ID: 358583
Cookbook: browseurl.jbs
Time: 21:48:37
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

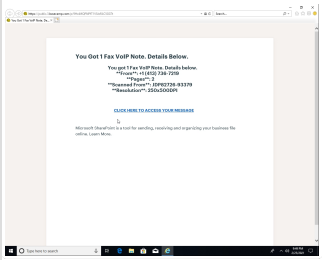
Analysis Report https://public.3.basecamp.com/p/9HoiM…

Overview

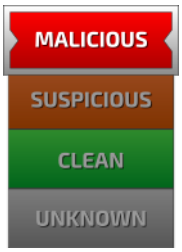
General Information

Sample URL:	http://https://public.3.basecamp.com/p/9HoiMQPNPfT1V5JoFAC5GG7t
Analysis ID:	358583
Infos:	

Most interesting Screenshot:



Detection

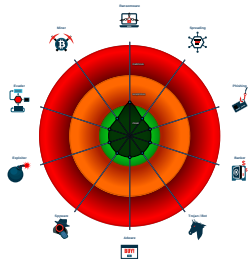


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Antivirus / Scanner detection for sub…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 1956 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 3980 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1956 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 4664 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1956 CREDAT:82952 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

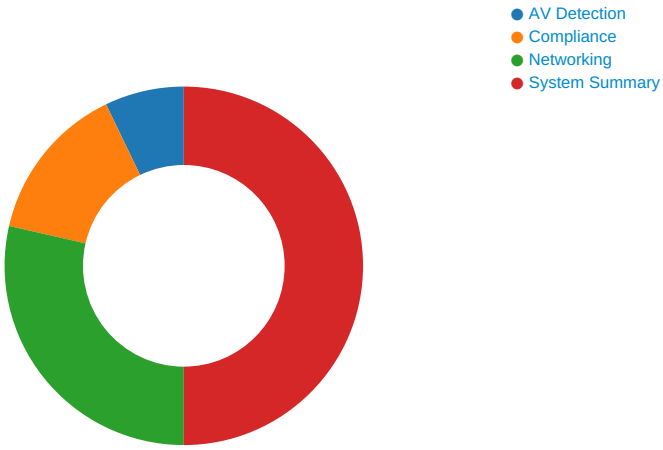
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Compliance:

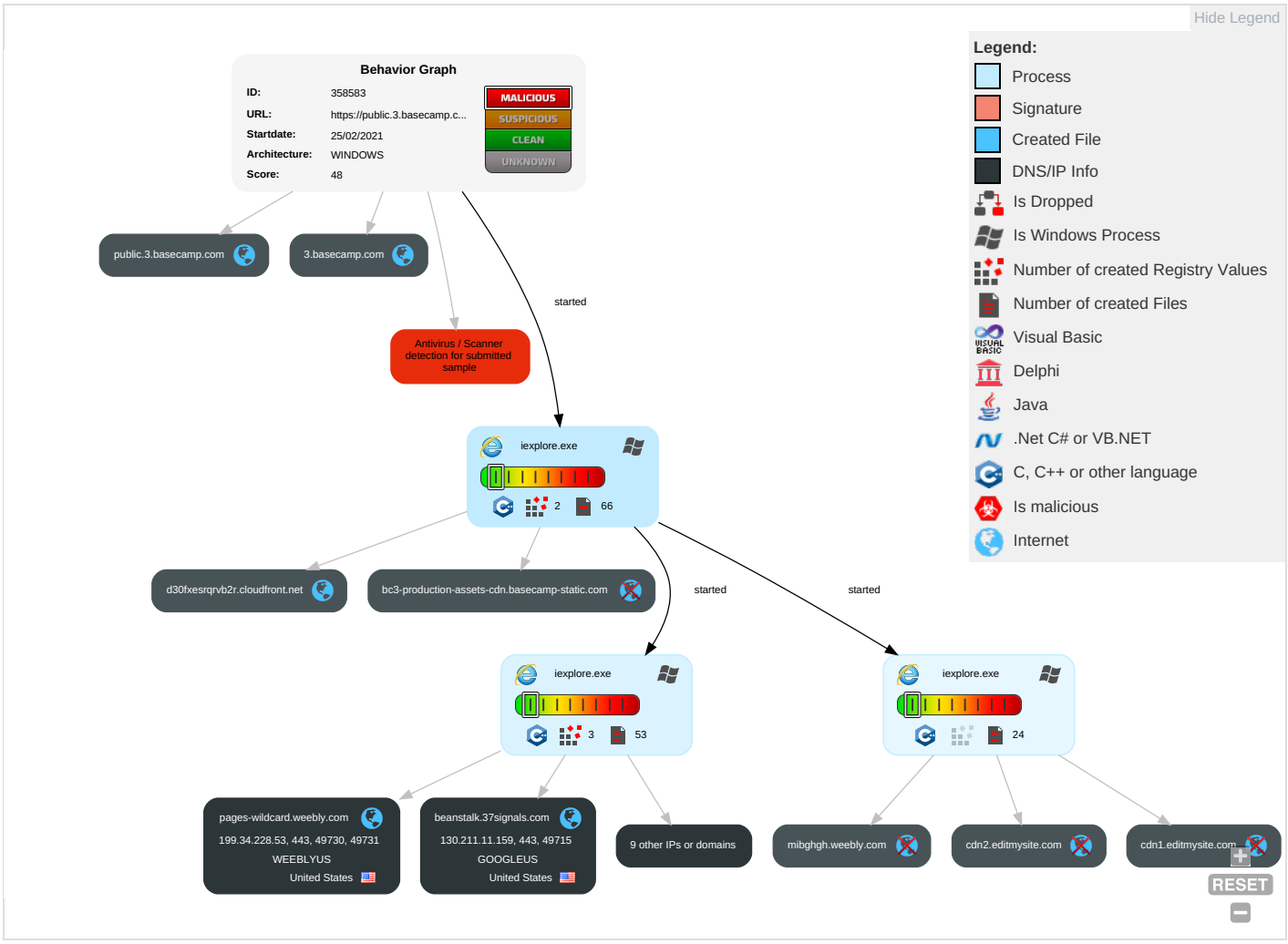
Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Mitre Att&ck Matrix

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

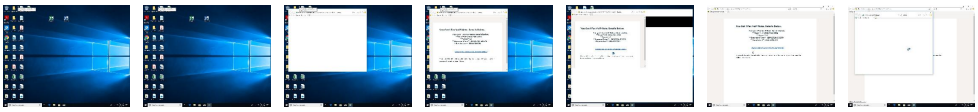
Behavior Graph

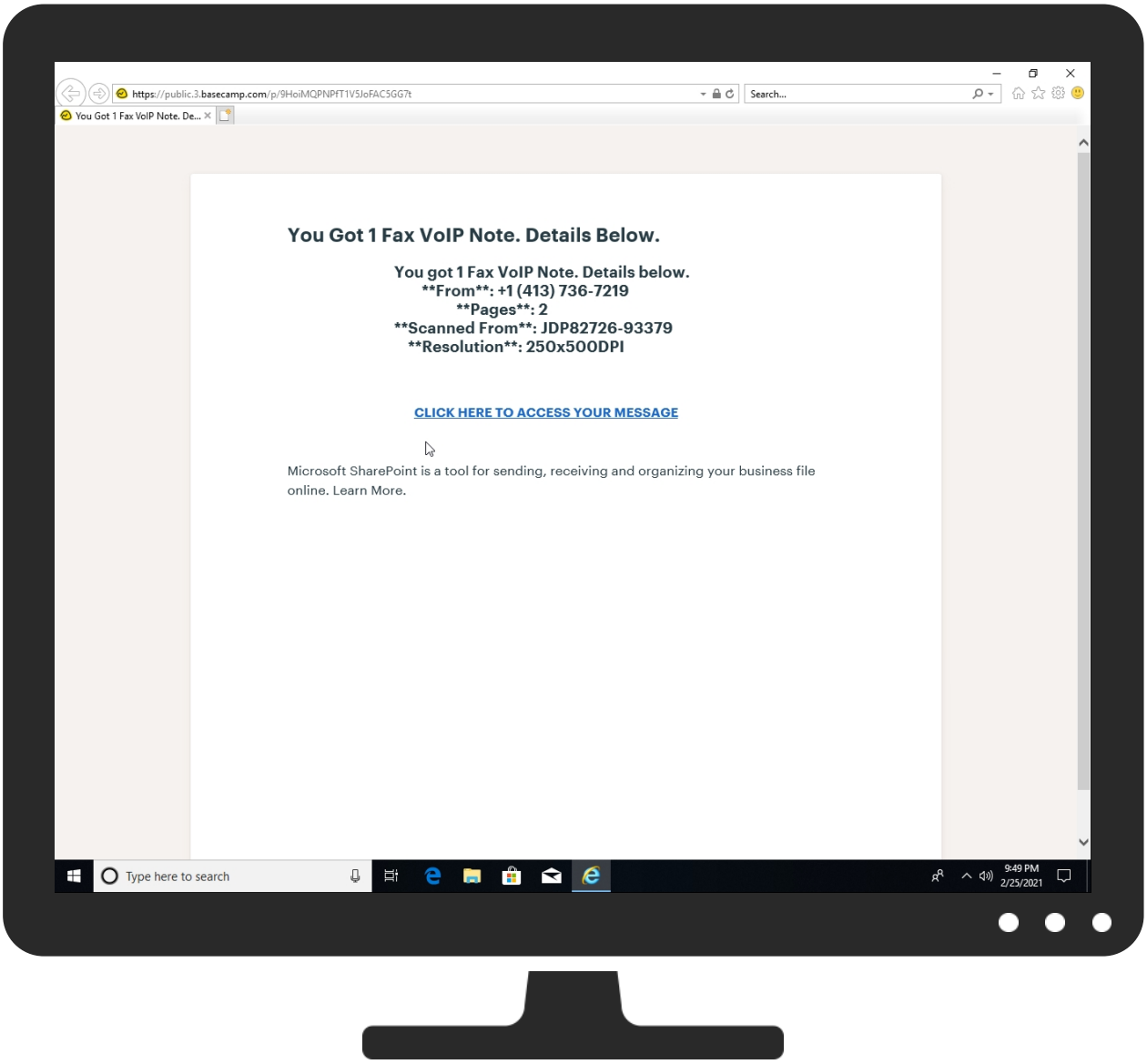


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://public.3.basecamp.com/p/9HoiMQPNPfT1V5JoFAC5GG7t	0%	Virustotal		Browse
http://https://public.3.basecamp.com/p/9HoiMQPNPfT1V5JoFAC5GG7t	0%	Avira URL Cloud	safe	
http://https://public.3.basecamp.com/p/9HoiMQPNPfT1V5JoFAC5GG7t	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
http://https://bc3-production-assets-cdn.basecamp-static.com	0%	Avira URL Cloud	safe	
http://https://bc3-production-assets-cdn.basecamp-static.com/assets/desktop-09334a52f8be90f7ab2c69fb59eb0ea	0%	Avira URL Cloud	safe	
http://https://public.3..com/m/p/9HoiMQPNPfT1V5JoFAC5GG7tRoot	0%	Avira URL Cloud	safe	
http://https://bc3-production-assets-cdn.basecamp-static.com/assets/packs/libraries-a6ab6002c86dc39bd54d.js	0%	Avira URL Cloud	safe	
http://https://public.3.64149-dc5b-475a-9b3e-4a282877b833	0%	Avira URL Cloud	safe	
http://https://bc3-production-assets-cdn.basecamp-static.com/assets/billing-4200b9e83e3eb94932d80c6cbcaca79	0%	Avira URL Cloud	safe	
http://https://bc3-production-assets-cdn.basecamp-static.com/assets/fonts-0adca736826e5341a26aa294e6302bb22	0%	Avira URL Cloud	safe	
http://https://mibghgh.weeblyamp.com/p/9HoiMQPNPfT1V5JoFAC5GG7t	0%	Avira URL Cloud	safe	
http://https://public.3.Root	0%	Avira URL Cloud	safe	
http://https://bc3-production-assets-cdn.basecamp-static.com/assets/rich_text-7df2a91e108ef44ef372558ec3956	0%	Avira URL Cloud	safe	
http://https://mibghgh.weebly	0%	Avira URL Cloud	safe	
http://https://bc3-production-assets-cdn.basecamp-static.com/assets/public-e8b06a8ee10d5c07ccf7e91ef27eaae0	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pages-wildcard.weebly.com	199.34.228.53	true	false		high
3.basecamp.com	64.202.125.15	true	false		high
d30fxesrqrvb2r.cloudfront.net	13.224.94.73	true	false		high
weebly.map.fastly.net	151.101.1.46	true	false		unknown
beanstalk.37signals.com	130.211.11.159	true	false		high
public.3.basecamp.com	64.202.125.18	true	false		high
mibghgh.weebly.com	unknown	unknown	false		high
cdn2.editmysite.com	unknown	unknown	false		high
cdn1.editmysite.com	unknown	unknown	false		high
bc3-production-assets-cdn.basecamp-static.com	unknown	unknown	false		unknown

Contacted URLs

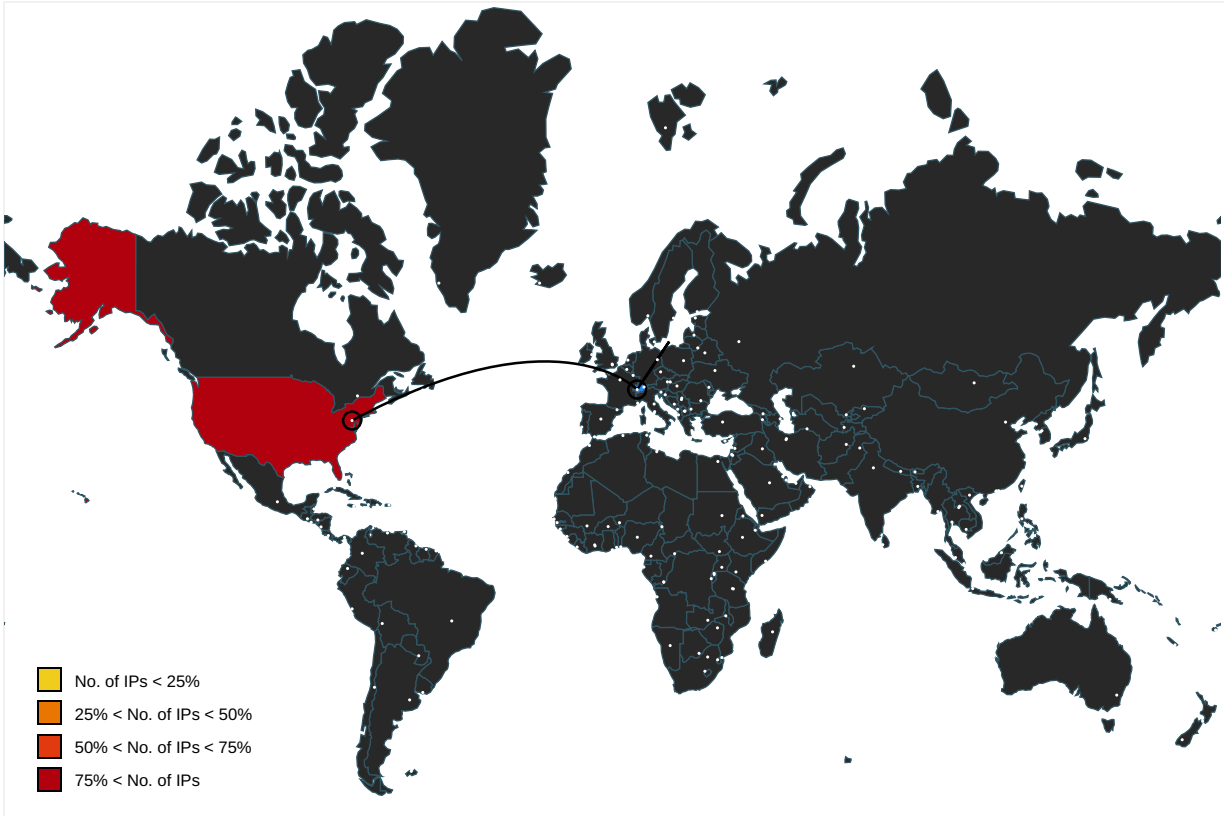
Name	Malicious	Antivirus Detection	Reputation
http://https://mibghgh.weebly.com/	false		high
http://https://public.3.basecamp.com/p/9HoiMQPNPfT1V5JoFAC5GG7t	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://public.3.basecamp.com/favicon-32x32.png	imagestore.dat.2.dr	false		high
http://https://bc3-production-assets-cdn.basecamp-static.com	9HoiMQPNPfT1V5JoFAC5GG7t[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bc3-production-assets-cdn.basecamp-static.com/assets/desktop-09334a52f8be90f7ab2c69fb59eb0ea	9HoiMQPNPfT1V5JoFAC5GG7t[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://public.3..com/m/p/9HoiMQPNPfT1V5JoFAC5GG7tRoot	{6043F06E-77F6-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	low
http://https://public.3.basecamp.com/p/9HoiMQPNPfT1V5JoFAC5GG7tamp.com/p/9HoiMQPNPfT1V5JoFAC5GG7tRoot	{6043F06E-77F6-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://bc3-production-assets-cdn.basecamp-static.com/assets/packs/libraries-a6ab6002c86dc39bd54d.js	9HoiMQPNPfT1V5JoFAC5GG7t[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://mibghgh.weebly.com/m/p/9HoiMQPNPfT1V5JoFAC5GG7thttps://public.3.basecamp.com/p/9HoiMQPNPfT1V	~DF6BBB7B606C065428.TMP.1.dr	false		high
http://https://public.3.64149-dc5b-475a-9b3e-4a282877b833	{6043F06E-77F6-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	low
http://https://public.3.basecamp.com/p/9HoiMQPNPfT1V5JoFAC5GG7tRoot	{6043F06E-77F6-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://bc3-production-assets-cdn.basecamp-static.com/assets/billing-4200b9e83e3eb94932d80c6cbcaca79	9HoiMQPNPfT1V5JoFAC5GG7t[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bc3-production-assets-cdn.basecamp-static.com/assets/fonts-0adca736826e5341a26aa294e6302bb22	9HoiMQPNPfT1V5JoFAC5GG7t[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://public.3.basecamp.com/buckets/20950190/vaults/3492664608	9HoiMQPNPfT1V5JoFAC5GG7t[1].htm.2.dr	false		high
http://https://public.3.basecamp.com/p/9HoiMQPNPfT1V5JoFAC5GG7t	~DF6BBB7B606C065428.TMP.1.dr	false		high
http://https://public.3.basecamp.com/p/9HoiMQPNPfT1V5JoFAC5GG7tNYou	~DF6BBB7B606C065428.TMP.1.dr	false		high
http://https://mibghgh.weebly.com/m/p/9HoiMQPNPfT1V5JoFAC5GG7t	~DF6BBB7B606C065428.TMP.1.dr	false		high
http://https://mibghgh.weeblyamp.com/p/9HoiMQPNPfT1V5JoFAC5GG7t	{6043F06E-77F6-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://mibghgh.weebly.com/	~DF0D8C6DAD15B4076B.TMP.1.dr	false		high
http://https://mibghgh.weebly.com/Root	{6E5CB5AC-77F6-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://mibghgh.weebly.com	9HoiMQPNPfT1V5JoFAC5GG7t[1].htm.2.dr	false		high
http://https://public.3.Root	{6043F06E-77F6-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://bc3-production-assets-cdn.basecamp-static.com/assets/rich_text-7df2a91e108ef44ef372558ec3956	9HoiMQPNPfT1V5JoFAC5GG7t[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://mibghgh.weebly	{6043F06E-77F6-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://bc3-production-assets-cdn.basecamp-static.com/assets/public-e8b06a8ee10d5c07ccf7e91ef27eaae0	9HoiMQPNPfT1V5JoFAC5GG7t[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
64.202.125.18	unknown	United States		25657	BASECAMPUS	false
64.202.125.15	unknown	United States		25657	BASECAMPUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
130.211.11.159	unknown	United States		15169	GOOGLEUS	false
151.101.1.46	unknown	United States		54113	FASTLYUS	false
13.224.94.82	unknown	United States		16509	AMAZON-02US	false
199.34.228.53	unknown	United States		27647	WEEBLYUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358583
Start date:	25.02.2021
Start time:	21:48:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://public.3.basecamp.com/p/9HoiMQPNPfT1V5JoFAC5GG7t
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 • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.win@5/26@13/6
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://mibghgh.weebly.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, 13.88.21.125, 104.43.193.48, 104.42.151.234, 88.221.62.148, 168.61.161.212, 51.104.139.180, 152.199.19.161, 184.30.20.56 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs.microsoft.com, ie9comview.vo.msecnd.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, 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\DOMStore\IV79EF3F\public.3.basecamp[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FE D
Malicious:	false
Reputation:	low
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{6043F06C-77F6-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	51400
Entropy (8bit):	2.0695242709757293
Encrypted:	false
SSDEEP:	384:rJEPCiLCLyJayf5yX5eO5esuEuTuaupuHuh:D
MD5:	3C860EEE0DC6FB6F348C30385D4C89F6
SHA1:	A1996C5774844DEEFB0F11DED289B755670D6DA2

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{6043F06C-77F6-11EB-90E4-ECF4BB862DED}.dat	
SHA-256:	FD9DF29B3E864E5AD4A1792AFE5A4F658B097230EA841CB62A57782862F9B664
SHA-512:	36F31BD79AB679C259C5ED53F8840175B0F829C5EE5139768F200FC27A3B4BC83A0255A0AB3F10055DB5C55F2BD1CE83F12B6F3AE03BE0327FA8FDD70BFD249C
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\{6043F06E-77F6-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	40902
Entropy (8bit):	2.04004764813314
Encrypted:	false
SSDEEP:	192:r2ZpTQD6Nknj52tWdM17ag8AmuY4j44t4L4hiC7dL:ry2m2jIEuFnBmTVKyG9
MD5:	93F4F86A80FB14B6D96E65841A29EAD0
SHA1:	B44A915219998810ECBE52C519D11E7479FA6ED8
SHA-256:	E59DEFF23C0CF7C83B58EC2FD4706099430F5FE65DD45926057083A0E2B011B4
SHA-512:	77B2315A7D109D5CCAAC9FD9954A7DCAC4E03151D711B9A96142CD4A4809CBBA33D4DD536615C5DE874B7A141273955B05CD7068F87A396D48BD0200C398CF6
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\{6043F06F-77F6-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5629150766363615
Encrypted:	false
SSDEEP:	48:Iw8Gcpr7ZGwpawG4pQIGrapbSxGQpKbG7HpRcTGIpG:rgZ7TQw6WBSLaaTIA
MD5:	45B50D6EA1F5764C45A40EB7D775AA36
SHA1:	BAA65AAC983EA0A22A3B1547B754CDE0273B5A4D
SHA-256:	5EB67BCF0A7C98E6BFC225E0B1B1238CE21207FD9AB19C3F9D34C9076B4FBA22
SHA-512:	A415F294F8E1EBBAC85D28D3C2D6B5B62B3582D3DA431B1918E3137AD287ED0056D5C52F8872823EF8A16216BD46DCA1358A858CB2E2B9BECDD46199D7C2A84
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\{6E5CB5AC-77F6-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24164
Entropy (8bit):	1.6236380601926026
Encrypted:	false
SSDEEP:	48:IwnGcpriZGwpaeG4pQyGrapbSGGQpBSGHHpcgTGUp8fGzYpmmqGopSQKFA/GmXpm:rNZiTQe60BS+jp2oWtMF4HAHg
MD5:	AF9B2F1C08A4275B958A5D3F2F0EBBC0
SHA1:	E500C6F0480B92E1B1F96683095838E9A8E8BB28
SHA-256:	C57B2EBC71C8A89D0A51A3B1A56C6D3ECD233F8C8C8B3D5D057253605BB0804E
SHA-512:	4061FD8FF6F2315EBE02D905A6481F7CFDA68B99FB6EFB2AE551CC88B0009129FBDAB7D28AC00C54B94F86B23F8174CE5D65BF37326BE48D317C35772D3B748
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{6E5CB5AC-77F6-11EB-90E4-ECF4BB862DED}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{6E5CB5AD-77F6-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5639911601291632
Encrypted:	false
SSDEEP:	48:Iw2GcprBZGwpaOG4pQ6GrapbSyGQpK1G7HpRCTGIpG:rqZBTQu6sBSaAkTWA
MD5:	39A549490D7D90603B63450EF5CCB1E2
SHA1:	3278BC888A30F7D5A7A493C433316952F54CD667
SHA-256:	6C19303665C58479920EF3EFEC9DE3783764DE9D8CCB410B6BC5F0AE3D688C50
SHA-512:	AD31046E1A1915BE05D6695895AD53C1A0D279EFC69D7149805FC2E81DE41D21A0591C8091D7BD1C178CBDEDB8755C09731271C0FA849142EC6CFFAA95C77F 3
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	2450
Entropy (8bit):	7.69186596823512
Encrypted:	false
SSDEEP:	48:UInneQzFhtb7xLFZ5bcbzN++Qf1QSK1IGUVVUyeJdp1wT3ltsjEHY:nt7xP5gbU+CySpGUdoC3lty
MD5:	CEAE00A6E6FFA00EB5317AACB97BBE7A
SHA1:	F2D741D9FE137378E7288E0F8E23BC7E4CFBBAF0
SHA-256:	72D17C97D1F6BFCE77D76F7D7B2E309288E5540706F4825444D319CB111E8D9C
SHA-512:	F73D32BA5A3F34665E6A6B71110BD01F5123ADA7535C9D17C9E842804DBF588888E98B592DBACD723AA5A431F2C6BE21CC859760D299D17D0A6BE1DB5BCD5D 9F
Malicious:	false
Reputation:	low
Preview:	/.h.t.t.p.s.:././.p.u.b.l.i.c...3...b.a.s.e.c.a.m.p...c.o.m./.f.a.v.i.c.o.n.-.3.2.x.3.2...p.n.g.....PNG.....IHDR... ... .szz.....gAMA.....a.... cHRM..z&.....u0...`..:....p..Q<....bKG D.....tIME.....&....2....IDATX..{pU....{.s....}.!1..... ...Sy.SQ.L.U.d...Aig..u.Q..'u...j:V.....ZZ.E..... ...>rs.g..q..4.:....=.g....|...^{....C.'.u..G7....v ...N . ..K.....[...3..".&`...9.|.l...}= "#...w...UHf..D\.....fSdz.d.,.Sk..h^.~.t.....x..W...3.Nv.N..1/g/:...$-.ih.|I..E.cN.s*..]J.x...P.-.b....&$.....~...l.t.I&SaR.....!..X03....2.$.....@.p$.5.o.j.....B...`),..T..P<:F..".58q..:/ ...h....x..&fW.A.....4.....x.....e...".Z..L..A..l..!.}I...!+)8....?.uO.}...~6.9...A.... :..7.,....yY..ku.K.x.VV..Fzz.....<.bqI.6?.xm..>...!.].)...~4....V....2$.....P...f.....K.p;U..ZC.ih*'DP...{9..@. .U.M)(...B?.x..U.I&...[Gs...M....-...z...tLX".z....XP.@i.;.C.= .....}5.).j}..'..aaU.+.....a....?5.?..s..7...{[....3`..N?.....A...E.@_TR..OO.$?'.K[.YWV.-Z..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\31AC96_1_0[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 46052, version 0.0
Category:	downloaded
Size (bytes):	46052
Entropy (8bit):	7.9887889934165575
Encrypted:	false
SSDEEP:	768:7JzF4duQslnWgRpPD+dfFhPaHQBFmMvhEhc28OeNHxa++JdI4qUEkXqfjkHT:7dF4diWIJSpTawBFt+wOoRa3r0UEk6b6
MD5:	61F3BC4FC6146CC65961A8C8E917855A
SHA1:	02E25E22CF1C0A26D838A477B1F21BF33B71CA38
SHA-256:	AABC1A485E0941F1E2927B6A4BEED2B368431466977483068BBE367DE253A05C
SHA-512:	77CDA181F023FF6597D3B7A0FD269CEE76306EA650E2CC6FDDCBEF675C245B3D9F95178FE8A9D5EF65A5D8CA3DC0D3F675DBFB49DB05DAFC1FE822D79506(7B4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn2.editmysite.com/components/ui-framework/fonts/proxima-nova-regular/31AC96_1_0.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\31AC96_1_0[1].woff	
Preview:	wOFF.....W.....x...l.....OS/2.....X...`.>..cmap.....cvt ...$...(...(....fpgm...L.....C>..gasp.....#glyf..,.....<head...d...6...6....hhea.....!...$.d.rhmtx... ....\...@...loca..$<...W.....d.maxp...D... ... ....name..... ..l.post.....|..)D..D.prep.....v....zQ.....P.`..`.....d.F.....AB..t_.<.....|..E...p.....x.c`f.c..... ....D.....X.A....S;P....rs.....~.0.....<.....|...c..@J.....)x..ytU.....d . ...r..mm)H..H....*.b.. Z)....EdJ.$.2.y0B.*.Ae...C....=...0F...g..j.._..k...a..Z.|{.P..X.....[H@M.1Y.Z.1...0..#..9. 3.....&...2T..V...U$../.e.L.dI.%.F2$Kr4um]W...~N?....:E.....K.`...e...X#...E.m;...-.i..-..v.....=.l'.K...j;..jos4p4t...#.....Hq*gMg]g}g....r>...s.vnt..N.....S#.^...ZD..Q.lgYQYIYi..[. .....6Z.qt.@..H.....*.>..?y..|.L2.I2Cf.2Y+.d.!W.....nk._.:Y....RV.eYN...g....y.!o`G...a.....|.=.N....2{.....'..O...eGr.y=C..>. g..V..*..e...r.r.n

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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):	2318
Entropy (8bit):	7.797964457453817
Encrypted:	false
SSDEEP:	48:gneQzFhtb7xLFZ5bcbzN++Qf1QSK1IGUVVUyeJdp1wT3ltsjEHT:6t7xP5gbU+CySpGUdoC3ltN
MD5:	BB5321E1CB9B06F7573B5134772CD790
SHA1:	CDB34803B4EF038770A4F1B7265112ED7FCC3754
SHA-256:	60DC043471398565D32B4966ADAFEEDF804E1F9DA1E4F2E79D11684FA931230F
SHA-512:	7B0A7F55012655A067373EAA67902B82F1F4A34438F0262709F69725C85E31520555F906996EDDB9E7920414767ACDE6FEBAF2A1253489AC6B27CE76B4AF4AE8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://3.basecamp.com/favicon-32x32.png
Preview:	.PNG.....IHDR... ... .szz.....gAMA.....a.... cHRM..z&.....u0...`..:....p..Q<....bKGD.....tIME.....&....2....IDATX..{pU....{.s....}.!1..... ...Sy.SQ.L.U.d...Aig..u.Q..'u...j:V .....ZZ.E..... ...>rs.g..q..4.:...=.g....|...^{....C.'.u..G7....v ...N . ..K.....[...3..''..&`...9.|.l...}="#...w...UHf..D\.....fSdz.d.,.Sk..h^.~.t.....x..W...3.Nv.N..1/g/:...$-.ih.|I..E.cN.s*..]J.x... P.-.b....&$.....~...l.t.I&SaR.....!..X03....2.$.....@.p$.5.o.j.....B...`).,..T..P<:F..".58q.../...h....x..&fW.A.....4.....x.....e...".Z..L..A..l..!.}I...!+)8....?.uO.}...~6.9...A.... :..7.,....y Y..ku.K.x.VV..Fzz.....<.bqI.6?.xm..>...!.].)...~4....V....2$.....P...f.....K.p;U..ZC.ih*'DP...{9..@..U.M)(...B?.x..U.I&...[Gs...M....-...z...tLX".z....XP.@.i.;.C.= .....}5.).j}..'..aaU.+.. ...a....?5.?..s..7...{[....3`..N?......A...E.@_TR..OO.$?'.K[.YWV.-Z....-..7.7v....|RAEY..n.F..{$...i .....%....?X.c_..)a..*.G..E...9.....>...^.v....N.M"%,....f..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\public-e8b06a8ee10d5c07ccf7e91ef27eaae0ca5404d0c4d5ba63c7fc633b29923020[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	86791
Entropy (8bit):	5.566738227460659
Encrypted:	false
SSDEEP:	1536:QF/UQBU4yJDNzcD2v42e3XIzaJxxjt7YNqBY1WnusZYltRtc4U7jG6sKb5G5GWfD:QF4xJDNAD2v42e3XIza7YNqy67jGR6oL
MD5:	2C62A42A265EB61425AA177A7EA220B1
SHA1:	749500441C8A8C98A2FBF9C2689FF167DB3709CF
SHA-256:	1D2617B41B6304457C8B3741BA2A81410E6DD5B353736242B9B7BA83E38C6634
SHA-512:	7032C7D5E7A579B44A7D781F0D9AA37EFE417487E9A2C2885E9521B2B9478060E8258CC1D0B68C92761702FB5D04D0E4F4CFED4ECF7F84C353E87DCC867E134
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bc3-production-assets-cdn.basecamp-static.com/assets/public-e8b06a8ee10d5c07ccf7e91ef27eaae0ca5404d0c4d5ba63c7fc633b29923020.js
Preview:	(function(){this.BC={Timeline:{}}}).call(this),function(){var e,t;BC.animateElementWithClass=function(t,u,n){return e(t,u,"animationend",n)},BC.transitionElementWithClass =function(t,u,n){return e(t,u,"transitionend",n)},BC.shakeElement=function(e){return BC.animateElementWithClass(e,"oops-shake-it")},e=function(e,u,n,a){var s,i,r,o;return o=!1,r=function(){if(!o)return o=!0,e.removeEventListener(n,r),requestAnimationFrame(function(){return e.classList.remove(u),"function"==typeof a?a():void 0})},e.addEven tListener(n,r),e.classList.add(u),i=(s=t(e,n))?s+200:500,setTimeout(r,i)},t=function(e,t){var u,n;if(n="animationend"===t?"animation":"transition",u=getComputedStyle(e)[n +"Duration"])return/ms/.test(u)?parseInt(u,10):1e3*parseFloat(u)}}.call(this),function(){var e,t=[].indexOf||function(e){for(var t=0,u=this.length;t<u;t++)if(t in this&&this[t]===e)return t;return-1};BC.arrayFrom=e=function(e){var t,u,n,a,s;if(Array.isArray(e))return e;if(null!=Array.from)return Array.from(e);if(null!=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\31AC96_0_0[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT)
Category:	downloaded
Size (bytes):	38931
Entropy (8bit):	7.976189653860157
Encrypted:	false
SSDEEP:	768:ZcFgT73C8tQ56CjNW2HvS6aqRnnxjOKAOIxRn3wiElfaW1nu/PSE8NQYbv:Si3Cl7N8S2JAOIxl7OptuUr7
MD5:	7C30957EB7A237DF8696E09CBDDE124B
SHA1:	02C7B7953DBB7AE44F086A723DC947BE0E1AEE0B
SHA-256:	1DD1965136AE270F9FE9D8C318ACCE7D00F637BF54F128683AFB4DDDA45C1343
SHA-512:	E508D7C51F7C4C5B2D1B795C8492D84DE2BC1A9E6F885232958820D555F0FDCA83643044BCB69923BFF1706ED39CAF5AABBD75B6B7F99CA8F4EF8108B8E121E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn2.editmysite.com/components/ui-framework/fonts/proxima-nova-light/31AC96_0_0.eot?

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\31AC96_0_0[1].eot	
Preview:	.....LP... ....|.....&....V.e.r.s.i.o.n. .3...0.0.1.;.c.o.m...m.y.f.o.n.t.s...m.a.r.k.s.i.m.o.n.s.o.n...p.r.o.x.i.m.a.-.n.o.v.a...l.i.g.h.t...w.f.k.i.t.2. ..h.F.J.o...&..&P.r.o.x.i.m.a. .N.o.v.a. .L.i.g.h.t.....BSGP..... P.....(.....Y.D.N....x...>..KPJQ....n..6....@.J..*.I.U.....L..io..{?X..\xG..70...o.n-&.....&LW`x..Sk."Z..j..N'...&. ....9].<8.e8.*...._.d.Im.d..KR|...Bl.....gPF.lwku.xn..Qv.zz....0.A.$.....d{@O...q_.,F-.^...T`p..<..*...i..k~W..?;.y0o.I..Qr.".m.$....4.s.....CO....`..p.r...Ri,..;...).....I.p..D=Z(....E.j.q..9../; (.....'\...K8].....X...../.Q.....Y[.y.L..9..Y.|.G.{...DcC"...F<.N..>...qO.....00f..x.....j{..\.A.....Q;[..l.;r..L7@.?shQc.].....V]1..... .G_.....E.0^.,.LD..Qy....Q9.1.Y..Y...fC.a. [.],..(..6}dd....qz.a.f..e..D.y.....e.X..('*..|.Mb..z\..{%)d/...y7.S...\M..a1...'a.....12..X ..b...N.X...1.D.F.C.....i.HK.Q..\.j.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\31AC96_2_0[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT)
Category:	downloaded
Size (bytes):	38300
Entropy (8bit):	7.974402289492323
Encrypted:	false
SSDEEP:	768:v/2N3fpmfNc5fQ7RhbCclfmR4On5mg6XKvqm1bGYv:XY3fUfOfQlNoqOnsKCmhGYv
MD5:	12B5BF0F4F082E07C41803E75183EFF8
SHA1:	51C2C509B0DA204C6E4ED1E3F164927BA265263E
SHA-256:	8F19E7604EE75D48AB7EB5E8F4D14E35BAB7E79B9E44890828504283C45C213D
SHA-512:	BB50EE62D565B3261197938780F5FDFE513A1D18298ECA00819306B7B5F35878A236318E8CEA7D7ECCE181A48B29073486E72A6EA5625EC1ABBA5ABA7D5C16B 2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn2.editmysite.com/components/ui-framework/fonts/proxima-nova-semibold/31AC96_2_0.eot?
Preview:	....f.....LP... ....&....V.e.r.s.i.o.n. .3...0.0.1.;.c.o.m...m.y.f.o.n.t.s...m.a.r.k.s.i.m.o.n.s.o.n...p.r.o.x.i.m.a.-.n.o.v.a...s.e.m.i.b.o.l.d...w.f. k.i.t.2...h.F.J.o...,..&P.r.o.x.i.m.a. .N.o.v.a. .S.e.m.i.b.o.l.d.....BSGP.....F.....Y.D.N....x...>..KPJQ....n..6....@.J..*.I.U.....L..io..{?X..\xG..70...o..-&....^.Rrd.v..?...- ..qT.....w9.....].Lr..$+.\T....Mr.w17R1.#..2!...grFU.....RN...x.....O.....$Y.n.f..t.....;p;W.1i..W.....xKp`.U~.(CXZ..w.$Ns.1P..#._..E.:.....p.fn=....X.....?[.jUQ....'B._. `.LC....# .Q....+...$.G..Ql.+..Y..l..+a*.UJP[...qA..3b.zE@h..'..r.$.....;.0..tN..b4..},4.L6..mk.y..h.V.\]M..K.A.-1..W....._....]..]....O..&G.....2.....];y.[`.d`.F.h.]q.^Y..U]$I...a..U.....a.W.... .91..Y.....T.U.z/Cn.b.[NA.DIBzl.D..(.Wm...t.ES.....$Bj..Z0ub`.k2....Pp.F.6.`...v#.y.H.8bj.SL...+.K..Y...<.V....l'..b.&6..L...b..p.....#.....V..U.....\x8..v...xYA.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\desktop-09334a52f8be90f7ab2c69fb59eb0eaf1a2a7c3015b9151b4e641a 93284fe9d1[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines
Category:	downloaded
Size (bytes):	494264
Entropy (8bit):	5.2066400059494375
Encrypted:	false
SSDEEP:	6144:Y9N3DxHp9N3DxHLlsGFCJVyDWTKOeASS16l5Y9ofh:cFCuYSS+
MD5:	2D9C48D6330C135EB1224B69A2F0915D
SHA1:	70F5450AD2718BEAD8A3C5163C7401FF256A3BD3
SHA-256:	19AEED5179B3110518DD2CD4A88380E3CC73C509038F81C865EDA51537965BD5
SHA-512:	E544255AF1C78FE5EE1E84272186574C0E4889CBD3BD896907B625A3FCAE26833B4CB1C933527975DF9B101815167B65E172409DE25AA26DE840EBD306FBD23
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bc3-production-assets-cdn.basecamp-static.com/assets/desktop-09334a52f8be90f7ab2c69fb59eb0eaf1a2a7c3015b9151b4e641a93284fe9d1.css
Preview:	./*! normalize.css v3.0.1 | MIT License | git.io/normalize */html{font-family:sans-serif;-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%}body{margin:0}article,asi de,details,figcaption,figure,footer,header,hgroup,main,nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-align:baseline}audio:no t([controls]){display:none;height:0}[hidden],template{display:none}a{background:transparent}a:active,a:hover{outline:0}abbr[title]{border-bottom:1px dotted}b,strong{font-weight:bold}dfn{font-style:italic}h1{font-size:2em;margin:0.67em 0}mark{background:#ff0;color:#283c46;text-decoration:inherit}small{font-size:80%}sub,sup{font-size:75%;li ne-height:0;position:relative;vertical-align:baseline}sup{top:-0.5em}sub{bottom:-0.25em}img{border:0}svg:not(:root){overflow:hidden}figure{margin:1em 40px}hr{-moz-box-sizing:content-box;box-sizing:content-box;height:0}pre{overflow:auto}code,kbd,pre,samp{font-family:monospace, monospace;font-size:1em}button,input,optg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\libraries-a6ab6002c86dc39bd54d[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	436577
Entropy (8bit):	5.313317571692481
Encrypted:	false
SSDEEP:	6144:v0pVcJIGHPmICr9LtP5P/dWjEqqMfmv7gY:EcJIgCnXWj/X6
MD5:	0697FC0B478CFBD5D146879015679A41
SHA1:	839820629A3134D8D138DC722F128799F48E633B
SHA-256:	D7A0E827B469575FDBB6C1FF092E37AEB1E133ACCBCF31950FABB5BCF1B6A554
SHA-512:	61A57F31481CBD2D2421F56D5762D0BB97C2E3B93C5401FC8E59C6C894B149E6F99F2E2109B9B3E931F94A20B1E30E85E721908BBD9DBC3084EACE92BDDD57 4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bc3-production-assets-cdn.basecamp-static.com/assets/packs/libraries-a6ab6002c86dc39bd54d.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\libraries-a6ab6002c86dc39bd54d[1].js	
Preview:	!function(t){var e={};function n(r){if(e[r])return e[r].exports;var i=e[r]={i:r,l:!1,exports:{}};return t[r].call(i.exports,i,i.exports,n),i.l=!0,i.exports}n.m=t,n.c=e,n.d=function(t,e,r){n.o(t,e)||Object.defineProperty(t,e,{configurable:!1,enumerable:!0,get:r})},n.n=function(t){var e=t&&t.__esModule?function(){return t.default}:function(){return t};return n.d(e,"a",e),e},n.o=function(t,e){return Object.prototype.hasOwnProperty.call(t,e)},n.p="https://bc3-production-assets-cdn.basecamp-static.com/assets/packs/",n(n.s=151)}([,,,function(t,e){var n=t.exports="undefined"!=typeof window&&window.Math==Math?window:"undefined"!=typeof self&&self.Math==Math?self:Function("return this")();"number"==typeof __g&&(__g=n)},function(t,e,n){var r=n(127)("wks"),i=n(90),o=n(3).Symbol,a="function"==typeof o;(t.exports=function(t){return r[t]||(r[t]=a&&o[t]||(a?o:i)("Symbol."+t))}).store=r},function(t,e,n){var r=n(3),i=n(6),o=n(79),a=n(80),s=n(12),u=function(t,e,n){var c,l,f,d,p=t&u.F,h=t&u.G,g=t&u.S,v=t

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\fonts-0adca736826e5341a26aa294e6302bb2284836e97151246bbe094a75e994e2fc[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	207798
Entropy (8bit):	5.923284654738747
Encrypted:	false
SSDEEP:	3072:0SWTG/p0BuDZN8lIs9De9nPHUy1tT7FviU/v4fPt3NTC5SctgSPrqeLgqh:0cpWuDH8Sle9nP0yJ5/vgVqHtgrsgy
MD5:	2F8E5177916AE095C90A065ABAE35143
SHA1:	36261FC1EA18909D8BDC362A3AD914F3C6FF8005
SHA-256:	C112991B36561E40E831982DBDE30560A8A4DA1A9F8BBD4426DE35FEA6CA6429
SHA-512:	1DB787704441FF814FE9246982054057CD589419791A1AD7B7836CBE38D0A7EFC25C0D61F4D6B9C75659AC3851584EA732AA323DD662E7CC756F5DD805A802B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bc3-production-assets-cdn.basecamp-static.com/assets/fonts-0adca736826e5341a26aa294e6302bb2284836e97151246bbe094a75e994e2fc.css
Preview:	@font-face{font-family:'Graphik';font-weight:normal;font-style:normal;src:url(data:application/font-woff;base64,d09GRgABAAAAAQ36ABIAAAACfngAAAAAAAEMvAAAAT4AAAJ9AAAAAAAAAABHUE9TAAC7oAAASNoAAP3sydoFQUdTVUlAAQR8AAAIPgAAEqAgYeHsTFRTSAAACQwAAAAWAAAC%2Fb%2B%2BwcBPUy8yAAACEAAAAFUAAABgaRJyvmNtYXAAAApcAAADUQAABLgAgjzPY3Z0IAAAD7gAAABIAAAASBBGAu9mcGdtAAANsAAAAPgAAAFhkkIa%2Bmdhc3AAALuUAAAADAAAAwABwAHZ2x5ZgAAFegAAJbIAAEunN9HnXFoZG14AAAJJAAAATgAAAMEx7nTq2hlYWQAAAGUAAAANgAAADYEm1S9aGhlYQAAAcwAAAAhAAAAJAdCBcloboXR4AAACaAAABqMAAAvkcreh8GxvY2EAABAAAAAF5QAABfT2c0AkbWF4cAAAAfAAAAAgAAAAIAUTA0FuYW1lAACs0AAAAesAAARzXmkLLHBvc3QAAK68AAAM1wAAGQVieOv8cHJlcAAADqgAAAEQAAABfVFhmW0AAQAAAAEAAO1v8nRfDzz1ABkD6AAAAADLdRiIAAAAANaO99L%2FIP8kBEoEWQAAAAkAAgAAAAAAAHjaY2BkYGC%2B%2Bt%2BWgYGl6L%2FCfwUWLwagCDJg%2BgkAhPUGFAAAAAABAAAC%2BQBkAAcAYwAFAAEAAAAAAAAoAAAIAAngAAwABeNpjYGbSYZzAwMrAwLSHqYuBgaEHQjPeZTBi%2BAUU5WZlZmZiYmNiBrLbGZCAs7%2BvL4MDA8NvJuar%2F20ZGJivMhxWYGCYD5Jj4mY6zaAAhDwArJYOnwAAAHjahZZ7aNZVGMe%2F55y3wmY287rppnNz7e7c2s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\weebly-logo-blue[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 174 x 62, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	3740
Entropy (8bit):	7.667019795291803
Encrypted:	false
SSDEEP:	96:n/vYP8+xpcOARUGDc8tYwolxPIw+Dyh056Jx+O:y8h3Cc2h05Wxn
MD5:	6907726EDE4FC851BEEAFB7B9FF6EEB9
SHA1:	86B1E9AF4A07E02A426EC9475E37A13DFCEDCB3C
SHA-256:	2B37CA56C61B7F2F892D75655CC37699EF847DD9139C94171414E5F92FFD97ED
SHA-512:	11A22B8DBE694646895F16D38738C3A481DB168C7CA0D92A247BD35078FA1AC13153B5ADE7EFFDE36FA5DA10AB9EDE1ADE5698EF477483D6EDB21EDA6B1F2DE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn1.editmysite.com/images/weebly-logo-blue.png
Preview:	.PNG.....IHDR.....>.....PLTE...-..*..*..*..)..)..*..+..I..+..*..*..*..)..)..)..3....)..)....,..*..*..*..)..*..-..)..*..+..+..*..7..+..*..*..)..)..)..*..)..*..*..*..*..)..+..+..*..+..9..)..)..+...+.....*..)..+..)..*..+..*..*..*..+..*..*..*..6..*..@..,..*.....+..*..*..*..*..*..*.....,..)..0..U..0...,..3.....1..*...,..*..)..*..)..*..*..*..3..+..*..+..+..)..)..)..)....*..)..*..*..,..)..)..)..+..)..)....)..)..)..*..+..)..*..*..@..3..*..-..)..+../..+..*..*..+..+..)..*..*..*..+..)..*..+..*..+..+..+..+...+..)..*..)..+..)..*..*..)..*..)..*..)..)..1..)..*..*.....*..*../..*..*..*..*..)..*..*..;..)..*..+..+..)..)..)..)..*..)..-..3...,..)..)..*..)..+..*...,.....*..+..)..*...,..*..+..+..*..-..)..)..+..)..+..)..)..)..+..+..)...,..+..)..)..)..*..)..*..)..*..)..*..)..+..*..+..+.....+..+..*..*..*..-..+...,..+..+..*...z.....tRNS."....M.d.....{....!E..t..-].....6s.....0....@q.C..1A.....[....#.2...+.....D....x.w....\...)o..`.F....c.b...?.G&_..TB.7..<.f.p*kL.....'gh....|..J

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\9HoiMQPNPfT1V5JoFAC5GG7t[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):	5102
Entropy (8bit):	5.335108613309519
Encrypted:	false
SSDEEP:	96:jFPEGb31qFF7QynYfdQ+cIYZV6hu6LDMz41QzFZefM:K+31qFF7QynJIS0wMMCQ1
MD5:	82242CBFF06085E6411121C3051B053E
SHA1:	17C00A5BDC341D5EDAEE80EF374C0A514E2D85B1
SHA-256:	554FC2CCC17094F0187E6BED727F947C5B378A5E1C6A81EEE63A3F1A79898F81
SHA-512:	026CB60738DE91E8FC202F4AC35E3F3B6C91CEA915A06B1778883AB1F307F8F4EF7FDBF5F18851AF595236A07F682F719248ACDAC3EC702F62A23575DC9480B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\9HoiMQPNPfT1V5JoFAC5GG7t[1].htm	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://public.3.basecamp.com/p/9HoiMQPNPfT1V5JoFAC5GG7t
Preview:	<!DOCTYPE html>.<html lang="en" class="" data-theme="">.<head>.<script type="text/javascript" data-turbolinks-eval="false">var Timing = { times: {}, mark: function(e, t) { Timing.times[e] = t || new Date().getTime() } }; Timing.mark("firstbyte")</script>..<meta charset="utf-8">..<title data-bridge-alt="You Got 1 Fax VoIP Note. Details Bel ow.">You Got 1 Fax VoIP Note. Details Below.</title>..<meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no">.<meta name="robots" content="none">..<meta name="referrer" content="origin-when-cross-origin">..<meta name="csrf-param" content="authenticity_token" />.<meta name ="csrf-token" content="chWXOgdwFxhC4xx5uGUFtjDEVZ1WehFVVsdUgZBwlulcaumbA3VJfC9OOBWO1JQO4S9yd-AlbBs91caiLFyLUg" />..<meta name="turbolinks-ro ot" content="/4972760" />..<meta name="turbolinks-cache-control" content="cache" />..<meta name="cable-url" content="wss://chat.public.3.basecamp.com/4972760" />.. <meta name="current-account-slug-path

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\Graphik-RegularItalic-Cy-Gr-Web-a10a70f48489dfe7e0ab1fe80eebaa027610df48 049f44cd1724ddcbce3ec509[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 73940, version 0.0
Category:	downloaded
Size (bytes):	73940
Entropy (8bit):	**7.991862566913847**
Encrypted:	**true**
SSDEEP:	1536:Bf9xdGq4WsE8l6qHdnLEzdFimXjgv6n5hPNBaAinOREhPeeL:Bf9x0q4W0PH6Tgvs14nCK
MD5:	B17BB2A0EA500EC4C31CBB96080B5AFE
SHA1:	CD5690833C747BD80971393BCE01F6F8B11ED6C9
SHA-256:	A10A70F48489DFE7E0AB1FE80EEBAA027610DF48049F44CD1724DDCBCE3EC509
SHA-512:	C396C110D433A3FD1AC56164DEE240052DC20A1D4AF278CF1B19A88E4C759EB953AB0F11A945C2A00E14695AA0BD563310A558E82494F680944B0CF103159275
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bc3-production-assets-cdn.basecamp-static.com/assets/Graphik-RegularItalic-Cy-Gr-Web-a10a70f48489dfe7e0ab1fe80eebaa027610df48049f44cd1724ddcbce3ec509.woff
Preview:	wOFF..... .....X.....D.....GPOS.....O...."+..OGSUB...X...7....9b.wOS/2.....U...`i.r.cmap...T...Q.....<.cvt .....H...H._..fpgm.....a.B..gasp...x.....glyf.....8.t ..3head...l...6...6.-.hhea.....#...$...jhmtx...@.....g..Lloca.....maxp..... ... ...Sname...t.....?@mpost...l.....3rTk.prep.....}.^.....?Sv1_.<.....u.....VFB. ..$.B.Y.....x.c`d``.....%....OX.._0.2 ....".....p...i.....x....x.c`fRg.....B3.e0b....feffb.eb...../.#..o&..m....2.V``...c.f:...<..5.b...x...l.W.....f.4...#e|.B...m..BK.e--E.. .2{1...:...Y..q,a.m...%.&N4..[..-*...&.. ...)...w...A.x.'...{>.....?..E.....Y.j...L].3...25.e.....@)W..jr..s....s..g.....Q../....j%Zg..`;..R....Q.;.)....'...)...R...R{.^...N.t..`..5.....B..>..3~y. .A..5..o.....>.k....2w@..m...%.).....B.....j.c..V.....r.9.h....=Fu.^..okT..0.=...5..2....%....?e....?..h.z.....)F..4...k..=M.....~.F.....}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\Graphik-SemiboldItalic-Cy-Gr-Web-9331e9964cf8f0a6ec536ecafb1cc fb7bde3bad32248b64a51b31142786bc3f3[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 79628, version 0.0
Category:	downloaded
Size (bytes):	79628
Entropy (8bit):	**7.992385547934622**
Encrypted:	**true**
SSDEEP:	1536:GIkeT0RHpMDXNdWGnRZrtevtXzc0xgXhohZ8n43vyr1np:GIgM3ZraVc00+zNar/
MD5:	14A6EDE8AC93E36D96D78FCF696FDAD8
SHA1:	D27CB2D866A51F97431F7B77EB61DC712E20D08F
SHA-256:	9331E9964CF8F0A6EC536ECAFB1CCFB7BDE3BAD32248B64A51B31142786BC3F3
SHA-512:	9541B8ACC86157874E83231B8784D237FE59612378CB7D17A860BF2A92324B18E304375459B56355DEBF2457D63B65C9F18844F0B0E9DF50B045AF3A92F9D563
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bc3-production-assets-cdn.basecamp-static.com/assets/Graphik-SemiboldItalic-Cy-Gr-Web-9331e9964cf8f0a6ec536ecafb1ccfb7bde3bad32248b64a51b31142786bc3f3.woff
Preview:	wOFF.....7.....5....D.....GPOS...$..._]../..k[+GSUB..-....C.....OS/2.....U...`i.t.cmap...`...Q.....<.cvt .....b...b.&..fpgm.....a.B..gasp.....glyf...,.....;. =...head...l...6...6.-.hhea.....#...$....hmtx...@.....}e.loca...<.....F.maxp..... ... ..."name.....?...post.....3..].prep.....*..... k.....H..X_.<.....x.....VF.....h.... .....x.c`d``.....e.....XZ._0.2 .....S.....j...h.....N....x.c`frf.``e``.....2.1...r.3331.21....H.....7.....W..+00...1q3.fP.B...Q.I...x...l.E....A....z,]..lIii.B.k9L.....H..\.i.4^ .h.A.*..c...A..A..G.Gb<A.E.(.9....7.[l....f.{3.....].f...-.@G.p.O...{.H.e.i.Q..}h...BF.*.e....f...K.l.z..~..)...W.J.>....iz....2.T. 3...%..R.,.4.....E.....\.?#..Sd..Z{..5.....x-...../O.....y2]. `.6.e.Y....5..%.....f.m.p.5[j..n.Y/.N.... Q....R..G.N..oJ$bJ.:.. ....2.7..R.D.....Q.Zjl.j....*.q...(.L.4..n.9.s.~.{7J.v...~..`.\;S..."s..2d2c7..$.Z

C:\Users\user\AppData\Local\Temp\dat724C.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 69114, version 0.0
Category:	dropped
Size (bytes):	69114
Entropy (8bit):	**7.990634841442928**
Encrypted:	**true**
SSDEEP:	1536:Ivb6vGR527CoPZDh6nHDQw6wSEruG9UrIYPaeDCzFN:Iv9Wv5wLSEruG9UrIGLDE/
MD5:	FCCD32C4512A8C252EB55BAFBA24F472
SHA1:	8DBCF712C1AE5FA5AB4421E85859A62C8D2C76D9

C:\Users\user\AppData\Local\Temp\dat724C.tmp	
SHA-256:	28FC14EF04AB26D01042FE366E72CD7AE3E76EB21FDABBD03319D3737F7459CA
SHA-512:	ABC6147CFA86FADB1E1D21C1CF6DF87BEDDBF7DE673B6D89AE78BC988E0CBFAA19CF4356F2BA50B03E1E5DF5260BD4430B984368FE47C9F15A07FFDA22103367
Malicious:	false
Reputation:	low
Preview:	wOFF.....~x.....>...}.....GPOS.....H.....AGSUB...|...>.... a..LTSH.....OS/2.....U...`i.r.cmap...\...Q.....<.cvt .....H...H.F..fpgm.....a.B..gasp..... ....glyf.....G.qhdmx...$...8.....head.....6...6..T.hhea.....!...$.B..hmtx...h.....r...loca.....s@$maxp..... ... ...Aname.....s^i.,post.....bx..prep.....}Qa.m..... .o.t_.<.....u..... .$.J.Y.....x.c`d``...../...2`.....d...c.....x....x.c`f.a.....B3.e0b....feffbbcb...../....o&..m....2.V``...c.f:...<.....x..{h.U....f6..ss.... .t.....4_../..pl....."[Y...U..D..EDV..I..aBZ.Oo...7.f....<..|...q...nZ.2.....U..U.....T.AZm...O.....^9.zU...Wi..]m>G..&..w..Uk.,.).;.^J.....}.....!..Z.G.6P.....4.....oC.#.X.2..1w ..}..9#...(..;...-....M.\.....=.s..}...7.....j.kU..[.vY....l..5....<...s.....>.D.B.... O..Z..Q.|oE.O.|..P.o.!.....0.g..

C:\Users\user\AppData\Local\Temp\dat727C.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 76130, version 0.0
Category:	dropped
Size (bytes):	76130
Entropy (8bit):	**7.992283303407725**
Encrypted:	**true**
SSDEEP:	1536:0XNh9ZMNO0L60R679aMJ1bAlAiC5jqMGsgOXHS+jYSRT:KONbUFJ18AikwhSh
MD5:	C0ABC3FF95FA29E0154416B04A69B174
SHA1:	280B46CA89DBF5983D4402BF1C9C2F443F6DF225
SHA-256:	2AFD0C6F1A0642526FB2DF8018C801CD21D5A428FD2618D17C0FC5EFE7552335
SHA-512:	D83753274E543A772ABD2B16CF7862677A0B8B7A5EFCC4DA5636C17398AAFA54A0479AA6C8C10874E823DC70A71FDDDDEFFF113BDBE65B36AA23A5FD333AF570
Malicious:	false
Reputation:	low
Preview:	wOFF.....)b.....p.....($...>...~.....GPOS.....U=....,...JGSUB.....C.....OS/2.....U...`i.t.cmap.....Q.....<.cvt .....b...b.&..fpgm...\.....a.A..gasp.....glyf.....A$.Q z.head...l...6...6..+.hhea.....!...$.}..hmtx...@.....~Gloca.....maxp..... ... ...#name.....yF.\|.post.....3..].prep...T...+.....{.'.....=..._.<.....L.....VE.....h..... .....x.c`d``.....e.....,.@.d.....p...c.....N....x.c`fre.``e``.....2.1...r.3331.11....H.....7.....W..+00...1q3.fP.B.....x..ol.....9.dB..J{.....{.....dC@.:%F.d.O. 00....l.D.[...&.p..f.b.ot.[.b.D7.e.1l.....u.w.o..s.s.y...<....kp[5.^R.uj.=.f.Z...*hJ=n.:....Z.Ky.:.M.\.....~.f.Ev..W..O..n.2{LE;....&.QUv...^.x.e../h..^....*.....M..i...4.n.{..../1...(!.`.?.?t.} ...k.^S...}..&....S.....V....yn\kl.2...ne..j.a5....3.....kN.l5.M.....,.v4...5..).N..~m.....m...U....-.....=...h.v..i5.1doW#:..a}..V..$..D.ql.K.F...j.

C:\Users\user\AppData\Local\Temp\~DF0D8C6DAD15B4076B.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34357
Entropy (8bit):	0.34546280763037485
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwE9lw09l2C9l2i9l/mF:kBqoxKAuvScS+XZbSmImsQKFAn
MD5:	120541B8D7CF2D7D0A3B747127F6BA10
SHA1:	D3FF1DF3B2DC9B719579074A05A32663DBA2858A
SHA-256:	54DFF38A2F0FDDDBC464612D35076DD46FCF04823ED061B4EB316AFA642C79DE
SHA-512:	50CB9B790A50558E4F4B274B47EE0B5C4F091D9141FCA14EFFA03CF9EBB1160454B482B86E2798AC47ED8BE263C011577A912E80C870CC2BE01CCE6F2C52DBD2
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF1C7CA79F6B9C8B59.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

C:\Users\user\AppData\Local\Temp\~DF1C7CA79F6B9C8B59.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF6BBB7B606C065428.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	49045
Entropy (8bit):	0.6869073714079538
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+yU+XkjDbDwvpKUfwsh4AewvpKUfw3w7Ae7KUfw3:kBqoxKAuqR+yU+Xkj3mp4ol7
MD5:	9D6E0B08307C928C09E0E54DD5F2A546
SHA1:	22F9EC3FDEFCBED0F046B1719ED73874EDA9A73F
SHA-256:	661DEC78A4552A4CCE52C650E97B6B31FD1DC3093AC64C80778EFDE40BB0D92E
SHA-512:	9FCCE0A944FB2D1BE50C282DFBE1DC32928075CC7DEBCDD5DFCB96B61AB5B9C84127A43BE14047F4C35777CA63660B5C52376B4080F7379400EF2E04AB4478 C0
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF877946F9E557D7B0.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13413
Entropy (8bit):	0.7167893011508769
Encrypted:	false
SSDEEP:	48:kBqoI464E4jt+Wot+zI+zhC/o/t+zhOo+zhOf+zhOE:kBqoI/JpinlylODlOmlOE
MD5:	CACD0321E5EE04EAC97395E3843E0AFE
SHA1:	8A370097E32B1F5C098CF250E1EA5CC68BE2B57B
SHA-256:	7DE22A6BA199F730D67BFE5F21C78E8A94CE3AD3AD6AA251E64C83A1A15AFED6
SHA-512:	31A6DED5EB70069D4C1BAF5A19D54DAB513A84F92E9BD964ED984816EC1AE76917F241048976C4B767833B4673AB1FCF30E2407735561A5047842F9813C401EE
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

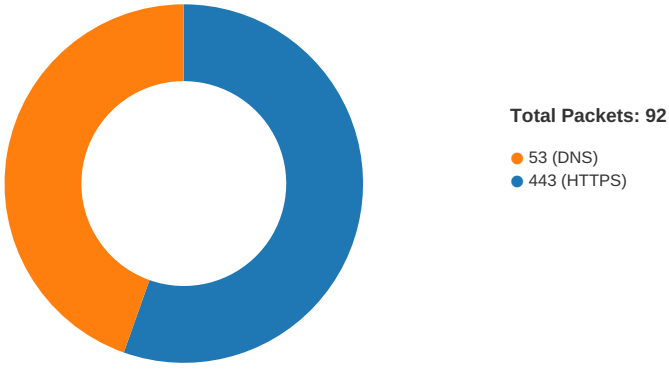
C:\Users\user\AppData\Local\Temp\~DF906810C93805B27E.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.29508429005407383
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAo:kBqoxxJhHWSVSEabo
MD5:	09D784F386D0449E0982EF757394D4FB
SHA1:	5EE9F8583A80253BAEA8DC9823EDDE0E5B7F6164
SHA-256:	C514BAC3DF9F60B035B0A6CF1ADE0E9C61F5505B1517385CECEB76954610ED69
SHA-512:	D449A9569A0CF3CFDC213ADE7BF2434EC31BC4E828C310B66812B88DEFD0D42AE12D0BCE68C9583F82C8729E4AC8F340F447603C9B3F19E9EECBA5B4441B8 F9
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
Feb 25, 2021 21:49:25.331934929 CET	49706	443	192.168.2.3	64.202.125.18
Feb 25, 2021 21:49:25.331954956 CET	49707	443	192.168.2.3	64.202.125.18
Feb 25, 2021 21:49:25.466870070 CET	443	49707	64.202.125.18	192.168.2.3
Feb 25, 2021 21:49:25.466998100 CET	49707	443	192.168.2.3	64.202.125.18
Feb 25, 2021 21:49:25.477456093 CET	49707	443	192.168.2.3	64.202.125.18
Feb 25, 2021 21:49:25.488169909 CET	443	49706	64.202.125.18	192.168.2.3
Feb 25, 2021 21:49:25.488292933 CET	49706	443	192.168.2.3	64.202.125.18
Feb 25, 2021 21:49:25.489438057 CET	49706	443	192.168.2.3	64.202.125.18
Feb 25, 2021 21:49:25.613909006 CET	443	49707	64.202.125.18	192.168.2.3
Feb 25, 2021 21:49:25.614670038 CET	443	49707	64.202.125.18	192.168.2.3
Feb 25, 2021 21:49:25.614710093 CET	443	49707	64.202.125.18	192.168.2.3
Feb 25, 2021 21:49:25.614742041 CET	443	49707	64.202.125.18	192.168.2.3
Feb 25, 2021 21:49:25.614785910 CET	49707	443	192.168.2.3	64.202.125.18
Feb 25, 2021 21:49:25.614860058 CET	49707	443	192.168.2.3	64.202.125.18
Feb 25, 2021 21:49:25.647344112 CET	443	49706	64.202.125.18	192.168.2.3
Feb 25, 2021 21:49:25.649302959 CET	443	49706	64.202.125.18	192.168.2.3
Feb 25, 2021 21:49:25.649359941 CET	443	49706	64.202.125.18	192.168.2.3
Feb 25, 2021 21:49:25.649399996 CET	49706	443	192.168.2.3	64.202.125.18
Feb 25, 2021 21:49:25.649425030 CET	443	49706	64.202.125.18	192.168.2.3
Feb 25, 2021 21:49:25.649460077 CET	49706	443	192.168.2.3	64.202.125.18
Feb 25, 2021 21:49:25.649477959 CET	49706	443	192.168.2.3	64.202.125.18
Feb 25, 2021 21:49:25.661716938 CET	49707	443	192.168.2.3	64.202.125.18
Feb 25, 2021 21:49:25.661844015 CET	49706	443	192.168.2.3	64.202.125.18
Feb 25, 2021 21:49:25.667768955 CET	49707	443	192.168.2.3	64.202.125.18
Feb 25, 2021 21:49:25.667890072 CET	49706	443	192.168.2.3	64.202.125.18
Feb 25, 2021 21:49:25.667943954 CET	49707	443	192.168.2.3	64.202.125.18
Feb 25, 2021 21:49:25.798446894 CET	443	49707	64.202.125.18	192.168.2.3
Feb 25, 2021 21:49:25.799108982 CET	443	49707	64.202.125.18	192.168.2.3
Feb 25, 2021 21:49:25.799138069 CET	443	49707	64.202.125.18	192.168.2.3
Feb 25, 2021 21:49:25.799252987 CET	49707	443	192.168.2.3	64.202.125.18
Feb 25, 2021 21:49:25.799292088 CET	49707	443	192.168.2.3	64.202.125.18
Feb 25, 2021 21:49:25.800925970 CET	49707	443	192.168.2.3	64.202.125.18
Feb 25, 2021 21:49:25.802512884 CET	443	49707	64.202.125.18	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:49:25.802540064 CET	443	49707	64.202.125.18	192.168.2.3
Feb 25, 2021 21:49:25.802645922 CET	443	49707	64.202.125.18	192.168.2.3
Feb 25, 2021 21:49:25.802690983 CET	49707	443	192.168.2.3	64.202.125.18
Feb 25, 2021 21:49:25.819746971 CET	443	49706	64.202.125.18	192.168.2.3
Feb 25, 2021 21:49:25.820413113 CET	443	49706	64.202.125.18	192.168.2.3
Feb 25, 2021 21:49:25.820482969 CET	443	49706	64.202.125.18	192.168.2.3
Feb 25, 2021 21:49:25.820559025 CET	49706	443	192.168.2.3	64.202.125.18
Feb 25, 2021 21:49:25.820605993 CET	49706	443	192.168.2.3	64.202.125.18
Feb 25, 2021 21:49:25.822016001 CET	49706	443	192.168.2.3	64.202.125.18
Feb 25, 2021 21:49:25.823777914 CET	443	49706	64.202.125.18	192.168.2.3
Feb 25, 2021 21:49:25.823920965 CET	443	49706	64.202.125.18	192.168.2.3
Feb 25, 2021 21:49:25.824054956 CET	49706	443	192.168.2.3	64.202.125.18
Feb 25, 2021 21:49:25.848959923 CET	443	49707	64.202.125.18	192.168.2.3
Feb 25, 2021 21:49:25.849178076 CET	49707	443	192.168.2.3	64.202.125.18
Feb 25, 2021 21:49:25.849528074 CET	443	49707	64.202.125.18	192.168.2.3
Feb 25, 2021 21:49:25.849561930 CET	443	49707	64.202.125.18	192.168.2.3
Feb 25, 2021 21:49:25.849591017 CET	443	49707	64.202.125.18	192.168.2.3
Feb 25, 2021 21:49:25.849642992 CET	49707	443	192.168.2.3	64.202.125.18
Feb 25, 2021 21:49:25.849745035 CET	49707	443	192.168.2.3	64.202.125.18
Feb 25, 2021 21:49:25.939774990 CET	443	49707	64.202.125.18	192.168.2.3
Feb 25, 2021 21:49:25.979451895 CET	443	49706	64.202.125.18	192.168.2.3
Feb 25, 2021 21:49:25.986515999 CET	49709	443	192.168.2.3	13.224.94.82
Feb 25, 2021 21:49:25.986604929 CET	49710	443	192.168.2.3	13.224.94.82
Feb 25, 2021 21:49:25.986792088 CET	49711	443	192.168.2.3	13.224.94.82
Feb 25, 2021 21:49:25.986958981 CET	49712	443	192.168.2.3	13.224.94.82
Feb 25, 2021 21:49:26.035403967 CET	443	49709	13.224.94.82	192.168.2.3
Feb 25, 2021 21:49:26.035449028 CET	443	49711	13.224.94.82	192.168.2.3
Feb 25, 2021 21:49:26.035545111 CET	49709	443	192.168.2.3	13.224.94.82
Feb 25, 2021 21:49:26.035574913 CET	49711	443	192.168.2.3	13.224.94.82
Feb 25, 2021 21:49:26.035726070 CET	443	49710	13.224.94.82	192.168.2.3
Feb 25, 2021 21:49:26.035801888 CET	49710	443	192.168.2.3	13.224.94.82
Feb 25, 2021 21:49:26.035846949 CET	443	49712	13.224.94.82	192.168.2.3
Feb 25, 2021 21:49:26.035912037 CET	49712	443	192.168.2.3	13.224.94.82
Feb 25, 2021 21:49:26.036885023 CET	49709	443	192.168.2.3	13.224.94.82
Feb 25, 2021 21:49:26.037118912 CET	49711	443	192.168.2.3	13.224.94.82
Feb 25, 2021 21:49:26.037327051 CET	49710	443	192.168.2.3	13.224.94.82
Feb 25, 2021 21:49:26.038630962 CET	49712	443	192.168.2.3	13.224.94.82
Feb 25, 2021 21:49:26.086311102 CET	443	49709	13.224.94.82	192.168.2.3
Feb 25, 2021 21:49:26.086647034 CET	443	49709	13.224.94.82	192.168.2.3
Feb 25, 2021 21:49:26.086688995 CET	443	49709	13.224.94.82	192.168.2.3
Feb 25, 2021 21:49:26.086725950 CET	443	49709	13.224.94.82	192.168.2.3
Feb 25, 2021 21:49:26.086729050 CET	49709	443	192.168.2.3	13.224.94.82
Feb 25, 2021 21:49:26.086786985 CET	49709	443	192.168.2.3	13.224.94.82
Feb 25, 2021 21:49:26.086796045 CET	49709	443	192.168.2.3	13.224.94.82
Feb 25, 2021 21:49:26.087095022 CET	443	49710	13.224.94.82	192.168.2.3
Feb 25, 2021 21:49:26.087121964 CET	443	49711	13.224.94.82	192.168.2.3
Feb 25, 2021 21:49:26.087472916 CET	443	49711	13.224.94.82	192.168.2.3
Feb 25, 2021 21:49:26.087512970 CET	443	49711	13.224.94.82	192.168.2.3
Feb 25, 2021 21:49:26.087549925 CET	443	49711	13.224.94.82	192.168.2.3
Feb 25, 2021 21:49:26.087580919 CET	49711	443	192.168.2.3	13.224.94.82
Feb 25, 2021 21:49:26.087635040 CET	49711	443	192.168.2.3	13.224.94.82
Feb 25, 2021 21:49:26.087642908 CET	49711	443	192.168.2.3	13.224.94.82
Feb 25, 2021 21:49:26.087943077 CET	443	49710	13.224.94.82	192.168.2.3
Feb 25, 2021 21:49:26.087985992 CET	443	49710	13.224.94.82	192.168.2.3
Feb 25, 2021 21:49:26.088016987 CET	49710	443	192.168.2.3	13.224.94.82
Feb 25, 2021 21:49:26.088049889 CET	49710	443	192.168.2.3	13.224.94.82
Feb 25, 2021 21:49:26.088063955 CET	443	49710	13.224.94.82	192.168.2.3
Feb 25, 2021 21:49:26.088113070 CET	49710	443	192.168.2.3	13.224.94.82
Feb 25, 2021 21:49:26.088315010 CET	443	49712	13.224.94.82	192.168.2.3
Feb 25, 2021 21:49:26.089442968 CET	443	49709	13.224.94.82	192.168.2.3
Feb 25, 2021 21:49:26.089530945 CET	49709	443	192.168.2.3	13.224.94.82
Feb 25, 2021 21:49:26.091015100 CET	443	49710	13.224.94.82	192.168.2.3
Feb 25, 2021 21:49:26.091099024 CET	49710	443	192.168.2.3	13.224.94.82
Feb 25, 2021 21:49:26.094418049 CET	443	49712	13.224.94.82	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:49:26.094461918 CET	443	49712	13.224.94.82	192.168.2.3
Feb 25, 2021 21:49:26.094497919 CET	443	49712	13.224.94.82	192.168.2.3
Feb 25, 2021 21:49:26.094502926 CET	49712	443	192.168.2.3	13.224.94.82

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:49:17.286596060 CET	64938	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:17.345793962 CET	53	64938	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:18.050299883 CET	60152	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:18.104048967 CET	53	60152	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:19.215588093 CET	57544	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:19.264679909 CET	53	57544	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:20.160375118 CET	55984	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:20.209058046 CET	53	55984	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:21.114171982 CET	64185	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:21.166510105 CET	53	64185	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:22.325562000 CET	65110	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:22.378707886 CET	53	65110	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:23.301532030 CET	58361	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:23.353847980 CET	53	58361	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:24.181025028 CET	63492	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:24.239998102 CET	53	63492	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:25.268937111 CET	60831	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:25.322552919 CET	53	60831	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:25.383434057 CET	60100	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:25.432259083 CET	53	60100	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:25.917709112 CET	53195	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:25.925796032 CET	50141	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:25.974991083 CET	53	53195	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:25.980706930 CET	53	50141	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:28.189841032 CET	53023	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:28.247411966 CET	53	53023	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:28.300460100 CET	49563	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:28.359801054 CET	53	49563	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:28.510569096 CET	51352	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:28.563039064 CET	53	51352	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:29.731276035 CET	59349	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:29.784682989 CET	53	59349	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:30.886276960 CET	57084	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:30.937625885 CET	53	57084	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:32.783762932 CET	58823	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:32.832597971 CET	53	58823	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:34.106650114 CET	57568	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:34.156490088 CET	53	57568	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:35.048470020 CET	50540	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:35.097455978 CET	53	50540	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:36.059900999 CET	54366	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:36.120413065 CET	53	54366	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:37.006988049 CET	53034	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:37.064371109 CET	53	53034	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:38.008500099 CET	57762	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:38.058423042 CET	53	57762	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:42.540930986 CET	55435	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:42.610852003 CET	53	55435	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:43.228043079 CET	50713	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:43.288203955 CET	53	50713	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:45.966713905 CET	56132	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:46.023678064 CET	53	56132	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:46.739063978 CET	58987	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:46.802226067 CET	53	58987	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:48.440766096 CET	56579	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:48.474061012 CET	60633	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:48.501581907 CET	53	56579	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:49:48.523150921 CET	53	60633	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:48.702863932 CET	61292	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:48.761353016 CET	53	61292	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:49.172709942 CET	63619	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:49.231225967 CET	53	63619	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:49.429764986 CET	64938	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:49.481251955 CET	53	64938	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:54.186676025 CET	61946	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:54.238806009 CET	53	61946	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:54.882503033 CET	64910	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:54.947849035 CET	53	64910	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:55.135951042 CET	52123	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:55.182568073 CET	61946	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:55.210967064 CET	53	52123	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:55.245373011 CET	53	61946	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:55.882908106 CET	64910	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:55.935851097 CET	53	64910	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:56.194578886 CET	61946	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:56.246766090 CET	53	61946	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:56.897816896 CET	64910	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:56.957748890 CET	53	64910	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:58.194988966 CET	61946	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:58.255223989 CET	53	61946	8.8.8.8	192.168.2.3
Feb 25, 2021 21:49:58.897901058 CET	64910	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:49:58.959810019 CET	53	64910	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 21:49:25.268937111 CET	192.168.2.3	8.8.8.8	0x8219	Standard query (0)	public.3.basecamp.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:25.917709112 CET	192.168.2.3	8.8.8.8	0x384c	Standard query (0)	bc3-production-assets-cdn.basecamp-static.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:25.925796032 CET	192.168.2.3	8.8.8.8	0x83ed	Standard query (0)	bc3-production-assets-cdn.basecamp-static.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:28.189841032 CET	192.168.2.3	8.8.8.8	0x8d77	Standard query (0)	3.basecamp.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:28.300460100 CET	192.168.2.3	8.8.8.8	0xe4b5	Standard query (0)	beanstalk.37signals.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:42.540930986 CET	192.168.2.3	8.8.8.8	0x9bd2	Standard query (0)	public.3.basecamp.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:43.228043079 CET	192.168.2.3	8.8.8.8	0xe7e0	Standard query (0)	3.basecamp.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:46.739063978 CET	192.168.2.3	8.8.8.8	0x1481	Standard query (0)	mibghgh.weebly.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:48.440766096 CET	192.168.2.3	8.8.8.8	0xba61	Standard query (0)	mibghgh.weebly.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:48.474061012 CET	192.168.2.3	8.8.8.8	0x6fcd	Standard query (0)	cdn1.editmysite.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:48.702863932 CET	192.168.2.3	8.8.8.8	0x956d	Standard query (0)	cdn2.editmysite.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:49.172709942 CET	192.168.2.3	8.8.8.8	0xd843	Standard query (0)	cdn1.editmysite.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:49.429764986 CET	192.168.2.3	8.8.8.8	0x4b3b	Standard query (0)	cdn2.editmysite.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 21:49:25.322552919 CET	8.8.8.8	192.168.2.3	0x8219	No error (0)	public.3.basecamp.com		64.202.125.18	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:25.974991083 CET	8.8.8.8	192.168.2.3	0x384c	No error (0)	bc3-production-assets-cdn.basecamp-static.com	d30fxesrqrvb2r.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:49:25.974991083 CET	8.8.8.8	192.168.2.3	0x384c	No error (0)	d30fxesrqrvb2r.cloudfront.net		13.224.94.73	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 21:49:25.974991083 CET	8.8.8.8	192.168.2.3	0x384c	No error (0)	d30fxesrqrvb2r.cloudfront.net		13.224.94.67	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:25.974991083 CET	8.8.8.8	192.168.2.3	0x384c	No error (0)	d30fxesrqrvb2r.cloudfront.net		13.224.94.30	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:25.974991083 CET	8.8.8.8	192.168.2.3	0x384c	No error (0)	d30fxesrqrvb2r.cloudfront.net		13.224.94.82	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:25.980706930 CET	8.8.8.8	192.168.2.3	0x83ed	No error (0)	bc3-production-assets-cdn.basecamp-static.com	d30fxesrqrvb2r.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:49:25.980706930 CET	8.8.8.8	192.168.2.3	0x83ed	No error (0)	d30fxesrqrvb2r.cloudfront.net		13.224.94.82	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:25.980706930 CET	8.8.8.8	192.168.2.3	0x83ed	No error (0)	d30fxesrqrvb2r.cloudfront.net		13.224.94.30	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:25.980706930 CET	8.8.8.8	192.168.2.3	0x83ed	No error (0)	d30fxesrqrvb2r.cloudfront.net		13.224.94.73	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:25.980706930 CET	8.8.8.8	192.168.2.3	0x83ed	No error (0)	d30fxesrqrvb2r.cloudfront.net		13.224.94.67	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:28.247411966 CET	8.8.8.8	192.168.2.3	0x8d77	No error (0)	3.basecamp.com		64.202.125.15	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:28.359801054 CET	8.8.8.8	192.168.2.3	0xe4b5	No error (0)	beanstalk.37signals.com		130.211.11.159	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:42.610852003 CET	8.8.8.8	192.168.2.3	0x9bd2	No error (0)	public.3.basecamp.com		64.202.125.18	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:43.288203955 CET	8.8.8.8	192.168.2.3	0xe7e0	No error (0)	3.basecamp.com		64.202.125.15	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:46.802226067 CET	8.8.8.8	192.168.2.3	0x1481	No error (0)	mibghgh.weebly.com	pages-wildcard.weebly.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:49:46.802226067 CET	8.8.8.8	192.168.2.3	0x1481	No error (0)	pages-wildcard.weebly.com		199.34.228.53	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:46.802226067 CET	8.8.8.8	192.168.2.3	0x1481	No error (0)	pages-wildcard.weebly.com		199.34.228.54	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:48.501581907 CET	8.8.8.8	192.168.2.3	0xba61	No error (0)	mibghgh.weebly.com	pages-wildcard.weebly.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:49:48.501581907 CET	8.8.8.8	192.168.2.3	0xba61	No error (0)	pages-wildcard.weebly.com		199.34.228.53	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:48.501581907 CET	8.8.8.8	192.168.2.3	0xba61	No error (0)	pages-wildcard.weebly.com		199.34.228.54	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:48.523150921 CET	8.8.8.8	192.168.2.3	0x6fcd	No error (0)	cdn1.editmysite.com	weebly.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:49:48.523150921 CET	8.8.8.8	192.168.2.3	0x6fcd	No error (0)	weebly.map.fastly.net		151.101.1.46	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:48.523150921 CET	8.8.8.8	192.168.2.3	0x6fcd	No error (0)	weebly.map.fastly.net		151.101.65.46	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:48.523150921 CET	8.8.8.8	192.168.2.3	0x6fcd	No error (0)	weebly.map.fastly.net		151.101.129.46	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:48.523150921 CET	8.8.8.8	192.168.2.3	0x6fcd	No error (0)	weebly.map.fastly.net		151.101.193.46	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:48.761353016 CET	8.8.8.8	192.168.2.3	0x956d	No error (0)	cdn2.editmysite.com	weebly.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:49:48.761353016 CET	8.8.8.8	192.168.2.3	0x956d	No error (0)	weebly.map.fastly.net		151.101.1.46	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:48.761353016 CET	8.8.8.8	192.168.2.3	0x956d	No error (0)	weebly.map.fastly.net		151.101.65.46	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 21:49:48.761353016 CET	8.8.8.8	192.168.2.3	0x956d	No error (0)	weebly.map.fastly.net		151.101.129.46	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:48.761353016 CET	8.8.8.8	192.168.2.3	0x956d	No error (0)	weebly.map.fastly.net		151.101.193.46	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:49.231225967 CET	8.8.8.8	192.168.2.3	0xd843	No error (0)	cdn1.editmysite.com	weebly.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:49:49.231225967 CET	8.8.8.8	192.168.2.3	0xd843	No error (0)	weebly.map.fastly.net		151.101.1.46	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:49.231225967 CET	8.8.8.8	192.168.2.3	0xd843	No error (0)	weebly.map.fastly.net		151.101.65.46	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:49.231225967 CET	8.8.8.8	192.168.2.3	0xd843	No error (0)	weebly.map.fastly.net		151.101.129.46	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:49.231225967 CET	8.8.8.8	192.168.2.3	0xd843	No error (0)	weebly.map.fastly.net		151.101.193.46	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:49.481251955 CET	8.8.8.8	192.168.2.3	0x4b3b	No error (0)	cdn2.editmysite.com	weebly.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:49:49.481251955 CET	8.8.8.8	192.168.2.3	0x4b3b	No error (0)	weebly.map.fastly.net		151.101.1.46	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:49.481251955 CET	8.8.8.8	192.168.2.3	0x4b3b	No error (0)	weebly.map.fastly.net		151.101.65.46	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:49.481251955 CET	8.8.8.8	192.168.2.3	0x4b3b	No error (0)	weebly.map.fastly.net		151.101.129.46	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:49.481251955 CET	8.8.8.8	192.168.2.3	0x4b3b	No error (0)	weebly.map.fastly.net		151.101.193.46	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 25, 2021 21:49:25.614742041 CET	64.202.125.18	443	192.168.2.3	49707	CN=*.3.basecamp.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Aug 14 02:00:00 CEST 2019 Mon Nov 06 13:23:33 CET 2017	Tue Oct 12 14:00:00 CEST 2021 Sat Nov 06 13:23:33 CET 2027	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
Feb 25, 2021 21:49:25.649425030 CET	64.202.125.18	443	192.168.2.3	49706	CN=*.3.basecamp.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Aug 14 02:00:00 CEST 2019 Mon Nov 06 13:23:33 CET 2017	Tue Oct 12 14:00:00 CEST 2021 Sat Nov 06 13:23:33 CET 2027	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 25, 2021 21:49:26.089442968 CET	13.224.94.82	443	192.168.2.3	49709	CN=*.basecamp-static.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Tue May 12 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Jun 12 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Feb 25, 2021 21:49:26.091015100 CET	13.224.94.82	443	192.168.2.3	49710	CN=*.basecamp-static.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Tue May 12 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Jun 12 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 25, 2021 21:49:26.098315001 CET	13.224.94.82	443	192.168.2.3	49711	CN=*.basecamp-static.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Tue May 12 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Jun 12 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Feb 25, 2021 21:49:26.098808050 CET	13.224.94.82	443	192.168.2.3	49712	CN=*.basecamp-static.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Tue May 12 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Jun 12 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Feb 25, 2021 21:49:28.469053030 CET	130.211.11.159	443	192.168.2.3	49715	CN=*.37signals.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Oct 14 02:00:00 CEST 2019 Mon Nov 06 13:23:33 CET 2017	Sun Dec 12 13:00:00 CET 2021 Sat Nov 06 13:23:33 CET 2027	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
Feb 25, 2021 21:49:28.520421028 CET	64.202.125.15	443	192.168.2.3	49713	CN=*.basecamp.com CN=RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Feb 15 01:00:00 CET 2021 Thu Jul 16 14:25:27 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Sat Mar 19 00:59:59 CET 2022 Thu Jun 01 01:59:59 CEST 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 16 14:25:27 CEST 2020	Thu Jun 01 01:59:59 CEST 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Feb 25, 2021 21:49:28.523822069 CET	64.202.125.15	443	192.168.2.3	49714	CN=*.basecamp.com CN=RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Feb 15 01:00:00 CET 2021 Thu Jul 16 14:25:27 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Sat Mar 19 00:59:59 CET 2022 Thu Jun 01 01:59:59 CEST 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 16 14:25:27 CEST 2020	Thu Jun 01 01:59:59 CEST 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Feb 25, 2021 21:49:42.907296896 CET	64.202.125.18	443	192.168.2.3	49725	CN=*.3.basecamp.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Aug 14 02:00:00 CEST 2019 Mon Nov 06 13:23:33 CET 2017	Tue Oct 12 14:00:00 CEST 2021 Sat Nov 06 13:23:33 CET 2027	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 25, 2021 21:49:43.561736107 CET	64.202.125.15	443	192.168.2.3	49726	CN=*.basecamp.com CN=RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Feb 15 01:00:00 CET 2021 Thu Jul 16 14:25:27 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Sat Mar 19 00:59:59 CET 2022 Thu Jun 01 01:59:59 CEST 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 16 14:25:27 CEST 2020	Thu Jun 01 01:59:59 CEST 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Feb 25, 2021 21:49:47.208034992 CET	199.34.228.53	443	192.168.2.3	49730	CN=*.weebly.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Oct 04 02:00:00 CEST 2019 Mon Nov 06 13:23:33 CET 2017	Thu Dec 02 13:00:00 CET 2021 Sat Nov 06 13:23:33 CET 2027	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
Feb 25, 2021 21:49:47.208102942 CET	199.34.228.53	443	192.168.2.3	49731	CN=*.weebly.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Oct 04 02:00:00 CEST 2019 Mon Nov 06 13:23:33 CET 2017	Thu Dec 02 13:00:00 CET 2021 Sat Nov 06 13:23:33 CET 2027	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
Feb 25, 2021 21:49:48.625901937 CET	151.101.1.46	443	192.168.2.3	49734	CN=editmysite.com, O="Weebly, Inc.", L=San Francisco, ST=California, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 21 20:34:09 CEST 2020 Wed Aug 19 02:00:00 CEST 2015	Thu Apr 22 20:34:09 CEST 2021 Tue Aug 19 02:00:00 CEST 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		
Feb 25, 2021 21:49:48.626081944 CET	151.101.1.46	443	192.168.2.3	49735	CN=editmysite.com, O="Weebly, Inc.", L=San Francisco, ST=California, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 21 20:34:09 CEST 2020 Wed Aug 19 02:00:00 CEST 2015	Thu Apr 22 20:34:09 CEST 2021 Tue Aug 19 02:00:00 CEST 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

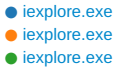
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		
Feb 25, 2021 21:49:48.853130102 CET	151.101.1.46	443	192.168.2.3	49736	CN=editmysite.com, O="Weebly, Inc.", L=San Francisco, ST=California, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 21 20:34:09 CEST 2020 Wed Aug 19 02:00:00 CEST 2015	Thu Apr 22 20:34:09 CEST 2021 Tue Aug 19 02:00:00 CEST 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		
Feb 25, 2021 21:49:48.853914976 CET	151.101.1.46	443	192.168.2.3	49737	CN=editmysite.com, O="Weebly, Inc.", L=San Francisco, ST=California, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 21 20:34:09 CEST 2020 Wed Aug 19 02:00:00 CEST 2015	Thu Apr 22 20:34:09 CEST 2021 Tue Aug 19 02:00:00 CEST 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		
Feb 25, 2021 21:49:48.855201006 CET	151.101.1.46	443	192.168.2.3	49738	CN=editmysite.com, O="Weebly, Inc.", L=San Francisco, ST=California, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 21 20:34:09 CEST 2020 Wed Aug 19 02:00:00 CEST 2015	Thu Apr 22 20:34:09 CEST 2021 Tue Aug 19 02:00:00 CEST 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		
Feb 25, 2021 21:49:48.913009882 CET	199.34.228.53	443	192.168.2.3	49733	CN=*.weebly.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Oct 04 02:00:00 CEST 2019 Mon Nov 06 13:23:33 CET 2017	Thu Dec 02 13:00:00 CET 2021 Sat Nov 06 13:23:33 CET 2027	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
Feb 25, 2021 21:49:48.913327932 CET	199.34.228.53	443	192.168.2.3	49732	CN=*.weebly.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Oct 04 02:00:00 CEST 2019 Mon Nov 06 13:23:33 CET 2017	Thu Dec 02 13:00:00 CET 2021 Sat Nov 06 13:23:33 CET 2027	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 25, 2021 21:49:49.322285891 CET	151.101.1.46	443	192.168.2.3	49739	CN=editmysite.com, O="Weebly, Inc.", L=San Francisco, ST=California, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 21 20:34:09 CEST 2020 Wed Aug 19 02:00:00 CEST 2015	Thu Apr 22 20:34:09 CEST 2021 Tue Aug 19 02:00:00 CEST 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		
Feb 25, 2021 21:49:49.322662115 CET	151.101.1.46	443	192.168.2.3	49740	CN=editmysite.com, O="Weebly, Inc.", L=San Francisco, ST=California, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 21 20:34:09 CEST 2020 Wed Aug 19 02:00:00 CEST 2015	Thu Apr 22 20:34:09 CEST 2021 Tue Aug 19 02:00:00 CEST 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		
Feb 25, 2021 21:49:49.573685884 CET	151.101.1.46	443	192.168.2.3	49741	CN=editmysite.com, O="Weebly, Inc.", L=San Francisco, ST=California, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 21 20:34:09 CEST 2020 Wed Aug 19 02:00:00 CEST 2015	Thu Apr 22 20:34:09 CEST 2021 Tue Aug 19 02:00:00 CEST 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		
Feb 25, 2021 21:49:49.622750998 CET	151.101.1.46	443	192.168.2.3	49742	CN=editmysite.com, O="Weebly, Inc.", L=San Francisco, ST=California, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 21 20:34:09 CEST 2020 Wed Aug 19 02:00:00 CEST 2015	Thu Apr 22 20:34:09 CEST 2021 Tue Aug 19 02:00:00 CEST 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 1956 Parent PID: 792

General

Start time:	21:49:23
Start date:	25/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff774510000
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: 3980 Parent PID: 1956

General

Start time:	21:49:23
Start date:	25/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1956 CREDAT:17410 /prefetch:2
Imagebase:	0x1200000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 4664 Parent PID: 1956

General

Start time:	21:49:46
Start date:	25/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1956 CREDAT:82952 /prefetch:2
Imagebase:	0x1200000
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	Completion	Count	Source Address	Symbol

Disassembly