ID: 339454
Cookbook: browseurl.jbs
Time: 05:01:31
Date: 14/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

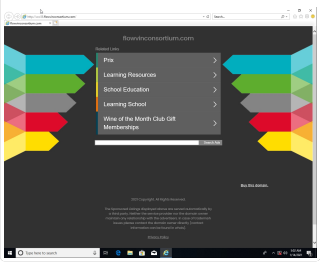
Analysis Report http://www.flowvinconsortium.com

Overview

General Information

Sample URL:	http://www.flowvinconsortium.com
Analysis ID:	339454

Most interesting Screenshot:



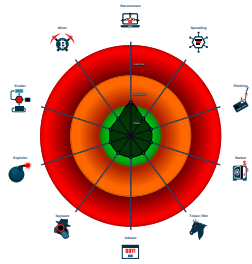
Detection

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

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 4736 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5860 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4736 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

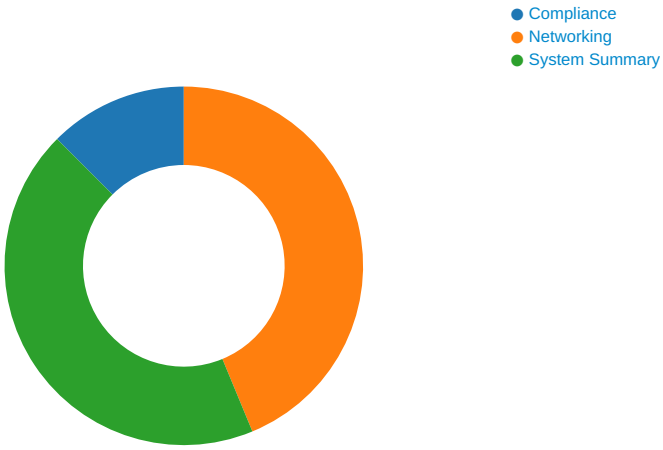
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



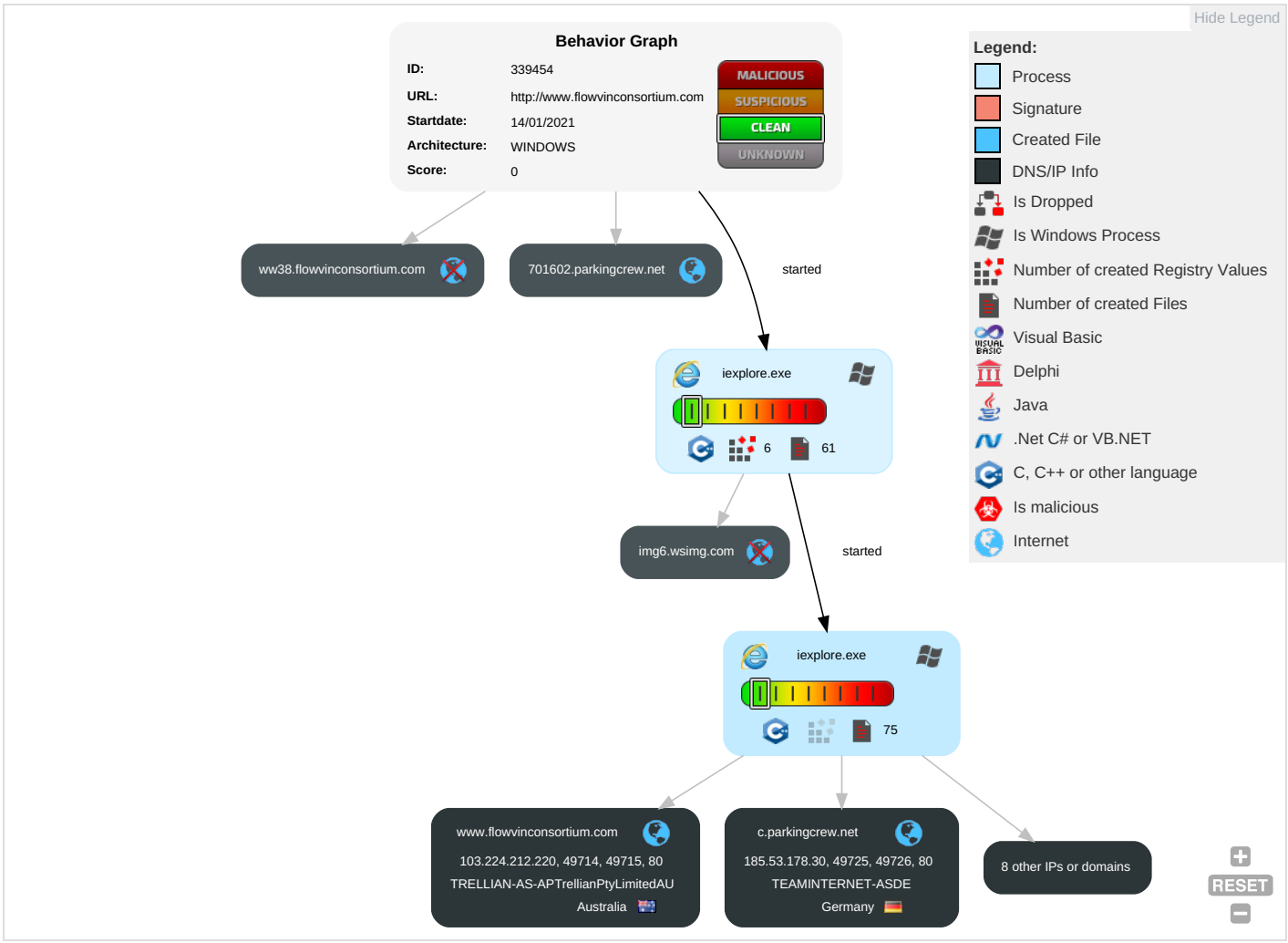
Click to jump to signature section

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	Impa
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 Partit
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 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
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 4	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap		Carri Billin Fraud

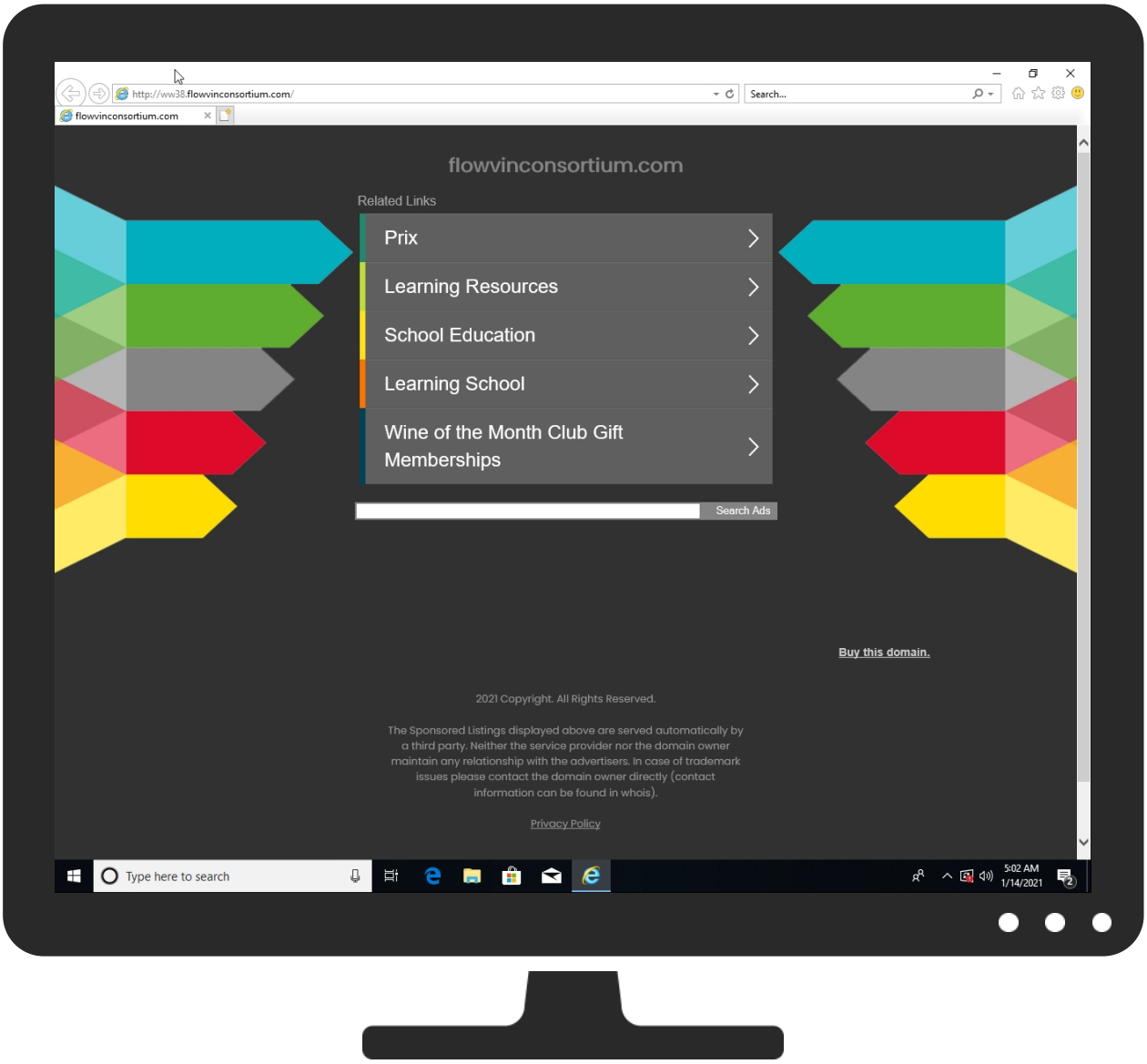
Behavior Graph



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://www.flowvinconsortium.com	0%	Virustotal		Browse
http://www.flowvinconsortium.com	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
www.flowvinconsortium.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://ww38.flowvinconsortium.com/favicon.ico	0%	Avira URL Cloud	safe	
http://https://img6.dev-wsimg.com/px/cart/661/js/cart.min.js	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://ch.godaddy.comsortium.com/	0%	Avira URL Cloud	safe	
http://ww38.flowvinconsortium.com/ls.php	0%	Avira URL Cloud	safe	
http://ww38.flowvinconsortium.com/Root	0%	Avira URL Cloud	safe	
http://ww38.flowvinconsortium.com/track.php?domain=flowvinconsortium.com&caf=1&toggle=answercheck&answer=yes&uid=MTYxMDU5NjkzNi44NjM4OjJlMjliMzNjYzE2ZDNhMTM5ZGFhZWJjMjBlMmIxYmEzYWNlZTk5ZjQyMjgwZmMzNTc3ZTM4MzU2NTQzMDBlZjU6NWZmZmMyNDhkMmU1OA%3D%3D	0%	Avira URL Cloud	safe	
http://ww38.flowvinconsortium.com/?ts=fENsZWFuUGVwcGVybWludEJsYWNrfHw1Y2U4NHxidWNrZXQxMDZ8fHx8fHw1Zm	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
d3uxovyp91rmcf.cloudfront.net	13.224.89.135	true	false		high
701602.parkingcrew.net	76.223.26.96	true	false		high
www.flowvinconsortium.com	103.224.212.220	true	false	• 0%, Virustotal, Browse	unknown
d1lxhc4jvstzrp.cloudfront.net	13.224.89.16	true	false		high
c.parkingcrew.net	185.53.178.30	true	false		high
img1.wsimg.com	unknown	unknown	false		high
www.godaddy.com	unknown	unknown	false		high
ch.godaddy.com	unknown	unknown	false		high
img6.wsimg.com	unknown	unknown	false		high
ww38.flowvinconsortium.com	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://c.parkingcrew.net/scripts/sale_form.js	false		high
http://d1lxhc4jvstzrp.cloudfront.net/scripts/js3caf.js	false		high
http://d1lxhc4jvstzrp.cloudfront.net/themes/cleanPeppermint_7a82f1f3/style.css	false		high
http://ww38.flowvinconsortium.com/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://d1lxhc4jvstzrp.cloudfront.net/themes/assets/style.css	false		high
http://ww38.flowvinconsortium.com/	false		unknown
http://ww38.flowvinconsortium.com/ls.php	false	• Avira URL Cloud: safe	unknown
http://ww38.flowvinconsortium.com/track.php?domain=flowvinconsortium.com&caf=1&toggle=answercheck&answer=yes&uid=MTYxMDU5NjkzNi44NjM4OjJlMjliMzNjYzE2ZDNhMTM5ZGFhZWJjMjBlMmIxYmEzYWNlZTk5ZjQyMjgwZmMzNTc3ZTM4MzU2NTQzMDBlZjU6NWZmZmMyNDhkMmU1OA%3D%3D	false	• Avira URL Cloud: safe	unknown

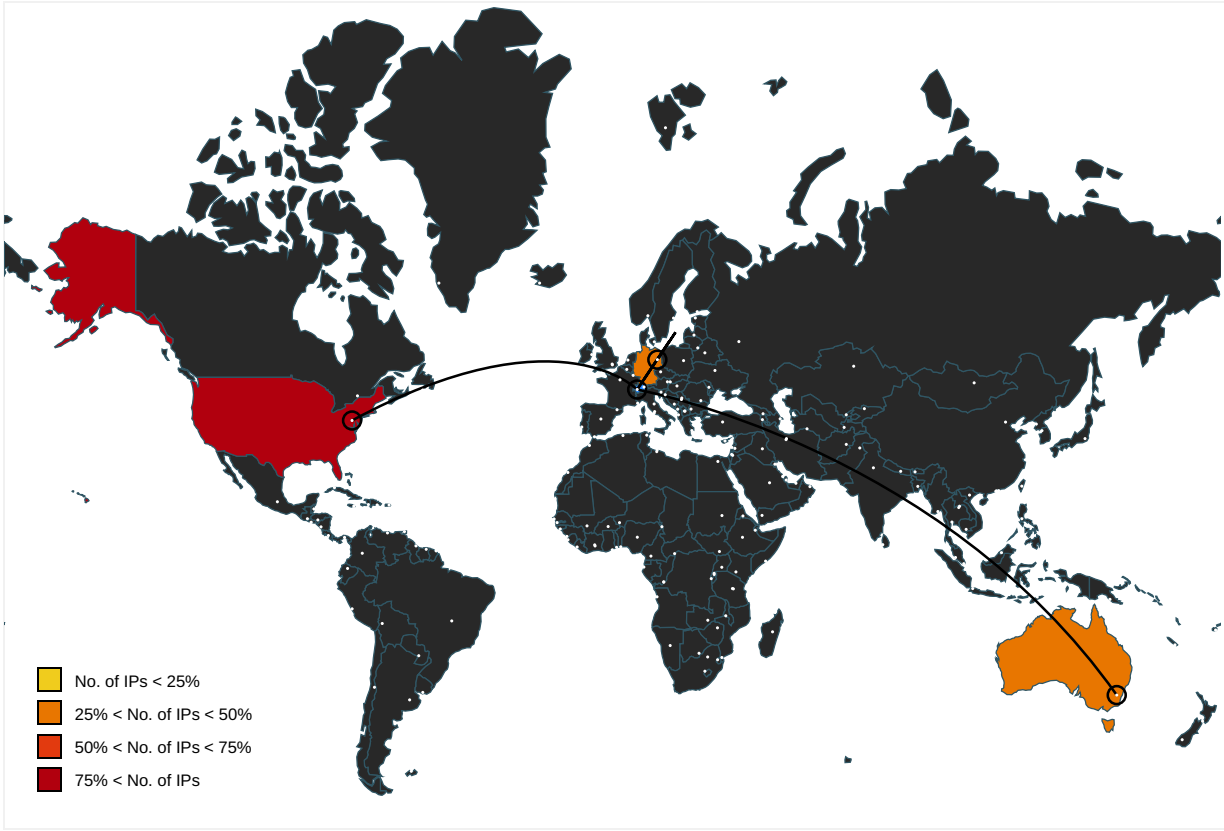
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://img6.wsimg.com/serp-assets/static/b9221d4/client-search-page.min.js	find[1].htm.2.dr	false		high
http://https://fr.godaddy.com	find[1].htm.2.dr	false		high
http://https://supportcenter.godaddy.com/AbuseReport	find[1].htm.2.dr	false		high
http://https://ch.godaddy.com/promos/renewal-codes	find[1].htm.2.dr	false		high
http://https://nz.godaddy.com	find[1].htm.2.dr	false		high
http://https://ch.godaddy.com/help	find[1].htm.2.dr	false		high
http://https://www.godaddy.com	find[1].htm.2.dr	false		high
http://https://ch.godaddy.com/pro	find[1].htm.2.dr	false		high
http://https://img6.wsimg.com/wrhs/e215bf73159eb903a5e02d56e64bf46d/salesheader.min.js	find[1].htm.2.dr	false		high
http://https://in.godaddy.com/hi	find[1].htm.2.dr	false		high
http://https://img6.wsimg.com/wrhs/016f5deda0ac62c233959d03597fbb2a/header-cart-loader.js	find[1].htm.2.dr	false		high
http://https://sso.godaddy.com?realm=idp&path=%2Fproducts&app=account	find[1].htm.2.dr	false		high
http://https://ch.godaddy.com/fr	find[1].htm.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://img6.wsimg.com/wrhs/d6c7b1acb132140b70d61ad9ce6bc527/heartbeat.min.js	find[1].htm.2.dr	false		high
http://https://vn.godaddy.com	find[1].htm.2.dr	false		high
http://https://img6.wsimg.com/serp-assets/static/b9221d4/client-search-page.min.css	find[1].htm.2.dr	false		high
http://https://img6.wsimg.com/wrhs/d4829b8fe08d413dc0c4ea769565a72e/tcc.min.js	find[1].htm.2.dr	false		high
http://https://ch.godaddy.com/web-security/domain-validation-ssl-certificate	find[1].htm.2.dr	false		high
http://https://ch.godaddy.com/online-marketing/digital-marketing-suite	find[1].htm.2.dr	false		high
http://https://ch.godaddy.com/web-security/ov-ssl-certificate	find[1].htm.2.dr	false		high
http://https://nl.godaddy.com	find[1].htm.2.dr	false		high
http://https://no.godaddy.com	find[1].htm.2.dr	false		high
http://https://sso.godaddy.com/account/create?realm=idp&path=%2fproducts&app=account&marketid=de-CH	find[1].htm.2.dr	false		high
http://https://fi.godaddy.com	find[1].htm.2.dr	false		high
http://https://account.godaddy.com/products?acctid=44	find[1].htm.2.dr	false		high
http://https://sso.godaddy.com/logout?realm=idp	find[1].htm.2.dr	false		high
http://https://img1.wsimg.com/wrhs/browser-deprecation-warning/Chrome.png	upgrade-your-browser[1].htm.2.dr	false		high
http://https://ch.godaddy.com/it	find[1].htm.2.dr	false		high
http://https://gr.godaddy.com	find[1].htm.2.dr	false		high
http://https://img6.wsimg.com/wrhs/8423ef1d32036a5af0c0d8b0d1d8e328/uxcore2.min.js	find[1].htm.2.dr	false		high
http://https://mx.godaddy.com	find[1].htm.2.dr	false		high
http://https://my.godaddy.com	find[1].htm.2.dr	false		high
http://https://es.godaddy.com	find[1].htm.2.dr	false		high
http://https://ch.godaddy.com/domains/bulk-domain-search	find[1].htm.2.dr	false		high
http://https://certs.godaddy.com	find[1].htm.2.dr	false		high
http://https://pe.godaddy.com	find[1].htm.2.dr	false		high
http://https://img1.wsimg.com/wrhs/browser-deprecation-warning/logo.png	upgrade-your-browser[1].htm.2.dr	false		high
http://https://find.godaddy.com/v1/jserror?error=preload_loader_img	find[1].htm.2.dr	false		high
http://https://img6.wsimg.com/wrhs/044e80af893940b9c2e2dd4096f44d0f/header-cart.header-chunk.js	find[1].htm.2.dr	false		high
http://https://ch.godaddy.com/domains/domain-name-search	find[1].htm.2.dr	false		high
http://https://ch.godaddy.com/business/office-365	find[1].htm.2.dr	false		high
http://https://ch.godaddy.com/whois	find[1].htm.2.dr	false		high
http://https://ve.godaddy.com	find[1].htm.2.dr	false		high
http://https://ch.godaddy.com/trust-center	find[1].htm.2.dr	false		high
http://https://sso.godaddy.com?realm=idp&path=%2Fproducts&app=account	find[1].htm.2.dr	false		high
http://https://img6.dev-wsimg.com/px/cart/661/js/cart.min.js	find[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://ch.godaddy.com/online-marketing/seo-tools	find[1].htm.2.dr	false		high
http://https://use.typekit.net	webfont[1].js.2.dr	false		high
http://https://img1.wsimg.com/wrhs/browser-deprecation-warning/Safari.png	upgrade-your-browser[1].htm.2.dr	false		high
http://https://dk.godaddy.com	find[1].htm.2.dr	false		high
http://https://tw.godaddy.com	find[1].htm.2.dr	false		high
http://https://preferences-mgr.truste.com/?pid=godaddy01&aid=godaddy01&type=godaddy	find[1].htm.2.dr	false		high
http://https://ch.godaddy.com/site-map	find[1].htm.2.dr	false		high
http://https://careers.godaddy.com/search-jobs/Germany	find[1].htm.2.dr	false		high
http://https://dcc.godaddy.com	find[1].htm.2.dr	false		high
http://https://ch.godaddy.comsortium.com/	{B82B1B74-5668-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://ch.godaddy.com/domains/domain-transfer	find[1].htm.2.dr	false		high
http://https://sg.godaddy.com/zh	find[1].htm.2.dr	false		high
http://https://img6.wsimg.com/	find[1].htm.2.dr	false		high
http://https://ch.godaddy.com/web-security/multi-domain-san-ssl-certificate	find[1].htm.2.dr	false		high
http://https://id.godaddy.com	find[1].htm.2.dr	false		high
http://https://ch.godaddy.com/domains/gtld-domain-names	find[1].htm.2.dr	false		high
http://https://pk.godaddy.com	find[1].htm.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ch.godaddy.com/websites/website-builder	find[1].htm.2.dr	false		high
http://https://ch.godaddy.com/legal/agreements/privacy-policy	find[1].htm.2.dr	false		high
http://https://ch.godaddy.com/offers/ssl-certificate/ssl-selector	find[1].htm.2.dr	false		high
http://https://ch.godaddy.com/web-security/ev-ssl-certificate	find[1].htm.2.dr	false		high
http://https://cart.godaddy.com	find[1].htm.2.dr	false		high
http://ww38.flowvinconsortium.com/Root	{B82B1B74-5668-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://hk.godaddy.com	find[1].htm.2.dr	false		high
http://https://sso.godaddy.com/account/create?realm=idp&path=%2Fproducts&app=account	find[1].htm.2.dr	false		high
http://https://ch.godaddy.com/domains/domain-broker	find[1].htm.2.dr	false		high
http://https://hk.godaddy.com/en	find[1].htm.2.dr	false		high
http://https://de.godaddy.com	find[1].htm.2.dr	false		high
http://https://ch.godaddy.com/reseller-program	find[1].htm.2.dr	false		high
http://https://ch.godaddy.com/upgrade-your-browserckAvail=1&domainToCheck=flowvinconsortium.com	~DF404FE72635615315.TMP.1.dr	false		high
http://parkingcrew.net/assets	FCO7OGE7.htm.2.dr	false		high
http://https://ca.godaddy.com/fr	find[1].htm.2.dr	false		high
http://https://dcc.godaddy.com/domains	find[1].htm.2.dr	false		high
http://https://ch.godaddy.com/promos/hot-deals	find[1].htm.2.dr	false		high
http://https://ch.godaddy.com/upgrade-your-browser	find[1].htm.2.dr	false		high
http://https://img6.wsimg.com/wrhs/1d4ea1012b1fc81cb9412dc42a2747dc/salesheader.min.css	find[1].htm.2.dr	false		high
http://https://ch.auctions.godaddy.com/trpItemBuild.aspx	find[1].htm.2.dr	false		high
http://https://img6.wsimg.com/wrhs/9d2d57f6dd630cb051724eacb63d2a91/uxcore2.min.css	find[1].htm.2.dr	false		high
http://https://ch.godaddy.com/contact-us	find[1].htm.2.dr	false		high
http://https://d3uxovyp91rmcf.cloudfront.net/hivemind-v2.js	find[1].htm.2.dr	false		high
http://https://ch.godaddy.com/domain-value-appraisal	find[1].htm.2.dr	false		high
http://https://img6.wsimg.com/ux/favicon/favicon-32x32.png	imagestore.dat.2.dr	false		high
http://https://sg.godaddy.com	find[1].htm.2.dr	false		high
http://ww38.flowvinconsortium.com/?ts=fENsZWFuUGVwcGVybWludEJsYWNrfHw1Y2U4NHxidWNrZXQxMDZ8fHx8fHw1Zm	FCO7OGE7.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://img6.wsimg.com/wrhs/c7fa7d66354b8b79c171eeb460286ef1/vendors~notifications.header-chunk.min.	find[1].htm.2.dr	false		high
http://https://se.godaddy.com	find[1].htm.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.224.89.16	unknown	United States		16509	AMAZON-02US	false
13.224.89.135	unknown	United States		16509	AMAZON-02US	false
103.224.212.220	unknown	Australia		133618	TRELLIAN-AS-APTrellianPtyLimitedAU	false
76.223.26.96	unknown	United States		16509	AMAZON-02US	false
185.53.178.30	unknown	Germany		61969	TEAMINTERNET-ASDE	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339454
Start date:	14.01.2021
Start time:	05:01:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://www.flowvinconsortium.com
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	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@3/37@11/5
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://www.godaddy.com/domainsearch/find?checkAvail=1&domainToCheck=flowvinconsortium.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): 52.147.198.201, 40.88.32.150, 88.221.62.148, 108.177.119.106, 108.177.119.103, 108.177.119.99, 108.177.119.147, 108.177.119.105, 108.177.119.104, 108.177.126.95, 108.177.127.94, 173.194.79.95, 108.177.126.94, 51.11.168.160, 104.83.98.9, 2.17.185.233, 152.199.19.161 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, fonts.googleapis.com, arc.msn.com.nsatc.net, e2836.g.akamaiedge.net, fonts.gstatic.com, ajax.googleapis.com, e6001.dscx.akamaiedge.net, ie9comview.vo.msecnd.net, arc.msn.com, skypedataprdcoleus16.cloudapp.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, skypedataprdcoleus15.cloudapp.net, wildcard-ipv6.godaddy.com.edgekey.net, go.microsoft.com, global-wildcard.wsimg.com.edgekey.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, www.google.com, watson.telemetry.microsoft.com, www.gstatic.com, cs9.wpc.v0cdn.net • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{B82B1B72-5668-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8522508150543266
Encrypted:	false
SSDEEP:	48:IwlGcproGwpLwG/ap8FrGIpcrbGvnZpvrVGoZqp9rLGo4RpmrYGW7h9rhGWxhvrQ:r7ZwZq2F9Wr8tryfrsRMrarjrXfrjsX
MD5:	F054EB2CE9F8BABB3343915C41C89067
SHA1:	12B64E9F9FECD0DE554DA060723558727D379CEC
SHA-256:	59758BF1430CAAB7CD4E459EF7E8BD7CF710C5EF76583CDED529272A122909A9
SHA-512:	8828C3D956B2BBF2A615FD253CB53D27B2420D31DDCDA8D02C3FBDB65775FBB4AF6EB095E4AA9BEC7017C9F539A74CE860DE2935E925A94B8DB87FB8AA772 7C
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\{B82B1B74-5668-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	63424
Entropy (8bit):	2.878746003413683
Encrypted:	false
SSDEEP:	384:rS6scYhA8z9JjPkjJFJ6JEJgoJEJ3jJFJ6JEJEoJEJR4SzvqhtsptJ:8WLU2mo2hLU2qo2MaSh+ptJ
MD5:	1FF74E2A1735DD069D9668BC2CF2B250
SHA1:	C5ABB3D481CD2410C888AE4805045843210CBFAB
SHA-256:	3C0F1773597B43BA317C72B8353A67C844FEAA4B0955815645117B2F7296382C
SHA-512:	97AD17D0F5D5CE1DD05BEDA9B174C30E9B63713BBD2A210E3732B5BEAFAD76DA79159B96BEF01FABCE1E213D65C7F48DAE8824F7C9C57C5004B0E107E6A75 E88
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\{B82B1B75-5668-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5641070029361444
Encrypted:	false
SSDEEP:	48:IwNGcprs7GwpagG4pQoGrapbSyrGQpKaG7HpRpsTGIpG:rTZsVQA62BSyFA1Tp4A
MD5:	EAD48F1E130F21446753239B81F9FA42
SHA1:	5F66AFD0E5A40E49F93AD69A03CD29487281BE1A
SHA-256:	28058F1DE3E6769EF0D04EFF9A58A27A387FAA4E3CBDE2B5FB33212B5B325D7D
SHA-512:	E61C342A215AC7265CBD3C757D6B6DE738F01EDB56E5A03EA9DD1CDE48CCFF8FE3583A3CD950F8D7E07D355DE6F5C1B749756CEE8FF2FB4D7250049A743C1 AC
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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
File Type:	data
Category:	modified
Size (bytes):	1073
Entropy (8bit):	7.450906014608403
Encrypted:	false
SSDEEP:	12:oLmuyDCjtlUv/7ioSOdCKR5lNakbwQ/2xHFXhNOMPgZvCJmydAv/A2eVd5vuNzby:oLnqLp0ZF//Jt/7d5+fR8W4gQU72YI
MD5:	C542E3C02FA77C1A8E40F01B06E50E99
SHA1:	16ED714ADE6BCAFFFF6D515528DCA57D0B510E45
SHA-256:	FC83916EA8B681A162FEAB3C350B7AEC670FA4541E3631E83050A8D25F4D3563
SHA-512:	5870495CD12683924D78E16F2A292FB2A9CF399D58B991D63136D8E5142854A9F20F236D78421E1A3C0E2A057C84176940F055EE75DC62CD4EF7C7100F20B5E9
Malicious:	false
Reputation:	low
Preview:	3.h.t.t.p.s.:././.i.m.g.6...w.s.i.m.g...c.o.m./.u.x./.f.a.v.i.c.o.n./.f.a.v.i.c.o.n.-.3.2.x.3.2...p.n.g.....PNG.....IHDR... ... .szz....IIDATx.....%Y...g.m.m..n....w...m.=.5.N..TN../..... '...42...R.{p.N@A.....F9w.R..N..Y....e(.F.A;..c\.1.....)S.q.yV..x..`)Tb<..Y...#7.+...`...P.....&.bR.1m.S[5V.d.ze....K....(vc.p4..d.....b.j....\..P..0i.C.L.X..ix..)..!h..V(.....N..I...0.. 3.]......Q.?.|.$.T..I'...[.[.....&H*B}...);x.\.^..Q`..".&Hz..`X.kS4.Aa.k...&..Q8(....v..)...O. .b.z`t.^...a.....4..?<A.<.>.T..q...^...,j'.8s...:/'h~..t.)..S..p..(0..e8'.|...0.G..K.<&.7Y..5.^..^.YQ ....x8...L.....G.....0y=.yX.....g.R..`p.....s..c..w....{....?...,\.^.....>...Kp>|..p.....0.(V.hLpS~el...M....y.T.=....t.P.*..{3.Q.Kx...`.."3....38...X.j.....z{&<l.....G....C2..C...Z.....!a.c.q{...0.' fp.'....p.j.z<..?....n...n.f...l}.%J<....>.~...~.>..C..*.F.K.AyN...u..7.7....a.,..G&.;.m`.j.....s....`.d....=4..}G.!...(.9.1.Md.b.....i..u.q.2!....p@.....h..X...N..x.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Firefox[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 128 x 128, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	5334
Entropy (8bit):	7.838231384483405
Encrypted:	false
SSDEEP:	96:nAu+AHnrY06Ja8iJLaLhXnPjRBlMNhIj9QlWIJplEpf7GF:nAuDHrlJ3NXnPjRMsj93W0R
MD5:	1AA50EE8234957E5B50D71E053281A6A
SHA1:	0B2C40A2898618CBD89F91B410C4F5219659E7AD
SHA-256:	6DF5062B41E82B1990D96B5AA75906011C9792C1B750BD80C1741AA35B14768A
SHA-512:	36207D2F052B933A1F6D9269EB44C139BE4D7490D66FE541A50B90542B52966807E8068F49C77AD4CBF9C436C681DF2ABD1615217A6F6C4BBC8B868026EA8166
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img1.wsimg.com/wrhs/browser-deprecation-warning/Firefox.png
Preview:	.PNG.....IHDR.....PLTE.....^..q..m.W5..X.S"....o.i...k.(5....q".....g..q. ?..s. C..s.. ..o.....O...X.l...H.....*3"h.....R....._.....1.(-....".J...:..?.|..V..k..A.. N..C.....m....%...L.8$.#2.?!.*+.1(.E..W..Q.....K.....D.....J.]..r...@.....b..!7J.u..G.m.....~..x.....;.}.....y...D.i..s..Q...I.f.....i.....=....F.....M...A....`.....U...:.\..B."':...T.. M..6.d.....m.....Y.....J...P.>.C....^..a...&7.6'.E.y.....i..2.....e..Z.....Q..W..-(4...'...< .....3-...!...,2.....v.!D.u...I."?...-.h.....:.y.~..?%..9.q..H.....L"....;..E'....3.. i.FC.2...z..p.MH.. .h&d.BW.b/..&.....) .OO.()..oS.U:.&.@.i.#E.0.90..J..!#.irv`Lj.0\Q5Z.V0..%.!.s.(..$t..oa.....?...v.6isGP..F.s.....e.....+.\...k=-\.H..v.y.l+....R..L.+..I..E../~..=...=tRNS.....% ..G..<(.T>...^.`}c...Z.....b;....W.....7....F.....HIDATx..wLSQ.....[..^q.X...@...:P\h...nM.;.Q$j.b..A...B...DQq.....gk]x..#9....._.i1...b.5.7.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Safari[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 128 x 128, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	7175
Entropy (8bit):	7.922609296000784
Encrypted:	false
SSDEEP:	192:fuJ0+zNsMG3OJIVXQ8oK7RgKDNQXxm5oNRN0b:fuJbK3jK3KRNQo5oNRab
MD5:	BDB8B329A8DD71C276215560A8A09B44
SHA1:	1928D7FE2B1A9AAA5CC21C5FB07BDD2291BAA9B7
SHA-256:	56FE01D22EC671B3D6E8D6A4E29695A63BEE3FB4299EED4EDDD97C71AA72F07B
SHA-512:	A7E9AD17B8B0CD1564C138A59FFC72BC0497D9A5807A2207CB2D02F8FEB4E890734E3A87CD762CCE87C8996D45622A53A9E954F66D081B8BF917DD7596CEFE 3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img1.wsimg.com/wrhs/browser-deprecation-warning/Safari.png
Preview:	.PNG.....IHDR.....PLTE...444)))..... .....BBB..... .....```..... .....ddd.....PM.....e.....k..... .....q..... .....}.....^.....v.... .y.....}..q....5.....x.....&.....j.....W..t.....3..... .....n..y.%.....>..)..%z..... .....a..... .....a.*.....}..... .....V....t..j..k.3..... .....".....r..Z... ....+...N....m.....GCF.....x..'l.A...z....<..e.....#|.....m..c..k.P.....9...b.....D...`..){.4...y.D~.Q..{.....3}.\..p....a.....4q.....u....r....F..._...Dn.....#x..M..k..i....}..N. %cv.N.Rr....4..y...$#1No...k..o...Y[.$*.....k{.ck._\,-....,=3...`.a9MHDVo3=Fs..q..x.m T....'tRNS.....1$G..@...~.~a.x..].UB...!..r.....IDATx..?..P..m).t(.t...vi...`..'8.I...pP8K.x..1 .pP.#.R...0.....{.b...^.N>.r.&....Sz....j4;.N..../..t..z.a.57j.....z...0`

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\caf[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	176334

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\caf[1].js	
Entropy (8bit):	5.583758613713527
Encrypted:	false
SSDEEP:	1536:zuqeYVTyHVpFuCpmBPyeTZAWQIbNpXM4QCNvH2JkgKzj7jhb6GdSvSm6bHIJKJaZ:ioaBGVMnS3hb6GvPbH0Carg5VqjMY7
MD5:	64C36C65181412AC819E38ACD66AD6DD
SHA1:	C0BC1843B2E771C5DE55FB9E61C80E3F3B101DAC
SHA-256:	6BDEA0F4CC13921A428FD03D1495336CB7D44BFCE797077A8C3A400943A7E79E
SHA-512:	F8ABC4B317943748E01F03F258C53566D2E70956112D0E87C88D8D6F417BB457B0E155D4A9C45D7AE6E937D1E61B797CD3BB1A656110D9C2B2DF1444D9370C9
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.google.com/adsense/domains/caf.js
Preview:	if(!window['googleNDT_']){window['googleNDT_']=(new Date()).getTime();}window._googCsaExpIds='17300441,17300443,17300494,17300496,17300584,17300586';window._googCsaAlwaysHttps=1;window._googEnableCcpa=1;window._googEnableCcpaForCanoeV2=1;window._googEnablePurposeOneEnforcement=1;window._googEnableQup=1;window._googErrorTurnOffPersonalization=1;window._scs_mismatch=1;window._googTimeoutTurnOffPersonalization=1;window._googLazyLoadingRootMargin=0;window._googTcfApiTimeout=-1;window._googUspApiTimeout=500;(function() {window.googleAltLoader=3;var version_='1.0';var hash_='15753162209046399873';var module_='ads';var packages_='domains';var googleApisBase_='https://ajax.googleapis.com/ajax';var serviceBase_='https://www.google.com/uds';var serviceHost_='www.google.com';/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var h;function aa(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}var ca="function"==typeof Object.definePro

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\caf[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	176320
Entropy (8bit):	5.5838167542349595
Encrypted:	false
SSDEEP:	1536:wuqeYVTyHVpFuCpmBPyeTZAWQIbNpXM4QCNvH2JkgKzj7jhb6GdSvSm6bHIJKJaZ:FoaBGVMnS3hb6GvPbH0Carg5VqjMY7
MD5:	04D7A531A9F8A30632BC5050023E12F7
SHA1:	A755A9FEB11FA56292A2E9FF036DCE901BC20840
SHA-256:	F56D000A405D06162C55B330BB7908A230D80C13A9A8BDEBD7B14487AC6A67AE
SHA-512:	67FACF4EC1E80E2F15E15F4B94F6B9F464950C53D41B283E882B370ED3A84564DBA7AD3833CF366DA4564E1B1B68BAEAC97E720238B7E0A158083526A7B3306
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/adsense/domains/caf.js
Preview:	if(!window['googleNDT_']){window['googleNDT_']=(new Date()).getTime();}window._googCsaExpIds='17300002,17300441,17300443,17300494,17300496,17300580,17300582';window._googCsaAlwaysHttps=1;window._googEnableCcpa=1;window._googEnableCcpaForCanoeV2=1;window._googEnablePurposeOneEnforcement=1;window._googEnableQup=1;window._googErrorTurnOffPersonalization=1;window._googTimeoutTurnOffPersonalization=1;window._googLazyLoadingRootMargin=0;window._googTcfApiTimeout=-1;window._googUspApiTimeout=500;(function() {window.googleAltLoader=3;var version_='1.0';var hash_='15753162209046399873';var module_='ads';var packages_='domains';var googleApisBase_='https://ajax.googleapis.com/ajax';var serviceBase_='https://www.google.com/uds';var serviceHost_='www.google.com';/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var h;function aa(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}var ca="function"==typeof Object.defineProperties?Object

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\iframe[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):	1243
Entropy (8bit):	5.330848115660528
Encrypted:	false
SSDEEP:	24:0jH1hi7qOCKsudK82M6cENRRLAS4tyPWpRICMXilHm0F6QR2qEgbnYfO67yGwS:0JhPOnK8b6YS4tyPWp2PXihm0wQR2Fgu
MD5:	312F3540D8F0BD79762C2E5E87C294CB
SHA1:	3D2DCE7136637FE76409F03668F64E9A565A28A4
SHA-256:	C647877B7AAB52C58CB694A316C20B71A4832A7C310DB9CC15205C6ADEE368D0
SHA-512:	5D5D22E0D2A654B17F9F3BF9E9B1BC8D077A3CD192BE713E5C81B04DEB368459BC73964B2890446B06D6A93D9872BB99AE7F6E2A1818AE4B5AD7D9E4D2B01D89
Malicious:	false
Reputation:	low
Preview:	<!doctype html><html><head><meta name="ROBOTS" content="NOINDEX, NOFOLLOW"><meta name="format-detection" content="telephone=no"><meta content="origin" name="referrer"></head><body> <script nonce="huMrdUqGUH9fI5u6GrNjqg">if (window.name.match(/^{"name":"master-\d+"/)) {var script = document.createElement('script');script.src = "/adsense/search/ads.js";document.head.appendChild(script);window.IS_GOOGLE_AFS_IFRAME_ = true;}function populate(el) {var adBlock = document.getElementById('adBlock');adBlock.innerHTML += el;}function getMaster() {var m = null;var pIndex = window.name.indexOf('|');if (pIndex > -1 && window.name.charAt(0) != '{') {try {m = window.parent.frames[window.name.substring(pIndex + 1)];} catch (e) {}if (m) {return m;}var nameInfo = window.name.match(/^(slave-\d+)-(\d+)/);var masterNum = (nameInfo && nameInfo[2]) ? nameInfo[2] : null;if (masterNum) {try {m = window.parent.frames['master-' + masterNum];} catch (e) {}}}return m;}window.onresize = funct

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\logo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 313 x 65, 8-bit colormap, non-interlaced
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\logo[1].png	
Size (bytes):	4428
Entropy (8bit):	7.534636315290708
Encrypted:	false
SSDEEP:	96:D5gGUsFtsW3RlNxdyyro7bWhzRMKNaVzLzEFtmdSnU6ASAYSk3viXC/9WR5YCr2:FgGU6td3RlNxdyyr1hVpaVzvRSnThL5n
MD5:	B09B888933F7EEDA066F8928B10F6E63
SHA1:	572CFDB32915EE6C5A9DAA1116648D2A73078F16
SHA-256:	13CFEFAAF8D4DAE3A773FC689147BD33C18B299BC3670F726A62815E338EC10A
SHA-512:	0B4E049EEEB7DDD05BED382C6592A3C18CBA21270C68C52890856E9DFCFB1120322A83300D48266EB5473D312ED4B2854C13A729073B5F93FDA0BA559242276
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img1.wsimg.com/wrhs/browser-deprecation-warning/logo.png
Preview:	.PNG.....IHDR...9...A.....9#.....PLTE.....$$$...333.....UUU.....+++..... ....@@@..... ....0....tRNS..f...8.....=....."w.....!..%_..Z.....03...}.....$1...2..M..L.x...K..-p.9N.[v7.Y..u6..&...lP>.r.a.U....ye.).....g./.....:...T.`.^Vn.R..EI*...ctQ.. ...q.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\pxiEyp8kv8JHgFVrJJfedA[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 10536, version 1.1
Category:	downloaded
Size (bytes):	10536
Entropy (8bit):	7.942419499918068
Encrypted:	false
SSDEEP:	192:YLS34U1mA6N/1JO/mA4WIxpqVkHm8zXxykTBBq1SEOAY/y:YLSoU1mA6N/1A/2XqVkHfznN8Hv
MD5:	4FC29212BD42883C45EDD0BFBD91AD72
SHA1:	6FF25B6FAE5D1C35B9255A483283AA7F698A10E8
SHA-256:	12BCAA5F5203A347C58533BE7E0051BB7EA4432D27A472CC36E32C398A585B00
SHA-512:	A29A37030600435E64B19C1ACCA2E47C7533DCEAA2FE01BB3D3577DFFA4E29DA9FFC912D00FEC1C1DCC3FE50DADA9153B72090AF1FB290D14BFF8B92AE1D(249
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/poppins/v15/pxiEyp8kv8JHgFVrJJfedA.woff
Preview:	wOFF.....)(.....?.....GPOS..... ... DvLuGSUB...<.....0.H'kOS/2...l...M...`Y..cmap.....glyf...P.. Y..32.w..head.."....6...6..$ahhea.."........$.u..hmtx..#.....h.( .loca..%.....E.fmaxp..&.... ... .\.,name..&.....(.C.post..'....g.....]s.....DFLT.....x.c`d``.b.a.c`vq..a.II-3b.....r.,.@..?.....<....x.c`a.f.....=.|....3 ...7.....J.,R ..1...3.+00L..1.0..R..,.....x.c```.bf ....`.....aP..x.,^.:.....L{..1.b.. . . ....`..FQIIHI.....[.T..W-. . .Vm.....?...?.....}.`...6=X.`.Y.&>....{G.."....5..x.:.`SG..+c.md.."K.\%[.Y.U.b ..]r/.....:...HHo...\...+\.|.{.!.J..'G:..?..$.....N...f!.....9h>J@(Q.(."!O+..d).....w3...|. ...U.....v.3...1.3..".=t..K.#.....*.R."X./~a.w^.D..&.....`.$=]B/.+&-...X>..J.....)\.%/....!.K$_....t. .1_.e/....\|z.\.W.5.;o/n+~..=...~(....w...?..2.5D.0.).[..[.$..).....bu~.T.."T..,F.V....,"@....$i.*.....*..%..*IM..nM..}.T.V...i..U.....g....g.I.x-...>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\style[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	829
Entropy (8bit):	5.058569541320297
Encrypted:	false
SSDEEP:	24:wB02AmB02AmB02ApaGJ/CxJLZHuK7e5CZduSZ+:kHHca3TZGJ
MD5:	96F84D0985AF87B4D4F6AE8816F9C5C5
SHA1:	9CF62A3E426361587207124EB6CAF0AEEB3CB030
SHA-256:	93A1109ADA0CD55DEDEAF7E9C4251A7F91AC3C3E1AB85E25E37B6CD4E47D504B
SHA-512:	0423C77082E7CEDE3ED0C10219D8DCE268D2F137C2B5BD46D1A9FC1A15EEFD316D190BACD3AC22C60FDE155DC044ED3886646A2C1453EA3B82393ABDCF7D 2B3
Malicious:	false
Reputation:	low
IE Cache URL:	http://d1lxhc4jvstzrp.cloudfront.net/themes/assets/style.css
Preview:	.asset_star0 {..background: url('star0.gif') no-repeat center;..width: 13px;..height: 12px;..display: inline-block;.}...asset_star1 {..background: url('star1.gif') no-repeat center ;..width: 13px;..height: 12px;..display: inline-block;.}...asset_starH {..background: url('starH.gif') no-repeat center;..width: 13px;..height: 12px;..display: inline-block;.}...sitelink {..padding-right: 16px;.}...sellerRatings a:link,..sellerRatings a:visited,..sellerRatings a:hover,..sellerRatings a:active {..text-decoration: none;..cursor: text;.}...sellerRatings {..margin:0 0 3px 20px;.}...sitelinkHolder {..margin:-15px 0 15px 35px;.}..#ajaxloaderHolder {..display: block;..width: 24px;..height: 24px;..background: #fff;..padding: 8px 0 0 8px;..margin:10px auto;..-webkit-border-radius: 4px;..-moz-border-radius: 4px;..border-radius: 4px;.}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\upgrade-your-browser[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	2309
Entropy (8bit):	5.1050061989218465

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\upgrade-your-browser[1].htm	
Encrypted:	false
SSDEEP:	48:MhKZ6/MDchhmBoPwqn9hf/2hhgZKhc8rQeEh0DVpXEb1Rofl4Nzmv49vqu:aKY1h2oRIgyZPS0pp0b1Slaqu
MD5:	9971B9DC3ECF388378D7E4BE4353B6E3
SHA1:	164737994D7646F088272D1F67F6E546467FDFAE
SHA-256:	0301C15050948DE1BB1920BC05ADE0BFAD45E7030C6536103CC4767A48545DF5
SHA-512:	5906F31073EDA3D25396E11B74C75445E28A4E7A0F33F39697799B94F9366B978943286599493B727ECDD1BC2F80EC797754BF406E6D8410066801A70F9A7CAB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ch.godaddy.com/upgrade-your-browser
Preview:	<!DOCTYPE html><html lang=de-CH dir=ltr><head><title>Aktualisiere deinen Browser</title><link rel=stylesheet href=https://img1.wsimg.com/wrhs/browser-deprecation-warning/style-ltr.css><link rel=icon type=image/png sizes=32x32 href=//img6.wsimg.com/ux/favicon/favicon-32x32.png><meta http-equiv=Content-Type content=text/html><meta charset=utf-8></head><body> <img src=https://img1.wsimg.com/wrhs/browser-deprecation-warning/logo.png alt=GoDaddy> Wir m.chten dir bei der Verwirklichung deiner Idee helfen. Das k.nnen wir aber erst, nachdem du deinen Browser aktualisiert hast. Aktualisiere ihn jetzt, um loszulegen. Aktualisiere deinen Browser <ul id=browsers><li class=browser id=Chrome><img src=https://img1.wsimg.com/wrhs/browser-deprecation-warning/Chrome.png alt=Chrome> Chrome herunterladen <

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\webfont[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	13188
Entropy (8bit):	5.4223896155104025
Encrypted:	false
SSDEEP:	384:i11kqRm4UjryX2DfatZrT80NCGz5r2zItrX:iEqRm4cy338m7d
MD5:	7C96A5F11D9741541D5E3C42FF6380D7
SHA1:	D3FA2564C021CF730E58FFDDB138CF6B57ED126E
SHA-256:	81016AC6BE850B72DF5D4FAA0C3CEC8E2C1B0BA0045712144A6766ADFAD40BEE
SHA-512:	23C162A2E268951729B580E5035AD6CA9969CFCC5CE58A220817B912E76B38BE6C29C3CA7680CB4E8198863D95A72EA65BD06FF7189B5C8475E4C1CE501AEAE1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ajax.googleapis.com/ajax/libs/webfont/1/webfont.js
Preview:	/*. * Copyright 2016 Small Batch, Inc.. *. * Licensed under the Apache License, Version 2.0 (the "License"); you may not. * use this file except in compliance with the License. You may obtain a copy of. * the License at. *. * http://www.apache.org/licenses/LICENSE-2.0. *. * Unless required by applicable law or agreed to in writing, software. * distributed under the License is distributed on an "AS IS" BASIS, WITHOUT. * WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the. * License for the specific language governing permissions and limitations under. * the License.. */*/ Web Font Loader v1.6.26 - (c) Adobe Systems, Google. License: Apache 2.0 */(function(){function aa(a,b,c){return a.call.apply(a.bind,arguments)}function ba(a,b,c){if(!a)throw Error();if(2<arguments.length){var d=Array.prototype.slice.call(arguments,2);return function(){var c=Array.prototype.slice.call(arguments);Array.prototype.unshift.apply(c,d);return a.apply(b,c)}}return function(){return a.app

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Chrome[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 128 x 128, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	4382
Entropy (8bit):	7.911574758210219
Encrypted:	false
SSDEEP:	96:TBNw7rD/iH57qCD4BmLGryevuaosmhD0BTUahZ:o7rC8q4BQEy4gAlUahZ
MD5:	CA085FA787E0582020DCB817E45A8003
SHA1:	FEDF6CDE9ED9047E7899DD3B4E1B2E75EF6248A2
SHA-256:	C2691B43E248F35F496574DF9EEA8F64843EB335754FFD2F2E2848A12286B494
SHA-512:	0F1B66843EC7025150299D5A8EC307EA15A01A1609E33FBD649A104E503DFBCBB0BA160AD3E2E77540307FE9AD0B0506FE0525DE2C29E80FE3749B9C1291C20
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img1.wsimg.com/wrhs/browser-deprecation-warning/Chrome.png
Preview:	.PNG.....IHDR.....PLTE....Z#.Y.m`..A.L=..].t.H;4.c.xo.OB#.a.;..A..V.tk.>.].k..Z..X!.[.@.e[..W.ka.8..V.h].=..G.6.ka.<.F .Z).^..._.I.ri.oe).c._S.pg..G.A.qg.[O..a.c X.\P..C).k..D,.l5.s.~t.E.<.`U.;..B.=..J..?.M>..K.=..BL....A..]..DI...OC.NA.._.QE.SG..a..b!.d.K>..\..`N.....[..c.L@.I<..=..@.TG..B....RE..D..X..:..?$.f.PC.I;.J<.E7.N@.L?..P..A. .V.:....PD.....T..?..=.....S..@.RE.M@.E7..O.:....OB.WK.9..O.K>.J<...=....Q.....X.9....G:.F8...A....?.I:..g...C..j....H..?..:E....J.....aV..U.\Q.:@...8.....>4.A3p.....i..Kb..G..,.h ..J.PE.8.....7.9,.....O..M.;2..{..`..\.D8.A4.0.....D.`.._..]a\|US.T8.P!.M.yG.....I...y7.c..[s.XurQ.\D.H7.....b....C.z.yP.W.]T.S@.K;.C6....w..of..X~gJ.....S.....t.d. .V..Vs.R.<,.....EtRNS.....A.AA.X.'...XX.....C..40!..\|p...po.....2...\|.....IDATx..1j.@...]..y.a7B.B.D.6Ne..d4....\9!.\..\...s.\g...G.o.V....j...[.....C._2.....e...7..C..I..wM.....$K

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\arrows[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1500 x 600, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	15544
Entropy (8bit):	7.830892060370354

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\arrows[1].png	
Encrypted:	false
SSDEEP:	384:gH9eTHok3FZUG6SZhaQtDvcaiCjVpNLeQtf1cg:Cebokfn6SZhP8CxpNz1z
MD5:	72A92898F1DD7EA307CE6F2890D165F4
SHA1:	CF167FF00875385B08356A9E3B82C8930F019107
SHA-256:	8FCEB564C059D6FFAD5C8F3A5E5617A57D501C1E10DE1874357505831E2FDB4C
SHA-512:	14BFEDD1A64F62EF28D0A985FC525A0964BCCB8809878C9950813314C3831E6F4239C3AEDAB2912C2E7F18992CC593CC72BD3C963C76584821D9625389D364D
Malicious:	false
Reputation:	low
IE Cache URL:	http://d1lxhc4jvstzrp.cloudfront.net/themes/cleanPeppermint_7a82f1f3/img/arrows.png
Preview:	.PNG.....IHDR.....X.....Om.....tEXtSoftware.Adobe ImageReadyq.e<...(iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c145 79.163499, 2018/08/13-16:40:22 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:DocumentID="xmp.did:D3C817C4AD4111E981BCF119B51C018E" xmpMM:InstanceID="xmp.iid:D3C817C3AD4111E981BCF119B51C018E" xmp:CreatorTool="Adobe Photoshop CC 2017 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:AF76D76FB59311E68C42BF3A862DE99B" stRef:documentID="xmp.did:AF76D770B59311E68C42BF3A862DE99B"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>`.H.....PLTE111...ZZZ_./f....fj.U.....3@....)4.....Ual.\.X_.&4...Pa..e..C666.m.....+7..[mnY.8..{.hvwt\888.&3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\chevron-white[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 24 x 24, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	189
Entropy (8bit):	6.2222693012557855
Encrypted:	false
SSDEEP:	3:yionv//thPl5ljfRthwkBDsTBZt69/erFwEQDFcV7o5MU1/UARWm3125/GDvQoZL:6v/lhPZRnDspe2RGxcRoSsBRWmFC0blp
MD5:	B996E37F2AF75DB570F709C413F3251C
SHA1:	E1190674DE55B229F29BA9D61F0ABAB15958A442
SHA-256:	771371C2071711E80B64C41D28AB04287CD9DEB5F7CCBE5A1522827E9419DCCE
SHA-512:	587160189F46B2B5EAC2490D66FB2DAEF08F48F65791F275470A05EC3CA3188356CF39F9E0275E36B9CE3BF14068851F383219B980FD47A91B0EE4EB7692E81D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/domainads/images/chevron-white.png
Preview:	.PNG.....IHDR.....w=.....tEXtSoftware.Adobe ImageReadyq.e<..._IDATx.b`.H....~ N.....f..Z.....%.ij..P. >?j.%4..=..U....~Z.>..p..n.....5...5...\...../Q.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	179
Entropy (8bit):	5.067165111291868
Encrypted:	false
SSDEEP:	3:0SYWFFWIIYCNFSRI5XwDKLRIHDfFRWdFTfqzrZqcd+M+jgXNYARNin:0IFFNFS+56ZRWHTizlpd+M+cXFNin
MD5:	46FFF5C1AE13CAC68764A9BBF1B78C6B
SHA1:	3257E52A6E325355B6F596930457200988412 6FD
SHA-256:	2CA8E111AAE98F36D0F4671DBB9C6898627637AABA90A7626BDA425C28A4C35A
SHA-512:	6D8F5485A7C32E9F4AC2948CDAD2D077A693AAFDD258591E9F57927C59A6FF9206AA6615C3145A1ACFB01732C46A22BA1EE0306D671C4FCB63D5CE32EA4715 2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Poppins
Preview:	@font-face {. font-family: 'Poppins';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/poppins/v15/pxiEyp8kv8JHgFVrJJfedA.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\js3caf[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	7000
Entropy (8bit):	4.809324911486411
Encrypted:	false
SSDEEP:	192:wnS/jBKcACl3gC2z12a+hh9I3Dr+3SQ4sX5sU827yiQT+ddQ1:wS/jBKoBC2aQhKDy3SJs59ON1
MD5:	CCE7F943EC8E7B4BA13BE4ABA6B463D9
SHA1:	220F3E8CA723DAA91FD040CF518991A65F2BF110
SHA-256:	BA5B7354353B0EEC1637564DAE072FEE662A5B9862F6BF7ED5E60A5A76F2EF44

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\js3caf[1].js	
SHA-512:	5534D4EE216A7CBACE73E66D9BA9D36C78EEE2FEE0EFDD84A84042BD0DFCCFE0EC6BCF9CB6A6EC8968EE5EB252C865995BA9B730AE7E53F64167C0577A5181A5
Malicious:	false
Reputation:	low
IE Cache URL:	http://d1lxhc4jvstzrp.cloudfront.net/scripts/js3caf.js
Preview:	var pageLoadedCallbackTriggered = false;.var fallbackTriggered = false;.var formerCalledArguments = false;..var pageOptions = {. 'pubId': 'dp-teaminternet01',. 'resultsPageBaseUrl': '//parkingcrew.net/?ts=',. 'fontFamily': 'arial',. 'optimizeTerms': true,. 'maxTermLength': 40,. 'adtest': true,. 'clicktrackUrl': '//track.parkingcrew.net/track.php?',. 'attributionText': 'Ads',. 'colorAttribution': '#b7b7b7',. 'fontSizeAttribution': 16,. 'attributionBold': false,. 'rolloverLinkBold': false,. 'fontFamilyAttribution': 'arial',. 'adLoadedCallback': function(containerName, adsLoaded, isExperimentVariant, callbackOptions) {. if (!adsLoaded) {. try {. var ele = document.getElementById(container).getElementsByTagName('iframe')[0];. var vars = JSON.parse(ele.name.substr(ele.id.length + 1));. if (typeof vars[ele.id].type == "string" && vars[ele.id].type == "relatedsearch") {.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\prefetch.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):	18256
Entropy (8bit):	5.4611410543344
Encrypted:	false
SSDEEP:	384:3h3w2fnZjRL9Bd6Lkqs9TVH7yTA2EfySLSiVJgggcHZDAQKohqssAjok43Z3jsfs:C2f5B8kqs9TVbwf8ySLS0wYZMP6TsA4H
MD5:	2D35631C192E0E91A3FAB5801C810E63
SHA1:	9B12F867431789C8131BA3DE994184F2D3A41B18
SHA-256:	9131432B3DC3364C44F2C45C06F78535A3C03ABA3B59E3CCF444F541F10FD897
SHA-512:	4B2D5DF0E0CB2747FC8B5FC3CD7018C3E158F02F51587C22BFBCF4257FDA286A38D95864F749ACFF18A20E0B58BCE576B2C3958CB9169D682DFC2D5D66DB3C7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img6.wsimg.com/serp-assets/static/b9221d4/prefetch.min.js
Preview:	!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t():"function"==typeof define&&define.amd?define([],t):"object"==typeof exports?exports.prefetch=t():e.prefetch=t()}(window,(function(){return function(e){var t={};function n(a){if(t[a])return t[a].exports;var i=t[a]={i:a,l:!1,exports:{}};return e[a].call(i.exports,i,i.exports,n),i.l=!0,i.exports}return n.m=e,n.c=t,n.d=function(e,t,a){n.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:a})},n.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},n.t=function(e,t){if(1&t&&(e=n(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var a=Object.create(null);if(n.r(a),Object.defineProperty(a,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var i in e)n.d(a,i,function(t){return e[t]}.bind(null,i));return a},n.n=function(e){var t=e&&e.__esModule?function(){return

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\style-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):	1788
Entropy (8bit):	5.03810887574202
Encrypted:	false
SSDEEP:	24:tSeyZltD3OTbjfwigrzK3EZjqe1r7wPKb1iXR7KWMpnpfM1HKsC1uVaQku8pF:tSVuvfwi8z5QKpCSpK1qMgF
MD5:	3A39D6FF71EE3EBA907806A4DC3EB268
SHA1:	6253987B587709DE65C8F865D69B6E2E73BCDEC9
SHA-256:	1A029C78FCAA00ADD89F713FC8867099CA0028BEA0A925D9DB36D878E6E679F8
SHA-512:	085C9AEE72229A24936282DE43FFF93CD15695F65C987F9706FFF14C84130C7B5AA53E3048DAF1C8C8A10CD0B0EF335FD866DAC016159C38D95234F00F567EA3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img1.wsimg.com/wrhs/browser-deprecation-warning/style-ltr.css
Preview:	*,:after,:before{box-sizing:border-box}body,p{margin:0}body{background:#fff;color:#444;font-family:Helvetica,Arial,sans-serif}a:hover,a:link,a:visited{color:#09757a;text-decoration:none}a:hover{text-decoration:underline}a:active{color:#00a4a6}p{font-size:16px;line-height:24px}#content,#footer{min-width:840px}#card,#header-container{width:90%;margin-left:auto;margin-right:auto}#header{background-color:#d8efef;z-index:-1;padding-bottom:100px}#header-container{padding-top:24px}#banner{margin-bottom:48px}#banner>img{margin-top:7px;height:32px}h1,h2{color:#111}h1{font-family:serif;font-size:46px;line-height:56px;max-width:550px;margin:0 0 24px;letter-spacing:.01em}h2{margin:0 0 32px;font-weight:400}#card{margin-top:-64px;padding:32px;background-color:#fff;border:1px solid #d4dbe0;border-radius:4px}#card::after,#card::before{content:'';clear:both;display:table}#left,#right{float:left}#left{width:60%;max-width:570px}#right{width:40%;padding-left:32px;border-left:1px solid #d4dbe0}.pl #left{bo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\style[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	1417
Entropy (8bit):	4.785311295820333
Encrypted:	false
SSDEEP:	24:dvSFF9vW7UcfU5HKLUtFuac0PNTZpYj1qRbUJ9blQxkFzUzojULIbWNEc4DMk5Em:dvKHHK7ac0PNNJR49CkFW1w
MD5:	29952CF23B2A110A8085FBE5C29C14C0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\style[1].css	
SHA1:	CC0A7F1AD0A5B132821DBED19D593C98361C0CD0
SHA-256:	2E3C8229D7851FA3345FA481BA64B70590D92E466CBC4BCC3E9905AC27C80B2F
SHA-512:	2314407FD20B43DE1FAFDF10BAE22AAE7DFA28E50979EE708FDEF8FBDC9F247DE3445B64DA07C4D179061CF7FC5B21A694C4F4F328710FD59B891D9B3706FD9
Malicious:	false
Reputation:	low
IE Cache URL:	http://d1lxhc4jvstzrp.cloudfront.net/themes/cleanPeppermint_7a82f1f3/style.css
Preview:	* {margin:0;padding:0}..body {. background:#313131;. font-family: 'Poppins',sans-serif;. text-align: center;. font-size:1rem;.}...header {. padding:1rem 1rem 0;. overflow:hidden;.}..h1 {. color:#848484;. font-size:1.5rem;.}...wrapper1 {. margin:1rem;.}...wrapper2 {. background:url('img/bottom.png') no-repeat center bottom;. padding-bottom:140px;.}...wrapper3 {. background:#fff;. max-width:300px;. margin:0 auto 1rem;. padding-top:1px;. padding-bottom:1px;.}...onDesktop {. dis play:none;.}...tcHolder {. margin:1rem 4px 2rem;.}...adsHolder {. margin:1rem;. overflow:hidden;.}...searchHolder {. padding:1px 0 1px 1px;. margin:1rem auto;. background:#848484;.}...footer {. color:#949494;. padding:2rem 1rem;. font-size:.8rem;. margin:0 auto;. max-width:440px;.}...footer a:link,..footer a:visited {. col or:#949494;.}...wrapper1 .sale_link_bold a,..wrapper1 .sale_link a {. color:#ccc;.}...wrapper1 .sale_link_b

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\uxcore2.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	90042
Entropy (8bit):	5.070655574429959
Encrypted:	false
SSDEEP:	1536:Bc1PynrFaeNWqSre6e8XGxD/3SYiLENM6HN266:BEe6e1xD/3SYiLENM6HN266
MD5:	B6683F140400D49BACF0387C2D4465B1
SHA1:	8F8F2A999861D7B9687CE2C1D3EA1FC406AD299D
SHA-256:	314FF74DECDAE2F0E60596988559C63C81A6FD90DFEF9129614BFCE8CD645AE0
SHA-512:	C2264AD4318FB24CF50700DE812D05F797C23C6677AEBDC8366BA602C46DB0E54C563D59730572B47389A18AFDEF5E60539A94C36507CD18F5892F895529C60E
Malicious:	false
Reputation:	low
Preview:	:root{--uxp-font-weight-normal:500;--uxp-font-weight-semibold:600;--uxp-font-weight-bold:700}*,::after,::before{box-sizing:border-box}html{font-family:sans-serif;line-height:1.15;-webkit-text-size-adjust:100%;-ms-text-size-adjust:100%;-ms-overflow-style:scrollbar;-webkit-tap-highlight-color:transparent}article,aside,figcaption,figure,footer,header,hgroup,main,nav,section{display:block}body{margin:0;font-family:gdsherpa,Helvetica,Arial,sans-serif;font-size:1rem;font-weight:var(--bxjxgl,500);line-height:1.5rem;color:#111;text-align:left;background-color:#fff;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale}[tabindex="-1"]:focus{outline:0!important}hr{box-sizing:content-box;height:0;overflow:visible}h1,h2,h3,h4,h5,h6{margin-top:0;margin-bottom:.5rem}p{margin-top:0;margin-bottom:1.5rem;font-size:1rem;line-height:1.5rem}abbr[data-original-title],abbr[title]{-webkit-text-decoration:underline;text-decoration:underline;-webkit-text-decoration:underline dotted;text-decoratio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\YaMN4Oy8AhH-iW3da0J-Nuczn6meMMc-yumwdmwIUIQ[1].js	
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):	21984
Entropy (8bit):	5.5594185274243
Encrypted:	false
SSDEEP:	384:T7PhU5RRSU8QcV74RNeiDhSnK2XYylSohrNsHKTqM0s+LbYHiw52hK0Ud:HkRTcV0ZQNUqShK4QTd
MD5:	C3B7FD6FD68E34D3619107F3C29921D8
SHA1:	91E1FB9AF705728CF2B995E7058B5B8D362F27E2
SHA-256:	61A30DE0ECBC0211FE896DDD6B427E36E7339FA99E30C73ECAE9B0766C085084
SHA-512:	1821103406952E044454C250419656318B5BEB89D70522A154E8016BBD7596763373777AA2EA0A043E47449EBB204CC13D81E59EC24196F8A82F7C3525BC77D1
Malicious:	false
Reputation:	low
Preview:	(function(){var J=function(Q,l){if(!(l=(Q=null,v).trustedTypes,l)||!l.createPolicy)return Q;try{Q=l.createPolicy("bg",{createHTML:r,createScript:r,createScriptURL:r})}catch(h){v.console&&v.console.error(h.message)}return Q},r=function(Q){return Q},v=this||self;(0,eval)(function(Q){return(Q=J())&&1===eval(Q.createScript("1"))?function(l){return Q.createScript(l)}:function(l){return""+l}})(Array(7824*Math.random()|0).join("\n")+'(function(){var QX,m=function(Q,l){return(l=typeof Q,"object")==l&&null!=Q||"function"==l},R=this||self,lo=function(Q,l){return l<Q?-1:l>Q?1:0},vB=function(Q,l){function v(){}((Q.prototype=(Q.U5=(v.prototype=l.prototype,l).prototype,new v),Q).prototype.constructor=Q,Q).D$=function(h,H,r){for(var J=Array(arguments.length-2),U=2;U<arguments.length;U++)J[U-2]=arguments[U];return l.prototype[H].apply(h,J)}},rg=function(Q){for(Q=0;64>Q;++Q)Z[Q]="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789-_".charAt(Q),B["ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\YaMN4Oy8AhH-iW3da0J-Nuczn6meMMc-yumwdmwIUIQ[2].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):	21984
Entropy (8bit):	5.5594185274243
Encrypted:	false
SSDEEP:	384:T7PhU5RRSU8QcV74RNeiDhSnK2XYylSohrNsHKTqM0s+LbYHiw52hK0Ud:HkRTcV0ZQNUqShK4QTd
MD5:	C3B7FD6FD68E34D3619107F3C29921D8
SHA1:	91E1FB9AF705728CF2B995E7058B5B8D362F27E2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\YaMN4Oy8AhH-iW3da0J-Nuczn6meMMc-yumwdmwIUIQ[2].js	
SHA-256:	61A30DE0ECBC0211FE896DDD6B427E36E7339FA99E30C73ECAE9B0766C085084
SHA-512:	1821103406952E044454C250419656318B5BEB89D70522A154E8016BBD7596763373777AA2EA0A043E47449EBB204CC13D81E59EC24196F8A82F7C3525BC77D1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/js/bg/YaMN4Oy8AhH-iW3da0J-Nuczn6meMMc-yumwdmwIUIQ.js
Preview:	(function(){var J=function(Q,l){if(!(l=(Q=null,v).trustedTypes,l)||!l.createPolicy)return Q;try{Q=l.createPolicy("bg",{createHTML:r,createScript:r,createScriptURL:r})}catch(h){v.console&&v.console.error(h.message)}return Q},r=function(Q){return Q},v=this||self;(0,eval)(function(Q){return(Q=J())&&1===eval(Q.createScript("1"))?function(l){return Q.createScript(l)}:function(l){return""+l}})(Array(7824*Math.random()|0).join("\n")+'(function(){var QX,m=function(Q,l){return(l=typeof Q,"object")==l&&null!=Q||"function"==l},R=this||self,lo=function(Q,l){return l<Q?-1:l>Q?1:0},vB=function(Q,l){function v(){}((Q.prototype=(Q.U5=(v.prototype=l.prototype,l).prototype,new v),Q).prototype.constructor=Q,Q).D$=function(h,H,r){for(var J=Array(arguments.length-2),U=2;U<arguments.length;U++)J[U-2]=arguments[U];return l.prototype[H].apply(h,J)}},rg=function(Q){for(Q=0;64>Q;++Q)Z[Q]="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789-_".charAt(Q),B["ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\favicon-32x32[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	933
Entropy (8bit):	7.678718677370292
Encrypted:	false
SSDEEP:	12:6v/7ioSOdCKR5lNakbwQ/2xHFXhNOMPgZvCJmydAv/A2eVd5vuNzbxufojRWrWyG:QLp0ZF//Jt/7d5+fR8W4gQU72Yz
MD5:	8F5AF0AB459E5D5174640F2374392B4B
SHA1:	3F756A9A7197F6802CE255A552BA122815EEAF9E
SHA-256:	C6670425515377D60B8AECE9B9135B29A0BC0F67C11F7B06959D4985DFD24687
SHA-512:	D06F8B16FA8F1234EA994C6DFBD831ACE368751DFEF35A524269E1E3FAB68DFA01D686950AE5AD7AC8E515618566E88C5463C3CD1FA12448248B6E959BE11B6A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img6.wsimg.com/ux/favicon/favicon-32x32.png
Preview:	.PNG.....IHDR... ... .szz....IIDATx.....%Y...g.m.m..n....w...m.=.5.N..TN../.....'...42...R.{p.N@A.....F9w.R..N..Y....e(.F.A;..c\.1.....)S.q.yV..x..`)Tb<..Y...#7.+...`...P.....&.bR.1m.S[5V.d.ze....K....(vc.p4..d.....b.j....\..P..0i.C.L.X..ix..)..!h..V(.....N..I...0..3.]......Q.?.|.$.T..I'...[.[.....&H*B}...);x.\.^..Q`..".&Hz..`X.kS4.Aa.k...&..Q8(....v..)...O. .b.z`t.^...a.....4..?<A.<.>.T..q...^..,.j'.8s...:/'h~..t.)..S..p..(0..e8'.|...0.G..K.<&.7Y..5.^..^.YQ....x8...L.....G.....0y=.yX.....g.R..`p.....s..c..w....{....?..,.\.^.....>...Kp>|..p.....0.(V.hLpS~el...M...y.T.=....t.P.*..{3.Q.Kx...`.."3....38...X.j.....z{&<l.....G....C2..C...Z.....!a.c.q{...0.'fp.'....p.j.z<..?....n...n.f...l}.%J<....>.~...~.>..C..*.F.K.AyN...u..7.7....a.,..G&.;.m`.j.....s....`.d...=4..}G.!...(.9.1.Md.b.....i..u.q.2!....p@.....h..X...N..x.G.....8...V.L.....j...K."........IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\find[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	342424
Entropy (8bit):	5.373746750030165
Encrypted:	false
SSDEEP:	6144:ZY27Rdq3Q+eCol1d030va+5zZEZ09RcWzl7R5ZS5/MlpO3ZrYpO5U97Z0Jmp8IDa:GAMp0va+5zZEZ09RcWZ7R5ZS5/MlpO3j
MD5:	A04BDBCF8B884E2D173AFD49DDD971A4
SHA1:	C9D7CAA44A0081E2DF93615E230E8DFBEC4B1ABE
SHA-256:	7F8757B99AE3B26456C20F71387DF83A7D137647C764D0CF497BF3C4EBE933FF
SHA-512:	6D6593DD7BA13859E0D11F88D661898F943E8532FDE05DB8562ADBB4E818DBA37E372FE82BB147976EE28E0C5A6F1F6D2F0324414E4D90A0BBC3EB58B69EE32C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ch.godaddy.com/domainsearch/find?checkAvail=1&domainToCheck=flowvinconsortium.com
Preview:	<!DOCTYPE html><html lang="de" dir="ltr"><head><meta http-equiv="content-language" content="de-CH"/><meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no"/><meta http-equiv="x-ua-compatible" content="IE=edge"/><meta name="format-detection" content="telephone=no"/><meta name="google-site-verification" content="odAW2IckEFXrJjMrVxmnpjRPGNxEJp_xnCb7iBydgBY"/><meta name="msvalidate.01" content="9D246CEFA0D8894D78306DF6FBA618D9"/><meta name="robots" content="noindex"/><meta name="verify-v1" content="dV1r/ZJJdDEI++fKJ6iDEl6o+TMNtSu0kv18ONeqM0I="/><meta name="y_key" content="1e39c508e0d87750"/><meta name="description" content="Zahle weniger f.r Domainnamen. Mengenpreise und Optionen f.r die Registrierung privater Domainnamen. .bertrage Domainnamen risikofrei."/><script id="set-enhancement-id">. (function(){. let enhancement = { id: 'fast' };. const values = ['downlink', 'downlinkMax', 'effectiveType', 'rtt', 'saveData', 'typ

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\sale_form[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	761
Entropy (8bit):	4.695768067919445
Encrypted:	false
SSDEEP:	12:UeKpKct5WuSz7inigFM7xKlwoGEk5Cs+rTKESJ1nHmdUTAcUGslAfC:OpRt5WZjgFm24rCAJAdUTIGslA6

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\sale_form[1].js	
MD5:	64F809E06446647E192FCE8D1EC34E09
SHA1:	5B7CED07DA42E205067AFA88615317A277A4A82C
SHA-256:	F52CBD664986AD7ED6E71C448E2D31D1A16463E4D9B7BCA0C6BE278649CCC4F3
SHA-512:	5F61BBE241F6B8636A487E6601F08A48BFFD62549291DB83C1F05F90D26751841DB43357D7FE500FFBA1BC19A8AB63C6D4767BA901C7EDED5D65A1B443B1DD78
Malicious:	false
Reputation:	low
IE Cache URL:	http://c.parkingcrew.net/scripts/sale_form.js
Preview:	/*. * Sales form click tracker. *. * tlink() will load a 1x1 GIF to track clickouts to the contact form. * Some basic scrambling prevents (a lot of) web scrapers to follow the link. *. * Date: 2016-03-22.*/..// function tlink(v, wow).// v is a fixed string.// wow will contain the current domain name.function tlink(v, wow) {. if (document.location.search.indexOf('_xas') === -1) {. // define some compenents that will later form the link to the 1x1 GIF. var proto_suf = "tp",. string = "omainb",. parameter = "php?salelink=1";. // generate and load the 1x1 GIF. new Image().src= "ht" + proto_suf + ":" + "//" + "ww" + "w.myd" + string + "uy.com/sale_form." + parameter + "&dom" + "ain_name=" + wow;. }.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\Edge[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 128 x 128, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	11004
Entropy (8bit):	7.938351001240865
Encrypted:	false
SSDEEP:	192:wHGMybOMvKRZhUOhv30dSQ6NCDfdVv7HqWKw8CxwVE3bZX:wmAdZhUSv3YyGVv/b8KwVo
MD5:	D666A5613A6300B940300F93E78A3D62
SHA1:	6ABAF534C46B416F7472B6D4801BF791E7C906FB
SHA-256:	1421D289378C5B372D0939645432DB8EA3FD9402D8850A47A68A1BA7F7FAEC77
SHA-512:	2612097C7DE37C2AB6B5B73AD55C6C2406053FA8A7A9084010B98A3E9A671FC37E32240362CF242C78AC8891FD52B1D6C86E4BBD6CCDE799EB32FEAEF2F0A75
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img1.wsimg.com/wrhs/browser-deprecation-warning/Edge.png
Preview:	.PNG.....IHDR.....>a...*.IDATx^.}..]Wy.....n.dK^.....1..2.....b....{. 3....c..fB...T..!)....L..2v.....U.eKj-.V.[.....:...-.%...>.=*.....g.+...7.}.4S=G...p..x..c.;Z..`5@....Z.I.....t....{..VE.....?.....*/{..a.#'.d.....s..o..Ab[.c.+.%}1..<.....D..\....u..e.k...9u.3..\....2.w.p&` ..../.*.I.E..,I.....fz.....0.r...5.k.j.....,.N..}.6.....E....)...`.y.m.....p..x..g;.....=..%..x...KA..R./?_.{.A.W.R.....&.4.k6..j...5...%Mf=3"p.,:3k.....,.;.O...-Y..%P*/..].[..{.v...GnZ..s.....r....=. ..d ..`..rW...H .@.p.o2.....W.}....o...dx....l..M.w..q@.#D.....\..t.DH.{p.{.]..=.E."...8.>.8=B.,.y.I....S?p..-..~..;../..2..)~.....U....uX.0....eMv],.`.....P...$O.h..,r.....%.}...?...e.W...`.UO|.M....Ldq7..80=..9.u...UB.....)i...D.1d"pb.,...D....!A.d(....?t..[..|.+.....8@.d.....{...1.....!..."AD.B<..t..=.k.q.....M....W..._a.c~.#.....S...&B/...s....W ..- ....q....`..e."..*..S..5...._...`...40.C...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\FCO7OGE7.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	11048
Entropy (8bit):	5.8435318896431
Encrypted:	false
SSDEEP:	192:TiRfrHulcVZyziimI6yMyTQdjb0ErsW99iP2JW0eOG1HjlAhSC37D:TiRK6/yCI6yMJdjb0Er8eJW51HjlOn3X
MD5:	4D947CCBE1F0E51BA2B0C23C401B82A0
SHA1:	441EA3948D57DDEB09EE9B8AD038E99465CD4A88
SHA-256:	AB57F8F0B8A6E2F4ADB96D8C2581F99DC3495CDAB15EC68344B8A81A666A4B08
SHA-512:	C4C34C2C1206216A30DDA54DAB81962EC83C085851E5001FF0ABBA59FA8AF7BC1D4961D5F88836B1A8195D4DE7C4FE7A0A66F1ACA557BD3519E22DF67B2B64A7
Malicious:	false
Reputation:	low
IE Cache URL:	http://ww38.flowvinconsortium.com/
Preview:	<!DOCTYPE html>.<html data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBALquDFETXRn0Hr05fUP7EJT77xYnPmRbpMy4vk8KYiHnkNpednjOANJcaXDXcKQJN0nXKZJL7TciJD8AoHXK158CAwEAAQ==_fNNQ6VbKrjBpx6z/zwNCEfShkGBDmj9vEwmJLlKcPelTaGWGUTEKksn3A3DvxIhpwHcn0YAfak6NEddg2WnyPA==" xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">.<head>..<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>. <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />. <title>flowvinconsortium.com</title>..<script src="//www.google.com/adsense/domains/caf.js" type="text/javascript" ></script>..<link href="//d1lxhc4jvstzrp.cloudfront.net/themes/assets/style.css" rel="stylesheet" type="text/css" media="screen" />..<link href="//d1lxhc4jvstzrp.cloudfront.net/themes/cleanPeppermint_7a82f1f3/style.css" rel="stylesheet" type="text/css" media="screen" />..<link href="https://fonts.googleapis.com/css?family=Poppins:300" rel="stylesheet">..<meta name="description " content=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\ads[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):	10871
Entropy (8bit):	6.14974479329824
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\ads[1].htm	
SSDEEP:	192:X2gDhWHy12N4M+UbfZmhBykjmy3eOrLMcQwkL:GkHfM+UbRm2MMcJkL
MD5:	BF66B07A84A3D8B49B8B66C98B323A69
SHA1:	389244B14C89A693B3D4B4ACC45F7C4ED67FA679
SHA-256:	F9A4A9C94E8190090FEF020E8593825F9C32DECBFE3D7E5E8FAE579E69BBE282
SHA-512:	13A2B33F0B748A5278917E46A1A08594900BCB6B251219E4FB0E2325FC2EEB755697D2448B7E53DD38CF030930918B8CFE732BFEBA2A9EFB55E9F8C7FEA65786
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/dp/ads?max_radlink_len=40&r=m&cpp=0&client=dp-teaminternet09_3ph&channel=000001%2Cbucket106&hl=en&adtest=off&type=3&pcsa=false&swp=as-drid-2986208149972408&uiopt=true&oe=UTF-8&ie=UTF-8&fexp=21404%2C17300441%2C17300443%2C17300494%2C17300496%2C17300584%2C17300586&format=r5%7Cs&num=0&output=afd_ads&domain_name=ww38.flowvinconsortium.com&v=3&adext=as1%2Csr1&bsl=8&u_his=1&u_tz=-480&dt=1610629337018&u_w=1280&u_h=1024&biw=767&bih=554&psw=767&psh=877&frm=0&uio=ff2sa16fa2sl1sr1-st24sa14lt34-&cont=tc&csize=w522h0&inames=master-1&jsv=15753&rurl=http%3A%2F%2Fww38.flowvinconsortium.com%2F
Preview:	<!doctype html><html lang="en-GB"> <head> <meta content="NOINDEX, NOFOLLOW" name="ROBOTS"> <meta content="telephone=no" name="format-detection"> <meta content="origin" name="referrer"> </head> <body> <script nonce="daJ5qwojLWD1D6CTtfW5OA==">window.IS_GOOGLE_AFS_IFRAME_ = true;function populate(el) { var adBlock = document.getElementById("adBlock"); adBlock.innerHTML += el;}.var IS_GOOGLE_AFS_IFRAME_ = true;.var ad_json = {"caps":[{"n":"queryId","v":"SsL_X9epA9mgmAfbpaGgCg"},{"n":"isLtr","v":"t"},{"n":"popstripeRs","v":"#1F8A70,#BEDB39,#FFE11A,#FD7400,#004358"}],"iaa":{"t":"Ad","b":"Ads"},"bg":{"i":"https://www.google.com/js/bg/YaMN4Oy8AhH-iW3da0J-Nuczn6meMMc-yumwdmwIUIQ.js","p":"RPi806fAVA4UdJ0QMHAynQWLiNJDUdD9WDgebJAAWDCUZkLNXX/ZrNn6ccdLD/43byNXLxcUiOHTcMl7+OO1Hb0LEsripqRye6N1BnJEfr6oLTenz/QNCb5BMaZizNaWNRSLoUMSlY+34z3CF1jFVn35oYc7SItTOGbqkgMd09pJl5dOYG4fwHS0iPX/X2W/Snynuzj52MFs46Ucfj22ka8gTD9xb7OL4rljl0LvNHuXpYL81fCshkmZyt6J9+n2h8BQDo1VPdgOsVwEMFlxo1e8hE

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\client-search-page.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	125675
Entropy (8bit):	4.996838413233634
Encrypted:	false
SSDEEP:	768:mVm2+iy+TBKQk+0MewZajl4l6dr+pa/79jPFccEoYLa73KPy4YGbbC1XbgV8Fkrb:72+D7wG4l6dr+pa/79IrHws2n+0o5s/6
MD5:	CFF440355801CAFEAEA78090275B5860
SHA1:	8D7BB9DA1DA6C50DE451C2797EF3E4A9B7A87187
SHA-256:	C80D272C36AACB232CBE519E7B0381C8E566CC1A1B3C1234BAC1B52B1B9E3F83
SHA-512:	3C4AF469CEC766D08E4DB556B14BCDEAAA65412EAF9C7667D00B49366E75CF0938A6050BC4CF761C89E08462B510A34F607205CF95690B1ACC5F685B3187280
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://img6.wsimg.com/serp-assets/static/b9221d4/client-search-page.min.css
Preview:	:root{--uxp-font-weight-normal:500;--uxp-font-weight-semibold:600;--uxp-font-weight-bold:700}@use "sass:map";.dpp-results .exact-match{margin-bottom:20px}.dpp-results .spins-header{margin:20px 0}.dpp-results .cross-sell-container .cross-sell-wrap,.dpp-results .domain-result{float:left;min-width:290px;padding:10px 20px;vertical-align:middle;width:99%}.dpp-results .cross-sell-container .cross-sell-wrap .domain-name,.dpp-results .domain-result .domain-name{display:inline-block;vertical-align:top;word-break:break-all}.dpp-results .cross-sell-container .cross-sell-wrap .domain-name .hidden-break-1:before,.dpp-results .domain-result .domain-name .hidden-break-1:before{content:"\A"}.dpp-results .cross-sell-container .cross-sell-wrap .domain-name .domain-name-text,.dpp-results .domain-result .domain-name .domain-name-text{text-transform:lowercase;line-height:100%}.dpp-results .cross-sell-container .cross-sell-wrap .domain-name .tooltip-wrap,.dpp-results .domain-result .domain-name .tooltip-wra

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	183
Entropy (8bit):	5.149011623222219
Encrypted:	false
SSDEEP:	3:0SYWFFWIIYCNFSRI5XwDKLRIHDfFWYhfqzrZqcd+58d1gqdJtDQUYARNin:0IFFNFS+56ZzhizIpd+Gdeqd7JNin
MD5:	C8EF962B45D389627349DCA20FF07173
SHA1:	F5C9F3102E8258DB46005D9518E37F41339A1D0B
SHA-256:	7CF8B1AFE7BD63D68B7693798541404FC4DD9E962005D24A32F3B33E1EC72288
SHA-512:	131A8B9D6E32A63F42FC12FBC2BAC0C9CDE15E166C5DDBFC793EA5992D1ED67BBAEDFAE3B643FC0874A9289EB04CF69AEFC09B64DF99D6A043B2F3AF45B5C85D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Poppins:300
Preview:	@font-face {. font-family: 'Poppins';. font-style: normal;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/poppins/v15/pxiByp8kv8JHgFVrLDz8Z1xlEw.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\pxiByp8kv8JHgFVrLDz8Z1xlEw[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 10504, version 1.1
Category:	downloaded
Size (bytes):	10504

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\pxiByp8kv8JHgFVrLDz8Z1xlEw[1].woff	
Entropy (8bit):	7.94478537149278
Encrypted:	false
SSDEEP:	192:QfEodsD0GBYNXGNpEg/cKhMTcWRCD0Y6MSPUakMo8Hpia8f8D3C3IBH0ZRvz9/y:QfEom7BYNWP7hicWwoYmPUakMKae3l5h
MD5:	081C758544B2BD948EB5D9CC419A597E
SHA1:	E81D58D009D6B57A3ABC3A8FE9C26845C1F9D54B
SHA-256:	8E14553C0CA1D74DCD39B12E0DE5815C599710BEB7E2EAE43BA4FE6B6628D66D
SHA-512:	94F245D9B06D7235A91F23A063B15DBA416833C9A3AB482EF09C242C2CA6527B94BBDCE6D273C40BAAA126F5E468B118FB417464C550A94B3AED0A8E3A09D25 6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/poppins/v15/pxiByp8kv8JHgFVrLDz8Z1xlEw.woff
Preview:	wOFF.....).....? .....GPOS..... ... DvLuGSUB...<.....0.H'kOS/2...I...N...`Y...cmap.....glyf...P.. 5..3bAd.head.."....6...6..$Yhhea.."........$....hmtx.."........h.( mloca..$.....e.xmaxp..&.... ... .\.1name..&.....&e?bpost..'....g.....]s.....DFLT.....x.c`d``.b.a.c`vq..a.II-3b.....r.,.@..?.....<....x.c`a.a.a`e``.b.```...q.F...@.....H.3..... (..E.),.L.....ArLJL{.....m..x.c```.bf ....`.....aP..x.,^:.....L{..1.b.. . . .....`..FQIIHI.....[.T..W-. . .Vm.....?...?.....}.`...6=X.`.Y.&>....{G.."....5..x.Z.`....]....B...X.m...S.,[V. ...16.tL/)tx.?.'.'.....IOH...4.K..5.....;I.....t7.;;;;....t...Kr..P.....eI..X*...8K(....4|.{..'N.C'..8A.;.....X.%....A..i2....H .d..zF.#..!;3.2I...#.....q.....@...>..A_!.....S.S....*.{.....!.....y ....2 .w...`.pP.L.N..nU8....._._.o=i.....'adk.A...T.*.....X.+-.399.,....t..nd@.* b...q.^...A.....@...h0..V6.O.gT3.&#{.....e..b..7L..T.&aqvq.

C:\Users\user\AppData\Local\Temp\~DF0F7B05318EB42C76.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4803416098390057
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loqrF9loqR9lWqkGWUT44jc:kBqoItrLhyc
MD5:	D32658E008948C680FB7775257AC4F9F
SHA1:	A6A924638560D097911E72E470FCB12ABAC13449
SHA-256:	5255511792A4FB881C3FEBF51559B6ECCC8843AA7BFF032F9DC7CCD5648EF1AD
SHA-512:	1190D3BCCC15558297B2D10B294503F4F7650F068B640807D51F5C621E91564FC33251F44D55C09E832F38A6AB266FCC0AE1B9446E3B2B2BDEF36215B38B36DF
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF111C5866DED673E5.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\~DF404FE72635615315.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	68110
Entropy (8bit):	1.7192020176285407
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+qMWfM4fjJFJ6JEJgoJEJejJFJ6JEJEoJEJ2s6RjPt:ELU2mo20LU2qo269l
MD5:	4CDBD46F5E3BA9B51B0524D6ED48BEDE
SHA1:	A7507F6C328FAD09E99935F83BB5DEAA27F601FC

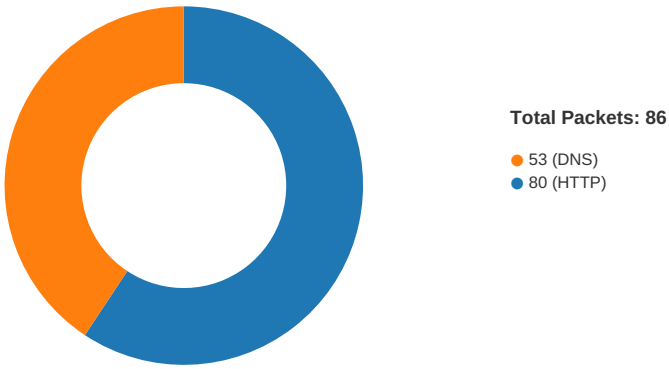
C:\Users\user\AppData\Local\Temp\~DF404FE72635615315.TMP	
SHA-256:	B114BBE340A9F7F5940AA83F273BFE0F2B49580F7AED28B6FAB6E84A1BA31CF8
SHA-512:	259187DDB2C3778F0E2922E91A9FE550045E64202528DFCC4EDDA7EA70758F6E67549CC9C33AF1E973EE27168930B5BEF0D68BA233BEEB1F7390CB695EAD30E0
Malicious:	false
Reputation:	low
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
Jan 14, 2021 05:02:16.231739044 CET	49714	80	192.168.2.3	103.224.212.220
Jan 14, 2021 05:02:16.231976986 CET	49715	80	192.168.2.3	103.224.212.220
Jan 14, 2021 05:02:16.416845083 CET	80	49714	103.224.212.220	192.168.2.3
Jan 14, 2021 05:02:16.416882038 CET	80	49715	103.224.212.220	192.168.2.3
Jan 14, 2021 05:02:16.416959047 CET	49714	80	192.168.2.3	103.224.212.220
Jan 14, 2021 05:02:16.416975975 CET	49715	80	192.168.2.3	103.224.212.220
Jan 14, 2021 05:02:16.417823076 CET	49714	80	192.168.2.3	103.224.212.220
Jan 14, 2021 05:02:16.610672951 CET	80	49714	103.224.212.220	192.168.2.3
Jan 14, 2021 05:02:16.610712051 CET	80	49714	103.224.212.220	192.168.2.3
Jan 14, 2021 05:02:16.610795021 CET	49714	80	192.168.2.3	103.224.212.220
Jan 14, 2021 05:02:16.610862017 CET	49714	80	192.168.2.3	103.224.212.220
Jan 14, 2021 05:02:16.618272066 CET	49714	80	192.168.2.3	103.224.212.220
Jan 14, 2021 05:02:16.690433025 CET	49716	80	192.168.2.3	76.223.26.96
Jan 14, 2021 05:02:16.690759897 CET	49717	80	192.168.2.3	76.223.26.96
Jan 14, 2021 05:02:16.730582952 CET	80	49716	76.223.26.96	192.168.2.3
Jan 14, 2021 05:02:16.730622053 CET	80	49717	76.223.26.96	192.168.2.3
Jan 14, 2021 05:02:16.730737925 CET	49717	80	192.168.2.3	76.223.26.96
Jan 14, 2021 05:02:16.730767012 CET	49716	80	192.168.2.3	76.223.26.96
Jan 14, 2021 05:02:16.731435061 CET	49716	80	192.168.2.3	76.223.26.96
Jan 14, 2021 05:02:16.771382093 CET	80	49716	76.223.26.96	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 05:02:16.803668022 CET	80	49714	103.224.212.220	192.168.2.3
Jan 14, 2021 05:02:16.904169083 CET	80	49716	76.223.26.96	192.168.2.3
Jan 14, 2021 05:02:16.904220104 CET	80	49716	76.223.26.96	192.168.2.3
Jan 14, 2021 05:02:16.904263020 CET	80	49716	76.223.26.96	192.168.2.3
Jan 14, 2021 05:02:16.904300928 CET	80	49716	76.223.26.96	192.168.2.3
Jan 14, 2021 05:02:16.904330969 CET	80	49716	76.223.26.96	192.168.2.3
Jan 14, 2021 05:02:16.904365063 CET	49716	80	192.168.2.3	76.223.26.96
Jan 14, 2021 05:02:16.904424906 CET	49716	80	192.168.2.3	76.223.26.96
Jan 14, 2021 05:02:16.904436111 CET	49716	80	192.168.2.3	76.223.26.96
Jan 14, 2021 05:02:16.924796104 CET	80	49716	76.223.26.96	192.168.2.3
Jan 14, 2021 05:02:16.924905062 CET	49716	80	192.168.2.3	76.223.26.96
Jan 14, 2021 05:02:17.053824902 CET	49718	80	192.168.2.3	13.224.89.16
Jan 14, 2021 05:02:17.054672956 CET	49719	80	192.168.2.3	13.224.89.16
Jan 14, 2021 05:02:17.056523085 CET	49722	80	192.168.2.3	13.224.89.16
Jan 14, 2021 05:02:17.099670887 CET	80	49718	13.224.89.16	192.168.2.3
Jan 14, 2021 05:02:17.099798918 CET	49718	80	192.168.2.3	13.224.89.16
Jan 14, 2021 05:02:17.100193024 CET	49718	80	192.168.2.3	13.224.89.16
Jan 14, 2021 05:02:17.100925922 CET	80	49719	13.224.89.16	192.168.2.3
Jan 14, 2021 05:02:17.101033926 CET	49719	80	192.168.2.3	13.224.89.16
Jan 14, 2021 05:02:17.101524115 CET	80	49722	13.224.89.16	192.168.2.3
Jan 14, 2021 05:02:17.101639986 CET	49722	80	192.168.2.3	13.224.89.16
Jan 14, 2021 05:02:17.103605986 CET	49722	80	192.168.2.3	13.224.89.16
Jan 14, 2021 05:02:17.145179987 CET	80	49718	13.224.89.16	192.168.2.3
Jan 14, 2021 05:02:17.145482063 CET	80	49718	13.224.89.16	192.168.2.3
Jan 14, 2021 05:02:17.145576000 CET	49718	80	192.168.2.3	13.224.89.16
Jan 14, 2021 05:02:17.145657063 CET	80	49718	13.224.89.16	192.168.2.3
Jan 14, 2021 05:02:17.145750046 CET	49718	80	192.168.2.3	13.224.89.16
Jan 14, 2021 05:02:17.147003889 CET	49719	80	192.168.2.3	13.224.89.16
Jan 14, 2021 05:02:17.148603916 CET	80	49722	13.224.89.16	192.168.2.3
Jan 14, 2021 05:02:17.148916960 CET	80	49722	13.224.89.16	192.168.2.3
Jan 14, 2021 05:02:17.148962975 CET	80	49722	13.224.89.16	192.168.2.3
Jan 14, 2021 05:02:17.148988008 CET	49722	80	192.168.2.3	13.224.89.16
Jan 14, 2021 05:02:17.149004936 CET	80	49722	13.224.89.16	192.168.2.3
Jan 14, 2021 05:02:17.149030924 CET	49722	80	192.168.2.3	13.224.89.16
Jan 14, 2021 05:02:17.149048090 CET	80	49722	13.224.89.16	192.168.2.3
Jan 14, 2021 05:02:17.149070978 CET	49722	80	192.168.2.3	13.224.89.16
Jan 14, 2021 05:02:17.149101973 CET	80	49722	13.224.89.16	192.168.2.3
Jan 14, 2021 05:02:17.149106026 CET	49722	80	192.168.2.3	13.224.89.16
Jan 14, 2021 05:02:17.149147034 CET	80	49722	13.224.89.16	192.168.2.3
Jan 14, 2021 05:02:17.149163008 CET	49722	80	192.168.2.3	13.224.89.16
Jan 14, 2021 05:02:17.149178982 CET	80	49722	13.224.89.16	192.168.2.3
Jan 14, 2021 05:02:17.149205923 CET	49722	80	192.168.2.3	13.224.89.16
Jan 14, 2021 05:02:17.149247885 CET	49722	80	192.168.2.3	13.224.89.16
Jan 14, 2021 05:02:17.151091099 CET	49725	80	192.168.2.3	185.53.178.30
Jan 14, 2021 05:02:17.151138067 CET	49726	80	192.168.2.3	185.53.178.30
Jan 14, 2021 05:02:17.192121983 CET	80	49726	185.53.178.30	192.168.2.3
Jan 14, 2021 05:02:17.192173004 CET	80	49725	185.53.178.30	192.168.2.3
Jan 14, 2021 05:02:17.192298889 CET	49726	80	192.168.2.3	185.53.178.30
Jan 14, 2021 05:02:17.192305088 CET	49725	80	192.168.2.3	185.53.178.30
Jan 14, 2021 05:02:17.192902088 CET	80	49719	13.224.89.16	192.168.2.3
Jan 14, 2021 05:02:17.193253040 CET	80	49719	13.224.89.16	192.168.2.3
Jan 14, 2021 05:02:17.193322897 CET	49719	80	192.168.2.3	13.224.89.16
Jan 14, 2021 05:02:17.193705082 CET	80	49719	13.224.89.16	192.168.2.3
Jan 14, 2021 05:02:17.193766117 CET	49719	80	192.168.2.3	13.224.89.16
Jan 14, 2021 05:02:17.232400894 CET	80	49726	185.53.178.30	192.168.2.3
Jan 14, 2021 05:02:17.232458115 CET	80	49725	185.53.178.30	192.168.2.3
Jan 14, 2021 05:02:17.232547998 CET	49725	80	192.168.2.3	185.53.178.30
Jan 14, 2021 05:02:17.272322893 CET	80	49725	185.53.178.30	192.168.2.3
Jan 14, 2021 05:02:17.272573948 CET	80	49725	185.53.178.30	192.168.2.3
Jan 14, 2021 05:02:17.272649050 CET	49725	80	192.168.2.3	185.53.178.30
Jan 14, 2021 05:02:17.498668909 CET	49716	80	192.168.2.3	76.223.26.96
Jan 14, 2021 05:02:17.538837910 CET	80	49716	76.223.26.96	192.168.2.3
Jan 14, 2021 05:02:17.659147024 CET	80	49716	76.223.26.96	192.168.2.3
Jan 14, 2021 05:02:17.663695097 CET	49716	80	192.168.2.3	76.223.26.96

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 05:02:17.684144020 CET	49716	80	192.168.2.3	76.223.26.96
Jan 14, 2021 05:02:17.724172115 CET	80	49716	76.223.26.96	192.168.2.3
Jan 14, 2021 05:02:17.845014095 CET	49719	80	192.168.2.3	13.224.89.16
Jan 14, 2021 05:02:17.852982044 CET	49716	80	192.168.2.3	76.223.26.96
Jan 14, 2021 05:02:17.890974045 CET	80	49719	13.224.89.16	192.168.2.3
Jan 14, 2021 05:02:17.891752958 CET	80	49719	13.224.89.16	192.168.2.3
Jan 14, 2021 05:02:17.891784906 CET	80	49719	13.224.89.16	192.168.2.3
Jan 14, 2021 05:02:17.891808987 CET	80	49719	13.224.89.16	192.168.2.3
Jan 14, 2021 05:02:17.891841888 CET	49719	80	192.168.2.3	13.224.89.16
Jan 14, 2021 05:02:17.891871929 CET	49719	80	192.168.2.3	13.224.89.16
Jan 14, 2021 05:02:17.891890049 CET	80	49719	13.224.89.16	192.168.2.3
Jan 14, 2021 05:02:17.891913891 CET	80	49719	13.224.89.16	192.168.2.3
Jan 14, 2021 05:02:17.891935110 CET	49719	80	192.168.2.3	13.224.89.16
Jan 14, 2021 05:02:17.891938925 CET	80	49719	13.224.89.16	192.168.2.3
Jan 14, 2021 05:02:17.891963005 CET	80	49719	13.224.89.16	192.168.2.3
Jan 14, 2021 05:02:17.891984940 CET	80	49719	13.224.89.16	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 05:02:11.368619919 CET	57544	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:11.425049067 CET	53	57544	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:12.178291082 CET	55984	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:12.228998899 CET	53	55984	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:13.023015976 CET	64185	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:13.079514027 CET	53	64185	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:13.912687063 CET	65110	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:13.961349964 CET	53	65110	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:14.922548056 CET	58361	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:14.980227947 CET	53	58361	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:15.153652906 CET	63492	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:15.204495907 CET	53	63492	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:16.001288891 CET	60831	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:16.165663004 CET	60100	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:16.210764885 CET	53	60831	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:16.216383934 CET	53	60100	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:16.627005100 CET	53195	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:16.685411930 CET	53	53195	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:16.986829042 CET	50141	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:16.990113020 CET	53023	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:17.025549889 CET	49563	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:17.045847893 CET	53	50141	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:17.046454906 CET	53	53023	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:17.058262110 CET	51352	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:17.081697941 CET	53	49563	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:17.117706060 CET	53	51352	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:17.501491070 CET	59349	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:17.557780981 CET	53	59349	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:17.849055052 CET	57084	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:17.913279057 CET	53	57084	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:18.006099939 CET	58823	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:18.054121971 CET	53	58823	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:18.717698097 CET	57568	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:18.783507109 CET	53	57568	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:19.653742075 CET	50540	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:19.704617023 CET	53	50540	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:20.449894905 CET	54366	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:20.497894049 CET	53	54366	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:21.279114008 CET	53034	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:21.327022076 CET	53	53034	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:22.072921038 CET	57762	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:22.120915890 CET	53	57762	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:22.924885035 CET	55435	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:22.981689930 CET	53	55435	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 05:02:23.852638006 CET	50713	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:23.903444052 CET	53	50713	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:24.709467888 CET	56132	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:24.768728971 CET	53	56132	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:32.779552937 CET	58987	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:32.838614941 CET	53	58987	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:35.963710070 CET	56579	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:36.011766911 CET	53	56579	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:37.742954016 CET	60633	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:37.800798893 CET	53	60633	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:38.103049040 CET	61292	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:38.169881105 CET	53	61292	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:38.730911970 CET	63619	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:38.754198074 CET	64938	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:38.789191008 CET	53	63619	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:38.813539982 CET	53	64938	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:38.871822119 CET	61946	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:38.933552027 CET	53	61946	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:39.840325117 CET	64910	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:39.897964001 CET	53	64910	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:44.923830986 CET	52123	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:44.974683046 CET	53	52123	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:45.583877087 CET	56130	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:45.646029949 CET	53	56130	8.8.8.8	192.168.2.3
Jan 14, 2021 05:02:45.924379110 CET	52123	53	192.168.2.3	8.8.8.8
Jan 14, 2021 05:02:45.983634949 CET	53	52123	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2021 05:02:16.001288891 CET	192.168.2.3	8.8.8.8	0x71f	Standard query (0)	www.flowvinconsortium.com	A (IP address)	IN (0x0001)
Jan 14, 2021 05:02:16.627005100 CET	192.168.2.3	8.8.8.8	0x902b	Standard query (0)	ww38.flowvinconsortium.com	A (IP address)	IN (0x0001)
Jan 14, 2021 05:02:16.990113020 CET	192.168.2.3	8.8.8.8	0xaed	Standard query (0)	d1lxhc4jvstzrp.cloudfront.net	A (IP address)	IN (0x0001)
Jan 14, 2021 05:02:17.058262110 CET	192.168.2.3	8.8.8.8	0xc299	Standard query (0)	c.parkingcrew.net	A (IP address)	IN (0x0001)
Jan 14, 2021 05:02:32.779552937 CET	192.168.2.3	8.8.8.8	0xf46f	Standard query (0)	ww38.flowvinconsortium.com	A (IP address)	IN (0x0001)
Jan 14, 2021 05:02:37.742954016 CET	192.168.2.3	8.8.8.8	0xc5fe	Standard query (0)	www.godaddy.com	A (IP address)	IN (0x0001)
Jan 14, 2021 05:02:38.103049040 CET	192.168.2.3	8.8.8.8	0x690c	Standard query (0)	ch.godaddy.com	A (IP address)	IN (0x0001)
Jan 14, 2021 05:02:38.730911970 CET	192.168.2.3	8.8.8.8	0x76f8	Standard query (0)	img6.wsimg.com	A (IP address)	IN (0x0001)
Jan 14, 2021 05:02:38.754198074 CET	192.168.2.3	8.8.8.8	0xf5b6	Standard query (0)	img6.wsimg.com	A (IP address)	IN (0x0001)
Jan 14, 2021 05:02:38.871822119 CET	192.168.2.3	8.8.8.8	0x91b0	Standard query (0)	d3uxovyp91rmcf.cloudfront.net	A (IP address)	IN (0x0001)
Jan 14, 2021 05:02:39.840325117 CET	192.168.2.3	8.8.8.8	0xd959	Standard query (0)	img1.wsimg.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2021 05:02:16.210764885 CET	8.8.8.8	192.168.2.3	0x71f	No error (0)	www.flowvinconsortium.com		103.224.212.220	A (IP address)	IN (0x0001)
Jan 14, 2021 05:02:16.685411930 CET	8.8.8.8	192.168.2.3	0x902b	No error (0)	ww38.flowvinconsortium.com	701602.parkingcrew.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 05:02:16.685411930 CET	8.8.8.8	192.168.2.3	0x902b	No error (0)	701602.parkingcrew.net		76.223.26.96	A (IP address)	IN (0x0001)
Jan 14, 2021 05:02:16.685411930 CET	8.8.8.8	192.168.2.3	0x902b	No error (0)	701602.parkingcrew.net		13.248.148.254	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2021 05:02:17.046454906 CET	8.8.8.8	192.168.2.3	0xaed	No error (0)	d1lxhc4jvstzrp.cloudfront.net		13.224.89.16	A (IP address)	IN (0x0001)
Jan 14, 2021 05:02:17.046454906 CET	8.8.8.8	192.168.2.3	0xaed	No error (0)	d1lxhc4jvstzrp.cloudfront.net		13.224.89.53	A (IP address)	IN (0x0001)
Jan 14, 2021 05:02:17.046454906 CET	8.8.8.8	192.168.2.3	0xaed	No error (0)	d1lxhc4jvstzrp.cloudfront.net		13.224.89.135	A (IP address)	IN (0x0001)
Jan 14, 2021 05:02:17.046454906 CET	8.8.8.8	192.168.2.3	0xaed	No error (0)	d1lxhc4jvstzrp.cloudfront.net		13.224.89.138	A (IP address)	IN (0x0001)
Jan 14, 2021 05:02:17.117706060 CET	8.8.8.8	192.168.2.3	0xc299	No error (0)	c.parkingcrew.net		185.53.178.30	A (IP address)	IN (0x0001)
Jan 14, 2021 05:02:32.838614941 CET	8.8.8.8	192.168.2.3	0xf46f	No error (0)	ww38.flowvinconsortium.com	701602.parkingcrew.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 05:02:32.838614941 CET	8.8.8.8	192.168.2.3	0xf46f	No error (0)	701602.parkingcrew.net		76.223.26.96	A (IP address)	IN (0x0001)
Jan 14, 2021 05:02:32.838614941 CET	8.8.8.8	192.168.2.3	0xf46f	No error (0)	701602.parkingcrew.net		13.248.148.254	A (IP address)	IN (0x0001)
Jan 14, 2021 05:02:37.800798893 CET	8.8.8.8	192.168.2.3	0xc5fe	No error (0)	www.godaddy.com	wildcard-ipv6.godaddy.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 05:02:38.169881105 CET	8.8.8.8	192.168.2.3	0x690c	No error (0)	ch.godaddy.com	wildcard-ipv6.godaddy.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 05:02:38.789191008 CET	8.8.8.8	192.168.2.3	0x76f8	No error (0)	img6.wsimg.com	global-wildcard.wsimg.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 05:02:38.813539982 CET	8.8.8.8	192.168.2.3	0xf5b6	No error (0)	img6.wsimg.com	global-wildcard.wsimg.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 05:02:38.933552027 CET	8.8.8.8	192.168.2.3	0x91b0	No error (0)	d3uxovyp91rmcf.cloudfront.net		13.224.89.135	A (IP address)	IN (0x0001)
Jan 14, 2021 05:02:38.933552027 CET	8.8.8.8	192.168.2.3	0x91b0	No error (0)	d3uxovyp91rmcf.cloudfront.net		13.224.89.229	A (IP address)	IN (0x0001)
Jan 14, 2021 05:02:38.933552027 CET	8.8.8.8	192.168.2.3	0x91b0	No error (0)	d3uxovyp91rmcf.cloudfront.net		13.224.89.79	A (IP address)	IN (0x0001)
Jan 14, 2021 05:02:38.933552027 CET	8.8.8.8	192.168.2.3	0x91b0	No error (0)	d3uxovyp91rmcf.cloudfront.net		13.224.89.139	A (IP address)	IN (0x0001)
Jan 14, 2021 05:02:39.897964001 CET	8.8.8.8	192.168.2.3	0xd959	No error (0)	img1.wsimg.com	global-wildcard.wsimg.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- www.flowvinconsortium.com
- ww38.flowvinconsortium.com
  - d1lxhc4jvstzrp.cloudfront.net
  - c.parkingcrew.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49714	103.224.212.220	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2021 05:02:16.417823076 CET	161	OUT	GET / HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www.flowvinconsortium.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2021 05:02:16.610672951 CET	168	IN	HTTP/1.1 302 Found Date: Thu, 14 Jan 2021 04:02:16 GMT Server: Apache/2.4.25 (Debian) Set-Cookie: __tad=1610596936.6514942; expires=Sun, 12-Jan-2031 04:02:16 GMT; Max-Age=315360000 Location: http://ww38.flowvinconsortium.com/ Content-Length: 0 Connection: close Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49716	76.223.26.96	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2021 05:02:16.731435061 CET	169	OUT	GET / HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: ww38.flowvinconsortium.com
Jan 14, 2021 05:02:16.904169083 CET	174	IN	HTTP/1.1 200 OK Date: Thu, 14 Jan 2021 04:02:16 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Server: nginx Vary: Accept-Encoding X-Check: 3c12dc4d54f8e22d666785b733b0052100c53444 X-Language: english X-Template: tpl_CleanPeppermintBlack_twoclick X-Buckets: bucket106 X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBALquDFETXRn0Hr05fUP7EJT77xYnPmRbpMy4vk8KYiH nkNpednjOANJcaXDXcKQJN0nXKZJL7TciJD8AoHXK158CAwEAAQ==_fNNQ6VbKrjBpx6z/zwNCEfShkGBDmj9vEwmJ LlKcPelTaGWGUTEKksn3A3DvxlhpwHcn0YAfak6NEddg2WnyPA== Content-Encoding: gzip Data Raw: 31 34 31 64 0d 0a 1f 8b 08 00 00 00 00 00 00 03 c5 5a 69 77 da 48 d6 fe 1c ff 0a 35 7d a6 b1 4f 6c 90 04 24 c6 31 e9 83 cd 62 48 10 06 8b 4d fd ce f1 d1 86 25 d0 16 49 20 a0 3b ff 7d 9e 5b 62 73 ec f4 36 f3 ce 90 d8 96 aa 6e 55 dd 7d 2b ae 7f a8 75 6f e5 c9 7d 9d b3 62 d7 f9 78 72 4d 7f 38 43 8d d5 0b d5 d0 1c 5f 9f cf cd 75 25 d3 69 24 49 ad 37 69 7f f2 95 96 b5 d4 a5 6a af 7e 73 d3 ab d6 1e 92 6a f2 50 6d df 54 3f 7f 59 d4 1a 75 79 dc f7 f8 bb 90 2f 4d 07 f7 ef eb 6d f9 fd fb d5 c4 bb 77 fb 5a d0 59 17 97 f3 cb 4f 13 fb ce 9b 4b 81 69 78 b3 6e 55 6a eb ea b8 36 d6 3f f5 da 12 ef 8d 3f 29 ed cf ef 65 dd 6e d7 2e ab fe dd f8 93 50 ba bc ad 26 f5 6a b5 57 a9 3c 4e 25 a9 f7 6e a8 7d 0a 67 37 c1 ea dd 26 bf 49 a4 db fa f4 c1 9a 37 6f 6a ee ac bc ac 27 6e fb b3 f3 49 bf 37 1d 59 6d 8e 9a 03 b9 fe 69 1e 79 85 6a a1 b6 5c b5 ac 20 b9 d3 3d 7e 52 9d aa f3 77 52 dd 30 9e c4 91 b7 be af 56 2a 19 6e e5 3a 5e 54 c9 58 71 1c 5c e5 f3 49 92 e4 92 42 ce 0f 9f f2 42 b9 5c ce af 88 1f 0c e8 ca 51 bd a7 4a c6 f4 32 dc fe 89 f8 65 aa c6 c7 93 37 d7 ae 19 ab e0 61 1c 5c 98 5f 16 f6 b2 92 b9 f5 bd d8 f4 e2 0b 79 1d 98 19 4e 4f df 2a 99 d8 5c c5 79 da f4 03 a7 5b 6a 18 99 71 65 11 4f 2f 2e 33 f9 8f 27 1c 7d d2 9d 3c d5 35 2b 99 a5 6d 26 81 1f c6 47 eb 13 db 88 ad 8a 61 2e 6d dd bc 60 2f e7 9c ed d9 b1 ad 3a 17 91 ae 3a 66 45 38 e7 22 2b b4 bd f9 45 ec 5f 4c ed b8 e2 f9 19 6e bb fb 75 6c c7 8e f9 71 ea f8 c9 d2 f6 80 54 84 dd ed 85 9b d3 7d f7 3a 9f 4e 82 98 48 0f ed 20 e6 a2 50 af 64 52 9e 3c f9 fe 93 63 12 58 5e 35 22 d3 8b cc bc e1 bb aa ed 45 79 5d 9d e6 66 51 86 8b 41 e8 96 be 99 ba 54 d3 3d 32 dc c7 eb 7c fa 48 5c 72 80 16 67 85 e6 94 f6 35 04 67 65 e9 c5 d9 32 8a 37 61 90 d3 1d 7f 61 4c 43 30 2a e7 99 71 3e b6 4c d7 8c f2 6a 04 16 45 f9 28 5e d3 f1 11 ce 09 4d a7 92 61 ef 91 65 9a e0 cd d1 c1 0c c0 35 0d 5b 05 88 1e 9a 24 2d 90 fe 77 0e d6 1d 53 f5 ee cd 20 30 43 d7 f6 e2 c7 f7 ea a5 38 15 a6 85 ff 24 2a a4 2f 11 b4 6e 0a a2 a3 5c ca 63 35 b0 23 c6 67 d0 f2 f3 54 75 6d 67 5d b9 f7 83 00 ac be 2a f0 fc 4b fa f7 da 97 ea 8c 61 a6 ec b6 7d 8f 3b d2 1b d9 b2 23 2e 15 19 e7 aa 6b 4e 33 b9 a9 1f 72 11 34 e6 87 2d 8f f2 a9 2e 9f 5c 6b be b1 e6 6c a3 92 51 a7 46 86 63 ac 26 5d 8c 6c cd 76 ec 78 7d 65 d9 86 01 ce 7e 3c c1 e7 da b0 97 9c ee 40 Data Ascii: 141dZiwH5}Ol$1bHM%I ;}{bs6nU}+uo}bxrM8C_u%i$I7ij~sjPmT?Yuy/MmwZYOKixnUj6??)en.P&jW<N%n}g 7&I7oj'nI7Ymiyj\ =~RwR0V*n:^TXq\lBB\QJ2e7a_yNO*\y[jqeO/.3'}<5+m&Ga.m`/::fE8"+E_LnulqT}:NH PdR<cX^5" Ey]fQAT=2|H\rg5ge27aaLC0*q>LjE(^Mae5[$-wS 0C8$*/n\c5#gTumg]*Ka};#.kN3r4-.\klQFc&]lvx}e~<@
Jan 14, 2021 05:02:17.498668909 CET	275	OUT	GET /track.php?domain=flowvinconsortium.com&toggle=browserjs&uid=MTYxMDU5NjkzNi44NjM4OjJlMjliMzNjYzE 2ZDNhMTM5ZGFhZWJjMjBlMmIxYmEzYWNlZTk5ZjQyMjgwZmMzNTc3ZTM4MzU2NTQzMDBlZjU6NWZmZmM yNDhkMmU1OA%3D%3D HTTP/1.1 Accept: */* Referer: http://ww38.flowvinconsortium.com/ Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: ww38.flowvinconsortium.com Connection: Keep-Alive
Jan 14, 2021 05:02:17.659147024 CET	282	IN	HTTP/1.1 200 OK Date: Thu, 14 Jan 2021 04:02:17 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Server: nginx Vary: Accept-Encoding X-Custom-Track: browserjs Access-Control-Allow-Origin: * Content-Encoding: gzip Data Raw: 31 34 0d 0a 1f 8b 08 00 00 00 00 00 00 03 03 00 00 00 00 00 00 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 140

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2021 05:02:17.684144020 CET	283	OUT	POST /ls.php HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 Referer: http://ww38.flowvinconsortium.com/ Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: ww38.flowvinconsortium.com Content-Length: 2130 Connection: Keep-Alive Cache-Control: no-cache
Jan 14, 2021 05:02:18.011837006 CET	330	IN	HTTP/1.1 201 Created Date: Thu, 14 Jan 2021 04:02:17 GMT Content-Type: text/javascript; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive Server: nginx X-Log-Success: 5fffc2495fe65e55583dde26 Access-Control-Allow-Origin: Access-Control-Allow-Methods: POST, OPTIONS Access-Control-Max-Age: 86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Jan 14, 2021 05:02:18.654031992 CET	467	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: ww38.flowvinconsortium.com Connection: Keep-Alive
Jan 14, 2021 05:02:18.824378014 CET	467	IN	HTTP/1.1 200 OK Date: Thu, 14 Jan 2021 04:02:18 GMT Content-Type: image/x-icon Content-Length: 0 Connection: keep-alive Server: nginx Last-Modified: Tue, 17 Mar 2020 13:25:51 GMT ETag: "5e70cfdf-0" Accept-Ranges: bytes
Jan 14, 2021 05:02:19.145750046 CET	484	OUT	GET /track.php?domain=flowvinconsortium.com&caf=1&toggle=answercheck&answer=yes&uid=MTYxMDU5NjkzNi44NjM4OjJlMjliMzNjYzE2ZDNhMTM5ZGFhZWJjMjBlMmIxYmEzYWNlZTk5ZjQyMjgwZmMzNTc3ZTM4MzU2NTQzMDBlZjU6NWZmZmMyNDhkMmU1OA%3D%3D HTTP/1.1 Accept: */* Referer: http://ww38.flowvinconsortium.com/ Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: ww38.flowvinconsortium.com Connection: Keep-Alive
Jan 14, 2021 05:02:19.305296898 CET	485	IN	HTTP/1.1 200 OK Date: Thu, 14 Jan 2021 04:02:19 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Server: nginx Vary: Accept-Encoding X-Custom-Track: answercheck Access-Control-Allow-Origin: * Content-Encoding: gzip Data Raw: 31 34 0d 0a 1f 8b 08 00 00 00 00 00 00 03 03 00 00 00 00 00 00 00 00 00 0d 0a Data Ascii: 14

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49718	13.224.89.16	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2021 05:02:17.100193024 CET	182	OUT	GET /themes/cleanPeppermint_7a82f1f3/style.css HTTP/1.1 Accept: text/css, */* Referer: http://ww38.flowvinconsortium.com/ Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: d1lxhc4jvstzrp.cloudfront.net Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2021 05:02:17.145482063 CET	184	IN	HTTP/1.1 200 OK Content-Type: text/css Transfer-Encoding: chunked Connection: keep-alive Server: nginx Date: Wed, 13 Jan 2021 11:51:07 GMT Last-Modified: Tue, 17 Mar 2020 13:25:50 GMT Content-Encoding: gzip ETag: W/"5e70cfde-589" Vary: Accept-Encoding X-Cache: Hit from cloudfront Via: 1.1 eb7b239aed47669f8a7b6ac95bc8aff1.cloudfront.net (CloudFront) X-Amz-Cf-Pop: ZRH50-C1 X-Amz-Cf-Id: s7NAMNza-1e9kN-xJKHkzs-MeD5soPeIn2WfFJjf9GEsIIHBc_5zEw== Age: 58270 Data Raw: 32 33 62 0d 0a Data Ascii: 23b

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49722	13.224.89.16	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2021 05:02:17.103605986 CET	183	OUT	GET /scripts/js3caf.js HTTP/1.1 Accept: application/javascript, */*;q=0.8 Referer: http://ww38.flowvinconsortium.com/ Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: d1lxhc4jvstzrp.cloudfront.net Connection: Keep-Alive
Jan 14, 2021 05:02:17.148916960 CET	186	IN	HTTP/1.1 200 OK Content-Type: application/javascript Content-Length: 7000 Connection: keep-alive Server: nginx Date: Wed, 13 Jan 2021 09:46:30 GMT Last-Modified: Fri, 04 Sep 2020 07:42:12 GMT Accept-Ranges: bytes ETag: "5f51efd4-1b58" X-Cache: Hit from cloudfront Via: 1.1 c202f63846a430afd2d556266be8b50c.cloudfront.net (CloudFront) X-Amz-Cf-Pop: ZRH50-C1 X-Amz-Cf-Id: L8xyrai__EkNsMIFLmA23SIsBlHQrFnQ350t5gAhcQaFTL6lruOVyw== Age: 65747

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49719	13.224.89.16	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2021 05:02:17.147003889 CET	185	OUT	GET /themes/assets/style.css HTTP/1.1 Accept: text/css, */* Referer: http://ww38.flowvinconsortium.com/ Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: d1lxhc4jvstzrp.cloudfront.net Connection: Keep-Alive
Jan 14, 2021 05:02:17.193253040 CET	195	IN	HTTP/1.1 200 OK Content-Type: text/css Transfer-Encoding: chunked Connection: keep-alive Server: nginx Date: Wed, 13 Jan 2021 05:53:15 GMT Last-Modified: Tue, 17 Mar 2020 13:25:50 GMT Content-Encoding: gzip ETag: W/"5e70cfde-33d" Vary: Accept-Encoding X-Cache: Hit from cloudfront Via: 1.1 a70d280cd058ea89c08954ea0ad67199.cloudfront.net (CloudFront) X-Amz-Cf-Pop: ZRH50-C1 X-Amz-Cf-Id: mn5MUKW68Tme_Rh0D33Q2zgobXoLXXccRcys2SSEqdMTAePUR9Prpg== Age: 79742 Data Raw: 31 35 37 0d 0a Data Ascii: 157

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2021 05:02:17.845014095 CET	298	OUT	GET /themes/cleanPeppermint_7a82f1f3/img/arrows.png HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: http://ww38.flowvinconsortium.com/ Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: d1lxhc4jvstzrp.cloudfront.net Connection: Keep-Alive
Jan 14, 2021 05:02:17.891752958 CET	301	IN	HTTP/1.1 200 OK Content-Type: image/png Content-Length: 15544 Connection: keep-alive Server: nginx Date: Thu, 14 Jan 2021 03:58:04 GMT Last-Modified: Tue, 17 Mar 2020 13:25:50 GMT Accept-Ranges: bytes ETag: "5e70cfde-3cb8" X-Cache: Hit from cloudfront Via: 1.1 a70d280cd058ea89c08954ea0ad67199.cloudfront.net (CloudFront) X-Amz-Cf-Pop: ZRH50-C1 X-Amz-Cf-Id: RlUxIK6oMgNhC6TWR11CowZT694K5IaPTti8zWdZVjBW3RZi7uR6mg== Age: 253

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49725	185.53.178.30	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2021 05:02:17.232547998 CET	216	OUT	GET /scripts/sale_form.js HTTP/1.1 Accept: application/javascript, */*;q=0.8 Referer: http://ww38.flowvinconsortium.com/ Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: c.parkingcrew.net Connection: Keep-Alive
Jan 14, 2021 05:02:17.272573948 CET	240	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 14 Jan 2021 04:02:17 GMT Content-Type: application/javascript Content-Length: 761 Connection: keep-alive Last-Modified: Tue, 17 Mar 2020 13:25:51 GMT ETag: "5e70cfdf-2f9" Accept-Ranges: bytes Data Raw: 2f 2a 0a 20 2a 20 53 61 6c 65 73 20 66 6f 72 6d 20 63 6c 69 63 6b 20 74 72 61 63 6b 65 72 0a 20 2a 0a 20 2a 20 74 6c 69 6e 6b 28 29 20 77 69 6c 6c 20 6c 6f 61 64 20 61 20 31 78 31 20 47 49 46 20 74 6f 20 74 72 61 63 6b 20 63 6c 69 63 6b 6f 75 74 73 20 74 6f 20 74 68 65 20 63 6f 6e 74 61 63 74 20 66 6f 72 6d 0a 20 2a 20 53 6f 6d 65 20 62 61 73 69 63 20 73 63 72 61 6d 62 6c 69 6e 67 20 70 72 65 76 65 6e 74 73 20 28 61 20 6c 6f 74 20 6f 66 29 20 77 65 62 20 73 63 72 61 70 65 72 73 20 74 6f 20 66 6f 6c 6c 6f 77 20 74 68 65 20 6c 69 6e 6b 0a 20 2a 0a 20 2a 20 44 61 74 65 3a 20 32 30 31 36 2d 30 33 2d 32 32 0a 2a 2f 0a 0a 2f 2f 20 66 75 6e 63 74 69 6f 6e 20 74 6c 69 6e 6b 28 76 2c 20 77 6f 77 29 0a 2f 2f 20 76 20 69 73 20 61 20 66 69 78 65 64 20 73 74 72 69 6e 67 0a 2f 2f 20 77 6f 77 20 77 69 6c 6c 20 63 6f 6e 74 61 69 6e 20 74 68 65 20 63 75 72 72 65 6e 74 20 64 6f 6d 61 69 6e 20 6e 61 6d 65 0a 66 75 6e 63 74 69 6f 6e 20 74 6c 69 6e 6b 28 76 2c 20 77 6f 77 29 20 7b 0a 20 20 20 20 69 66 20 28 64 6f 63 75 6d 65 6e 74 2e 6c 6f 63 61 74 69 6f 6e 2e 73 65 61 72 63 68 2e 69 6e 64 65 78 4f 66 28 27 5f 78 61 73 27 29 20 3d 3d 20 2d 31 29 20 7b 0a 20 20 20 20 20 20 20 20 2f 2f 20 64 65 66 69 6e 65 20 73 6f 6d 65 20 63 6f 6d 70 65 6e 65 6e 74 73 20 74 68 61 74 20 77 69 6c 6c 20 6c 61 74 65 72 20 66 6f 72 6d 20 74 68 65 20 6c 69 6e 6b 20 74 6f 20 74 68 65 20 31 78 31 20 47 49 46 0a 20 20 20 20 20 20 20 20 76 61 72 20 70 72 6f 74 6f 5f 73 75 66 20 3d 20 22 74 70 22 2c 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 73 74 72 69 6e 67 20 3d 20 22 6f 6d 61 69 6e 62 22 2c 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 72 61 6d 65 74 65 72 20 3d 20 22 70 68 70 3f 73 61 6c 65 6c 69 6e 6b 3d 31 22 3b 0a 20 20 20 20 20 20 20 20 2f 2f 20 67 65 6e 65 72 61 74 65 20 61 6e 64 20 6c 6f 61 64 20 74 68 65 20 31 78 31 20 47 49 46 0a 20 20 20 20 20 20 20 20 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 20 22 68 74 22 20 2b 20 70 72 6f 74 6f 5f 73 75 66 20 2b 20 22 3a 22 20 2b 20 22 2f 2f 22 20 2b 20 22 77 77 22 20 2b 20 22 77 2e 6d 79 64 22 20 2b 20 73 74 72 69 6e 67 20 2b 20 22 75 79 2e 63 6f 6d 2f 73 61 6c 65 5f 66 6f 72 6d 2e 22 20 2b 20 70 61 72 61 6d 65 74 65 72 20 2b 20 22 26 64 6f 6d 22 20 2b 20 22 61 69 6e 5f 6e 61 6d 65 3d 22 20 2b 20 77 6f 77 3b 0a 20 20 20 20 7d 0a 7d 0a Data Ascii: /* * Sales form click tracker * * tlink() will load a 1x1 GIF to track clickouts to the contact form * Some basic scrambling prevents (a lot of) web scrapers to follow the link * * Date: 2016-03-22*/// function tlink(v, wow)// v is a fixed string// wow will contain the current domain namefunction tlink(v, wow) { if (document.location.search.indexOf('_xas') === -1) { // define some compenents that will later form the link to the 1x1 GIF var proto_suf = "tp", string = "omainb", parameter = "php?salelink=1"; // generate and load the 1x1 GIF new Image().src= "ht" + proto_suf + ":" + "//" + "ww" + "w.myd" + string + "uy.com/sale_form." + parameter + "&dom" + "ain_name=" + wow; }}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	103.224.212.220	80	192.168.2.3	49715	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2021 05:02:21.600451946 CET	521	IN	HTTP/1.0 408 Request Time-out Cache-Control: no-cache Connection: close Content-Type: text/html Data Raw: 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 3c 68 31 3e 34 30 38 20 52 65 71 75 65 73 74 20 54 69 6d 65 2d 6f 75 74 3c 2f 68 31 3e 0a 59 6f 75 72 20 62 72 6f 77 73 65 72 20 64 69 64 6e 27 74 20 73 65 6e 64 20 61 20 63 6f 6d 70 6c 65 74 65 20 72 65 71 75 65 73 74 20 69 6e 20 74 69 6d 65 2e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <html><body> 408 Request Time-out Your browser didn't send a complete request in time.</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49743	76.223.26.96	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2021 05:02:32.923202038 CET	581	OUT	GET /favicon.ico HTTP/1.1 User-Agent: AutoIt Host: ww38.flowvinconsortium.com
Jan 14, 2021 05:02:33.083719969 CET	581	IN	HTTP/1.1 200 OK Date: Thu, 14 Jan 2021 04:02:33 GMT Content-Type: image/x-icon Content-Length: 0 Connection: keep-alive Server: nginx Last-Modified: Tue, 17 Mar 2020 13:25:51 GMT ETag: "5e70cfdf-0" Accept-Ranges: bytes

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
Jan 14, 2021 05:02:39.028393984 CET	13.224.89.135	443	192.168.2.3	49757	CN=*.cloudfront.net, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Tue May 26 02:00:00 CEST 2020 Thu Aug 01 14:00:00 CEST 2013 Mon Nov 06 01:00:00 CET 2017	Wed Apr 21 14:00:00 CEST 2021 Tue Aug 01 14:00:00 CEST 2028 Sun Nov 06 00:59:59 CET 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert Global CA G2, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		
Jan 14, 2021 05:02:39.028995037 CET	13.224.89.135	443	192.168.2.3	49758	CN=*.cloudfront.net, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Tue May 26 02:00:00 CEST 2020 Thu Aug 01 14:00:00 CEST 2013 Mon Nov 06 01:00:00 CET 2017	Wed Apr 21 14:00:00 CEST 2021 Tue Aug 01 14:00:00 CEST 2028 Sun Nov 06 00:59:59 CET 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert Global CA G2, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		

Code Manipulations

Statistics

Behavior

System Behavior

Analysis Process: iexplore.exe PID: 4736 Parent PID: 792

General

Start time:	05:02:13
Start date:	14/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff79d3d0000
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: 5860 Parent PID: 4736

General

Start time:	05:02:14
Start date:	14/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4736 CREDAT:17410 /prefetch:2
Imagebase:	0x200000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly