/^(?:(?:https?|mailto|ftp):|[^:/?#]*(?:[/?#]|$))/i;var v=window,x=document,y=function(a,b){x.addEventListener?x.addEventListener(a,b,!1):x.attachEvent&&x.attachEvent("on"+a,b)};var z={},A=function(){z.TAGGING=z.TAGGING\|\|[];z.TAGGING[1]=!0};var B=/:[0-9]+$/,C=function(a,b,c){a=a.split("&");for(var d=0;d<a.length;d++){var e=a[d].split("=");if(decodeURIComponent(e[0]).replace(/\+/g," ")===b)return b=e.slice(1).join("="),c?b:decodeURIComponent(b).replace(/\+/g," ")}},F=function(a,b){b&&(b=String(b).toLowerCase());if("p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\app_store_badge[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 168 x 50, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	2657
Entropy (8bit):	7.911319941393114

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\app_store_badge[1].png	
Encrypted:	false
SSDEEP:	48:p1annWsosZKHOnIaWfRQOmCrLpQ7GysqJN0D8QFX/kCzTJeRhEv:IfZIHOjqRQOmjGysqn0D8QmCzT0O
MD5:	F10DE02C4BFF18DE91C5F8FDAFC2FB67
SHA1:	DCCAA08E336F8E6658544D999A6ACCAFE0F3B179
SHA-256:	952F13396B98EF6F08ECC127A36CF326DDB028A5050146F5A00604909C620764
SHA-512:	1F66F205EE4020BF396278647D7FEDEAFAEB41B763CAFDD76BC575DC31A090D969CEBE141C2ECD9BFE0FCD39107A31156C9669E65AE425AEA70EBCF1166D1D8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://keepn.com/graphics/lpgraphics/landing_pages/htm/calendars/calendar/app_store_badge.png
Preview:	.PNG.....IHDR.....2.....h`....VPLTE...MMN.....667.....QRS.....=?@.....466.....022(**.....+.."%%.....Z\\.....tuujkl.....prrUWW.....|}}....ADD ""....bddPRRJLL.....?AA%".....MOO:==8::.....wyyFHHCEE....._aa.....]^^...noofhh.....7.S....tRNS."....S.....[X8f.1....IDATx...{.H.G3<.o..v.*rZ..9..N.Laff.....q..@..U9G.|j.(..j.....27>...<|.....F...1.....}....H,.m.....o...!><<.;..`?Q.....c_Q ..!....n..s6._...6.....FT.t..n....N.O...._,....-.....J!X.O..v.g.S.=.]..B[..3n.;..Jx...XO..(.....;....%.e.....&.a.M.....A"1...I..[.c.\..c..A.K.@.:....7MD)...d.q.....Z.^..z.....O.W.ehQT...k .^=..l...G.....z.A..(....(u....o*....6H1..C.....(..-.....R.....pzB.".\..... 0N..y..U..N i.g=...Q.<..A.Z...k.a.....<.&...O...l.fa.7pZ<../...i%..9.!Fe.4vF..9.PqE.....N./.. ."KF..O.(...B!..P....s.=..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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):	37045
Entropy (8bit):	5.174934618594778
Encrypted:	false
SSDEEP:	768:o2rGy27UwlNqMl95qNmCFejhqs8snmi+CSFXfbx8Gf3Zq7Q:Jg73zhq0GvbJ3ZKQ
MD5:	5869C96CC8F19086AEE625D670D741F9
SHA1:	430A443D74830FE9BE26EFCA431F448C1B3740F9
SHA-256:	53964478A7C634E8DAD34ECC303DD8048D00DCE4993906DE1BACF67F663486EF
SHA-512:	8B3B64A1BB2F9E329F02D4CD7479065630184EBAED942EE61A9FF9E1CE34C28C0EECB854458977815CF3704A8697FA8A5D096D2761F032B74B70D51DA3E37F4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.keepandshare.com/global/lp/js/bootstrap/3.3.7/js/bootstrap.min.js
Preview:	/*!. * Bootstrap v3.3.7 (http://getbootstrap.com). * Copyright 2011-2016 Twitter, Inc.. * Licensed under the MIT license. */.if("undefined"==typeof jQuery)throw new Error ("Bootstrap's JavaScript requires jQuery");+function(a){"use strict";var b=a.fn.jquery.split(" ")[0].split(".");if(b[0]<2&&b[1]<9||1==b[0]&&9==b[1]&&b[2]<1||b[0]>3)throw new Error("Bootstrap's JavaScript requires jQuery version 1.9.1 or higher, but lower than version 4")}(jQuery),+function(a){"use strict";function b(){var a=document.creat eElement("bootstrap"),b={WebkitTransition:"webkitTransitionEnd",MozTransition:"transitionend",OTransition:"oTransitionEnd otransitionend",transition:"transitionend"};for(var c in b)if(void 0!==a.style[c])return{end:b[c]};return!1}a.fn.emulateTransitionEnd=function(b){var c=!1,d=this;a(this).one("bsTransitionEnd",function(){c=!0});var e=fu nction(){c||a(d).trigger(a.support.transition.end)};return setTimeout(e,b),this},a(function(){a.support.transition=b(),a.support.transition&&(a.event.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\cream_dust[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 50 x 50, 4-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	661
Entropy (8bit):	7.358161560946802
Encrypted:	false
SSDEEP:	12:6v/7gqvCQx9CAarCoOvCg1+qqHKD2x2speB4Km0Cz8pg6OR:H2C4zaroT1+qdD2x2Sm4Km6pg6e
MD5:	A8B426BDF54D58953C84589AF6D79EBE
SHA1:	EEF38C387DB75E461F07F1C3578942D8907E4F5A
SHA-256:	E1CF6492F2A93556D3AEFD9E91C10B206D100C5CD522FD0E50640341C6F9E47E
SHA-512:	CD3DC633654FDC7DFFAE7D7945D1BAC9B6E861C96DD707107D7C6F1340199546E63FFEF8F7DF2ECB3C3E600C2391F81256C6956FAC5F0C2DB17AA7385D679F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.keepandshare.com/graphics/homepage4/cream_dust.png
Preview:	.PNG.....IHDR...2...2.....PLTE.....AIDAT.....0.E.f..E..j`...?..n.W....u.OS..`....=.A..kf/.....Scf.k.jhx.}z.33s...iE.T...Y04.....Y...J.L..*..,0h*9]..i....."F(.`.1.. ..J..0..9f/.{yC.yW...x./y../GG.z.:"...bt.....h.]...A.Z...u....P.H4.....%..H..(.-...y}.S.t...d7.....4.h...0.....`....9..\s.L1.5..`p.XsH.#.{D.).uh^...y..4....Y....1.....y..\.}.kf.1<..P.....d... /..@..h@.....8.(...`.....'.W/..4.Y.I.X+..}C{b...V..tg7fp.....13..|Y..H...Y0...w..W"....-@...Ke..W..@..j...PK\.....5P.8,.....{S...X.qW...%.L.@.@...b...EL.1N.....`>.1.f..C..y.=.Ps... 1..P.]....+...(..K..Vz.7.j.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\fontawesome-webfont[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), FontAwesome family
Category:	downloaded
Size (bytes):	165742
Entropy (8bit):	6.705073372195656
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\fontawesome-webfont[1].eot	
SSDEEP:	3072:qbhEnD+IzsU9z9QJ6/P3Xe2iEiEPGFCMW1JVJG6wVTDsk6BmG6S1yKshojskO+b2:qenD+IzsU9z9QJ6/PO2FiEP2C/DVJG6I
MD5:	674F50D287A8C48DC19BA404D20FE713
SHA1:	D980C2CE873DC43AF460D4D572D441304499F400
SHA-256:	7BFCAB6DB99D5CFBF1705CA0536DDC78585432CC5FA41BBD7AD0F009033B2979
SHA-512:	C160D3D77E67EFF986043461693B2A831E1175F579490D7F0B411005EA81BD4F5850FF534F6721B727C002973F3F9027EA960FAC4317D37DB1D4CB53EC9D343A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.keepandshare.com/global/styles/css_source/font-awesome/4.7.0/fonts/fontawesome-webfont.eot?
Preview:	n.....LP.....Yx.....F.o.n.t.A.w.e.s.o.m.e.....R.e.g.u.l.a.r...$.V.e.r.s.i.o.n. .4...7...0. .2.0.1.6.....F.o.n.t.A.w.e.s.o.m.e.....PFFTMk .G.....GDEF.....p... OS/2.2z@...X...`cmap..:.....gasp.....h....glyf...M.....L.head...-.....6hhea.....$hmtxEy.....loca...\.....maxp.,.....8... name....gh....post.....k.... u.....xY_.<.....3.2.....3.2.....'.....@.....i.....3.....3...s.....pyrs.@. ....p.....U..... .....]..... .....y...n.....2.....@..... .....z.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\google_play_badge[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 169 x 50, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	2719
Entropy (8bit):	7.886287525246333
Encrypted:	false
SSDEEP:	48:dTShhW/qNjtIHtkAmTk3owPtLBDAHQtKzCD8v/LTWMmbRAJYhO:x2SH25Tk3tD/8W/bRjhO
MD5:	CAF65AC02780F4E724D92C73427A1EC0
SHA1:	A6E6E310592885689106D21088D492A77D2BF715
SHA-256:	C20E5BCDB91048366E2B759EF87CBE0E7C394E0FD64C0810ACD9C9A0FEE3EF13
SHA-512:	FC084A373A649D6C643AE543CAAED727D203C85828A95AA6E46E20F6517425C095C95248B26CAF490C4BC6275874FF3B731FBB73E94B57AC62C69AB0F6E24F2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://keepn.com/graphics/lpgraphics/landing_pages/htm/calendars/calendar/google_play_badge.png
Preview:	.PNG.....IHDR.....2.....PLTE.....@@@HHHSSScccwww.....IIILLL.....MMM.....}}}.....kkk===###.....l lleeeWWW:::777'".....bbbTTT---.....O.....uuu^^^YYY@@@.....M.....E....rrrpppphhh+++.....d.....X..J.....?..JJJCCCQ..G.....=.....111...^..]..Z..V..n.....T..H..X...yy y[[[GGG555!!!^..S.....8x..w..w..v..u.>h.>^333///C..B..j.:..:..}.c.7..3...L...z..xxxx..v..u.?tPPP.....R..J..I..?..L.4..u.N..W..I....D..@.....<...1.1|....c.....9..N..>..5..O..8...|.. z..p`.h.ua.B].=S.>K.h;*F;..7W.6!..7..)..w..O..K..O..j....6..S.P.N.....>.mE...g..{.....g....~..|..x.Qw.vp.Qn6tk.6kq&k.h..g..._.|\.\U.5U.4Ui"T4`S.zRUpP.yEJaC3.9.-5jV0[H, /&M.&D.....V.<....tRNS.....+.....}f_H7..4.....;IDATx....t$.....h....WU.:]m.I.1.m..m..|.{m.|..2.AgxN..q.s.E.....7w..\.z0%..~};..m.....Z...i.C.knF~t.....i...).b.).:..".....x...8.],T\..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\logo_48[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 48 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	2228
Entropy (8bit):	7.82817506159911
Encrypted:	false
SSDEEP:	48:4/6MuQu6DYYEcBDlBVzqawiHI1Oupgl8m7NCnagQJFknwD:4SabhtXqMHyCl8m7N0ag6D
MD5:	EF9941290C50CD3866E2BA6B793F010D
SHA1:	4736508C795667DCEA21F8D864233031223B7832
SHA-256:	1B9EFB22C938500971AAC2B2130A475FA23684DD69E43103894968DF83145B8A
SHA-512:	A0C69C70117C5713CAF8B12F3B6E8BBB9CDAF72768E5DB9DB5831A3C37541B87613C6B020DD2F9B8760064A8C7337F175E7234BFE776EEE5E3588DC5662419D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/recaptcha/api2/logo_48.png
Preview:	.PNG.....IHDR...0...0.....W.....gAMA.....a.... cHRM..z&.....u0...`.:....p..Q<....bKGD.....C.....pHYs.....IDATh...P....=..8.....Nx. ..PlP8..;.C.1iL#6...*.Z..!.....3.po . o.L.i.I..1fl..4..ujL&6$.....w.....,Z..z. ~....\.._.C.eK...g..%..P..L7...96..q....L.....k6...*..,xz.._.....B."#...L(n..f..Yb...*.8.;....K)N...H).%.F"Ic.LB.....jG.uD..B....Tm....T. .).A.}D.f..3.V.....O.....t_..].x.{o.....*....x?!W...j..@..G=Ed.XF.....J..E?../.?p..W..H..d5% WA+.....)2r..+..'qk8.../HS.[...u..z.P.*....-.A.}.....I .P.....S....|...)..KS4....I.....W...@....S. s..s..$`.X9.....E.x.=.u.*iJ.....k.....'...!.a....*+.....(...S..\h....@.....I.$..%.2....l.....a.|.....U....y.....t..8....TF.o.p.+.@<.g.....-.M.....:.@..(.....@.....>..=.ofm.WM{...e..,..D.r.. .....w....T.L.os..T@Rv..;.....9....56<.x.....2.k.1....dd.V.....m..y5../4|...G.p.V.....6...}.....B.....5...&..v..yTd.6...../m.K...(.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\main[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines
Category:	downloaded
Size (bytes):	77662
Entropy (8bit):	5.622819372856175
Encrypted:	false
SSDEEP:	1536:E5x2SwsSZ9vYguFDEL/KQKD8OaLHxRTjm/HfzQy+y4N0Osuj:EqsDmOadRT7
MD5:	54A85C8529E9EDFDD38EFFECA44FF4AA
SHA1:	CD7E8161B10E0330EC223EC228182131F23A7880

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\main[1].js	
SHA-256:	D5D9101888E9484F48ABF25BED40BFD18006D50A125351A34DFBBEB77CA660EE
SHA-512:	C5742F97BF8003274EEB0CDED11CE615E45BA1D89C5C6FAB73657AC102DD4D5C96D95D63E4CAF66E26078E79D6B5ADC79B089E95DAB7633F54C2318359A087A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://widget.trustpilot.com/trustboxes/539ad60defb9600b94d7df2c/main.js
Preview:	.!function a(o,i,u){function l(t,e){if(!i[t]){if(!o[t]){var r="function"==typeof require&&require;if(!e&&r)return r(t,!0);if(c)return c(t,!0);var n=new Error("Cannot find module '"+t+"'");throw n.code="MODULE_NOT_FOUND",n}var s=i[t]={exports:{}};o[t][0].call(s.exports,function(e){return l(o[t][1][e]||e)},s,s.exports,a,o,i,u)}return i[t].exports}for(var c="function"==typeof require&&require,e=0;e<u.length;e++)l(u[e]);return l}({1:[function(e,t,r){"use strict";i(e("promise"));var n=i(e("@trustpilot/trustbox-framework-vanilla/modules/impression")),s=e("@trustpilot/trustbox-framework-vanilla/modules/api"),z=e("@trustpilot/trustbox-framework-vanilla/modules/utils"),D=e("@trustpilot/trustbox-framework-vanilla/modules/dom"),H=e("@trustpilot/trustbox-framework-vanilla/modules/reviewsList"),V=e("@trustpilot/trustbox-framework-vanilla/modules/templates/stars"),B=e("@trustpilot/trustbox-framework-vanilla/modules/templates/logo"),U=e("@trustpilot/trustbox-framework-vanilla/modules/templates/summ

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\modalbox.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	4042
Entropy (8bit):	5.027147523207259
Encrypted:	false
SSDEEP:	96:jOct6Su6N7aklElAHN9GSl+YN9GDB8YDJuLkfElAHZCGSldN4:jOct6Su6N7aklElAHNZlnN9G18YDJuLk
MD5:	560BE2557FAEE985800880DB6A51D6EE
SHA1:	ACD7F18DE836C63B51B3F68D164A33697AFB15DD
SHA-256:	0D65DE6B87B750DE48564A9AA21267D63516CEB52EF8D624BC6E38E6DFF47030
SHA-512:	C8A2CE3F2E3AF6BD53DE1070C9803943B008028BD1F9C4CBE499F9AB39F447B3676623137F0478F378D108467838913C77932A40C8ABB411304307E4E3426041
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.keepandshare.com/global/ajax/modalbox/modalbox.min.js
Preview:	if(typeof Prototype.Browser.Version==='undefined'){if(Prototype.Browser.IE){var ua=new String(navigator.userAgent);var offset=ua.indexOf("MSIE ");Prototype.Browser.Version=parseFloat(ua.substring(offset+5,ua.indexOf(";",offset)))}}.if(!("console" in window)||!("log" in console)){if(!("console" in window)){window.console={}}.if(!("log" in console)){window.console.log=function(){}}}.var ModalBoxShading=Class.create({_setSize:function(){var dim=document.viewport.getDimensions();if(Prototype.Browser.WebKit){dim.width=document.body.scrollWidth;dim.height=document.body.scrollHeight}else if(Prototype.Browser.IE&&Prototype.Browser.Version<7.0){dim.width=Math.max(document.documentElement.clientWidth,document.body.clientWidth);dim.height=Math.max(document.documentElement.scrollHeight,document.body.scrollHeight)}else{dim.width=Math.max(dim.width,document.documentElement.offsetWidth);dim.height=Math.max(dim.height,document.documentElement.offsetHeight)}.if(this._element.offsetHeight!=dim.height){t

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\recaptcha__en[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	339223
Entropy (8bit):	5.672856332689809
Encrypted:	false
SSDEEP:	6144:/BtKuhzQnSScdtrRMR5AKoM9lLSdHC8LW9h0/hXk/s1uAbgrU:aiKczrRC5AK39lH8VXkExJ
MD5:	105FF5713D60E0B400E03A71BBF249E3
SHA1:	A601E6E6394C0B91350972C4B31A21EA636F9C50
SHA-256:	B6FCDD11C229160158B2399CFC0524BD1712B0B24E86E9D3432E5EEC78D9E518
SHA-512:	EC7BD71150AC82467919219475681CBE623A100B1058341FD3CAF18B32853F9E3FA55645A56F5545FC71662E8F3DD03C464F612A917A9AF6E4F20F8C88D5DE3C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/recaptcha/releases/6g5J7UfDQ9mLrweZHj04ekSP/recaptcha__en.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var D=function(){return[function(t,S,F,n,R){return t+2&(1==(1==(t>>1&((t>>2)%(n=[17,"INPUT",30],n)[0]||(q[23](59,n[1])||(q[34](48,this.Y,this.X(),"click",this.qh),this.$l=null),this.yW=!1,r[n[2]](21,10,this)),7))&&(S=S||{},F="",S.UR||(F+="Press R to replay the same challenge. "),R=Y(F+'Press the refresh button to get a new challenge. Learn how to solve this challenge.')),t-8&11)&&(13==S.keyCode?k[40](8,!1,this):this.I&&this.Y&&.0<e[14](48,"\n",this.Y).length&&this.pB(!1)),15)||(R=Object.prototype.hasOwnProperty.call(S,jS)&&S[jS]||(S[jS]=++FO)),R},function(t,S,F,n,R,B,p,J,h,H,G,L,C,Q,g,K){if(!(t|6)%(((g=[1,11,2],t)<<g[2])%19||(this.Y=[]),7))if(n){if(n=Number(n),isNaN(n)||n<S)throw Error("Bad port number "+n);F.B=n}else F.B=null;if(4==(t<<g[2]&15)){if(J=(G=(L=(p=(Q=(C=D[19].bind(null,g[0]),l[28](77,n)),C(R||SS,void 0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\screen_month_view[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, 1066x710, frames 3
Category:	downloaded
Size (bytes):	84892
Entropy (8bit):	7.90606838595961
Encrypted:	false
SSDEEP:	1536:zgkm09rl2i44XRu7taG7k00COXo3pOZWxwbZeqD2AkgA4fEmH7X/bbK5lyabOkr:zvth2i4/7t9BgWxikJAZhfEy7XPK5EqH
MD5:	D4E0F38B45125CCD42DF840921B56A0D

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

SHA1:	DA25838B8935F75979D89E1CB18F36F26368C29C
SHA-256:	90806E69CE3D21C0CDAEF46D4034AE993B194F507089258E4584DE1CF32A1D87
SHA-512:	6ACFD744BE81E4AFEAB51269D0130A1C0568AD407B4CDD8895348AD2563F7B88B418341F80399005DCF32EE4AC0426C03113BB76471935A6367E3DEE54405965
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://keepn.com/graphics/lpgraphics/core_pages/calendar_samples/screen_month_view.jpg
Preview:	......JFIF.............C..........................$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C..........=)#)==.. ......*...iP..C.r......A. ....@F....._?..z>V.>....^7..u}~.5...R3`T9...... ....9%...@*s......]..*..}y...~/.._...g.t;...e.Cb.C._:...Q....E...3K.f<.]..@FH..9e ..@.............................. ....+.......L.@...;.zb...mf.;(..................................`..... ..<.....}/...w._G..>o....L..eb.'.O.{...<....g.......~.=....d..+............................ ....j@hW....R..<.!.C.Z9.8......;...?...|......{_.....O....;*..{....^?..s}g.~..y........<..........~....~.......'./

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\styles__ltr[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):	51178
Entropy (8bit):	5.968129596292632
Encrypted:	false
SSDEEP:	768:+LUmmAWTe2uXYp8Mi+yKSrKebyBwxDl+xedtY5PoiDH1fkQJVEwY:4UcW6v+2rKwxDliP7dnY
MD5:	E548DC0AEF0A21A2DF5B964EF93118AA
SHA1:	983091AEC1E7BFEB79F768E4B997C43B55EDE14A
SHA-256:	6B08EA3A348838BC942AD470A757575975BD09459B63C1872C6E1129A6CA1939
SHA-512:	17A4EC0CB167C2C7653ABEF6384C68BE2BCEEE6FB657D3A27132B3508F28087AEEB8072409DB95F6D4BE7BFE1F54A51D6EB073AE5D902DA90ADA5ECDE72F29FC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/recaptcha/releases/6g5J7UfDQ9mLrweZHj04ekSP/styles__ltr.css
Preview:	.goog-inline-block{position:relative;display:-moz-inline-box;display:inline-block}* html .goog-inline-block{display:inline}*:first-child+html .goog-inline-block{display:inline}.recaptcha-checkbox{border:none;font-size:1px;height:28px;margin:4px;width:28px;overflow:visible;outline:0;vertical-align:text-bottom}.recaptcha-checkbox-border{-webkit-border-radius:2px;-moz-border-radius:2px;border-radius:2px;background-color:#fff;border:2px solid #c1c1c1;font-size:1px;height:24px;position:absolute;width:24px;z-index:1}.recaptcha-checkbox-borderAnimation{background-image:url(

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

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	102
Entropy (8bit):	4.904584411042069
Encrypted:	false
SSDEEP:	3:JSbMqSL1cdXWKQKI/b+7NHWaee:PLKdXNQKI/b+7FL
MD5:	63582536B71B4C6CBBB0FF6F71E43979
SHA1:	EDCAE8FFBB3020A57A620ED448F1CF955263A002
SHA-256:	9C2464ADD3C699D2BE6D7EC889EED8D56FF71327CE4FC9E43955CEA79B117FCE
SHA-512:	0FEF57308B381351319553E899715461F4096BF50E669B232382E45504F1402EE59889CC02240410E4F2A12EB8F5ADC684723596CF5D2F0E8B72C9ADD26369AE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/recaptcha/api2/webworker.js?hl=en&v=6g5J7UfDQ9mLrweZHj04ekSP
Preview:	importScripts('https://www.gstatic.com/recaptcha/releases/6g5J7UfDQ9mLrweZHj04ekSP/recaptcha__en.js');

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\59f77fc955540b22fa000038[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	17259
Entropy (8bit):	5.51486251654515
Encrypted:	false
SSDEEP:	384:hO5oEsFliKxdlh2dcdUdd79h99QD37qVqdaa18oS3tEnevbKjtdX62+N1fvTHrkT:hO5oEsFl1xdlh2dcdUdd79h99QDrqVqZ
MD5:	2504BB49A6034A5241D2C111A23767AD
SHA1:	158ED19173F8973C3FF998CC0F35A083AAFD2E1C
SHA-256:	F6E42E6DD0C039907B0D9BCC72C813A62F2AF201B9B6C459868E29D49E14028B
SHA-512:	7B7A6DF4094E80A9311A7246B573C67760A9E1FA9B4DEF19D34617C5DFEB8C7A7E51D0CED294E455E4A6354D38A6D5700D1F3867A98C4BD98A2A75E637A2CAF

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\59f77fc955540b22fa000038[1].js	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tag.marinsm.com/serve/59f77fc955540b22fa000038.js
Preview:	window._pa = window._pa || {};._pa.rtbHostname = "pixel-geo.prfct.co";._pa.segments = [{"name":"All visitors","id":10567892,"regex":".*"},{"name":"Visited \"calendar_group\"","id":10614800,"regex":"/htm/calendars/calendar_group\\.php.*/?([?#].*)*$"},{"name":"Signed up for Free Basic","id":10614832,"regex":"/business/registration_complete_setup\\.php\\?form=email.*/?([?#].*)*$"},{"name":"Signed up Free Trial","id":10614842,"regex":"/business/registration_complete_setup\\.php\\?form=free_trial.*/?([?#].*)*$"},{"name":"Subscription conversion","id":10614853,"regex":"/business/avangate/transaction_completed\\.php.*/?([?#].*)*$"},{"name":"ALWAYS EXCLUDE: Visited log in page","id":10614875,"regex":"/index_signin\\.php.*/?([?#].*)*$"},{"name":"Free Address Book","id":10878541,"regex":"/htm/free_online_address_books\\.php.*/?([?#].*)*$"},{"name":"/htm/calendars/free_calendars/free_calendar.php","id":10886278,"regex":"/htm/calendars/free_calendars/free_calendar\\.php.*/?([?#].*)*$"},{"name":"BA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\73f08661-a058-4e73-90df-bb12917a4ad6[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	178
Entropy (8bit):	4.560890767001816
Encrypted:	false
SSDEEP:	3:qVoB3tUROGclXqyvXboAc9FKEIHiHby4AqWSZUXqXlIVLLP61IwcWWGu:q43tISl6kXiWHiHuwWSU6Xll5LP8IpfB
MD5:	CD2E0E43980A00FB6A2742D3AFD803B8
SHA1:	81FFBD1712AFE8CDF138B570C0FC9934742C33C1
SHA-256:	BD9DF047D51943ACC4BC6CF55D88EDB5B6785A53337EE2A0F74DD521AEDDE87D
SHA-512:	0344C6B2757D4D787ED4A31EC7043C9DC9BF57017E451F60CECB9AD8F5FEBF64ACF2A6C996346AE4B23297623EBF747954410AEE27EE3C2F3C6CCD15A15D0F2D
Malicious:	false
Reputation:	low
Preview:	<html>..<head><title>301 Moved Permanently</title></head>..<body bgcolor="white">.. 301 Moved Permanently ..<hr> nginx ..</body>..</html>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AHRhs1D3ZquYsgAMpj5q2vpzkPMkbMfvPao1yrEQEiw[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):	21071
Entropy (8bit):	5.5815492796756425
Encrypted:	false
SSDEEP:	192:/8P1ugAnFOC6JNM290kPjHPmkzw/EM1WeaPsMtrB7OFhr5wAfpxseJ6qGvNXHGhK:UoOC6v56WjSELeMh9sLwAHb6qpiJO6UO
MD5:	6A685A8533248FD41EEB3A89430C2287
SHA1:	05C77E65C10AE254D471273C4529E9CAAA169938
SHA-256:	007461B350F766AB98B2000CA63E6ADAFA7390F3246CC7EF3DAA35CAB110122C
SHA-512:	A9B2D5B092F06E12E486318CC9A072088182423B332B8D1571D2996840169ECC734431AB0CE1ED41EE4D9234DA801FC9D28EAD3EADDDD239316E9087FF8C94BD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/js/bg/AHRhs1D3ZquYsgAMpj5q2vpzkPMkbMfvPao1yrEQEiw.js
Preview:	/* Anti-spam. Want to say hello? Contact (base64) Ym90Z3VhcmQtY29udGFjdEBnb29nbGUuY29t */ (function(){var h=function(F){return F},P=function(F,z){if(!(F=(z=null,V).trustedTypes,F)||!F.createPolicy)return z;try{z=F.createPolicy("bg",{createHTML:h,createScript:h,createScriptURL:h})}catch(Q){V.console&&V.console.error(Q.message)}return z},V=this||self;(0,eval)(function(F,z){return(z=P())&&1===F.eval(z.createScript("1"))?function(Q){return z.createScript(Q)}:function(Q){return""+Q}}(V)(Array(7824*Math.random()|0).join("\n")+'(function(){var zG=function(F,z){if(!(F=(z=null,k).trustedTypes,F)||!F.createPolicy)return z;try{z=F.createPolicy("bg",{createHTML:Fw,createScript:Fw,createScriptURL:Fw})}catch(Q){k.console&&k.console.error(Q.message)}return z},Q_=function(F,z){return[(F(function(Q){Q(z)}),function(){return z})]},hI=function(F,z,Q){for(Q in z)if(F.call(void 0,z[Q],Q,z))return true;return false},Pi=function(F,z,Q,V,G){return Q=V_(F,(V=function(){},G=void 0,function(h){V&&(z&&D(z),G=h,V(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\K&S_Logo@3x[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 717 x 144, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	5638
Entropy (8bit):	7.936402838948968
Encrypted:	false
SSDEEP:	96:H3Njcbg0E9rNB+/NYNCf92tMip+xNE1UlYKbwogmjpNpGrIinq0:H9mLE9rNIuNCfUG9xYUl9bwogmPinH
MD5:	0C01F827B25079066BEE794F7ACD2FD4
SHA1:	F6B5BA5169DD0C5AF58A6E30B86AF396B695AA32
SHA-256:	A5900A5D9512BAE84E0D44CF7A1F10F10D22BD86C856EA56545DD715228E366A
SHA-512:	FA8D44A9266839DC224A1973B09C24F6BFBE8F091EB3D133B3BA4D8D205A411B7E00B37A64820DB4C8683A97DB06F0E4032D29008787D7AB583BB61552963D13
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://keepn.com/graphics/logo/2015_KNS_Logo/K&S_Logo@3x.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\K&S_Logo@3x[1].png	
Preview:	.PNG.....IHDR.....PLTE....n..n..o..l..o..n..Z..n..o..n..h..m..d..l..m..n..n..n..n..n..n..n..n..m..n.....n.....n.....o.....*tRNS.....d....P..7q..Z..~.E..... `.vL.:..(.U.....IDATx^.....0.E.Y.\..V..4..c...\..D. 4z.|.p.....J.k.....O)G...u1_...f{.....R..c.B...Wi...AP....si.mi..5o.[.....7.;c...qg.....|..8..y.....%.+;...*..`..H..`.QAt.;....Y...9.....[gj...2. .L...M.2^.....Lq..'...)...j....x..I.P0e...`..{..?A.-.:.ug..}*.....1.R..g..<.[.qR..X...)..X.5...m.s.D-..35..w{.....Zo....6.U.....5....)...(..[..:.7LK.....5...%R2..OGi.....e:..Y.bf.f.A..V8.1.,{h. .....,VH.....Y5..K..<K....G..h .Q...C.J.%.....FEh"..kv5GH.(..u.v.;`.0F.h.4....#.K.-..7..?....fWs. a...5.5...0L.H9l/....9.b..].a..<.....7^...d.T....B..fW.$.f..M.A..E..8..`_...+.....jV.....i -<.....rCl.[..Y....-.s.....Q...9.5..=..`.sG.B.7o..wK.....]..R2..S.C.3.....8.J,x5....T`...8k....=.K`..Opjv5.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bat[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	28733
Entropy (8bit):	5.307228433868498
Encrypted:	false
SSDEEP:	384:otUVCwh9wC22xo1kB4KZrhbwM05Jkr9qNHfs9nB/wDSliNqCET8zT7QAEqny7YyV:pCwhBRMDOZwDhzT7QSnKYye0
MD5:	815C752A1218F66565366C60C0E4B265
SHA1:	615F539F4291D33C097AC72C75F69A14D5A6EEBE
SHA-256:	F14F0D4CA69DB0C2914322578F10BF3F9393771F439C9F670CC4D40971B0AF8D
SHA-512:	A8B6A69036D47649463F890EA3EFF428223300D8A7353273F931462A55B2F54FF4837262F38FF4437E214C07E40930CB6A094674590951C7A8AF51B987AE31F3
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.customE vt="custom";this.pageViewEvt="page_view";o.Ver=o.Ver!==undefined&&(o.Ver==="1"||o.Ver===1)?1:2;this.uetConfig={};this.beaconParams={};this.supportsCOR S=this.supportsXDR=!1;this.paramValidations={string_currency:{type:"regex",regex:/^[a-zA-Z]{3}$/,error:"{p} value must be ISO standard currency code"},number:{t ype:"num",digits:3,max:999999999999},integer:{type:"num",digits:0,max:999999999999},hct_los:{type:"num",digits:0,max:30},date:{type:"regex",regex:/^\d{4}-\d{2}- \d{2}$/,error:"{p} value must be in YYYY-MM-DD date format"},"enum":{type:"enum",error:"{p} value must be one of the allowed values"},array:{type:"array",error:"{p} must be an array with 1+ elements"}};this.knownParams={event_action:{beacon:"ea"},event_category:{beacon:"ec"},event_label:{beacon:"el"},event_value:{type:"number",b eacon:"ev"},page_title:{},page_location:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\hypnotize_bg[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, 400x400, frames 3
Category:	downloaded
Size (bytes):	15952
Entropy (8bit):	7.873155709594633
Encrypted:	false
SSDEEP:	384:T6VjZDtysTfy1mOnEyWNG3jMFoMNVbbWuANqRXI7hxVvwwMyh1Kx:eLe1HlPAPb6pq47hrtzKx
MD5:	74747D06042222DFBE0A46E650CF5949
SHA1:	4B64B5EF4B86B0C4E8F01CD7EF2D62A702873A20
SHA-256:	CDC86B519E06E92392B0B714F3C3161BF037A2E2FB21D6D10E3E32D44D48BACC
SHA-512:	4BA37C6D8E6331625F2C70CA56CB80C4C13F4097BD5EC7C4BA5789F3506181873F3178C380029BCC8F2E740B05BF0AE429ED9B2843B3873177A44DA29A568C0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://keepn.com/graphics/lpgraphics/landing_pages/htm/hypnotize_bg.jpg
Preview:	......JFIF.....C.....!*$..(..%2%(,-/0/.#484.7*./....C..... .N.tA(...k*8#..E.QE..Me3....2.(..C4..D..D...QZ.d....A.S(.k2....*k*%.QEk . .me..ID(.D..D..D.....(.X#:e(...M.....D....(..A.tA.QE.GP...hA.....gC4(.....U4(...M.!..e.5...3..L.(..Q.,.,.4.<.. <..IL.....<.O.2..0.F...tA.gr.....&.u.(..D.L.D.h.Zh.Z.34....).&]E.gD.&D..o...w(k..hA.gr....,j..3.k2..2.[Y.umfY.....K;L.!j`...Mf.....P..$.....J(..5...E.Zyi.yv.(..(..<..L.YE(.D..D..2 .`.Y. tQE6..+.J%..R.....U4G.d.(..(..B...r..i.yi.yi...Y.Y.!D...g.SD.3ak)(.D. .AR...QE.QE....h..i.yi.yi.yJ.....$..hL..2.me(....'..'.J..p..(..(..hA...D..D..D.....DYt.WE.....D.....3N.!j(..QEd.: .:kO- 4O-4O+..U4O-4&VD.B.Y5.+!E(.d.(..%.E.hA.j9.tQE6..3....U4O-4O+..&...D..BedA..,.B.u6....].Q*...: .3.CN.L.4..!SY*9...U.g.SBeZ.....k(i.+'....-L.L.f

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\js[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	91010
Entropy (8bit):	5.502513334144413
Encrypted:	false
SSDEEP:	1536:aSTlTcBsf3u50oB+HDztx1WeZeYzMIcGmBML0NN1gn1A9hKPZ3JdQ5VuoeNuIDJv:aSBTkS3u50vtxIeZezMUgOOofeh
MD5:	8D10AE258936E6C8B040DD0E833CA8DD
SHA1:	E84685AF2163C5E1CA1AC2314E86F588DACD15AC
SHA-256:	65180B1B5FD8A9861B05E2BA937F2F9109310625CA1AB77BE53E9A1531A3227C
SHA-512:	598917B1AFB9A4FA82AF74F7CC9261063879BE8CBEBD622C546C26B7F677531D2958A1E6908A4FAC0E83E41E259A1B813060CFDAA6DA6A43208E11BA33B191B 8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google-analytics.com/gtm/js?id=GTM-MDNV5QP&cid=1215391881.1616667433

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\js[1].js	
Preview:	.// Copyright 2012 Google Inc. All rights reserved..(function(){..var data = {."resource": {. "version":"78",. . "macros":[{. "function":"__e". },{. "function":"__dee". }],. "tags":[{. "function":"__asprv",. "vtp_globalName":"google_optimize",. "vtp_listenForMutations":false,. "tag_id":6. },{. "function":"__asprv",. "tag_id":7. }],. "predicates":[{. "function":"_eq",. "arg0":["macro",0],. "arg1":["macro",1]. },{. "function":"_eq",. "arg0":["macro",0],. "arg1":"optim ize.callback". }],. "rules":[. [["if",0],["add",0]],. [["if",1],["add",1]]].},."runtime":[].....};../*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0 .*/.var aa,ba=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}},ca=function(a){var b="undefined"!=typeof Symbol&&Symbol .iterator&&a[Symbol.iterator];return b?b.call(a):{next:ba(a)}},da="function"==typeof Objec

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\main[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines
Category:	downloaded
Size (bytes):	51409
Entropy (8bit):	5.536558756791254
Encrypted:	false
SSDEEP:	768:q0IPFruycGDzlc6amX7sAtJftzQyudtrUp4BjQ2+nbCElbO+Pxz:ExYGa6a+ftzQy+y4hQ2+mI7
MD5:	137B9ABABE3E2A97383A2597B91786A0
SHA1:	F3F701712FB5765F5D764F2A9262F78D852D19F2
SHA-256:	43174A7F2DBFD1C2235A0EC1609DC283FDDF1B31BE8F0845D072F118DB6CCE69
SHA-512:	F24AF7D7D479AF96EA8815550C35569D11056ED9A6C1476990B2244B76694C8FB4CA47B5B3119601016C1A913311CE14C868F605A1E7AC61F28A6AC319729B14
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://widget.trustpilot.com/trustboxes/5406e65db0d04a09e042d5fc/main.js
Preview:	.!function i(a,s,u){function l(t,e){if(!s[t]){if(!a[t]){var n="function"==typeof require&&require;if(!e&&n)return n(t,!0);if(c)return c(t,!0);var r=new Error("Cannot find module '" +t+"'");throw r.code="MODULE_NOT_FOUND",r}var o=s[t]={exports:{}};a[t][0].call(o.exports,function(e){return l(a[t][1][e]||e)},o,o.exports,i,a,s,u)}return s[t].exports}for(var c="function"==typeof require&&require,e=0;e<u.length;e++)l(u[e]);return l}({1:[function(e,t,n){"use strict";var r=s(e("@trustpilot/trustbox-framework-vanilla/modules /impression")),o=e("@trustpilot/trustbox-framework-vanilla/modules/api"),d=e("@trustpilot/trustbox-framework-vanilla/modules/utils"),i=e("@trustpilot/trustbox-framework-v anilla/modules/queryString"),f=e("@trustpilot/trustbox-framework-vanilla/modules/templates/stars"),p=e("@trustpilot/trustbox-framework-vanilla/modules/templates /logo"),v=e("@trustpilot/trustbox-framework-vanilla/modules/templates/summary"),a=s(e("@trustpilot/trustbox-framework-vanilla/modules/init"));functi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\main[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines
Category:	downloaded
Size (bytes):	82129
Entropy (8bit):	5.607457761029765
Encrypted:	false
SSDEEP:	1536:sTFo3qZsYor+7E11KQKD8OaTH3LTIHIZQzQy+y4NnxR8u5:s+zOa7LTj
MD5:	29BD80DF7C051084066709022D748C45
SHA1:	D1F303B1672677B5F651F6409DAB0C283535D530
SHA-256:	703D55C7607C1564783CF1F4DF1D6125F0064216FA2813CBDD0659AC1C3A438A
SHA-512:	050CD4AC4FC36CC3300625EB33C546B3041897CD8C6329DEA0C3B2E8B43FA8822BA122ADEA9D5514BBFDF595717070A1512C3F9116E99572519926BCB9319D5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://widget.trustpilot.com/trustboxes/539adbd6dec7e10e686debee/main.js
Preview:	.!function a(o,i,u){function l(t,e){if(!i[t]){if(!o[t]){var r="function"==typeof require&&require;if(!e&&r)return r(t,!0);if(c)return c(t,!0);var n=new Error("Cannot find module '" +t+"'");throw n.code="MODULE_NOT_FOUND",n}var s=i[t]={exports:{}};o[t][0].call(s.exports,function(e){return l(o[t][1][e]||e)},s,s.exports,a,o,i,u)}return i[t].exports}for(var c="function"==typeof require&&require,e=0;e<u.length;e++)l(u[e]);return l}({1:[function(e,t,r){"use strict";var n=i(e("@trustpilot/trustbox-framework-vanilla/modules/impressio n")),s=e("@trustpilot/trustbox-framework-vanilla/modules/api"),S=e("@trustpilot/trustbox-framework-vanilla/modules/utils"),a=e("@trustpilot/trustbox-framework-vanilla/mod ules/queryString"),_=function(e){{if(e&&e.__esModule)return e;var t={};if(null!=e)for(var r in e)Object.prototype.hasOwnProperty.call(e,r)&&(t[r]=e[r]);return t.default=e,t}} (e("@trustpilot/trustbox-framework-vanilla/modules/communication")),w=e("@trustpilot/trustbox-framework-vanilla/modules/dom"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\prototype-1.7.3.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	148134
Entropy (8bit):	5.247186972803087
Encrypted:	false
SSDEEP:	1536:NElClk2AJ4Om9/w5/wSxmvtyfv0fKUli/MYGHi1YmL46mR7CSfofDNKD0FRp0uFL:p64OwxyYG6lCSWPpq+D
MD5:	E0F66399BFE49D2BE6976726138869AB
SHA1:	CD6CC034C19B253E4A26A1107F61FEAD66532C4B
SHA-256:	F235FF9CA71534AF3417D8D2F8D7CFAB6BF88468DDBB9679F53B2B4C42081E94
SHA-512:	198A12138B476FE7C5A0A0A62685B608B50E64ED5C60099ED5DD0252C3F9BEC35FFA44123EC4E7B044135F7AF47EDF06BEDEB8E16FF10C61739BDEC19328715 B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.keepandshare.com/global/ajax/prototype/prototype-1.7.3.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\prototype-1.7.3.min[1].js	
Preview:	var Prototype={Version:'1.7.3',Browser:(function(){var ua=navigator.userAgent;var isOpera=Object.prototype.toString.call(window.opera)=='[object Opera]';return{IE:!!window.attachEvent&&!isOpera,Opera:isOpera,WebKit:ua.indexOf('AppleWebKit/')>-1,Gecko:ua.indexOf('Gecko')>-1&&ua.indexOf('KHTML')===-1,MobileSafari:/Apple.*Mobile/.test(ua)}})(),BrowserFeatures:{XPath:!!document.evaluate,SelectorsAPI:!!document.querySelector,ElementExtensions:(function(){var constructor=window.Element||window.HTMLElement;return!!(constructor&&constructor.prototype)})(),SpecificElementExtensions:(function(){if(typeof window.HTMLDivElement!=='undefined').return!0;var div=document.createElement('div'),form=document.createElement('form'),isSupported=!1;if(div.__proto__&&(div.__proto__!==form.__proto__)){isSupported=!0}.div=form=null;return isSupported})()},ScriptFragment:'<script[^>]*>([\\S\\s]*?)<\/script\\s*>',JSONFilter:/^\/*-secure-([\s\S]*)*\/\s*$/,emptyFunction:function(){},K:function(x){return x}};if(P

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\screen_day_view[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, 1066x710, frames 3
Category:	downloaded
Size (bytes):	53660
Entropy (8bit):	7.760115576888295
Encrypted:	false
SSDEEP:	1536:cmdUxwGWzyHHe3sPhX1777777777777KcPh:c3uG3Hp5Xoc5
MD5:	DFABD438268BFBA8E4EBCF2F6B4FE850
SHA1:	4EDEA995E8CD966FE4393A6881CD4ABF5138BDE2
SHA-256:	7C93F35E13747BB842C7BD39CAB1C15B4044B1613AA5C4044CCC25EF9C206496
SHA-512:	ADF691DC9F259BBB965D965B94E91B6CCEF27329FEDF13ACA934B341F8E5C1A205AFF2B694FB5BF515619A2060E932AC01C6D4DF4039B1FE5329EFC7E271C00
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://keepn.com/graphics/lpgraphics/core_pages/calendar_samples/screen_day_view.jpg
Preview:	......JFIF.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=====.. .....*.....i.....*.....A...Y.....4..21..j.....+..H.}.-7..Z...5..fM.. r..yj..... .....*N...@99.|...g..?.~{.<...._.....=/.....V....`W.....8@21....n..igY.{5.v.....1.Y.....#..... H.....".....W|.N.[...L...%.....@ ..q.~xo...<..W..{.....WW.y?.}..o...y.....C...g....x=....V.TH.....&....d.F'9 Dx#a.B..+..".._O.y.g....^....e.~\.....;k...:....#.x...}...Q....>.....'..z..u._W.g..?../..o.9..n=.{..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\screen_event_view[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, 1066x710, frames 3
Category:	downloaded
Size (bytes):	90000
Entropy (8bit):	7.8590923965505155
Encrypted:	false
SSDEEP:	1536:YR9tytMIq21PxD9bO2Mlqrc8wjPojk7Q6moYXW+O1l:YR7ZIddJd/MlqrcZbojRG3
MD5:	4CF34DB1E8F0B7EADF64E8C06C86CD0D
SHA1:	2821FABDFF7FB30AEF196623BFCA41613C664BF5
SHA-256:	1298FD22B241B849511A45A34E504317037BE9EC5DFCAAEAB128635A9D79B417
SHA-512:	387A79ECB719A62C535EB7327B3B8EE676C37868C68D7DF34C80776E8C833E4607AF3785A5FF3E938585FF67FC19EE7CE3FE4C645672886029EF6D1397297480
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://keepn.com/graphics/lpgraphics/core_pages/calendar_samples/screen_event_view.jpg
Preview:	......JFIF.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=====.. .....*.....iP.....C.r.....A. .....@F....._?..z>V.>....^7..u}~.5...R3`T9..... .....9%...@*s.....]..*..}y...~/.._...g.t;...e.Cb.C._:.....Q....E...3K.f<.]..@FH.....9e ..@..... .....+.....L.@...;.zb...mf.;(.....`..... ..<.....}/...w._G..>o....L..eb.'.O.{...<....g.....~.=....d..+..... .....j@hW....R..<.!.C.Z9.8.....;...?...|.....{_.....O....;*..{....^?..s}g.~..y.....<.....~....~.....'.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\screen_sbs_view[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, 1066x710, frames 3
Category:	downloaded
Size (bytes):	64571
Entropy (8bit):	7.865279269396666
Encrypted:	false
SSDEEP:	1536:RudByf9x0RUCKUc0nm6NtmfZkRJoDfYEoPdbjPZDQuf:RudByf9GU7UtnmktM2JcYnlPZ8uf
MD5:	737DD13976887ADD6513B1FB6B55F2F0
SHA1:	A0D67B3FC2B82EDFCB22C86E608D20BBF68FC17B
SHA-256:	4C5C72149BF1048BB90F515A81784921A7188BBEF359800B1B8A7F531DF4C982
SHA-512:	A28D7559659665EB18441C9128BCCAF0C866A09800643505EB350F6F1AE0E524AE064399A83EA60433E9B99A736BBAD62229F3C74FFE5D71E01BAC3E4A42D099
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://keepn.com/graphics/lpgraphics/core_pages/calendar_samples/screen_sbs_view.jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\screen_sbs_view[1].jpg	
Preview:	......JFIF.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=====.. .....*.....i.....fT.....A. ..t;.....0..@5.R...].V.{1.]..Zn/:...Y.[.:....'..... .....M}>G…]....9.K.....=/..Xo.9.M....q<.....$...@.,vu.^1..X.._L...@s:....Y.....`..... .....d.l.....&....&W .....;OS.k4.....d.....`..q.~xoK...../q.....\&Ta2.....S...?.....p...S...;..L..ep.Q.....N..pK0J5 #.G.:.D,.Eq\l_.....g/.....o.../1.|.....Z....0..?.y.....s|...U.y.W.....F.....~..z^....S5.W.M...;.{_7....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\screen_week_view[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, 1066x710, frames 3
Category:	downloaded
Size (bytes):	49220
Entropy (8bit):	7.761069076707196
Encrypted:	false
SSDEEP:	1536:UIp3aGIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIblqhonhKZt8:Ui3TIIIIIIIIIIIIIIIIIIIIIIIId
MD5:	EF13CA8782B23DE18679EEF6C3C05707
SHA1:	802D4873DA9A5F7358BC0FB86B2B9C0273868738
SHA-256:	7F38661A68D01F0F00B5637A5AC6103DA8F906BF8560D7562DBAEED577790C84
SHA-512:	00843B5B663E0D9E1BB095CAFC9D01223EE467D8271A696A67B3B70D8AF8EA02A97C7C36CB30F0224483B1B444F04522B803C1EA67F3A8DD519664AB26051E5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://keepn.com/graphics/lpgraphics/core_pages/calendar_samples/screen_week_view.jpg
Preview:	......JFIF.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=====.. .....*.....i.....a.9.....A.....AX.F ..q|..[...Xx.F5w..._;.....-+2...7..... ....js.....]..*..|y.c...../.z_.....]r.d.....T.....rM...@.Y.n..igY.<..A.X...A.o.0.....4.21..... .....Rdw.I!I+ ...;.zj...ef.9(.@.....@$.....#.xo....n.+.....|..,$.....>.....<....g...{...8..{o..V.B.J.J.....p ..X}...G8.....}?..}._G..{.....s...{.?..uxv..^...|.....3.}G.G...?..|.....p....7..+.x_....._n=n=.=.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\screen_year_view[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, 1066x710, frames 3
Category:	downloaded
Size (bytes):	100116
Entropy (8bit):	7.9401166103354495
Encrypted:	false
SSDEEP:	3072:zSyvYSOjQABwHVgUGzSbm8AH+A3WUrHT69bluYLO:5vYSOjzsVCR84pmCHT69BYLO
MD5:	FC888E7825101D287A88F0464BD1EF4A
SHA1:	5BB81EF67F2C037212AC8024F1AEE308A54FDD9A
SHA-256:	29CD376D7BBB1BE1E09AFDB7397E2846ABAE8CAB2EB8C7C08ECFDBDC766309C1
SHA-512:	887CBFD24A710526D719E956381F0B0D9AB30807DF5D93E9F706FEBA51A2F89E5C083C93C143C9AA9598C997A2678C562521798346E87FBA6B97688202F90012
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://keepn.com/graphics/lpgraphics/core_pages/calendar_samples/screen_year_view.jpg
Preview:	......JFIF.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=====.. .....*.....iP.....C.r.....A. .....@F....._?..z>V.>....^7..u}~.5...R3`T9..... .....9%...@*s.....]..*..}y...~/..._...g.t;...e.Cb.C._:.....Q....E...3K.f<.]..@FH.....9e ..@..... .....+.....L.@...;.zb...mf.;(.....`..... ..<....}/...w._G..>o....L..eb.'.O.{...<....g.....~.=....d..+..... ....j@hW....R..<.!.C.Z9.8.....;...?...|.....{_.....O....;*..{....^?..s}g.~..y.....<.....~....~.....'./

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\seg[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43
Entropy (8bit):	2.7374910194847146
Encrypted:	false
SSDEEP:	3:CUnl/7yltxlHh/:/+/
MD5:	07FFF40B5DD495ACA2AC4E1C3FBC60AA
SHA1:	E8AC224BA9EE97E87670ED6F3A2F0128B7AF9FE4
SHA-256:	A065920DF8CC4016D67C3A464BE90099C9D28FFE7C9E6EE3A18F257EFC58CBD7
SHA-512:	49B8DAF1F5BA868BC8C6B224C787A75025CA36513EF8633D1D8F34E48EE0B578F466FCC104A7BED553404DDC5F9FAFF3FEF5F894B31CD57F32245E550FAD65 A
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\tp.widget.bootstrap.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines
Category:	downloaded
Size (bytes):	21263
Entropy (8bit):	5.223505661574105
Encrypted:	false
SSDEEP:	384:qF6H8gJF7V2YHbwirdsnAgb08nL+xu1qz3w3FyjDrNL8XkVO5oInM2NHhBrI0v/B:qF6coF7VdrdsnAggaLMZz3w3FyhEZnMS
MD5:	7317650D5DFD754D6285A0B01E058AC8
SHA1:	7AD6BC8CE4663BD658CD3C4793E4F62C4A3FB704
SHA-256:	648C1DE13CB751E7C054B5A44ACC2082F58A05DD5753B9F9827A1BCD8865A278
SHA-512:	5C74A87FDBC103A1032ECCE28352A0F64C409780994D3A12F58613FF94002E014EBDDD05954EA43D9FD8205287DE880A72480EF964CB47358889C36B8AEC7988
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://widget.trustpilot.com/bootstrap/v5/tp.widget.bootstrap.min.js
Preview:	.!function o(r,a,u){function d(t,e){if(!a[t]){if(!r[t]){var n="function"==typeof require&&require;if(!e&&n)return n(t,!0);if(l)return l(t,!0);var i=new Error("Cannot find module '" +t+"'");throw i.code="MODULE_NOT_FOUND",i}var s=a[t]={exports:{}};r[t][0].call(s.exports,function(e){return d(r[t][1][e]||e)},s,s.exports,o,r,a,u)}return a[t].exports}for(var l="function"==typeof require&&require,e=0;e<u.length;e++)d(u[e]);return d}({1:[function(e,t,n){"use strict";var c=e("./constants.js").OFF,s=e("./xhr.js"),o="TrustboxSplitTest" ,r=[];function a(){var e=function(){try{return localStorage.getItem(o)}catch(e){return null}}();if(e)return e;var t=o+"=",n=document.cookie,i=n.indexOf(t);return-1<i?n.su bstring(i+t.length).split(";")[0]:void 0}function i(e,t){!function(e){try{return localStorage.setItem(o,e),!0}catch(e){return!1}}(e)&&(document.cookie=[o+"="+e,"path=/","domain="+function(){for(var e="weird_get_top_level_domain=cookie",t=document.location.hostname.split("."),n=t.length-1;0<=n;n--)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\voc_amy_kelly_md[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, progressive, precision 8, 200x194, frames 3
Category:	downloaded
Size (bytes):	10133
Entropy (8bit):	7.9429669875141276
Encrypted:	false
SSDEEP:	192:VJfINrwrhfDVSXnZFzLq358dj9eT2AfK+ndz4Pjj4UlQLUO:VJyrwdDk3C58dm2Ardz4GT
MD5:	04D1EE636642E007EC5E3DE2CEC87D7C
SHA1:	B92EBA370237EC04C0700CA0471AD56C66800E07
SHA-256:	EE5CE7B3D2BB601FA2D9B7C2D84B17AAD8CFDE82547FC705AD0A4076839FB810
SHA-512:	6229326842C306155601A4DF1D8A0138E66CDE547AC4D01E1F63F448820F6D281C22DDE38DDFF864990941A3262EB3344DDB6210E44A08D4D446C4813FA5D320
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://keepn.com/graphics/user_photos/voc_amy_kelly_md.jpg
Preview:	......JFIF.....`.`.....C.....!..... "$".$.....C..... "..... 5..d>..B\(S..A.,(...KB=.. TR.'.7..iv._..p.>!Lx....|.....+..\....(a..!.D|..c.=.....|7.e.%...Y..._M).....luK..{s...Y.3.2... f.J'....Q.m..n^.-..CM<...T..IQ5.3W...".{9,.:#.b.AM.@.....-.d.z..M.>!#C.....f.....5...;#.0.,.. .....y.E#.B.).&.D....&.....G..p...L....q.~ .."._....0.a.$}....MS.zI.....$.m....i.(...0.!...-S.n....rVO.F.O.....R....hu.Vs..2z...3....=:.....Z.h3.Dy..a..).....u{>R..=...{<.....tL0EX. ..Y..: .....H... ... G.3`.6_...{.AY..VHh.i...$.I...S#..Q.....>.5.....qr[4.Xb|...x..xe..aa.zc.....,...<...X.....h.LG.....@X...*.....$Y3>....V]v.}P.AN..u].....f...T.A.X .m..6i(L...N.....Y..C_.....BM...\,....W.(.....`].....i.....H2F...S%.N...\2..q.6R

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\1067089813[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	126
Entropy (8bit):	2.9881439641616536
Encrypted:	false
SSDEEP:	3:CUXPQE/xlEqjdfXPQE/xlEqjdfXPQE/xlEy:1QEoqh3QEoqh3QEoy
MD5:	7EDD19F8419144CEA07BFBE8887B944E
SHA1:	49D47C4F9EAFC111ED241D743F09D73C3A12F5C4
SHA-256:	605627E07A397426E1FDB473A8B69F252EB192CC953C266199DE9E5E63629F68
SHA-512:	19034777E93BFAAF0A80256EDFAED658D544E8EF9139C24C7FBBDE8CEAA9FFA5319558D33897DC692233784C147CAE7A9A5D80335A9206407ED0F15077BCE95 A
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D.;GIF89a.....!.....,.....D.;GIF89a.....!.....,.....D.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\1067089813[2].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	42
Entropy (8bit):	2.9881439641616536

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\1067089813[2].gif	
Encrypted:	false
SSDEEP:	3:CUXPQE/xlEy:1QEoy
MD5:	D89746888DA2D9510B64A9F031EAECD5
SHA1:	D5FCEB6532643D0D84FFE09C40C481ECDF59E15A
SHA-256:	EF1955AE757C8B966C83248350331BD3A30F658CED11F387F8EBF05AB3368629
SHA-512:	D5DA26B5D496EDB0221DF1A4057A8B0285D15592A8F8DC7016A294DF37ED335F3FDE6A2252962E0DF38B62847F8B771463A0124EF3F84299F262ED9D9D3CEE4
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\183487702480957[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	246714
Entropy (8bit):	5.470147234754284
Encrypted:	false
SSDEEP:	6144:Rk1HWCSntDV/H4K3V/H486EPjQHWuH3HpF:f6EA
MD5:	16641F0708FCFC0E580FD4135771EC3B
SHA1:	6542AE4E2683C78151FE40D12F6970B8E7100EEE
SHA-256:	B624D0AAADB541F3BF5120BF21D540BFB5C64B22615031FB4DB7713B22A54260
SHA-512:	E0DF903CE2E91AC9A108D6F210BFD64DF76E8E42C52E1B47D8E0E28BC6ACAAA782FC154CA8D5ED884D1F087630238273E3DAF5EFB8390723F4773EBF6395524
Malicious:	false
Reputation:	low
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\183487702480957[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	246714
Entropy (8bit):	5.470147234754284
Encrypted:	false
SSDEEP:	6144:Rk1HWCSntDV/H4K3V/H486EPjQHWuH3HpF:f6EA
MD5:	16641F0708FCFC0E580FD4135771EC3B
SHA1:	6542AE4E2683C78151FE40D12F6970B8E7100EEE
SHA-256:	B624D0AAADB541F3BF5120BF21D540BFB5C64B22615031FB4DB7713B22A54260
SHA-512:	E0DF903CE2E91AC9A108D6F210BFD64DF76E8E42C52E1B47D8E0E28BC6ACAAA782FC154CA8D5ED884D1F087630238273E3DAF5EFB8390723F4773EBF6395524
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://connect.facebook.net/signals/config/183487702480957?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\PSUEOSZZ\K6ngFdK5haaaRGBV8waDwA[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	2010Version
Category:	downloaded
Size (bytes):	74880
Entropy (8bit):	6.430447739075601
Encrypted:	false
SSDEEP:	1536:pMA3m69ACvjj/RFetMx1EoYIQc22wWmZHGdrIXwoerks2DvukDmS:qCYCvjj/RFoMx1zYIDKHarIXArksc5
MD5:	B31792FB6A5825FBE2B9779C52EFC219

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\K6ngFdK5haaaRGBV8waDwA[1].ttf	
SHA1:	990984BFC90351F2CE8B7FDA8141822AEF78F17B
SHA-256:	3E2FDF4BBF6D0768EDA9228A927F23B12C169BA359523CFEDA3AC767ECAA23F0
SHA-512:	66D1C7B646E4B36B8DF79833152B083F372320856BF3566F8850C63E3E24B8CDA773656A6052D55B68197BC714FE8CB97E5F66A671400311AFCAB9E4AE6850A8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/cabin/v9/K6ngFdK5haaaRGBV8waDwA.ttf
Preview:	.....0GDEF.....<....GPOS.$.....l..=.GSUB.....? ....OS/2kf....?,...`VDMXo.w?..?.....cmap..m..El....cvt .....F....(fpgm.A....F@...agasp.....G.....glyf{[....G.....hdmxa.....P..(.head.;<.....6hhea.-.a.....$hmtx..!R...4...Lloca..!.....maxp..... (... name.i6... H...ppost*.mV..!....prep..$)..#.....0...2.a...d.....,..DFLT.....kern......./@4D...D.....<.j.|.....8.Z.....4...&.....>.....".....`.<.....>...L.V.h.<.....b.....b.b.....6.....6.|.....:.R.H.b.l.....4.....<.....\.....<.V.<.<.<.<.....<.b.....L.....<.....0.....0.R.\.....!.=...B.\.1.a.a.L.k.k.M.n.o.N.z.z.P.~...Q.....i..... ..!.....H.....5...7...8...G...M...U...W...X.....+.....G...H...U...W...X.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\WV1W1JAQ.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	144365
Entropy (8bit):	6.106338266606129
Encrypted:	false
SSDEEP:	3072:uNn0YbaHAM75pNZ31Qe8be0P+xvHxgk3XdHCEuVBTkbKVHpWY75Q6Y9TdTb:waHAM75pue8C3nXHdHCDVBTkbKVHpWYO
MD5:	A06D9F6510BC3E09C0798EF1F5C2658B
SHA1:	0595E9A399968BB421B6612AB7FD3067A8800960
SHA-256:	72374C0946908A2FC040671A40CBE4B212FD51E39E5BA7D5E2B79FEC4955CA4F
SHA-512:	3AC34FD7BD45B0D6DC2F2C3863D557265C2710A6919B7B52CE6B01CEF20DF1731CE8AA0FEE3965ACC6B054D594B3514B0FC9BC81DCBE60E0893767F058042AD5
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>. [if IE 7]> <html class="ie7"> <![endif]-->. [if IE 8]> <html class="ie8"> <![endif]-->. [if IE 9]> <html class="ie9"> <![endif]-->. [if !(IE)]> > <html lang="en"> <![endif]-->.<head>. Using versions.php for latest print dialog javascript and css versions --> <script>. !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', '1947377292258582');. fbq('track', 'PageView');.</script>.<noscript></noscript> -->..<meta charset="utf-8">.<meta name="viewport" conte

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\api[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):	884
Entropy (8bit):	5.610797637679121
Encrypted:	false
SSDEEP:	24:2jkm94/zKPccAXU+KVCetW+1DYLY7sLqo40RWUnYN:VKEcKHKoeM+1DYLYwLrwUnG
MD5:	93F7625CED3CFAD104705C24F85422FB
SHA1:	4F5F6E23342926E05A7E554D76763F6A12191849
SHA-256:	27180C223B4AC955F47D663377D20B08C1C3DC638720B1A84163196604B7A2FB
SHA-512:	FBA5CDE41342FE568108916FCAA06D230A0C341BDAEA3F37DD916BA67F18B10D1F1E34EE8344ADF04029D58A45BCDDE00AD3AFA700EFE61430EAEFFD4229AE59
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/recaptcha/api.js?render=6LePRYAUAAAAAFOMetxSk3zNP53GLq1OntSUjnMP
Preview:	/* PLEASE DO NOT COPY AND PASTE THIS CODE. */(function(){var w=window,C='___grecaptcha_cfg',cfg=w[C]=w[C]||{},N='grecaptcha';var gr=w[N]=w[N]||{};gr.ready=gr.ready||function(f){(cfg['fns']=cfg['fns']||[]).push(f);};w['__recaptcha_api']='https://www.google.com/recaptcha/api2/';(cfg['render']=cfg['render']||[]).push('6LePRYAUAAAAAFOMetxSk3zNP53GLq1OntSUjnMP');w['__google_recaptcha_client']=true;var d=document,po=d.createElement('script');po.type='text/javascript';po.async=true;po.src='https://www.gstatic.com/recaptcha/releases/6g5J7UfDQ9mLrweZHj04ekSP/recaptcha__en.js';po.crossOrigin='anonymous';po.integrity='sha384-RuApWdDoPwLFNdUYlX+rsBAHAtQruqW8JHyDdyejk08kG6qc+NXpVxNUKhPYwyoI';var e=d.querySelector('script[nonce]'),n=e&&(e['nonce']||e.getAttribute('nonce'));if(n){po.setAttribute('nonce',n);}var s=d.getElementsByTagName('script')[0];s.parentNode.insertBefore(po, s);})();

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\email_validate[1].js	
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):	3314
Entropy (8bit):	4.983205547622022
Encrypted:	false
SSDEEP:	48:yiCr8l1G8XbUA/EosrlgrakdZuCK3LvxR/Y4yLkA9hy:SIbUA/Eosrlgr3cC6LOQ
MD5:	D516C69B5DFB7425A2F354DD3FCCB739
SHA1:	942F7FB271513510A49E78DA1C96204172CE752D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\email_validate[1].js	
SHA-256:	2AC4D39AAC6AEF2FF8238112D1AE1A24CCBA503C06B79D40E9700FCF35031B9F
SHA-512:	954FF8DA7EA2638FFE18AE9463AAEAAF1D486BA6F3F638338E62788F86C3FB623A333A1B31BC7D4D65CBDF20629B690470A83443143D178CE515D248EADB507E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.keepandshare.com/global/javascript/email_validate.js
Preview:	// email_validate.js Javascript functions to do initial validation of multiple email addresses..// addr = email address, man = 1 if email address is manatory, db = 1 if displaying error messages is ok....function validateEmail(addr,man,db) {...if (addr == '' && man) {.... if (db) alert('email address is mandatory');.... return false;...}...if (addr == '') return true;.....addr = addr.replace(/^\s+|\s+$/g, '');..// Trim left and right of spaces.....var invalidChars = '\/\'\\";:?!()[]\{\}^|'; // removed blank (space) from illegal chars...for (i=0; i<invalidChars.length; i++) {.... if (addr.indexOf(invalidChars.charAt(i),0) > -1) {.....if (db) alert('email address "' + addr + '" contains invalid characters');...../ /alert('rich');.....return false;.... }...}...for (i=0; i<addr.length; i++) {.... if (addr.charCodeAt(i)>127) {.....if (db) alert('email address "' + addr + '" contains non ascii characters.');.....return false;.... }...}.....var atPos = addr.indexOf('@',0);...i

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, with no line terminators
Category:	dropped
Size (bytes):	2273
Entropy (8bit):	5.746488937517749
Encrypted:	false
SSDEEP:	48:0VUUIqzPrqTnJcgVhkGCrWH/Oa2UxbSrWH/Oa2Ux06:+UURWTCgVhkvrnUxmrnUxN
MD5:	741422364D992103B2F373794554C039
SHA1:	AE5808860A21D6480020B55B243A845E7F72466F
SHA-256:	3D433D3A1E1878FA9C530D8410CC9B248433D1F71A3A12458095D16913C9B992
SHA-512:	744C7315B386E5E63B63F9479D3867233EE52481FC5A063FB72C79BBAB5B9EBB4FDFC2778191A1049C85225D27E27C84B9C00305D1F638FCFCFF30D2B027BD5
Malicious:	false
Reputation:	low
Preview:	(function(){var s = {};(function(){/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0 */ var c={},f=this||self;var l=/#|$/;function n(d){var g =d.search(l),a;a:{for(a=0;0<=(a=d.indexOf("fmt",a))&&a<g;){var b=d.charCodeAt(a-1);if(38==b||63==b)if(b=d.charCodeAt(a+3),!b||61==b||38==b||35==b)break a;a+=4}a=-1}if(0>a)return null;b=d.indexOf("&",a);if(0>b||b>g)b=g;a+=4;return decodeURIComponent(d.substr(a,b-a).replace(/\+/g," "))};function r(d,g,a){function b(){--p;if(0>=p){var e;(e=d.GooglebQhCsO)||(e={});var q=e[g];q&&(delete e[g],(e=q[0])&&e.call&&e())}}for(var p=a.length+1,m=0;m<a.length;m++){var h=n(a[m]),k=null;1!=h&&2!=h||!(h=d.document.getElementById("goog_conv_iframe"))||h.src||(k=h);k||(k=new Image);k.onload=b;k.src=a[m]}b()}var t=["ss_"],u=s||f;t[0]in u||"undefined"==typeof u.execScript||u.execScript("var "+t[0]); for(var v;t.length&&(v=t.shift());)t.length||void 0===r?u[v]&&u[v]!==Object.prototype[v]?u=u[v]:u=u[v]={}:u[v]=r;}).call(this);;s.ss_(window,'

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\fbevents[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	93376
Entropy (8bit):	5.3917536957896575
Encrypted:	false
SSDEEP:	1536:5M+OWt6w6aic9MeoJ2my8LuThe7KFv0a9sIOC1jaMu5Qm2B+QNSMngUSZYSlIUiZ:5OQRj1SVBYDG2
MD5:	1DE516A5B6B1C6033B92EE5F5D50C140
SHA1:	9E37DA5D5D789074D1DADD60977A9575A6332DD5
SHA-256:	9E7EA2B4BA8E2BCC4A964D6192E4671DC5F6863A1C7E35B52B229A3C1E67A68D
SHA-512:	99EF8E73A5D560CB3504B6BF1BC237957687280AFC99FCFF7A4B882FD2AE423B19721D6444FBD63D3ABCCFF8BD0A5CED79899CE02A2116D7710D2A89BEE370E3
Malicious:	false
Reputation:	low
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\forest_bokeh_bg_hero[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 1x1, segment length 16, progressive, precision 8, 1200x800, frames 3
Category:	downloaded
Size (bytes):	47588
Entropy (8bit):	7.959344400782048
Encrypted:	false
SSDEEP:	768:fP6ZwnHuk4K8ruotyQxqokeFV1aNmz1oeBfWby/xfpEQ3JUyVe11qy/fD/gh8Rqm:H6+nOk4K8rGErzisie8+5fKWJpVe1Tbb
MD5:	FB9117AA15F6CC14B6F8C69723225E99
SHA1:	D540DAA052598590D83FB383E8E338734CC1B581

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\forest_bokeh_bg_hero[1].jpg	
SHA-256:	32149A29621E5E7AB12F22B165FF37812E1719BF32AF71B5A3C01CBBDB350C08
SHA-512:	75947F1A848963E81AA0BCE2083B4D32F4629AA1B03C9BA41C6A19EDD9171611763F934B7D8EBED641D103E451A9304F1B469FC5FFC56AB13D0416F5E8D66D7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://keepn.com/graphics/lpgraphics/landing_pages/2014.10/forest_bokeh_bg_hero.jpg
Preview:	......JFIF.....C.....I......"$".$.....C..... ...".....UC@*X.T.x.....E.u.. ...sg...C...g..'.....~s..W.C..MY5.c\.Xf.6l91.Tc.oS..^.D'"#0U....$..Z.:th8$..%U...eT.^#..G.m.v:/....|.<..sR...s..^.....I$....\|.....Le.)X[..k....f..L..ms....=Z.b....n.T..B..X..t.....k.T4 .5R.....KN.A..2a.....I.kZ.:...}....rI%I...).MQ2.-*...._....6\.sf..h.t=..nm.(.*3s...FE' ..h..AdW.nJ....%J....R...my/>,....>LnsZ.n..z..v...I$.X....<.F.*..d.....L..g.?V...n.....Y..a."3f .....n.~...A.A._.....K.3e...\....kX.;....?B....IR..N.#.....(..... ...f...mv..k...m.zp'.^m..Xd..h...tU\...$.%I*.^..|...\...f...5.c].....~..%.RR.....p)iUY,.....>I.S.:m.....5.`.lN>n#:....:...dX. ....K...%<...ti{[...7.....kZ.{.....s..w..J....;...J..(a.0...Z3....}N.s.l+..f..<.u..1b.`o{..U].~.U%\...xq.....^...+...`C{Z.h.....:..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\hero_image.min_v2018[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 500, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	53323
Entropy (8bit):	7.978179667390943
Encrypted:	false
SSDEEP:	1536:tw65nXcMeN4mAQSrT5suFl+0W4tj5CnMayc:m65MM3mTSrT2X0Hntc
MD5:	9A7E637CDAE628BBDA254993003FF4ED
SHA1:	4751E25C1B02CC8C102D1F800D84166E342939B3
SHA-256:	553B8DBDD001F6A1FF249784B8C59953189D7328D3C4ACA744903D0950AD941E
SHA-512:	7BE5F0806C039289B1B883ED7C44044F31A8C9B0C64B20D013EDE9EBA857016AA8B9E35015C85CC94423A7B0CD72A2078C6E95E97DE558DC1BD5BEFAB69FF8 4D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://keepn.com/graphics/lpgraphics/core_pages/index/hero_image.min_v2018.png
Preview:	.PNG.....IHDR... .....J....PLTE.....jilTTTKKKBBB:::\\\rsp.....bbb'''''...***.....555zyx.....~~..... .....W....7.....d.....C.....h.....o.....y..r.....]j}.....~..l{.....z...+.....Z_o.|S.....J.....x~....?Wgko...NM.....~.....u.h.._.M tu~Z..=..[..H..=..4..2..9..?..-v..un.{X...c.K.....] .."b....zs.[f.R.....l..t|.o..m..n..lQ.nh.....r.....,..)..1..P..H.,,.*.....v...nk4../..'..*.....A.....xk..y..}..{..X....b.....!.....q;9QQQuuu.... .....~.....p..r.W{.ax.^u.7`-n.Wu.p.TP..x.lgT.C.`[..}L.=Ct7.IF.zq.zx..e].S....O.....x.....x.y.....tRNS..O`z..... .....Y.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\index[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):	7229
Entropy (8bit):	5.1436024840840835
Encrypted:	false
SSDEEP:	96:k70pR65H9SpAbyOeQDvXIiw69ouwsDlD9RTBMXp1eugmb5S:Lb63eT69olqlD9RTB61eFmbs
MD5:	789FDF5E4E812246D99D3B60008733E5
SHA1:	5CB5A30ED34393BD0DEBE76BE5A29DE200C5827A
SHA-256:	B1CE327D4B8E0F9E3C0D7A717BD98CF8CA6FB59C22D3BF5CE3A1131F8A43CA67
SHA-512:	3854B461782D762F56CC9D25F89DDFC8E6F023846BE5B0B83DD7BEDC7BAC07ACAA45391EF6691042DBA262A7B997FA1D219A58CADEDFA5BE3106760635FB0 54
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html><html id="ng-app">. <head>. <title>Trustpilot Custom Widget</title>. <meta charset="utf-8" />. <meta name="robots" content="noindex" />. <style>.html,body,div,span,applet,object,iframe,h1,h2,h3,h4,h5,h6,p,blockquote,pre,a,abbr,acronym,address,big,cite,code,del,dfn,em,img,ins,kbd,q,s,samp,small,strike ,strong,sub,sup,tt,var,b,u,i,center,dl,dt,dd,ol,ul,li,fieldset,form,label,legend,table,caption,tbody,tfoot,thead,tr,th,td,article,aside,canvas,details,embed,figure,figcaption,foote r,header,hgroup,menu,nav,output,ruby,section,summary,time,mark,audio,video{border:0;font:inherit;font-size:100%;margin:0;padding:0;vertical-align:baseline}artic le,aside,details,figcaption,figure,footer,header,hgroup,menu,nav,section{display:block}body{line-height:1}ol,ul{list-style:none}blockquote,q{quotes:none}blockquote::befor e,blockquote::after,q::before,q::after{content:'';content:none}table{border-collapse:collapse;border-spacing:0}body{font-family:"Segoe UI","Helvetica Neue","Hel

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\index[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	13780
Entropy (8bit):	5.116226974467753
Encrypted:	false
SSDEEP:	192:ub6PbeT69YkF8+xhhfpl/jpNZuAs6kRQeNf/DzCdE3duW3TolqS/S1wIAOE:xuaJxjpNIAs6kRQeV/DzrNu2TolqSgO
MD5:	F28F20391D42FD8E1F51F4060E320B68
SHA1:	F6D0B0FCF64FCC9CFAC142B4C514044AEE9B15E9
SHA-256:	D441B41E8E048C7F1A7453202C16B153B0EEA29667B06F543CA857812930E996

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\index[2].htm	
SHA-512:	D8997DD7E6D36A01CC8009405D946F9F24B842C94CD7F041D02414702F79F70138A8178EAE7008C9C824C543B935F6BA0524DA09A603B99096FC7F94D30E0FF8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://widget.trustpilot.com/trustboxes/539ad60defb9600b94d7df2c/index.html?businessunitId=5654e51c0000ff000585ead7&templateId=539ad60defb9600b94d7df2c
Preview:	<!DOCTYPE html>.<html>. <head>. <title>Trustpilot Custom Widget</title>. <meta charset="utf-8" />. <meta name="robots" content="noindex" />. <style >.html,body,div,span,applet,object,iframe,h1,h2,h3,h4,h5,h6,p,blockquote,pre,a,abbr,acronym,address,big,cite,code,del,dfn,em,img,ins,kbd,q,s,samp,small,strike,s trong,sub,sup,tt,var,b,u,i,center,dl,dt,dd,ol,ul,li,fieldset,form,label,legend,table,caption,tbody,tfoot,thead,tr,th,td,article,aside,canvas,details,embed,figure,figcaption,footer, header,hgroup,menu,nav,output,ruby,section,summary,time,mark,audio,video{border:0;font:inherit;font-size:100%;margin:0;padding:0;vertical-align:baseline}article ,aside,details,figcaption,figure,footer,header,hgroup,menu,nav,section{display:block}body{line-height:1}ol,ul{list-style:none}blockquote,q{quotes:none}blockquote::before, blockquote::after,q::before,q::after{content:'';content:none}table{border-collapse:collapse;border-spacing:0}body{font-family:"Segoe UI","Helvetica Neue","Helvetica","Ari

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\index[3].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	7229
Entropy (8bit):	5.1436024840840835
Encrypted:	false
SSDEEP:	96:k70pR65H9SpAbyOeQDvXIiw69ouwsDlD9RTBMXp1eugmb5S:Lb63eT69olqlD9RTB61eFmbs
MD5:	789FDF5E4E812246D99D3B60008733E5
SHA1:	5CB5A30ED34393BD0DEBE76BE5A29DE200C5827A
SHA-256:	B1CE327D4B8E0F9E3C0D7A717BD98CF8CA6FB59C22D3BF5CE3A1131F8A43CA67
SHA-512:	3854B461782D762F56CC9D25F89DDFC8E6F023846BE5B0B83DD7BEDC7BAC07ACAA45391EF6691042DBA262A7B997FA1D219A58CADEDFA5BE3106760635FB0054
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://widget.trustpilot.com/trustboxes/5406e65db0d04a09e042d5fc/index.html?businessunitId=5654e51c0000ff000585ead7&templateId=5406e65db0d04a09e042d5fc
Preview:	<!DOCTYPE html>.<html id="ng-app">. <head>. <title>Trustpilot Custom Widget</title>. <meta charset="utf-8" />. <meta name="robots" content="noindex" />. <style>.html,body,div,span,applet,object,iframe,h1,h2,h3,h4,h5,h6,p,blockquote,pre,a,abbr,acronym,address,big,cite,code,del,dfn,em,img,ins,kbd,q,s,samp,small,strike ,strong,sub,sup,tt,var,b,u,i,center,dl,dt,dd,ol,ul,li,fieldset,form,label,legend,table,caption,tbody,tfoot,thead,tr,th,td,article,aside,canvas,details,embed,figure,figcaption,foote r,header,hgroup,menu,nav,output,ruby,section,summary,time,mark,audio,video{border:0;font:inherit;font-size:100%;margin:0;padding:0;vertical-align:baseline}artic le,aside,details,figcaption,figure,footer,header,hgroup,menu,nav,section{display:block}body{line-height:1}ol,ul{list-style:none}blockquote,q{quotes:none}blockquote::befor e,blockquote::after,q::before,q::after{content:'';content:none}table{border-collapse:collapse;border-spacing:0}body{font-family:"Segoe UI","Helvetica Neue","Hel

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\jquery[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	92629
Entropy (8bit):	5.303443527492463
Encrypted:	false
SSDEEP:	1536:dnu00HWWaRxkqJg09pYxoxDKMXJrg8hXXO4dK3kyfiLJBhdSZE+I+Qg7rbaN1RUx:ddkWgoBhcZRQgmW42qe
MD5:	397754BA49E9E0CF4E7C190DA78DDA05
SHA1:	AE49E56999D82802727455F0BA83B63ACD90A22B
SHA-256:	C12F6098E641AACA96C60215800F18F5671039AECF812217FAB3C0D152F6ADB4
SHA-512:	8C64754F77507AB2C24A6FC818419B9DD3F0CECCC9065290E41AFDBEE0743F0DA2CB13B2FBB00AFA525C082F1E697CB3FFD76EF9B902CB81D7C41CA1C641DFB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.keepandshare.com/global/lp/js/jquery/1.9.1/jquery.js
Preview:	/*! jQuery v1.9.1 | (c) 2005, 2012 jQuery Foundation, Inc. | jquery.org/license.//@ sourceMappingURL=jquery.min.map.*/(function(e,t){var n,r,i=typeof t,o=e.document,a=e.l ocation,s=e.jQuery,u=e.$,l={},c=[],p="1.9.1",f=c.concat,d=c.push,h=c.slice,g=c.indexOf,m=l.toString,y=l.hasOwnProperty,v=p.trim,b=function(e,t){return new b.fn.init(e,t,r)},x=/[+-]?(?:\d*\.\|)\d+(?:[eE][+-]?\d+\|)/.source,w=/\S+/g,T=/^[\s\uFEFF\xA0]+\|[\s\uFEFF\xA0]+$/g,N=/^(?:(<[\w\W]+>)[^>]*|#([\w-]*))$/,C=/^<(\w+)\s*\/?>(?:<\/\1>\|)$/,k=/^[\],:{}\s]*$/,E=/(?:^|:|,)(?:\s*\[)+/g,S=/\\(?:["\\\/bfnrt]|u[\da-fA-F]{4})/g,A=/"[^"\\\r\n]*"|true|false|null|-?(?:\d+\.|)\d+(?:[eE][+-]?\d+|)/g,j=/^-ms-/,D=/-([\da-z])/gi,L=function(e,t){return t.toUpperCase()},H=function(e){(o.addEventListener||"load"===e.type||"complete"===o.readyState)&&(q(),b.ready())},q=function(){o.addEventListener?(o.removeEventListener("DOMContentLoaded",H,!1),e.removeEventListener("load",H,!1)):(o.detachEvent("onreadystatechange",H),e.detachEvent("onload",H)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\keepandshare_calendar_screenshot_01[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, 1066x710, frames 3
Category:	downloaded
Size (bytes):	102675
Entropy (8bit):	7.939213781995525
Encrypted:	false
SSDEEP:	1536:TGZc7e3ESnZX7OCwnaK8XKXfSZJF4CzQeCttKrGajw1lRom9wrJP44f/dnMUcGQJ:SZc29X7OCwnaKrX6CDeCttAbjGEAmnCz
MD5:	BF335D8CE98EBDC0402D2BABCA2B2004

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\keepandshare_calendar_screenshot_01[1].jpg	
SHA1:	395DCA3C67F14BDD11564B43C18C572FF9DBC390
SHA-256:	3FCBD302B8F5498A4FACBDF51814F63C212F2960BE818888D0F08EF1F7D03FD1
SHA-512:	BBEC88840478EE20F5831C6722590381583C12EE9EBD9D051099651E6A238FD18C6C619CA697B51EA2F735620613AD215A83051B83502034274BB5D7628FB3E2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://keepn.com/graphics/lpgraphics/core_pages/calendar_samples/keepandshare_calendar_screenshot_01.jpg
Preview:	......JFIF.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=========.. .....*.....D.....4G..... FDNN.....+..dxx.b.noco..{...V....py.^.FK.lLz`dzR5. .....AH.3..U.....y.j.....>{..=..={c2C.#...6F.....j.@....c..h.Ah.+..l... *.....f'..... .....3..0.....316.4I...4Xz.....b..n..bD.....<=....@.....,M~U..=o.f....>?.^.f..b...l...b..w.l.._o]....=.".-..m/N?L.9.a^.[Fc!.$H..... .....H.06.RB..>xxu.bJzs.f&.5...x.L}..=.;.....u..{.....N.....Ns.n.....k.K..;..O.c.....M'W?W.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\keepandshare_calendar_screenshot_02[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, 1066x710, frames 3
Category:	downloaded
Size (bytes):	97233
Entropy (8bit):	7.938099729139223
Encrypted:	false
SSDEEP:	1536:iEjhznMnMc3Vm6omqHaGZ+BH+azcyEnFvqTS0hcuuAGK3VA9mNeKvbQZDDDUd5Zn:iTnMc3YvvmBH+KcjFvqzivAGoVA9miDg
MD5:	7390FF7964D6A34B78134CF7A38D85A9
SHA1:	354222FE7702FE17A5B0D46D5616AE2D7E291E28
SHA-256:	F7D63B379A9B694147CD79419C38D18DBD9E2C5632354244AD20014573062D5F
SHA-512:	C27FD32FF5EBFC10C0EDFC05137B494527F81FC74729D6B6F0F9D202F2FBD539368C21273898417964ECFBF0649F441A40989689A9D51E03E332744E782E669C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://keepn.com/graphics/lpgraphics/core_pages/calendar_samples/keepandshare_calendar_screenshot_02.jpg
Preview:	......JFIF.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=========.. .....*.....D.....8F....&7.....V"....k7..}....g...-m.||.....~...X.....:GH..... .....r.@....^~.%...[.=...[.....~'.7...>...!...T.#.....9. ..L.k7..T55...t... *.....`..... .....0.....Ia.f.....7.....?C.....n;$\.....hy.sS.X..W..>....z...I...N...k[!.....c;...Rv...~.].....-c]N....?L..Nl.W.mgQ...$Q..... U#8....I.....N.b.....Y...}...|\...z.=.3.....}=.....?5.....Wg.x~]..R....x...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\keepandshare_calendar_screenshot_03[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, 1066x710, frames 3
Category:	downloaded
Size (bytes):	72397
Entropy (8bit):	7.8952163924582015
Encrypted:	false
SSDEEP:	1536:ccBh4K1/CSZGa6a+ZExLWUfHTN3hbrOSGeP8v4xZyvBlEaQL:f1KSZGa6aAbUfHTJZp8v4byZle
MD5:	DE789842C9A536F57435008E608AC20C
SHA1:	1373A7B9A6CBE6A947AD9CC2988B40151E042958
SHA-256:	A731D138A868C300B12389F26BBECF093C0A2E4A2BB748AD5FA57B9816699FEC
SHA-512:	D2EA1A07DC0578E489DD4B3C9DFE0F3930BEE2DA6E18F82D76F7C7AAAF169BD8BEB4D65FB9E5D7CD33C7938359F319B7FFC2A5C72076AA96C72C032B4D1E6 2E6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://keepn.com/graphics/lpgraphics/core_pages/calendar_samples/keepandshare_calendar_screenshot_03.jpg
Preview:	......JFIF.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=========.. .....*.....D.....8F....&7.....V"....k3.kv:.<...1..]>F.7...<...M....y.:@ .....R....*..y....._....+...M..^.....Ny.:@.....R.....=..P.k1..:.....gD.....QL.sS..... .....sR.0.....nju.di$...!....#..{{_.....d..... .. ...<nju....v.>.Cs.....?N.R..kd6X.h.e..s..;....._..Gw.k....]...q.sc...6..3Z.D.2..... .....g..b.)!T..<0z...<..,\~-.\M,.O.w<wGK.....lxf=n...:.....O9.]oC.|..kG..R..3{.t.z>yk.....z

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\keepandshare_calendar_screenshot_04[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, 1066x710, frames 3
Category:	downloaded
Size (bytes):	96401
Entropy (8bit):	7.934255018544342
Encrypted:	false
SSDEEP:	1536:wFPTrlCgpldTi7qELQqtxjPUVjNhw010qqooLGn8v/XzLL+h1P56eOQ:ZgEmE1/gVPwa08YXPmB557
MD5:	4D3359C959C2840576C4797658AD6E3C
SHA1:	3548B3220F13A424CBD087E8AF4C07FCAFA1A3E2
SHA-256:	9D87B6E8A18E726592100FF86A0C6D8A6C6768B95EB5B984B8CF62B00946945A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\keepandshare_calendar_screenshot_04[1].jpg	
SHA-512:	385F3A5D4168FE388E423D0671C664B5E3D4F94BCE2937F9BDB4D88525FE3764DB0C74D27E7DF050D759C33110E79E5764F44133BD56B0A874B483AE9AC44D7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://keepn.com/graphics/lpgraphics/core_pages/calendar_samples/keepandshare_calendar_screenshot_04.jpg
Preview:	......JFIF.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=========.. .....*.....AjQ.....n.M...w;..... .....:nob.....m{}...lv2hld.W.E..... .....!.nj`.u.y/?.}Gw.....=.zwO].....W.E.....!.nj`.Y....e5..r..ps:.!.,.....Q..sS.....sRi .....Xnj[..i.^9c.d2....gQ.v.....c/....r.....0d..0d.....KrE..^..x;(:.....q.p.[8."e.r.....w..]o.....G..J.+M..zt.3...c...2..... ....)... .t".....'S'.75-....}....i..s.z<U..Xi.Q.1.x..y.y...{./.....s.oC.~U....k.W..;.G..c.-q.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\keepandshare_calendar_screenshot_05[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, 1066x710, frames 3
Category:	downloaded
Size (bytes):	98072
Entropy (8bit):	7.935706332260381
Encrypted:	false
SSDEEP:	1536:O4/oadQqFLl7AcS331d4lEAVmwRO7H/GBcTN23ZtzYCG2TNWwYEF19m:0Zq1wYynw4D/GBQQ3ZVG2TNzYEF19m
MD5:	716E808A3A379FC7DAC8919DA0A13C1B
SHA1:	04702C6C7B33AE8B332DC814D9B4D18435D74FED
SHA-256:	24649193E9349A1E29392410045368FBC5ADCC86F1CE780B8924E1D27D356099
SHA-512:	8F3B76615D2214F88F2B9A6AD904180D8508DBDD5BFD1DDFE7BB78AF6029018550DC74F0F35550F9ED982F65C4EC0420D9A66556A1B04378B60E5035F6E53567
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://keepn.com/graphics/lpgraphics/core_pages/calendar_samples/keepandshare_calendar_screenshot_05.jpg
Preview:	......JFIF.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=========.. .....*.....D.....O.....+*//.....: .s7.y.....G-u.|~G....f....ptI...H..... .....b...e.../....~^...o.?G.~...O.}7...>.X....y.z@.....1.vr@.3}\%CS.....^.....z'.....<...g$..... .....M.....a.....i.n.....o.....?....f}g^7],.....$.. .....~....=~..~?.....I.5.U....{.J.....?.>...z.;x..?.|o.vt3.:...hu.(..... .....e+<`z...)....}y.%..<vrz..E.8....}..>/7./C._#..c.|^..>...9.....S.?5.....+..^....W...w.}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\nHiQo1BypvYzt95zlPq1TvesZW2xOQ-xsNqO47m55DA[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	2010Cabin BoldV
Category:	downloaded
Size (bytes):	66484
Entropy (8bit):	6.0567504437800865
Encrypted:	false
SSDEEP:	1536:D+vxyTbTc5/Pe2AUNELczyEYTfYH6Laq4+GoJ8dlfjbFh1aF:exh5/P/aczyEYTfKif4XoJIFQ
MD5:	D1A2CB0C1D2AAD18D96942A189674EA4
SHA1:	E4B12FDA6D8605F011301109ADEC5A885E022755
SHA-256:	87C66ED7F873B9B9C5E39DB419CF7AEC79FEFB281995887211B3683096D54891
SHA-512:	2E6B5464344C855652BF2710D75665011608CFBCAB9510D1A9405CB196A462654F2CEB11D89EFB64A9F61EF94F3FEEB73BE36F975182D1BA9F2E0E97D2AFD046
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/cabin/v9/nHiQo1BypvYzt95zlPq1TvesZW2xOQ-xsNqO47m55DA.ttf
Preview:	..... GPOSVP.....,..1.GSUB.....28....OS/2l. ...2D...`VDMX...9..2.....cmap..m..>`....cvt .....?....,fpgm.A....?8...agasp.....@.....glyfH.....@.....hdmxO.....h..#xhead.M... .....6hhea.8.r.....$hmtx.~.....<...Lloca..8.....maxp.....0... name.D7....P...xpost*.mV.....prep..o.....,..latn.....kern.....P.....N.j.@.j.p.....<.r. \|.....8.B.\.b.....<.V.\|.....2.h.....h.....$.f.....".P.....4.r.....8.....".`.....@...J.....0...0.6.@.....!.(...+.....1.1. .3.3.!.5.=.".B.H.+.L.M.2.S.U.4.W.\. 7.a.a.=.n.o.>.v.v.@.z.z.A.~.~.B.....C.....E.....F.....I.....K.....M...5...7...8...H...M...U...W...X.....+.....H...U...W...X.....5...7...8...H.....7... ....5...7...8...U...W...X.....7...H.....".."...5...7...9...:...;...=...>...^.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\seg[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43
Entropy (8bit):	3.2226627197680635
Encrypted:	false
SSDEEP:	3:CUMllRPQEsJQEn:Gl3QEsJQEn
MD5:	592EBEFC7104D681D57852665E9AD514
SHA1:	15CDF8DF32AA251DD6DD590A60BF9CF74474E7C5
SHA-256:	4B5B6B15C6255109E06720CCE42A06D3AEAD8B7874423D9C52CB0303212C25EF
SHA-512:	71DB01662075FAC031DEA18B2C766826C77DBAB01400A8642CDC7059394841D5DF9020076554C3BECA6F808187D42E1A1ACC98FAD9A0E1AD32AE869145F5374
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\seg[1].gif	
Preview:	GIF89a.....!.....,.....@..L..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\seg[2].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43
Entropy (8bit):	3.2226627197680635
Encrypted:	false
SSDEEP:	3:CUMllRPQEsJQEn:Gl3QEsJQEn
MD5:	592EBEFC7104D681D57852665E9AD514
SHA1:	15CDF8DF32AA251DD6DD590A60BF9CF74474E7C5
SHA-256:	4B5B6B15C6255109E06720CCE42A06D3AEAD8B7874423D9C52CB0303212C25EF
SHA-512:	71DB01662075FAC031DEA18B2C766826C77DBAB01400A8642CDC7059394841D5DF9020076554C3BECA6F808187D42E1A1ACC98FAD9A0E1AD32AE869145F5374
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....@..L..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\tagjs[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	59
Entropy (8bit):	4.866131719683245
Encrypted:	false
SSDEEP:	3:7LW0wWAbR66lypNOVMWXcZ:7i0wWAQbyjOVZu
MD5:	795F65F2963B2F8E8A0C3AC171B9C193
SHA1:	4F6D9B8AE6641CCD7098A27144CD392330F98B8D
SHA-256:	C7394C66A2FDFC18AA171EB0A30FE53C1617F584B85B449F121877E71DC13B1B
SHA-512:	CA7AE80D8566FBB1EB5CB10BB5DD9062F0E0A4168A556E7B997B94611CD15618794A47E69276D6A9D011CA8A7647F397E2F43DC96CC51A3893A084556A9432D
Malicious:	false
Reputation:	low
Preview:	_pa.setUserMap('pa_CH5wV3NKlEb7diMh9');._pa.looperReady();.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\tp.widget.sync.bootstrap.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines
Category:	downloaded
Size (bytes):	1312
Entropy (8bit):	5.294081621424985
Encrypted:	false
SSDEEP:	24:V6lLh2hP262JkiaOgB4lLv1GFURW3tRWZNtnkRW85VJ4KPtICjddjH3iMZc5j3:V67UPl2a4F1jw9wZTnkw85v48ICjPJiD
MD5:	901928912893C693700FE1B09842B5DD
SHA1:	08773982E60D89A23E354DACB481E6C347946D1E
SHA-256:	BD90495A01D0E283633E1B39FA2E683C85DB34C41D8BD4611D3B222EE8E80CA8
SHA-512:	9BB29868DCF94BCB62CE9D476A8DF8E6444AFF8D9B4D340317845FE403AEE90ABFAF980CC0661AECD8D95F78E311C68D74EACF675B8FE8853AA182439D2365D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://widget.trustpilot.com/bootstrap/v5/tp.widget.sync.bootstrap.min.js
Preview:	.!function i(a,s,l){function d(t,e){if(!s[t]){if(!a[t]){var r="function"==typeof require&&require;if(!e&&r)return r(t,!0);if(u)return u(t,!0);var n=new Error("Cannot find module '" +t+"'");throw n.code="MODULE_NOT_FOUND",n}var o=s[t]={exports:{}};a[t][0].call(o.exports,function(e){return d(a[t][1][e]||e)},o,o.exports,i,a,s,l)}return s[t].exports}for(var u="function"==typeof require&&require,e=0;e<l.length;e++)d(l[e]);return d}({1:[function(e,t,r){"use strict";!function(){function e(){var e=void 0,t=void 0,r=void 0;if(s.getElementsByClassName)e=s.getElementsByClassName("trustpilot-widget");else if(s.querySelectorAll)e=s.querySelectorAll(".trustpilot-widget");else{var n=[],o=new RegExp("(^|)trustpilot-widget(|$)"),i=s.body.getElementsByTagName("*");for(t=0,r=i.length;t<r;t++)o.test(i[t].className)&&n.push(i[t]);e=n}for(t=0;t<e.length;++t)for(var a=e[t];a.firstChild&&"IFRAME"!==a.firstChild.tagName;)a.removeChild(a.firstChild)}var s=document;"loading"!==s.readyState&&e(),s.addEventList

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\tr[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):	44
Entropy (8bit):	2.8317663774021287

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\tr[1].gif	
Encrypted:	false
SSDEEP:	3:CU9yltxlHhn:mn
MD5:	B798F4CE7359FD815DF4BDF76503B295
SHA1:	F8CC6ADDF1707AD236AD9970B0A48F9733D07DA5
SHA-256:	10D8D42D73A02DDB877101E72FBFA15A0EC820224D97CEDEE4CF92D571BE5CAA
SHA-512:	921944DC10FBFB6224D69F0B3AC050F4790310FD1BCAC3B87C96512AD5ED9A268824F3F5180563D372642071B4704C979D209BAF40BC0B1C9A714769ABA7DFC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.facebook.com/tr?id=183487702480957&ev=ViewContent&cd[rtb_id]=14453604&noscript=1
Preview:	GIF89a.....!.....,.....D..;.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\tr[2].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	44
Entropy (8bit):	2.8317663774021287
Encrypted:	false
SSDEEP:	3:CU9yltxlHhn:mn
MD5:	B798F4CE7359FD815DF4BDF76503B295
SHA1:	F8CC6ADDF1707AD236AD9970B0A48F9733D07DA5
SHA-256:	10D8D42D73A02DDB877101E72FBFA15A0EC820224D97CEDEE4CF92D571BE5CAA
SHA-512:	921944DC10FBFB6224D69F0B3AC050F4790310FD1BCAC3B87C96512AD5ED9A268824F3F5180563D372642071B4704C979D209BAF40BC0B1C9A714769ABA7DFC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.facebook.com/tr?id=183487702480957&ev=ViewContent&cd[rtb_id]=10567892&noscript=1
Preview:	GIF89a.....!.....,.....D..;.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\539ad60defb9600b94d7df2c[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	14238
Entropy (8bit):	5.0418085632513385
Encrypted:	false
SSDEEP:	384:haJbBb4SVH7lfdHZba8Jr01R+sohufFIdUacMY93AyWotNkiAIyj:AbZLVH7lfdHZba8Jr01FosNVahY93Ajx
MD5:	FA5561CB0B8DDB211798ADF6302F5D8D
SHA1:	721404362F9D1AF55513C3B54372966FD339746D
SHA-256:	A31B1B4AE132615E426A496C46282028415C7EB3B3626B52C1CE9B273E70A9AE
SHA-512:	92AF40451810CA90168FB81283A5B1C2A7EAD6402F085DB06105F9A1D89419F20825D750D5FAFC81D00C8FEA8098B4A791A0A8BF0DF9FB32B3DF44986BB9454
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://widget.trustpilot.com/trustbox-data/539ad60defb9600b94d7df2c?businessUnitId=5654e51c0000ff000585ead7&locale=en-US&reviewStars=4%2C5&reviewTagValue=favorite&reviewsPerPage=20
Preview:	{"businessUnit":{"stars":4.5,"trustScore":4.7,"displayName":"Keep&Share","numberOfReviews":{"total":1975,"oneStar":10,"twoStars":16,"threeStars":77,"fourStars":314,"fiveStars":1558},"websiteUrl":"https://www.keepandshare.com"},"businessEntity":{"stars":4.5,"trustScore":4.7,"displayName":"Keep&Share","numberOfReviews":{"total":1975,"oneStar":10,"twoStars":16,"threeStars":77,"fourStars":314,"fiveStars":1558},"websiteUrl":"https://www.keepandshare.com"},"reviews":[{"stars":5,"createdAt":"2020-12-17T18:50:21Z","title":"K&S has been great for our sportsmen's.","text":"K&S has been great for our sportsmen's club, especially in these days of COVID craziness.\n\nWe needed a scheduling capability to be in compliance with our Governor's health order. But, we soon found it invaluable for our members to be sure when they arrived at our facility, there would be an open shooting position on one of our many ranges. Before K&S, it was like rolling the dice that there would be an open spot where we w

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\539adbd6dec7e10e686debee[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	10727
Entropy (8bit):	5.11931317371094
Encrypted:	false
SSDEEP:	192:hS5SJB4SJagM2rgi+SWyi3JyLZ5prKDBJYzDqOIFeXjzi/OIh14ZLC:haoB4SJag91+RyccLZ5pKDBJVXeXjW2U
MD5:	382C17E59EC63F9EF7FCD75F654D9933
SHA1:	8979D465D5E0F04747100F8DE8B5D97D8355A531
SHA-256:	940CE521E57944A4A68948AA7B3A44CD15FFA79F1DA0FA3B5F5FC964A3091C7D
SHA-512:	12D29C8B33C863C62312AAB59A1F81B4FD3D17B51C55FD45119F70E48C02780EA7FD08CE966BFFAA9FED707471F22F2A93778CE3FB9548D23514601761555C42

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\539adbd6dec7e10e686debee[1].json	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://widget.trustpilot.com/trustbox-data/539adbd6dec7e10e686debee?businessUnitId=5654e51c0000ff000585ead7&locale=en-US&reviewStars=4%2C5&reviewTagValue=support&reviewsPerPage=20
Preview:	{"businessUnit":{"stars":4.5,"trustScore":4.7,"displayName":"Keep&Share","numberOfReviews":{"total":1975,"oneStar":10,"twoStars":16,"threeStars":77,"fourStars":314,"fiveStars":1558},"websiteUrl":"https://www.keepandshare.com"},"businessEntity":{"stars":4.5,"trustScore":4.7,"displayName":"Keep&Share","numberOfReviews":{"total":1975,"oneStar":10,"twoStars":16,"threeStars":77,"fourStars":314,"fiveStars":1558},"websiteUrl":"https://www.keepandshare.com"},"reviews":[{"stars":5,"createdAt":"2020-12-04T01:50:02Z","title":"Fantastic program","text":"Fantastic program, great customer service.","reviewUrl":"https://www.trustpilot.com/reviews/5fc995ca5e693f07049f3a8b","consumer":{"displayName":"Pacc Director of Operation"},"companyReply":null},{"stars":5,"createdAt":"2020-10-31T18:10:49Z","title":"virtual festival...60 poets.","text":"I am working on a virtual festival....a poetry festival. It includes 60 artist, and about 20 hosts - all connecting up to my computer to record their introduction

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\anchor[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):	13581
Entropy (8bit):	5.955807571275182
Encrypted:	false
SSDEEP:	384:3/SqBe0xRYleQTB9wjS1dOVDiRptFutuoocwDEP:3/Sqvx+wjSaVDipFao0
MD5:	F3146C4EA36B7B020E4C92F9FE5400B9
SHA1:	E55CFA8717DDA6AA098DA49E74C5BDB210E0FF93
SHA-256:	7823CA108304BC7BC032892C42ED7567C2A59D8567AE9D9140F0A95EFA539774
SHA-512:	E4939CAD65D390EA9EA5217D5EF246183A2061C04C3BC9E746ABCCBF135CD9F5AE6ACEC6369B38A9CB1DF78CC37B1A7346771B736B42F05F7C984CC0A9E3555
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML><html dir="ltr" lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.<meta http-equiv="X-UA-Compatible" content="IE=edge">.<style type="text/css">.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxP.ttf) format('truetype');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 500;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc9.ttf) format('truetype');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 900;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmYUtfBBc9.ttf) format('truetype');.}..</style>.<link rel="stylesheet" type="text/css" href="https://www.gstatic.com/recaptcha/releases/6g5J7UfDQ9mLrweZHj04ekSP/styles__ltr.css" nonce="xyOsweFzO1rj9kPpVZwWeQ">.<script nonce="xyOsweFzO1rj9kPpVZwWeQ" type="text/javascript">window['__recaptcha_api'] = 'https://www.google.c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\contact_us[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, LF line terminators
Category:	dropped
Size (bytes):	34733
Entropy (8bit):	5.447580760849073
Encrypted:	false
SSDEEP:	768:A4WPeJwq/0YmgnxT1x1ta0dHCEuVBTkbKVHpWY75Q6KX5PzDmS+OWaPahaXR:AbJq/0YmgxT1xDa0dHCEuVBTkbKVHpWz
MD5:	281A2078EE85F42E581DC69FD82E1A52
SHA1:	2B58759BB3498AF32A271EE81FC6512699B91A11
SHA-256:	F7E2425173884CD4F6AE9674F28013882C2352FCAC153DFF3EA46778F2AC2B4E
SHA-512:	17DFAA92F8E044F922A10578B4CE48497D886C7DB21A2E1F4117AA7CA1CEB75AF174619721DC9EE2E2EBE621F2FC7B350E9C6AB0BEB8596A9BC4D9898FDE9EA3
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>. [if IE 7]> <html class="ie7"> <![endif]-->. [if IE 8]> <html class="ie8"> <![endif]-->. [if IE 9]> <html class="ie9"> <![endif]-->. [if !(IE)]> > <html lang="en"> <![endif]-->. <script>. !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', '1947377292258582');. fbq('track', 'PageView');.</script>.<noscript></noscript> -->..<head>. Using versions.php for latest print dialog javascript and css versions --><meta charset="utf-8">.<meta name="viewport" conte

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\email_image_support_v3[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 221 x 21, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	2635
Entropy (8bit):	7.917293489933644
Encrypted:	false
SSDEEP:	48:sndnkd3LE9it9sKVQDo0J9lHbc2kAXrgcMkb/TPecEFHVaDgQ7g/GKs:snNE3o9iTjd0VHbcdAXr31rTgFdGF
MD5:	BA3D13F4F64FF22383685EAC2FD183F2
SHA1:	EE6C7AE4BA9B16B748119A6F788C2DCAD745E6B2
SHA-256:	361DC73F5E7B41977AD9AD5E1BADC116B243AB6EF785FB22E5E6F89ED85660EE

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\email_image_support_v3[1].png	
SHA-512:	7C5B490705B6AB628CCB8EF60D7D2631966654C18BDF360D811FB779CA6419E4C8564A352B09259DAAECA77918FA164496550FBA0701EA87FCD82DA6AD6D18C A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://keepn.com/graphics/homepage2/email_image_support_v3.png
Preview:	.PNG.....IHDR.....PLTE.....jpZ7?!.....V]E>F*:B%...../8.+4.<E(MT:.....v|ggnWZaI..|OW=3;.....xnt_JR8.....^eMGN3@H,..... y.kdkTBJ/.....DL1HP5.....ahQ.....s.....|.nRZArxd.....&0..)..[.v....IDATx.....$1.Da.r.efffff.._h.Xi.ghQ...If.H....F}..d..v!r=..ff....F].*.m...-..r..1.U..z..v..:l. E.ELG...4V.v.6....| ...e..]~#....+...UB.u.....:..4.Q1.6.K1.K.p...86.|.^.z....7..?.Ok.....#.=....E..`.s.).''..1.....O"E..w..N.y.....G^G.p.Bl 6.w.T...r.w.....TP..@..{.@.A...Pq.y.3E-.7.\p...o..?..O.9.F.Ax .3...D.Ef}..T.v@o../.5V...L.%.#(.T.....jvP"...#...U.s....L.....a23....C...W..rN..~...K./...#.#1.d'.ti..ld*..`.z.l..-.d*H..4.....Z.N..l.(T.:...YB...c..Sa;.y"J.M...9.$3.N.n.>..V8..)....v.P).....{.. ..j..:.....e. 9M...C...n.!J...g.uT.b.j....a..D.Gfp...x..[.j..q.....Am.....2.....=..F..`T5GB.-..H..6.j7z.7..G]..r.."XV[+uho8}...|.>.X.Ks....*Y.:.+q....T.\.Vr.y...O_.V2....u....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\episodes-002.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	9443
Entropy (8bit):	5.386420294775449
Encrypted:	false
SSDEEP:	192:TAGdxIVf6W6E6/L6rkfLLWXvVvdLgIpEgW/J5n:NdxIVFoLCVFLgLgWh5n
MD5:	97CF79BD7D3ADE1CCC3366CA70648489
SHA1:	76DECF0175F52889E5766D8967988C4C8B5DA8E7
SHA-256:	2EAC2A80F2AB8BAE3DECD6F3392D99E96B304E35A4DDA243300658CA9A0FA702
SHA-512:	5252F5CB1EB60D575087887FC9770D14995B7930B35083DD17F804435483D0AD40C9E73F68BF61639A34FD55CCCCA64376720BB79AE3DE3BC76317689EDFEDD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.keepandshare.com/global/javascript/episodes-002.min.js
Preview:	var EPISODES=EPISODES||{};EPISODES.q=EPISODES.q||[];EPISODES.setDefault=function(b,a){if("undefined"==typeof(EPISODES[b])){EPISODES[b]=a}return EPISODES[b]};EPISODES.setDefault("bSendBeacon",0);EPISODES.setDefault("beaconUrl","/images/beacon.gif");EPISODES.setDefault("bResourceTimingAgg",1);EPISODES.setDefault("autorun",1);EPISODES.targetOrigin=document.location.protocol+"//"+document.location.hostname;EPISODES.bPostMessage=("undefined" !=typeof(window.postMessage));EPISODES.version="0.3";EPISODES.init=function(){EPISODES.bDone=!1;EPISODES.marks={};EPISODES.measures={};EPISO DES.starts={};EPISODES.hResourceTiming=undefined;EPISODES.findStartTime();EPISODES.addEventListener("beforeunload",EPISODES.beforeUnload,!1) ;EPISODES.processQ();if("complete"==document.readyState){if("undefined"!=typeof(performance)&&"undefined"!=typeof(performance.timing)&&"undefined"!=typeof(perfo rmance.timing.loadEventEnd)){EPISODES.mark("firstbyte",performance.timing.responseStart);EPISODES.mark("onload",performa

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\f[1].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	43572
Entropy (8bit):	5.510562136634652
Encrypted:	false
SSDEEP:	384:K9nqQQAS4idwk2zCzkuH1Asfb2R2uTLZa2p5hHx0jb85kjU82HhsC1WDAR8j8WpW:hQ9oxp6axU5kI8EUjyQKcAbkj8
MD5:	54C16810EE87E9AFD39E301B9EC91C7B
SHA1:	7CB1BDC6F31FD505B6E488C28EF38A4F0B0098EF
SHA-256:	42CC3140ECABA3FF0E14EC131C74C3556477488F76C063D5292F659A820A02E5
SHA-512:	6BA91A418AD40AC769D596B0F141D27880ECC20A03777EE6FB1CC114E555DCEC100DF67964FAB3A68654B36AA24F7B9C8E28A66AB468D47102E94A2B105778C A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.googleadservices.com/pagead/conversion.js
Preview:	(function(){/* . . Copyright The Closure Library Authors. . SPDX-License-Identifier: Apache-2.0 .*/ .function aa(a){var b=0;return function(){return b<a.length?{done:!1,v alue: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 glob al&&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 t(a,b,c){if(b)a:{var d=a.sp lit(".");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\WJ8I2OL4\f[2].txt	
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):	2313
Entropy (8bit):	5.747969160776892
Encrypted:	false
SSDEEP:	48:0VUUIqzPrqTnJcgVhkGYrl8ONwbSrl8ONw06:+UURWTCgVhkprSmrSN
MD5:	1786530DFBCB5C7C582C919FE6D779DF
SHA1:	C18E4D1F59978B48B670E464543A486C2684ED07

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\f[2].txt	
SHA-256:	1A879B6DA684AAC032B25F55C73A89B3CB2DEE7F55273B2B904FBD61FB152BA6
SHA-512:	0AB0693A7563ED03E1C185F9252A110B0BD3068811BEA1DCCDD8087ECB66B3A0F2C05474D99B90CCA7E401862EF9D52E4450DA2908599EF30994C75AC7F6693
Malicious:	false
Reputation:	low
Preview:	(function(){var s = {};(function(){/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0 */ var c={},f=this||self;var l=/#|$/;function n(d){var g =d.search(l),a;a:{for(a=0;0<=(a=d.indexOf("fmt",a))&&a<g;){var b=d.charCodeAt(a-1);if(38==b||63==b)if(b=d.charCodeAt(a+3),!b||61==b||38==b||35==b)break a;a+=4}a=-1}if(0>a)return null;b=d.indexOf("&",a);if(0>b||b>g)b=g;a+=4;return decodeURIComponent(d.substr(a,b-a).replace(/\+/g," "))};function r(d,g,a){function b(){--p;if(0>=p){var e; (e=d.GooglebQhCsO)||(e={});var q=e[g];q&&(delete e[g],(e=q[0])&&e.call&&e())}}for(var p=a.length+1,m=0;m<a.length;m++){var h=n(a[m]),k=null;1!=h&&2!=h||!(h=d.document.getElementById("goog_conv_iframe"))||h.src||(k=h);k||(k=new Image);k.onload=b;k.src=a[m]}b()}var t=["ss_"],u=s||f;t[0]in u||"undefined"==typeof u.e xecScript||u.execScript("var "+t[0]); for(var v;t.length&&(v=t.shift());)t.length||void 0===r?u[v]&&u[v]!==Object.prototype[v]?u=u[v]:u=u[v]={}:u[v]=r;}).call(this);;s.ss_(window,'

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 3 icons, 16x16, 32 bits/pixel, 32x32, 32 bits/pixel
Category:	downloaded
Size (bytes):	15086
Entropy (8bit):	4.083582584678546
Encrypted:	false
SSDEEP:	96:DFq+j7+4fRKx5JU0/4fme+4+f+Yxsin/CM/afZRuYGza/fAou9WAjLLhzar8ckn9:Rq+yxIO4faJxn6FDGCfARLkrxxxm
MD5:	82E5E07E96E0A870AC967FE12F943182
SHA1:	AC7094A348025B555394350A4B0856A35C6C58B9
SHA-256:	38201057679984F727499876D1E981239624DA6FD362E2AD1ED711D8672450C4
SHA-512:	566C000B96306D4142451262331875DC67A7B2A85E5D6570CA8E52EFDF78E69C8BC96002EDDC2BD70B658730E128041E632900C1318A9E03B64685E19A7D7F34
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.keepandshare.com/favicon.ico
Preview:	..... .h...6... ....00.... ..%..F...(..... ....y.s.y...y...y...y...y...y...y...y...y...y...y...y...y...y.s.y...y...y...y...x...{...~...~...z...x...x...z...{...y...y...y...y...y...y... {...._.G...3...4...J.....V...!.`...Z....|...y...y...y...y...y..p.w.....*.....1.....S..x...y...y...y....".-.....e..... .d.....!...r.u..}...y...y...y...x....8. ...!.....8..x...z..]..... '.....3..x.. .y...y...y...y....!.-.....u.p..y..t.r..... ...,.....i....y...y...y...y...y...y..p.w.....%...V...%.....f.....V.K.....\..y...y...y...y...y...y...{..t.q.&.....2.....$..y...z...y...y...y...y...y...y...y...x...~..9..... .....U....~...y...y...y...y...y...y...y...x..v.n.....+...~.c.D.....i....y...y...y...y...y...y...y...y..Q.....`....w....P.....G....z...y...y...y...y...y...y...y...y..l.}.....4...p.w.E.....g....y...y...y...y ...y...y...y...y...y...~..Z...(... ...'...X.....y...y...y...y...y...y...y

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\fbevents[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	93376
Entropy (8bit):	5.3917536957896575
Encrypted:	false
SSDEEP:	1536:5M+OWt6w6aic9MeoJ2my8LuThe7KFv0a9sIOC1jaMu5Qm2B+QNSMngUSZYSlIUiZ:5OQRj1SVBYDG2
MD5:	1DE516A5B6B1C6033B92EE5F5D50C140
SHA1:	9E37DA5D5D789074D1DADD60977A9575A6332DD5
SHA-256:	9E7EA2B4BA8E2BCC4A964D6192E4671DC5F6863A1C7E35B52B229A3C1E67A68D
SHA-512:	99EF8E73A5D560CB3504B6BF1BC237957687280AFC99FCFF7A4B882FD2AE423B19721D6444FBD63D3ABCCFF8BD0A5CED79899CE02A2116D7710D2A89BEE370 E3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://connect.facebook.net/en_US/fbevents.js
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be.* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\index[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	14783
Entropy (8bit):	5.103575935666359
Encrypted:	false
SSDEEP:	384:xuaJxjpNIAs6kRQeV/DzrNu2Tolq7y8f/xO6:xNWbJt
MD5:	C59716939D5AED2388BF0F9EBB68EFB5
SHA1:	20B1A6862E0F4D82DC69172711A7FA1A5C2A410D
SHA-256:	D7F8AA3896680688E0C2054A74A965098B28EE300FEC36E75B42FC857BE07D04

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\index[1].htm	
SHA-512:	13FB95CC15F0CAFDA778C447F240DE2C6F0C0D69704F9622C3AFA6E456E9F8B75CA399E5ADA720F583625E770E002ABA254EABA22745230937A1436AB081DE8D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://widget.trustpilot.com/trustboxes/539adbd6dec7e10e686debee/index.html?businessunitId=5654e51c0000ff000585ead7&templateId=539adbd6dec7e10e686debee
Preview:	<!DOCTYPE html>.<html>. <head>. <title>Trustpilot Custom Widget</title>. <meta charset="utf-8" />. <meta name="robots" content="noindex" />. <style >.html,body,div,span,applet,object,iframe,h1,h2,h3,h4,h5,h6,p,blockquote,pre,a,abbr,acronym,address,big,cite,code,del,dfn,em,img,ins,kbd,q,s,samp,small,strike,strong,sub,sup,tt,var,b,u,i,center,dl,dt,dd,ol,ul,li,fieldset,form,label,legend,table,caption,tbody,tfoot,thead,tr,th,td,article,aside,canvas,details,embed,figure,figcaption,footer,header,hgroup,menu,nav,output,ruby,section,summary,time,mark,audio,video{border:0;font:inherit;font-size:100%;margin:0;padding:0;vertical-align:baseline}article,aside,details,figcaption,figure,footer,header,hgroup,menu,nav,section{display:block}body{line-height:1}ol,ul{list-style:none}blockquote,q{quotes:none}blockquote::before,blockquote::after,q::before,q::after{content:'';content:none}table{border-collapse:collapse;border-spacing:0}body{font-family:"Segoe UI","Helvetica Neue","Helvetica","Ari

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\keepandshare_calendar_screenshot_01[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	162
Entropy (8bit):	4.43530643106624
Encrypted:	false
SSDEEP:	3:qVoB3tUROGclXqyvXboAcMBXqWSZUXqXllVLLP61IwcWWGu:q43tISl6kXiMIWSU6Xll5LP8IpfGu
MD5:	4F8E702CC244EC5D4DE32740C0ECBD97
SHA1:	3ADB1F02D5B6054DE0046E367C1D687B6CDF7AFF
SHA-256:	9E17CB15DD75BBBD5DBB984EDA674863C3B10AB72613CF8A39A00C3E11A8492A
SHA-512:	21047FEA5269FEE75A2A187AA09316519E35068CB2F2F76CFAF371E5224445E9D5C98497BD76FB9608D2B73E9DAC1A3F5BFADFDC4623C479D53ECF93D81D3CF
Malicious:	false
Reputation:	low
Preview:	<html>..<head><title>301 Moved Permanently</title></head>..<body>.. 301 Moved Permanently ..<hr> nginx ..</body>..</html>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\keepandshare_calendar_screenshot_02[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	162
Entropy (8bit):	4.43530643106624
Encrypted:	false
SSDEEP:	3:qVoB3tUROGclXqyvXboAcMBXqWSZUXqXllVLLP61IwcWWGu:q43tISl6kXiMIWSU6Xll5LP8IpfGu
MD5:	4F8E702CC244EC5D4DE32740C0ECBD97
SHA1:	3ADB1F02D5B6054DE0046E367C1D687B6CDF7AFF
SHA-256:	9E17CB15DD75BBBD5DBB984EDA674863C3B10AB72613CF8A39A00C3E11A8492A
SHA-512:	21047FEA5269FEE75A2A187AA09316519E35068CB2F2F76CFAF371E5224445E9D5C98497BD76FB9608D2B73E9DAC1A3F5BFADFDC4623C479D53ECF93D81D3CF
Malicious:	false
Reputation:	low
Preview:	<html>..<head><title>301 Moved Permanently</title></head>..<body>.. 301 Moved Permanently ..<hr> nginx ..</body>..</html>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\keepandshare_calendar_screenshot_03[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	162
Entropy (8bit):	4.43530643106624
Encrypted:	false
SSDEEP:	3:qVoB3tUROGclXqyvXboAcMBXqWSZUXqXllVLLP61IwcWWGu:q43tISl6kXiMIWSU6Xll5LP8IpfGu
MD5:	4F8E702CC244EC5D4DE32740C0ECBD97
SHA1:	3ADB1F02D5B6054DE0046E367C1D687B6CDF7AFF
SHA-256:	9E17CB15DD75BBBD5DBB984EDA674863C3B10AB72613CF8A39A00C3E11A8492A
SHA-512:	21047FEA5269FEE75A2A187AA09316519E35068CB2F2F76CFAF371E5224445E9D5C98497BD76FB9608D2B73E9DAC1A3F5BFADFDC4623C479D53ECF93D81D3CF
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\keepandshare_calendar_screenshot_03[1].htm	
Preview:	<html>..<head><title>301 Moved Permanently</title></head>..<body>.. 301 Moved Permanently ..<hr> nginx ..</body>..</html>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\keepandshare_calendar_screenshot_04[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	162
Entropy (8bit):	4.43530643106624
Encrypted:	false
SSDEEP:	3:qVoB3tUROGclXqyvXboAcMBXqWSZUXqXIlVLLP61IwcWWGu:q43tISl6kXiMIWSU6XlI5LP8IpfGu
MD5:	4F8E702CC244EC5D4DE32740C0ECBD97
SHA1:	3ADB1F02D5B6054DE0046E367C1D687B6CDF7AFF
SHA-256:	9E17CB15DD75BBBD5DBB984EDA674863C3B10AB72613CF8A39A00C3E11A8492A
SHA-512:	21047FEA5269FEE75A2A187AA09316519E35068CB2F2F76CFAF371E5224445E9D5C98497BD76FB9608D2B73E9DAC1A3F5BFADFDC4623C479D53ECF93D81D3C F
Malicious:	false
Reputation:	low
Preview:	<html>..<head><title>301 Moved Permanently</title></head>..<body>.. 301 Moved Permanently ..<hr> nginx ..</body>..</html>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\keepandshare_calendar_screenshot_05[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	162
Entropy (8bit):	4.43530643106624
Encrypted:	false
SSDEEP:	3:qVoB3tUROGclXqyvXboAcMBXqWSZUXqXIlVLLP61IwcWWGu:q43tISl6kXiMIWSU6XlI5LP8IpfGu
MD5:	4F8E702CC244EC5D4DE32740C0ECBD97
SHA1:	3ADB1F02D5B6054DE0046E367C1D687B6CDF7AFF
SHA-256:	9E17CB15DD75BBBD5DBB984EDA674863C3B10AB72613CF8A39A00C3E11A8492A
SHA-512:	21047FEA5269FEE75A2A187AA09316519E35068CB2F2F76CFAF371E5224445E9D5C98497BD76FB9608D2B73E9DAC1A3F5BFADFDC4623C479D53ECF93D81D3C F
Malicious:	false
Reputation:	low
Preview:	<html>..<head><title>301 Moved Permanently</title></head>..<body>.. 301 Moved Permanently ..<hr> nginx ..</body>..</html>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\master_external-20180124_1031.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	231703
Entropy (8bit):	5.242083346744755
Encrypted:	false
SSDEEP:	1536:DwdYqeIuDHlqmm68lv/6gPSW+gM+oICkiBwQL/mt1H9cMvzCCJHubIyC:j9qqW+5+pCkiBwQbmq+Ci
MD5:	B20FF516B9810F6E7CA8EFA5A3235F3B
SHA1:	1E26F09610D6BB740FB4DE9B7961810264BFC420
SHA-256:	10005B2C7735A68A86F165BF726EBBB3C3985AFBF52571FFC3083FE0158AB14E
SHA-512:	1FC0B47B75E03FDDA64F38A18329C7DC8055C247D17E69EB372B427E6BFBF397BC61DC3DC27682364964FB25BCCEACAD69F710D5F0B70E23B4987232DC029E 4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.keepandshare.com/global/styles/css_source/master_external/master_external-20180124_1031.min.css
Preview:	@charset "UTF-8";/*!. * Bootstrap v3.3.7 (http://getbootstrap.com). * Copyright 2011-2016 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). *//*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css */html{-webkit-text-size-adjust:100%;-ms-text-size-adjust:100%}body{margin:0}article,aside,details,figcaption,figure,footer,header,hgroup,main,menu,nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-align:baseline}audio:not([controls]){display:none;height:0}[hidden],template{display:none}a{background-color:transparent}a:active,a:hover{outline:0}b,strong{font-weight:700}dfn{font-style:italic}mark{color:#000;background:#ff0}sub,sup{position:relative;font-size:75%;line-height:0;vertical-align:baseline}sup{top:-.5em}sub{bottom:-.25em}img{border:0}svg:not(:root){overflow:hidden}hr{height:0;-moz-box-sizing:content-box;box-sizing:content-box}pre{overflow:auto}code,kbd,pre,samp{font-size:1em}button,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\matchMedia[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\matchMedia[1].js	
Category:	downloaded
Size (bytes):	1700
Entropy (8bit):	4.454507965784852
Encrypted:	false
SSDEEP:	24:t8EPD32/c9bpGD3uOuaRWUnNoeiMghSdF1xcxxwqfVlaW5VNf16/7CLTrr8:tR2/cDGDbwUnxF1OvlVN1qeL/r8
MD5:	89F369588D629240D6A8D4F8788490C8
SHA1:	FB014487044FE7F608FA3E19E868ED5F9C41AA00
SHA-256:	76B8C213B84808D8F2986BFA38E79E3F2D1A94F065E517A143999B198ABD8BD6
SHA-512:	3B56E247349C10375E3BCA06B1471EDE80AF199F9148D88A4B2CD488A8A25BF70773C998C5A744562F01DCC27EC116483B38816D345A06B81233834DD5798D30
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.keepandshare.com/global/lp/js/matchMedia/0.1.1/matchMedia.js
Preview:	/*! matchMedia() polyfill - Test a CSS media type/query in JS. Authors & copyright (c) 2012: Scott Jehl, Paul Irish, Nicholas Zakas, David Knight. Dual MIT/BSD license */ ..window.matchMedia || (window.matchMedia = function() {. "use strict";.. // For browsers that support matchMedium api such as IE 9 and webkit. var styleMedia = (window.styleMedia || window.media);.. // For those that don't support matchMedium. if (!styleMedia) {. var style = document.createElement('style'),. script = document.getElementsByTagName('script')[0],. info = null;.. style.type = 'text/css';. style.id = 'matchmediajs-test';.. script.parent Node.insertBefore(style, script);.. // 'style.currentStyle' is used by IE <= 8 and 'window.getComputedStyle' for all other browsers. info = ('getComputedStyle' in win dow) && window.getComputedStyle(style, null) || style.currentStyle;.. styleMedia = {. matchM

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\registration[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	32455
Entropy (8bit):	5.583199188196404
Encrypted:	false
SSDEEP:	768:gvx3M5wQzukS0rs2eb84TjrvPj0YmgsVCLgfUouBhkybmhoB5Zz6gzDmSLjaPah/:gIUDPj0Ymg7LgfUouBooB51RzKSLjaPw
MD5:	2C95B918DFC0ABCDA3389114E962C3D1
SHA1:	6843FF9DAF75F2F0E70419935D1B985A1AD6AD4B
SHA-256:	A5DB4BD2215E8D1423CE9223B98157EB28ED1B677B3663ABA13156FDBC1615C6
SHA-512:	62BB178C9A02FB02904E4A20C46DC57F8BF95EAD8D833B5EBEF0AC802F4C868BC4F584A9BC5BB9DD4F8A27A860EBCF18A175C0AE09013E0F1BF07028C2F380 46
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.keepandshare.com/business/registration.php?form=free_trial&ifr=y&lp=
Preview:	<!DOCTYPE html>. [if IE 7]> <html class="ie7"> <![endif]-->. [if IE 8]> <html class="ie8"> <![endif]-->. [if IE 9]> <html class="ie9"> <![endif]-->. [if !(IE)]> > <html lang="en"> <![endif]--><head>.. Using versions.php for latest print dialog javascript and css versions --> <script>. !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.createEl ement(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_U S/fbevents.js');. fbq('init', '1947377292258582');. fbq('track', 'PageView');.</script><noscript></noscript> -->..<meta charset="utf-8">.<meta name="viewport" cont

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\tr[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	44
Entropy (8bit):	2.8317663774021287
Encrypted:	false
SSDEEP:	3:CU9yltxlHhn:mn
MD5:	B798F4CE7359FD815DF4BDF76503B295
SHA1:	F8CC6ADDF1707AD236AD9970B0A48F9733D07DA5
SHA-256:	10D8D42D73A02DDB877101E72FBFA15A0EC820224D97CEDEE4CF92D571BE5CAA
SHA-512:	921944DC10FBFB6224D69F0B3AC050F4790310FD1BCAC3B87C96512AD5ED9A268824F3F5180563D372642071B4704C979D209BAF40BC0B1C9A714769ABA7DFC
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D..;.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\tr[2].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	44
Entropy (8bit):	2.8317663774021287
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\tr[2].gif	
SSDEEP:	3:CU9yltxlHhn:mn
MD5:	B798F4CE7359FD815DF4BDF76503B295
SHA1:	F8CC6ADDF1707AD236AD9970B0A48F9733D07DA5
SHA-256:	10D8D42D73A02DDB877101E72FBFA15A0EC820224D97CEDEE4CF92D571BE5CAA
SHA-512:	921944DC10FBFB6224D69F0B3AC050F4790310FD1BCAC3B87C96512AD5ED9A268824F3F5180563D372642071B4704C979D209BAF40BC0B1C9A714769ABA7DFC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.facebook.com/tr?id=183487702480957&ev=ViewContent&cd[rtb_id]=17289136&noscript=1
Preview:	GIF89a............!.......,...........D..;.

C:\Users\user\AppData\Local\Temp\~DF5715D24817D4D378.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFC1456364037F95DB.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4790728101883442
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lojF9lop9lWEIjjoPedKF:kBqoIysE0joPJ
MD5:	42DDFCA2E5EFEEC92FABE513C70E6F79
SHA1:	B7B950E0FE909140E2E52F3F98B37487E56A77ED
SHA-256:	804500B19107DC2B7F4EE700BAE7D4F693747C6DE0022ABE02999B7D807E881F
SHA-512:	9B559F931BA7BCB73785BF71B949CFFDCB3E5087B9C717023A1D43CEE122F8A8478FD071540A24C296159B5702E101A014812160A6AFCDD1802F29A3DD608B1
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFF9C80A2350DB77A3.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	66554
Entropy (8bit):	1.6156295292450555
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+yU+XkfAZDFPhYryNkFPhYXdNkFPhYtyLe7h751ojsoKY+KF2ofNmY:e/oK8FfVf
MD5:	61033240299A434ECC87FB6D331A51AF
SHA1:	636C8ACF12ECFF915CC58241D1AFD9919D67F9BD
SHA-256:	19663C218F179BDC7A25E180920531858420E7ECC42983B716EA4499EF60BE5D
SHA-512:	D421BB4BFA815F427FF5CE2A2B4F4DBA8AA68AAC0782226111072053440FAFA50748E1516258AE1B3A405D0D7C438D53BA367EFF36403CDAF9AC135BC5B6AF 6
Malicious:	false
Reputation:	low

Copyright Joe Security LLC 2021

C:\Users\user\AppData\Local\Temp\~DFF9C80A2350DB77A3.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 25, 2021 03:16:53.329314947 CET	49712	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:53.330090046 CET	49713	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:53.486294985 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:53.486519098 CET	49712	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:53.487657070 CET	443	49713	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:53.487878084 CET	49713	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:53.493124962 CET	49712	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:53.493849039 CET	49713	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:53.650080919 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:53.651381016 CET	443	49713	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:53.651650906 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:53.651679993 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:53.651777983 CET	49712	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:53.651787996 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:53.651815891 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:53.651834011 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:53.651937008 CET	49712	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:53.653182983 CET	443	49713	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:53.653218031 CET	443	49713	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:53.653237104 CET	443	49713	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:53.653259993 CET	443	49713	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:53.653278112 CET	443	49713	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:53.653326035 CET	49713	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:53.653394938 CET	49713	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:53.692554951 CET	49712	443	192.168.2.3	64.71.144.43

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 25, 2021 03:16:53.692800045 CET	49713	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:53.698540926 CET	49712	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:53.698692083 CET	49712	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:53.698796988 CET	49713	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:53.849685907 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:53.849844933 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:53.849843025 CET	49712	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:53.849941015 CET	49712	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:53.850598097 CET	443	49713	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:53.850615978 CET	443	49713	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:53.850804090 CET	49713	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:53.853049994 CET	49713	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:53.853337049 CET	49712	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:53.855431080 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:53.855531931 CET	49712	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:53.856034040 CET	443	49713	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:53.856230974 CET	49713	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:53.881835938 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:53.881860971 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:53.881947041 CET	49712	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:53.881983995 CET	49712	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:53.957412958 CET	49712	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:53.985573053 CET	49714	443	192.168.2.3	66.160.183.118
Mar 25, 2021 03:16:53.985748053 CET	49715	443	192.168.2.3	66.160.183.118
Mar 25, 2021 03:16:54.049607038 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:54.050385952 CET	443	49713	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:54.114252090 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:54.116765976 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:54.116794109 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:54.116833925 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:54.116903067 CET	49712	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:54.116931915 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:54.116966963 CET	49712	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:54.116986036 CET	49712	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:54.117043972 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:54.117089033 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:54.117110014 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:54.117124081 CET	49712	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:54.117134094 CET	49712	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:54.117157936 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:54.117183924 CET	49712	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:54.117187977 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:54.117212057 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:54.117223024 CET	49712	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:54.117242098 CET	49712	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:54.117273092 CET	49712	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:54.142678022 CET	443	49715	66.160.183.118	192.168.2.3
Mar 25, 2021 03:16:54.142831087 CET	49715	443	192.168.2.3	66.160.183.118
Mar 25, 2021 03:16:54.143088102 CET	443	49714	66.160.183.118	192.168.2.3
Mar 25, 2021 03:16:54.143176079 CET	49714	443	192.168.2.3	66.160.183.118
Mar 25, 2021 03:16:54.143532991 CET	49715	443	192.168.2.3	66.160.183.118
Mar 25, 2021 03:16:54.143779993 CET	49714	443	192.168.2.3	66.160.183.118
Mar 25, 2021 03:16:54.273829937 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:54.273859024 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:54.273874998 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:54.273891926 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:54.273979902 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:54.274028063 CET	49712	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:54.274055958 CET	49712	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:54.274061918 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:54.274127007 CET	49712	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:54.274147034 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:54.274166107 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:54.274194956 CET	443	49712	64.71.144.43	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 25, 2021 03:16:54.274225950 CET	49712	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:54.274246931 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:54.274279118 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:54.274287939 CET	49712	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:54.274308920 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:54.274341106 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:54.274360895 CET	49712	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:54.274370909 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:54.274431944 CET	49712	443	192.168.2.3	64.71.144.43
Mar 25, 2021 03:16:54.274502993 CET	443	49712	64.71.144.43	192.168.2.3
Mar 25, 2021 03:16:54.274561882 CET	49712	443	192.168.2.3	64.71.144.43

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 25, 2021 03:16:44.535176992 CET	49199	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:16:44.548686981 CET	53	49199	8.8.8.8	192.168.2.3
Mar 25, 2021 03:16:45.556579113 CET	50620	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:16:45.569494009 CET	53	50620	8.8.8.8	192.168.2.3
Mar 25, 2021 03:16:46.594026089 CET	64938	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:16:46.607969999 CET	53	64938	8.8.8.8	192.168.2.3
Mar 25, 2021 03:16:47.702744007 CET	60152	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:16:47.716375113 CET	53	60152	8.8.8.8	192.168.2.3
Mar 25, 2021 03:16:48.848664999 CET	57544	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:16:48.861437082 CET	53	57544	8.8.8.8	192.168.2.3
Mar 25, 2021 03:16:49.969837904 CET	55984	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:16:49.984724045 CET	53	55984	8.8.8.8	192.168.2.3
Mar 25, 2021 03:16:50.820538044 CET	64185	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:16:50.833429098 CET	53	64185	8.8.8.8	192.168.2.3
Mar 25, 2021 03:16:51.975080013 CET	65110	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:16:51.993746996 CET	53	65110	8.8.8.8	192.168.2.3
Mar 25, 2021 03:16:52.172629118 CET	58361	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:16:52.185590982 CET	53	58361	8.8.8.8	192.168.2.3
Mar 25, 2021 03:16:53.145847082 CET	63492	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:16:53.264954090 CET	60831	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:16:53.277508020 CET	53	60831	8.8.8.8	192.168.2.3
Mar 25, 2021 03:16:53.313164949 CET	53	63492	8.8.8.8	192.168.2.3
Mar 25, 2021 03:16:53.968075037 CET	60100	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:16:53.980803967 CET	53	60100	8.8.8.8	192.168.2.3
Mar 25, 2021 03:16:54.246400118 CET	53195	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:16:54.258465052 CET	53	53195	8.8.8.8	192.168.2.3
Mar 25, 2021 03:16:56.130847931 CET	50141	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:16:56.144581079 CET	53	50141	8.8.8.8	192.168.2.3
Mar 25, 2021 03:16:57.203264952 CET	53023	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:16:57.216746092 CET	53	53023	8.8.8.8	192.168.2.3
Mar 25, 2021 03:16:58.122052908 CET	49563	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:16:58.135812998 CET	53	49563	8.8.8.8	192.168.2.3
Mar 25, 2021 03:16:59.121746063 CET	51352	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:16:59.135111094 CET	53	51352	8.8.8.8	192.168.2.3
Mar 25, 2021 03:16:59.924146891 CET	59349	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:16:59.936484098 CET	53	59349	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:01.755186081 CET	57084	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:01.767719984 CET	53	57084	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:02.935121059 CET	58823	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:02.947664022 CET	53	58823	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:03.775746107 CET	57568	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:03.788427114 CET	53	57568	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:09.722585917 CET	50540	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:09.738770962 CET	53	50540	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:12.526767015 CET	54366	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:12.546153069 CET	53	54366	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:13.183017969 CET	53034	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:13.209711075 CET	53	53034	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:13.211374044 CET	57762	53	192.168.2.3	8.8.8.8

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 25, 2021 03:17:13.226785898 CET	55435	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:13.237700939 CET	53	57762	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:13.402308941 CET	53	55435	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:13.424550056 CET	50713	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:13.450732946 CET	53	50713	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:13.618856907 CET	56132	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:13.629653931 CET	58987	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:13.638636112 CET	56579	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:13.639447927 CET	60633	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:13.645164013 CET	53	56132	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:13.651350975 CET	53	56579	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:13.652708054 CET	53	60633	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:13.656167984 CET	53	58987	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:13.787580013 CET	61292	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:13.794735909 CET	63619	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:13.800180912 CET	53	61292	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:13.808903933 CET	64938	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:13.823306084 CET	53	64938	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:13.834381104 CET	53	63619	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:13.863502026 CET	61946	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:13.890275002 CET	53	61946	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:14.122369051 CET	64910	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:14.126338959 CET	52123	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:14.136737108 CET	56130	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:14.140891075 CET	53	64910	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:14.140913963 CET	53	52123	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:14.167690039 CET	53	56130	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:14.556807041 CET	56338	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:14.558083057 CET	59420	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:14.569572926 CET	53	56338	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:14.570498943 CET	53	59420	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:14.587095976 CET	58784	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:14.592186928 CET	63978	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:14.599839926 CET	53	58784	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:14.604820967 CET	53	63978	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:14.623733997 CET	62938	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:14.657458067 CET	55708	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:14.664968967 CET	53	62938	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:14.670128107 CET	53	55708	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:14.707803011 CET	56803	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:14.750617027 CET	53	56803	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:21.974123001 CET	57145	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:21.987049103 CET	53	57145	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:22.778944969 CET	55359	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:22.790939093 CET	53	55359	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:22.986452103 CET	57145	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:23.000439882 CET	53	57145	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:23.049488068 CET	58306	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:23.083939075 CET	53	58306	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:23.765853882 CET	55359	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:23.779254913 CET	53	55359	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:23.985718966 CET	57145	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:23.998723030 CET	53	57145	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:24.781056881 CET	55359	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:24.794019938 CET	53	55359	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:26.000236988 CET	57145	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:26.015284061 CET	53	57145	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:26.125166893 CET	64124	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:26.138593912 CET	53	64124	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:26.796806097 CET	55359	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:26.809045076 CET	53	55359	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:30.018121958 CET	57145	53	192.168.2.3	8.8.8.8
Mar 25, 2021 03:17:30.031913996 CET	53	57145	8.8.8.8	192.168.2.3
Mar 25, 2021 03:17:30.812839985 CET	55359	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 25, 2021 03:17:30.826194048 CET	53	55359	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 25, 2021 03:16:53.145847082 CET	192.168.2.3	8.8.8.8	0x3675	Standard query (0)	www.keepandshare.com	A (IP address)	IN (0x0001)
Mar 25, 2021 03:16:53.968075037 CET	192.168.2.3	8.8.8.8	0x3c9e	Standard query (0)	keepn.com	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:09.722585917 CET	192.168.2.3	8.8.8.8	0xeb4e	Standard query (0)	www.keepandshare.com	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:12.526767015 CET	192.168.2.3	8.8.8.8	0x1526	Standard query (0)	widget.trustpilot.com	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:13.226785898 CET	192.168.2.3	8.8.8.8	0x80c7	Standard query (0)	www.keepn.com	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:13.618856907 CET	192.168.2.3	8.8.8.8	0x66d5	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:13.629653931 CET	192.168.2.3	8.8.8.8	0xaa8a	Standard query (0)	bid.g.doubleclick.net	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:13.638636112 CET	192.168.2.3	8.8.8.8	0xb06d	Standard query (0)	tag.marinsm.com	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:13.794735909 CET	192.168.2.3	8.8.8.8	0xe067	Standard query (0)	www.google.ch	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:13.808903933 CET	192.168.2.3	8.8.8.8	0x3502	Standard query (0)	cdn.mouseflow.com	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:13.863502026 CET	192.168.2.3	8.8.8.8	0x6630	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:14.122369051 CET	192.168.2.3	8.8.8.8	0x998b	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:14.126338959 CET	192.168.2.3	8.8.8.8	0xf1cb	Standard query (0)	pixel-geo.prfct.co	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:14.556807041 CET	192.168.2.3	8.8.8.8	0x8b45	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:14.558083057 CET	192.168.2.3	8.8.8.8	0x73af	Standard query (0)	secure.adnxs.com	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:14.587095976 CET	192.168.2.3	8.8.8.8	0x1700	Standard query (0)	ads.yahoo.com	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:14.592186928 CET	192.168.2.3	8.8.8.8	0xdcf5	Standard query (0)	us-u.openx.net	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:14.623733997 CET	192.168.2.3	8.8.8.8	0xbb	Standard query (0)	pixel.rubiconproject.com	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:14.657458067 CET	192.168.2.3	8.8.8.8	0x1483	Standard query (0)	analytics.twitter.com	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:14.707803011 CET	192.168.2.3	8.8.8.8	0x407c	Standard query (0)	cm.g.doubleclick.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 25, 2021 03:16:53.313164949 CET	8.8.8.8	192.168.2.3	0x3675	No error (0)	www.keepandshare.com		64.71.144.43	A (IP address)	IN (0x0001)
Mar 25, 2021 03:16:53.313164949 CET	8.8.8.8	192.168.2.3	0x3675	No error (0)	www.keepandshare.com		64.62.174.126	A (IP address)	IN (0x0001)
Mar 25, 2021 03:16:53.313164949 CET	8.8.8.8	192.168.2.3	0x3675	No error (0)	www.keepandshare.com		66.160.183.121	A (IP address)	IN (0x0001)
Mar 25, 2021 03:16:53.313164949 CET	8.8.8.8	192.168.2.3	0x3675	No error (0)	www.keepandshare.com		64.62.174.128	A (IP address)	IN (0x0001)
Mar 25, 2021 03:16:53.313164949 CET	8.8.8.8	192.168.2.3	0x3675	No error (0)	www.keepandshare.com		66.160.183.123	A (IP address)	IN (0x0001)
Mar 25, 2021 03:16:53.313164949 CET	8.8.8.8	192.168.2.3	0x3675	No error (0)	www.keepandshare.com		66.160.183.135	A (IP address)	IN (0x0001)
Mar 25, 2021 03:16:53.313164949 CET	8.8.8.8	192.168.2.3	0x3675	No error (0)	www.keepandshare.com		64.71.144.72	A (IP address)	IN (0x0001)
Mar 25, 2021 03:16:53.313164949 CET	8.8.8.8	192.168.2.3	0x3675	No error (0)	www.keepandshare.com		66.160.183.118	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 25, 2021 03:16:53.980803967 CET	8.8.8.8	192.168.2.3	0x3c9e	No error (0)	keepn.com		66.160.183.118	A (IP address)	IN (0x0001)
Mar 25, 2021 03:16:53.980803967 CET	8.8.8.8	192.168.2.3	0x3c9e	No error (0)	keepn.com		66.160.183.123	A (IP address)	IN (0x0001)
Mar 25, 2021 03:16:53.980803967 CET	8.8.8.8	192.168.2.3	0x3c9e	No error (0)	keepn.com		64.62.174.126	A (IP address)	IN (0x0001)
Mar 25, 2021 03:16:53.980803967 CET	8.8.8.8	192.168.2.3	0x3c9e	No error (0)	keepn.com		64.62.174.128	A (IP address)	IN (0x0001)
Mar 25, 2021 03:16:53.980803967 CET	8.8.8.8	192.168.2.3	0x3c9e	No error (0)	keepn.com		66.160.183.121	A (IP address)	IN (0x0001)
Mar 25, 2021 03:16:53.980803967 CET	8.8.8.8	192.168.2.3	0x3c9e	No error (0)	keepn.com		64.71.144.72	A (IP address)	IN (0x0001)
Mar 25, 2021 03:16:53.980803967 CET	8.8.8.8	192.168.2.3	0x3c9e	No error (0)	keepn.com		64.71.144.43	A (IP address)	IN (0x0001)
Mar 25, 2021 03:16:53.980803967 CET	8.8.8.8	192.168.2.3	0x3c9e	No error (0)	keepn.com		66.160.183.135	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:09.738770962 CET	8.8.8.8	192.168.2.3	0xeb4e	No error (0)	www.keepandshare.com		64.62.174.126	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:09.738770962 CET	8.8.8.8	192.168.2.3	0xeb4e	No error (0)	www.keepandshare.com		66.160.183.135	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:09.738770962 CET	8.8.8.8	192.168.2.3	0xeb4e	No error (0)	www.keepandshare.com		64.71.144.43	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:09.738770962 CET	8.8.8.8	192.168.2.3	0xeb4e	No error (0)	www.keepandshare.com		66.160.183.123	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:09.738770962 CET	8.8.8.8	192.168.2.3	0xeb4e	No error (0)	www.keepandshare.com		66.160.183.118	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:09.738770962 CET	8.8.8.8	192.168.2.3	0xeb4e	No error (0)	www.keepandshare.com		64.62.174.128	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:09.738770962 CET	8.8.8.8	192.168.2.3	0xeb4e	No error (0)	www.keepandshare.com		64.71.144.72	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:09.738770962 CET	8.8.8.8	192.168.2.3	0xeb4e	No error (0)	www.keepandshare.com		66.160.183.121	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:12.546153069 CET	8.8.8.8	192.168.2.3	0x1526	No error (0)	widget.trustpilot.com		52.84.138.122	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:12.546153069 CET	8.8.8.8	192.168.2.3	0x1526	No error (0)	widget.trustpilot.com		52.84.138.36	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:12.546153069 CET	8.8.8.8	192.168.2.3	0x1526	No error (0)	widget.trustpilot.com		52.84.138.40	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:12.546153069 CET	8.8.8.8	192.168.2.3	0x1526	No error (0)	widget.trustpilot.com		52.84.138.46	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:13.402308941 CET	8.8.8.8	192.168.2.3	0x80c7	No error (0)	www.keepn.com		64.62.174.128	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:13.402308941 CET	8.8.8.8	192.168.2.3	0x80c7	No error (0)	www.keepn.com		64.71.144.72	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:13.402308941 CET	8.8.8.8	192.168.2.3	0x80c7	No error (0)	www.keepn.com		66.160.183.123	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:13.402308941 CET	8.8.8.8	192.168.2.3	0x80c7	No error (0)	www.keepn.com		64.71.144.43	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:13.402308941 CET	8.8.8.8	192.168.2.3	0x80c7	No error (0)	www.keepn.com		64.62.174.126	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:13.402308941 CET	8.8.8.8	192.168.2.3	0x80c7	No error (0)	www.keepn.com		66.160.183.135	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 25, 2021 03:17:13.402308941 CET	8.8.8.8	192.168.2.3	0x80c7	No error (0)	www.keepn.com		66.160.183.118	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:13.402308941 CET	8.8.8.8	192.168.2.3	0x80c7	No error (0)	www.keepn.com		66.160.183.121	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:13.645164013 CET	8.8.8.8	192.168.2.3	0x66d5	No error (0)	googleads.g.doubleclick.net		172.217.168.34	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:13.651350975 CET	8.8.8.8	192.168.2.3	0xb06d	No error (0)	tag.marinsm.com	g.global-ssl.fastly.net		CNAME (Canonical name)	IN (0x0001)
Mar 25, 2021 03:17:13.651350975 CET	8.8.8.8	192.168.2.3	0xb06d	No error (0)	g.global-ssl.fastly.net		151.101.0.65	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:13.651350975 CET	8.8.8.8	192.168.2.3	0xb06d	No error (0)	g.global-ssl.fastly.net		151.101.64.65	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:13.651350975 CET	8.8.8.8	192.168.2.3	0xb06d	No error (0)	g.global-ssl.fastly.net		151.101.128.65	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:13.651350975 CET	8.8.8.8	192.168.2.3	0xb06d	No error (0)	g.global-ssl.fastly.net		151.101.192.65	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:13.656167984 CET	8.8.8.8	192.168.2.3	0xaa8a	No error (0)	bid.g.doubleclick.net	ads-bid.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Mar 25, 2021 03:17:13.656167984 CET	8.8.8.8	192.168.2.3	0xaa8a	No error (0)	ads-bid.l.doubleclick.net		74.125.133.154	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:13.656167984 CET	8.8.8.8	192.168.2.3	0xaa8a	No error (0)	ads-bid.l.doubleclick.net		74.125.133.155	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:13.656167984 CET	8.8.8.8	192.168.2.3	0xaa8a	No error (0)	ads-bid.l.doubleclick.net		74.125.133.156	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:13.656167984 CET	8.8.8.8	192.168.2.3	0xaa8a	No error (0)	ads-bid.l.doubleclick.net		74.125.133.157	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:13.823306084 CET	8.8.8.8	192.168.2.3	0x3502	No error (0)	cdn.mouseflow.com	rec.mouseflowaps.netdna-cdn.com		CNAME (Canonical name)	IN (0x0001)
Mar 25, 2021 03:17:13.823306084 CET	8.8.8.8	192.168.2.3	0x3502	No error (0)	rec.mouseflowaps.netdna-cdn.com		23.111.9.38	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:13.834381104 CET	8.8.8.8	192.168.2.3	0xe067	No error (0)	www.google.ch		216.58.215.227	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:13.890275002 CET	8.8.8.8	192.168.2.3	0x6630	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Mar 25, 2021 03:17:13.890275002 CET	8.8.8.8	192.168.2.3	0x6630	No error (0)	stats.l.doubleclick.net		66.102.1.155	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:13.890275002 CET	8.8.8.8	192.168.2.3	0x6630	No error (0)	stats.l.doubleclick.net		66.102.1.156	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:13.890275002 CET	8.8.8.8	192.168.2.3	0x6630	No error (0)	stats.l.doubleclick.net		66.102.1.157	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:13.890275002 CET	8.8.8.8	192.168.2.3	0x6630	No error (0)	stats.l.doubleclick.net		66.102.1.154	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:14.140891075 CET	8.8.8.8	192.168.2.3	0x998b	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Mar 25, 2021 03:17:14.140891075 CET	8.8.8.8	192.168.2.3	0x998b	No error (0)	scontent.xx.fbcdn.net		157.240.17.15	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:14.140913963 CET	8.8.8.8	192.168.2.3	0xf1cb	No error (0)	pixel-geo.prfct.co	pixel-eu.prfct.co		CNAME (Canonical name)	IN (0x0001)
Mar 25, 2021 03:17:14.140913963 CET	8.8.8.8	192.168.2.3	0xf1cb	No error (0)	pixel-eu.prfct.co	prod-eu-pixel-collector-vpc-145135437.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 25, 2021 03:17:14.140913963 CET	8.8.8.8	192.168.2.3	0xf1cb	No error (0)	prod-eu-pixel-collector-vpc-145135437.eu-west-1.elb.amazonaws.com		52.215.255.105	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:14.140913963 CET	8.8.8.8	192.168.2.3	0xf1cb	No error (0)	prod-eu-pixel-collector-vpc-145135437.eu-west-1.elb.amazonaws.com		34.243.193.207	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:14.569572926 CET	8.8.8.8	192.168.2.3	0x8b45	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Mar 25, 2021 03:17:14.569572926 CET	8.8.8.8	192.168.2.3	0x8b45	No error (0)	star-mini.c10r.facebook.com		31.13.86.36	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:14.570498943 CET	8.8.8.8	192.168.2.3	0x73af	No error (0)	secure.adnxs.com	g.geogslb.com		CNAME (Canonical name)	IN (0x0001)
Mar 25, 2021 03:17:14.570498943 CET	8.8.8.8	192.168.2.3	0x73af	No error (0)	g.geogslb.com	ib.anycast.adnxs.com		CNAME (Canonical name)	IN (0x0001)
Mar 25, 2021 03:17:14.570498943 CET	8.8.8.8	192.168.2.3	0x73af	No error (0)	ib.anycast.adnxs.com		37.252.173.62	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:14.570498943 CET	8.8.8.8	192.168.2.3	0x73af	No error (0)	ib.anycast.adnxs.com		37.252.173.22	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:14.570498943 CET	8.8.8.8	192.168.2.3	0x73af	No error (0)	ib.anycast.adnxs.com		37.252.172.37	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:14.570498943 CET	8.8.8.8	192.168.2.3	0x73af	No error (0)	ib.anycast.adnxs.com		37.252.172.250	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:14.570498943 CET	8.8.8.8	192.168.2.3	0x73af	No error (0)	ib.anycast.adnxs.com		37.252.172.249	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:14.570498943 CET	8.8.8.8	192.168.2.3	0x73af	No error (0)	ib.anycast.adnxs.com		37.252.173.38	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:14.570498943 CET	8.8.8.8	192.168.2.3	0x73af	No error (0)	ib.anycast.adnxs.com		37.252.173.27	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:14.570498943 CET	8.8.8.8	192.168.2.3	0x73af	No error (0)	ib.anycast.adnxs.com		37.252.172.38	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:14.599839926 CET	8.8.8.8	192.168.2.3	0x1700	No error (0)	ads.yahoo.com	edge.gycpi.b.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
Mar 25, 2021 03:17:14.599839926 CET	8.8.8.8	192.168.2.3	0x1700	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.22	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:14.599839926 CET	8.8.8.8	192.168.2.3	0x1700	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.23	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:14.604820967 CET	8.8.8.8	192.168.2.3	0xdcf5	No error (0)	us-u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:14.604820967 CET	8.8.8.8	192.168.2.3	0xdcf5	No error (0)	us-u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:14.664968967 CET	8.8.8.8	192.168.2.3	0xbb	No error (0)	pixel.rubiconproject.com	pixel.rubiconproject.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
Mar 25, 2021 03:17:14.670128107 CET	8.8.8.8	192.168.2.3	0x1483	No error (0)	analytics.twitter.com	ads.twitter.com		CNAME (Canonical name)	IN (0x0001)
Mar 25, 2021 03:17:14.670128107 CET	8.8.8.8	192.168.2.3	0x1483	No error (0)	ads.twitter.com	s.twitter.com		CNAME (Canonical name)	IN (0x0001)
Mar 25, 2021 03:17:14.670128107 CET	8.8.8.8	192.168.2.3	0x1483	No error (0)	s.twitter.com		104.244.42.195	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:14.670128107 CET	8.8.8.8	192.168.2.3	0x1483	No error (0)	s.twitter.com		104.244.42.3	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 25, 2021 03:17:14.670128107 CET	8.8.8.8	192.168.2.3	0x1483	No error (0)	s.twitter.com		104.244.42.67	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:14.670128107 CET	8.8.8.8	192.168.2.3	0x1483	No error (0)	s.twitter.com		104.244.42.131	A (IP address)	IN (0x0001)
Mar 25, 2021 03:17:14.750617027 CET	8.8.8.8	192.168.2.3	0x407c	No error (0)	cm.g.doubleclick.net		172.217.168.66	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 25, 2021 03:16:53.651834011 CET	64.71.144.43	443	192.168.2.3	49712	CN=www.keepandshare.com, O=Gee Whiz Labs, L=San Francisco, ST=California, C=US, SERIALNUMBER=C2789919, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.2=California, OID.1.3.6.1.4.1.311.60.2.1.3=US CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Thu May 02 01:00:59 CEST 2019 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Tue Jun 01 21:12:23 CEST 2021 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Mar 25, 2021 03:16:53.653278112 CET	64.71.144.43	443	192.168.2.3	49713	CN=www.keepandshare.com, O=Gee Whiz Labs, L=San Francisco, ST=California, C=US, SERIALNUMBER=C2789919, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.2=California, OID.1.3.6.1.4.1.311.60.2.1.3=US CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Thu May 02 01:00:59 CEST 2019 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Tue Jun 01 21:12:23 CEST 2021 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Mar 25, 2021 03:16:54.308944941 CET	66.160.183.118	443	192.168.2.3	49715	CN=keepn.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Thu Jan 28 00:06:26 CET 2021 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Tue Mar 01 00:06:26 CET 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Mar 25, 2021 03:16:54.309748888 CET	66.160.183.118	443	192.168.2.3	49714	CN=keepn.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Thu Jan 28 00:06:26 CET 2021 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Tue Mar 01 00:06:26 CET 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Mar 25, 2021 03:17:12.617609978 CET	52.84.138.122	443	192.168.2.3	49727	CN=*.trustpilot.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 May 01 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 Jun 01 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Mar 25, 2021 03:17:12.620708942 CET	52.84.138.122	443	192.168.2.3	49726	CN=*.trustpilot.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 May 01 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 Jun 01 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 25, 2021 03:17:13.698822975 CET	151.101.0.65	443	192.168.2.3	49741	CN=tag.marinsm.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Mon Mar 22 18:55:42 CET 2021	Sat Apr 23 19:55:41 CEST 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=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Mar 25, 2021 03:17:13.699912071 CET	151.101.0.65	443	192.168.2.3	49743	CN=tag.marinsm.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Mon Mar 22 18:55:42 CET 2021	Sat Apr 23 19:55:41 CEST 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=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Mar 25, 2021 03:17:13.705188990 CET	172.217.168.34	443	192.168.2.3	49744	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 Feb 23 16:36:52 CET 2021	Tue May 18 17:36:51 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		
Mar 25, 2021 03:17:13.707580090 CET	172.217.168.34	443	192.168.2.3	49742	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Feb 23 16:36:52 CET 2021	Tue May 18 17:36:51 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		
Mar 25, 2021 03:17:13.722255945 CET	74.125.133.154	443	192.168.2.3	49740	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 Feb 23 16:36:52 CET 2021	Tue May 18 17:36:51 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
Mar 25, 2021 03:17:13.722871065 CET	74.125.133.154	443	192.168.2.3	49739	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 Feb 23 16:36:52 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue May 18 17:36:51 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Mar 25, 2021 03:17:13.767539978 CET	64.62.174.128	443	192.168.2.3	49736	CN=keepn.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Thu Jan 28 00:06:26 CET 2021 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Tue Mar 01 00:06:26 CET 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Mar 25, 2021 03:17:13.770658016 CET	64.62.174.128	443	192.168.2.3	49732	CN=keepn.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Thu Jan 28 00:06:26 CET 2021 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Tue Mar 01 00:06:26 CET 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Mar 25, 2021 03:17:13.772197962 CET	64.62.174.128	443	192.168.2.3	49735	CN=keepn.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Thu Jan 28 00:06:26 CET 2021 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Tue Mar 01 00:06:26 CET 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Mar 25, 2021 03:17:13.788101912 CET	64.62.174.128	443	192.168.2.3	49730	CN=keepn.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Thu Jan 28 00:06:26 CET 2021 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Tue Mar 01 00:06:26 CET 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 25, 2021 03:17:13.791084051 CET	64.62.174.128	443	192.168.2.3	49734	CN=keepn.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Thu Jan 28 00:06:26 CET 2021 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Tue Mar 01 00:06:26 CET 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Mar 25, 2021 03:17:13.862900019 CET	23.111.9.38	443	192.168.2.3	49749	CN=*.mouseflow.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Fri Jun 12 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Wed Sep 14 02:00:00 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 25, 2021 03:17:13.863972902 CET	23.111.9.38	443	192.168.2.3	49750	CN=*.mouseflow.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Fri Jun 12 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Wed Sep 14 02:00:00 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Mar 25, 2021 03:17:13.878273964 CET	216.58.215.227	443	192.168.2.3	49751	CN=*.google.ch, 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	Thu Mar 11 16:02:00 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Thu Jun 03 17:01:59 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Mar 25, 2021 03:17:13.885145903 CET	216.58.215.227	443	192.168.2.3	49752	CN=*.google.ch, 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	Thu Mar 11 16:02:00 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Thu Jun 03 17:01:59 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Mar 25, 2021 03:17:13.950414896 CET	66.102.1.155	443	192.168.2.3	49754	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 Feb 23 16:36:52 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue May 18 17:36:51 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 25, 2021 03:17:13.950651884 CET	66.102.1.155	443	192.168.2.3	49753	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 Feb 23 16:36:52 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue May 18 17:36:51 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Mar 25, 2021 03:17:14.196743965 CET	157.240.17.15	443	192.168.2.3	49755	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		
Mar 25, 2021 03:17:14.201637983 CET	157.240.17.15	443	192.168.2.3	49757	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		
Mar 25, 2021 03:17:14.228214025 CET	52.215.255.105	443	192.168.2.3	49756	CN=*.prfct.co, O=Marin Software Inc., L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Sep 03 02:00:00 CEST 2019 Fri Mar 08 13:00:00 CET 2013	Wed Oct 27 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Mar 25, 2021 03:17:14.259748936 CET	52.215.255.105	443	192.168.2.3	49758	CN=*.prfct.co, O=Marin Software Inc., L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Sep 03 02:00:00 CEST 2019 Fri Mar 08 13:00:00 CET 2013	Wed Oct 27 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 25, 2021 03:17:14.621753931 CET	37.252.173.62	443	192.168.2.3	49766	CN=*.adnxs.com, O=Xandr Inc., L=New York, ST=New York, C=US CN=GeoTrust ECC CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust ECC CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 05 01:00:00 CET 2021 Mon Nov 06 13:24:09 CET 2017	Sun Feb 20 00:59:59 CET 2022 Sat Nov 06 13:24:09 CET 2027	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust ECC CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:24:09 CET 2017	Sat Nov 06 13:24:09 CET 2027		
Mar 25, 2021 03:17:14.622189999 CET	37.252.173.62	443	192.168.2.3	49768	CN=*.adnxs.com, O=Xandr Inc., L=New York, ST=New York, C=US CN=GeoTrust ECC CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust ECC CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 05 01:00:00 CET 2021 Mon Nov 06 13:24:09 CET 2017	Sun Feb 20 00:59:59 CET 2022 Sat Nov 06 13:24:09 CET 2027	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust ECC CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:24:09 CET 2017	Sat Nov 06 13:24:09 CET 2027		
Mar 25, 2021 03:17:14.626368046 CET	31.13.86.36	443	192.168.2.3	49767	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		
Mar 25, 2021 03:17:14.629996061 CET	31.13.86.36	443	192.168.2.3	49765	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		
Mar 25, 2021 03:17:14.655848026 CET	34.98.64.218	443	192.168.2.3	49769	CN=*.openx.net, O=OpenX Technologies inc., L=Pasadena, ST=California, C=US CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jun 18 02:00:00 CEST 2020 Mon Nov 06 13:23:45 CET 2017 Fri Nov 10 01:00:00 CET 2006	Tue Aug 17 14:00:00 CEST 2021 Sat Nov 06 13:23:45 CET 2027 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Mar 25, 2021 03:17:14.663228035 CET	87.248.118.22	443	192.168.2.3	49771	CN=*.ads.yahoo.com, O=Oath Inc, L=Sunnyvale, 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	Sun Feb 28 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Wed Apr 14 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		
Mar 25, 2021 03:17:14.663460016 CET	87.248.118.22	443	192.168.2.3	49772	CN=*.ads.yahoo.com, O=Oath Inc, L=Sunnyvale, 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	Sun Feb 28 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Wed Apr 14 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		
Mar 25, 2021 03:17:14.666964054 CET	34.98.64.218	443	192.168.2.3	49770	CN=*.openx.net, O=OpenX Technologies inc., L=Pasadena, ST=California, C=US CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jun 18 02:00:00 CEST 2020 Mon Nov 06 13:23:45 CET 2017 Fri Nov 10 01:00:00 CET 2006	Tue Aug 17 14:00:00 CEST 2021 Sat Nov 06 13:23:45 CET 2027 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Mar 25, 2021 03:17:14.721298933 CET	104.244.42.195	443	192.168.2.3	49776	CN=*.twitter.com, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Feb 05 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Sat Feb 05 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 25, 2021 03:17:14.723860025 CET	104.244.42.195	443	192.168.2.3	49775	CN=*.twitter.com, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Feb 05 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Sat Feb 05 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Mar 25, 2021 03:17:14.796032906 CET	172.217.168.66	443	192.168.2.3	49777	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 Feb 23 16:36:52 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue May 18 17:36:51 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Mar 25, 2021 03:17:14.796340942 CET	172.217.168.66	443	192.168.2.3	49778	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 Feb 23 16:36:52 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue May 18 17:36:51 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		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 4692 Parent PID: 792

General

Start time:	03:16:50
Start date:	25/03/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff68bbf0000
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: 5288 Parent PID: 4692

General

Start time:	03:16:51
Start date:	25/03/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4692 CREDAT:17410 /prefetch:2
Imagebase:	0x320000
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

Copyright Joe Security LLC 2021

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