ID: 358584
Cookbook: browseurl.jbs
Time: 21:48:38
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

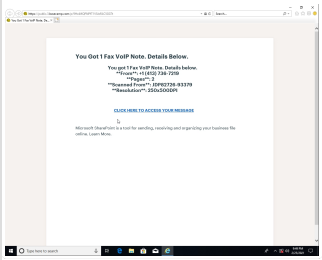
Analysis Report https://public.3.basecamp.com/p/9HoiM…

Overview

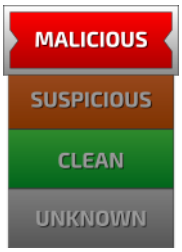
General Information

Sample URL:	http://https://public.3.basecamp.com/p/9HoiMQPNPfT1V5JoFAC5GG7t
Analysis ID:	358584
Infos:	

Most interesting Screenshot:



Detection

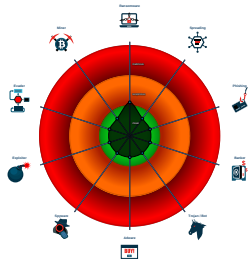


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Antivirus / Scanner detection for sub…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6136 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5888 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6136 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

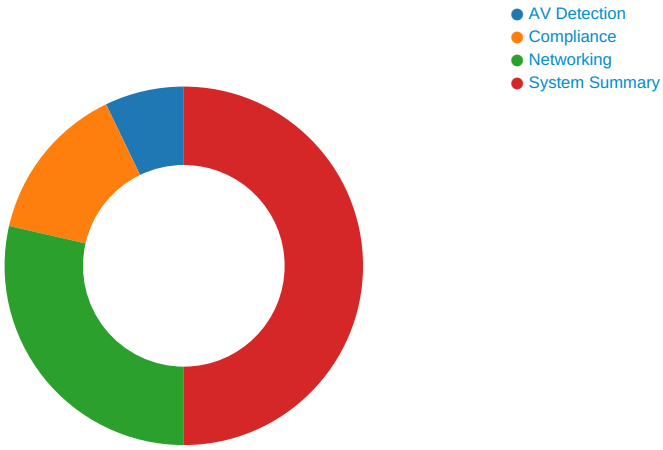
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Compliance:

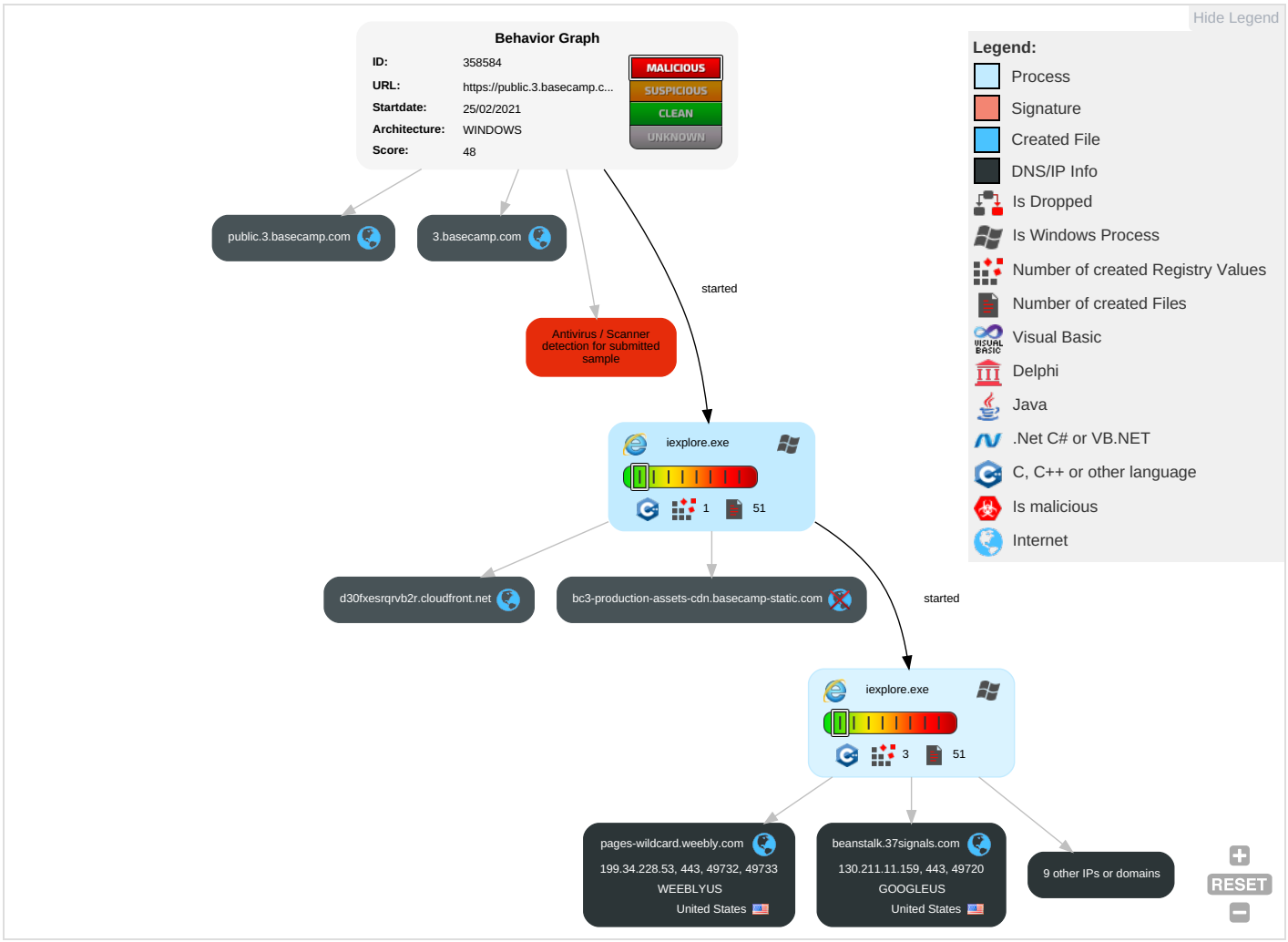
Uses new MSVCR Dlls

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

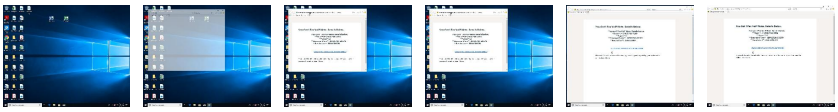
Behavior Graph

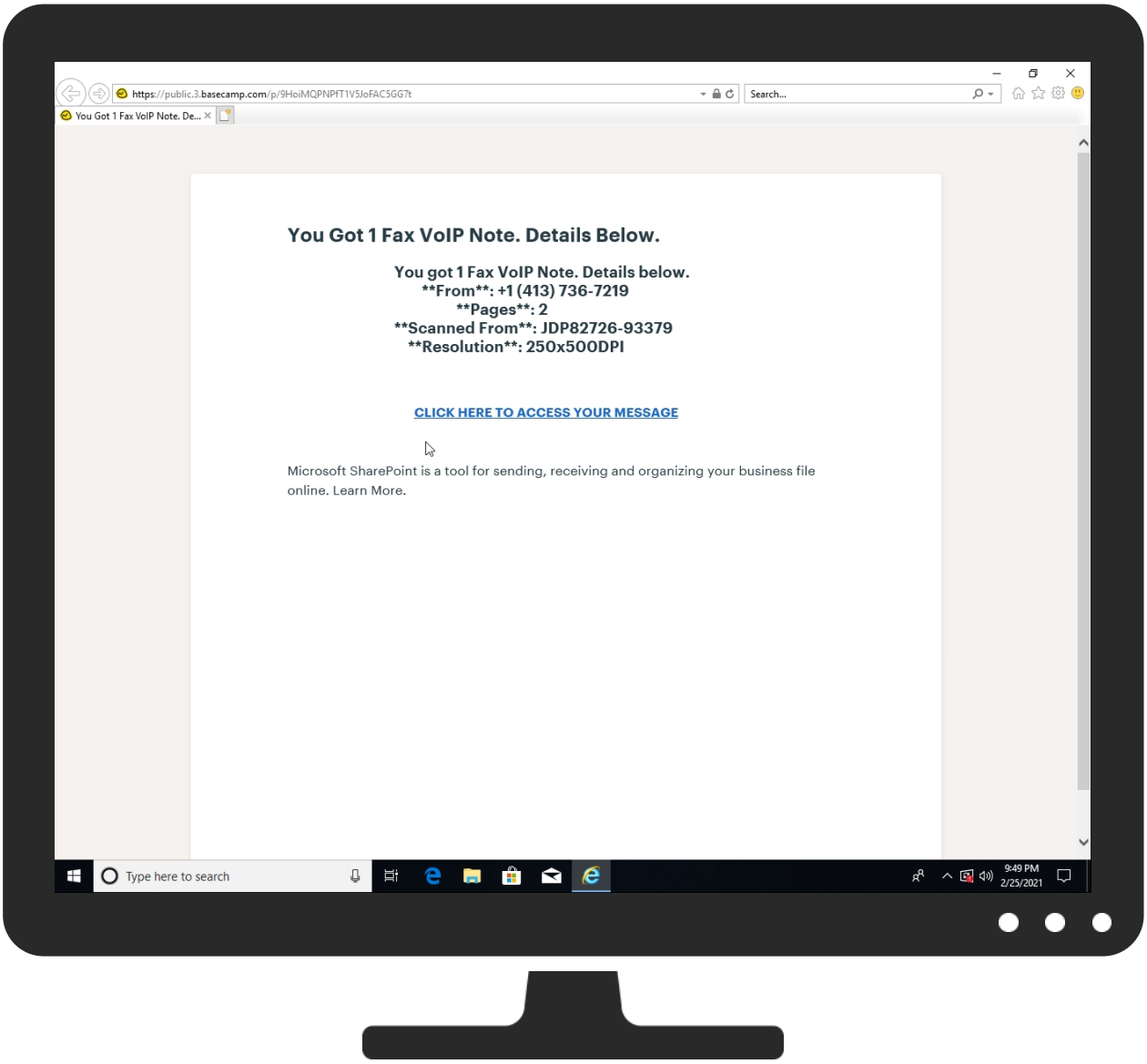


Screenshots

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

Source	Detection	Scanner	Label	Link
weebly.map.fastly.net	0%	Virustotal		Browse
bc3-production-assets-cdn.basecamp-static.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://bc3-production-assets-cdn.basecamp-static.com	0%	Virustotal		Browse
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://mibghgh.weeblyamp.com/p/9HoiMQPNPfT1V5JoFAC5GG7t	0%	Avira URL Cloud	safe	
http://https://public.3.ba24b-7732-4312-b6e5-6bb75d448e48	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/packs/libraries-a6ab6002c86dc39bd54d.js	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://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.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	• 0%, Virustotal, Browse	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	• 0%, Virustotal, Browse	unknown

Contacted URLs

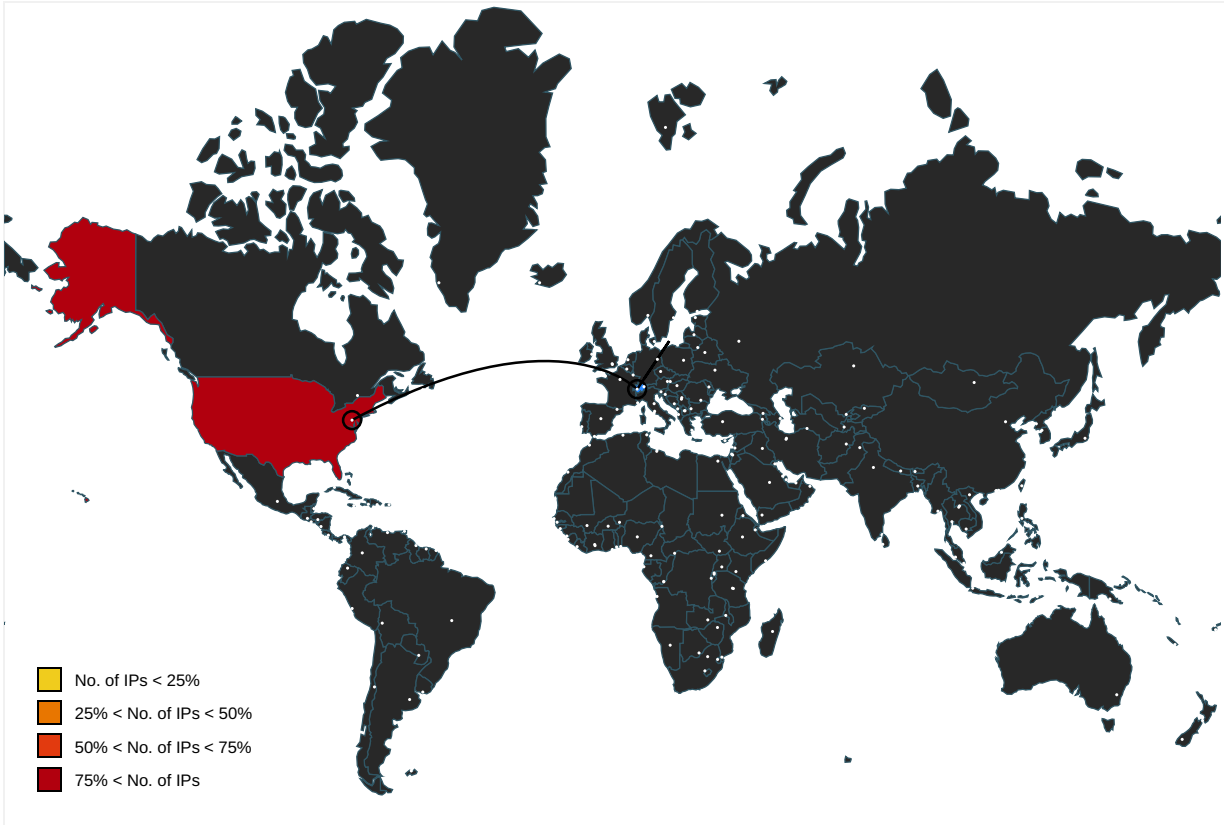
Name	Malicious	Antivirus Detection	Reputation
http://https://mibghgh.weebly.com/	false		high
http://https://public.3.basecamp.com/p/9HoiMQPNPfT1V5JoFAC5GG7t	false		high

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	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://public.3.basecamp.com/p/9HoiMQPNPfT1V5JoFAC5GG7t	~DFA5A270FBA6D61E89.TMP.1.dr	false		high
http://https://public.3.basecamp.com/p/9HoiMQPNPfT1V5JoFAC5GG7tNYou	~DFA5A270FBA6D61E89.TMP.1.dr	false		high
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	{EF122194-77AA-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	low
http://https://mibghgh.weebly.com/m/p/9HoiMQPNPfT1V5JoFAC5GG7t	~DFA5A270FBA6D61E89.TMP.1.dr	false		high
http://https://mibghgh.weeblyamp.com/p/9HoiMQPNPfT1V5JoFAC5GG7t	{EF122194-77AA-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://public.3.ba24b-7732-4312-b6e5-6bb75d448e48	{EF122194-77AA-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://mibghgh.weebly.com	9HoiMQPNPfT1V5JoFAC5GG7t[1].htm.2.dr	false		high
http://https://public.3.Root	{EF122194-77AA-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://public.3.basecamp.com/p/9HoiMQPNPfT1V5JoFAC5GG7tamp.com/p/9HoiMQPNPfT1V5JoFAC5GG7tRoot	{EF122194-77AA-11EB-90EB-ECF4BBEA1588}.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://public.3.basecamp.com/p/9HoiMQPNPfT1V5JoFAC5GG7tRoot	{EF122194-77AA-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false		high
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://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://mibghgh.weebly	{EF122194-77AA-11EB-90EB-ECF4BBEA1588}.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
http://https://public.3.basecamp.com/buckets/20950190/vaults/3492664608	9HoiMQPNPfT1V5JoFAC5GG7t[1].htm.2.dr	false		high

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
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:	358584
Start date:	25.02.2021
Start time:	21:48:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 47s
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:	3
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:	• EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.win@3/22@11/6
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://mibghgh.weebly.com/
Warnings:	Show All • Exclude process from analysis (whitelisted): ielowutil.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.113.196.254, 13.88.21.125, 168.61.161.212, 52.147.198.201, 104.43.193.48, 104.42.151.234, 88.221.62.148, 13.64.90.137 • Excluded domains from analysis (whitelisted): skypedataprdcolwus17.cloudapp.net, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, e11290.dspg.akamaiedge.net, teams-9999.teams-msedge.net, go.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, teams-ring.teams-9999.teams-msedge.net, watson.telemetry.microsoft.com, teams-ring.msedge.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\E5F0NRSV\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.{EF122192-77AA-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8572481636914955
Encrypted:	false
SSDEEP:	192:rtZrZC2IWOtMif38OzMJ2BRwDQsfp8fjX:rD9h/uh6wEvu
MD5:	E1D7EB63ED9A4254977233FE8701EED5
SHA1:	8ECCBF8E40A31DEA4C0FD9C0D0A8E4E080F433B3
SHA-256:	60FB656883E9701BC377ACC48B374483163B523434F030F31528DB43D30EFCCC
SHA-512:	79CD6534188D6467657970EF3A9889D859FF552F44E321BF2761A0ADEF4C238D33ACBD2228DBEC72D6C50AAB88F41039A693830D66D2D621E0A5BEFA6A6EA26
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\{EF122194-77AA-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{EF122194-77AA-11EB-90EB-ECF4BBEA1588}.dat	
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	40902
Entropy (8bit):	2.0423316255866326
Encrypted:	false
SSDEEP:	192:riZZQ967kLjB2pWqMy7ngBA+kXQb/rpACgVigOrDDg:re+oA3wYrUgS+kX2/rpzZBY
MD5:	42AC3A7479FF7176E66A86BB3B7B77F9
SHA1:	67D128E4B5D3CA22CA5C2F95B5EF08B3DC2E9D26
SHA-256:	8EA4483715460C866A13E1F0F0484D5D9595C06DA2AA601E1BC6BEC59C3D93F6
SHA-512:	D5C463D76427A3D1D8C36F665DB13EC7D47CEB56F50F6FE2CF8A7969138C4ABDADF4C8FA6D7077D6618A852D0836E5993C7ED2D25F755D8201E72B13EF19E9B
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\{EF122195-77AA-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5646085094285553
Encrypted:	false
SSDEEP:	48:IwAGcprRGwpajG4pQHGrapbSsGQpKXG7HpRGTGIpG:rkZLQV6bBSkA2TyA
MD5:	FA75D466028E223687F37C37D1E073C8
SHA1:	C2340825D7B2E2EB3F2CB970DE1517BB4840C125
SHA-256:	1F75B0798C358F7CC69348416F49487476DF6791488079B4576873FC9173A24C
SHA-512:	EB7FFAD6948405F725D520AB5FBC757C1CAD0418FAEB0805A51395EF1FB5E1AF1944EFE8BB30FEDB4B372116D65E8021A60F049EFC278DEB8D522AB4B1B611CC
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	2450
Entropy (8bit):	7.6921757625649665
Encrypted:	false
SSDEEP:	48:UInneQzFhtb7xLFZ5bcbzN++Qf1QSK1IGUVVUyeJdp1wT3ltsjEH8:nt7xP5gbU+CySpGUdoC3ltG
MD5:	3F191763ED4D53E44D641F5AA0A7BF75
SHA1:	4AA5E44314450869971B75C281A9AFD4AEFF7835
SHA-256:	C23970A37D64CB96AC8F5722E884B9E8C793EC1C2899EAC929A0D98CF65F270E
SHA-512:	DE12EAE6632A690427CE291139B158A1B5A84A374127D461C48ACFA61F646A3EAF3899D5E9B5D1E0900FA0B9C3B71D6110E269B3C6118374FA30D9E6302124CE
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<....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.,....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\2WF3MMUU\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):	5.334060273370188
Encrypted:	false
SSDEEP:	96:jFPEGE2qFF7QynYfdQ+cIYZV6hu6LDMz41QzFZefM:KT2qFF7QynJIS0wMMCQ1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\9HoiMQPNPfT1V5JoFAC5GG7t[1].htm	
MD5:	5F266ECA288347CB9624728C6E1A3B42
SHA1:	B3816D522B5922C5B515F99DC63F6F5DB08E99B1
SHA-256:	85E5458DF9F36137DAE5A84AFFB3CF3FC5D85196110C63ED7738C448D3E4E188
SHA-512:	40AAB557066F87BB726888FC6EE0BE321360274C56D30A18474487968F8809AFCDF68E087C4D10169376F440D48B8AA4364E875F606860EAFC5CAEB03F1BE179
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="ObnSMQh-uD0sbRWlXx_86UnWKfetvZ9YTanoR6bHO78op6n62aYqL_50Aeqvq-jwqLV77T4BPA8TD0pqu2hqnQ" />..<meta name="turbolinks-root" 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\2WF3MMUU\Graphik-RegularItalic-Cy-Gr-Web-a10a70f48489dfe7e0ab1fe80eebaa027610df48049f44cd1724ddcbce3ec509[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\2WF3MMUU\Graphik-SemiboldItalic-Cy-Gr-Web-9331e9964cf8f0a6ec536ecafb1ccfb7bde3bad32248b64a51b31142786bc3f3[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.]..llii.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\Microsoft\Windows\INetCache\IE\9026IKNJ\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\31AC96_1_0[1].woff	
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
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\9026IKNJ\desktop-09334a52f8be90f7ab2c69fb59eb0eaf1a2a7c3015b9151b4e641a93284fe9d1[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,aside,details,figcaption,figure,footer,header,hgroup,main,nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-align:baseline}audio:not([controls]){display:none;height:0}[hidden],template{display:none}a{background: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%;line-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\9026IKNJ\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
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\CS6IXJW6\public-e8b06a8ee10d5c07ccf7e91ef27eaae0ca5404d0c4d5ba63c7fc633b29923020[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\public-e8b06a8ee10d5c07ccf7e91ef27eaae0ca5404d0c4d5ba63c7fc633b29923020[1].js	
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.addEventListener(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\CS6IXJW6\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+xpcOARUGDc8tYwolxPlw+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\OR0WKIO1\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:Si3CI7N8S2JAOIxI7OptuUr7
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?
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..*.l.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.$.....d{@O...q_.,F-.^...T`p..<..*...i..k~W..?;.y0o.l..Qr."..m.$....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\OR0WKIO1\31AC96_2_0[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT)
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\31AC96_2_0[1].eot	
Size (bytes):	38300
Entropy (8bit):	7.974402289492323
Encrypted:	false
SSDEEP:	768:v/2N3fpmfNc5fQ7RhbCclfmR4On5mg6XKvqm1bGYv:XY3fUfOfQlNoqOnsKCmhGYv
MD5:	12B5BF0F4F082E07C41803E75183EFF8
SHA1:	51C2C509B0DA204C6E4ED1E3F164927BA265263E
SHA-256:	8F19E7604EE75D48AB7EB5E8F4D14E35BAB7E79B9E44890828504283C45C213D
SHA-512:	BB50EE62D565B3261197938780F5FDFE513A1D18298ECA00819306B7B5F35878A236318E8CEA7D7ECCE181A48B29073486E72A6EA5625EC1ABBA5ABA7D5C16B2
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..I..+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\OR0WKIO1\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..!.}l...!+)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....-..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\OR0WKIO1\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,d09GRgABAAAAAQ36ABIAAAACfngAAAAAAAEMvAAAAT4AAAJ9AAAAAAAAAABHUE9TAAC7oAAASNoAAP3sydoFQUdTVUIAAQR8AAAIPgAAEqAgYeHsTFRTSAAACQwAAAAWAAAC%2Fb%2B%2BwcBPUy8yAAACEAAAAFUAAABgaRJyvmNtYXAAAApcAAADUQAABLgAgjzPY3Z0IAAAD7gAAABIAAAASBBGAu9mcGdtAAANsAAAAPgAAAFhkkIa%2Bmdhc3AAALuUAAAADAAAAwABwAHZ2x5ZgAAFegAAJblAAEunN9HnXFoZG14AAAJJAAAATgAAAMEx7nTq2hlYWQAAAGUAAAANgAAADYEm1S9aGhlYQAAAcwAAAAhAAAAJAdCBcIobXR4AAACaAAABqMAAAvkcreh8GxvY2EAABAAAAAF5QAABfT2c0AkbWF4cAAAAfAAAAAgAAAAIAUTA0FuYW1lAACs0AAAAesAAARzXmkLLHBvc3QAAK68AAAM1wAAGQVieOv8cHJlcAAADqgAAAEQAAABfVFhmW0AAQAAAAEAAO1v8nRfDzz1ABkD6AAAAADLdRIlAAAAANaO99L%2FIP8kBEoEWQAAAAkAAgAAAAAAHjaY2BkYGC%2B%2Bt%2BWgYGl6L%2FCfwUWLwagCDJg%2BgkAhPUGFAAAAAABAAAC%2BQBkAAcAYwAFAAEAAAAAAAAoAAAIAAngAAwABeNpjYGbSYZzAwMrAwLSHqYuBgaEHQjPeZTBi%2BAUU5WZlZmZiYmNiBrLbGZCAs7%2BvL4MDA8NvJuar%2F20ZGJivMhxWYGCYD5Jj4mY6zaAAhDwArJYOnwAAAHjahZZ7aNZVGMe%2F55y3wmY287rppnNz7e7c2s	

C:\Users\user\AppData\Local\Temp\dat8C2F.tmp	
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:Ivb6vGR527CoPZDh6nHDQw6wSEruG9UrlYPaeDCzFN:Iv9Wv5wLSEruG9UrlGLDE/
MD5:	FCCD32C4512A8C252EB55BAFBA24F472
SHA1:	8DBCF712C1AE5FA5AB4421E85859A62C8D2C76D9
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_../..pI.....''[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\dat8C4F.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\~DF8853F3693435E5B4.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4776567813122901
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo39lo39lWs5pMl:kBqol4msC
MD5:	858BEFEC366699EDC75E50AC6E588333
SHA1:	265CAA3BBEA3B644D7E03A7E8737474011DBF3C4
SHA-256:	9E60778922D89049BAB884297A4B43C2C1DA1DF394F6CAE2C0608A78CFB71A21
SHA-512:	A735A2894B61675CE4F3590D1B08AB663635EBA9482F2A053AED9C08E09E4D3DFFFABF53DABA026790EB70C234B4CEBA180EA12DA03F1135CCE92B91FE057F1B
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFA00F9F0FC6A06177.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664

C:\Users\user\AppData\Local\Temp\~DFA00F9F0FC6A06177.TMP	
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFA5A270FBA6D61E89.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	49045
Entropy (8bit):	0.6561727746337892
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+Oi7ir4HLbLwvpKUfwlXrvpKUfwsXTgAeK9DAe:kBqoxKAuqR+OIir4Hv+kXrpXTgQ9D
MD5:	3E738BF0A9609BCA146D433358CA3E1D
SHA1:	7DEA6B70BC34DBF15CC708134ED1C739B171F411
SHA-256:	1AAF12C7D435ADBBFFAA6EA363B21718C0393DACF39FCD7D02D33E58C930008F
SHA-512:	DCB3BEB412ADEE43E2277243FA74F359FF5EAE9CD0720EA6379235ADBACAC2CABF3BE799ED8DF4D1F41FAEEB8E5F9008B71F69AB539745B1FB81E588026D4A85
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

Total Packets: 80

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:49:22.831516981 CET	49711	443	192.168.2.4	64.202.125.18
Feb 25, 2021 21:49:22.832314968 CET	49712	443	192.168.2.4	64.202.125.18
Feb 25, 2021 21:49:22.968234062 CET	443	49711	64.202.125.18	192.168.2.4
Feb 25, 2021 21:49:22.968342066 CET	49711	443	192.168.2.4	64.202.125.18
Feb 25, 2021 21:49:22.968744993 CET	443	49712	64.202.125.18	192.168.2.4
Feb 25, 2021 21:49:22.968833923 CET	49712	443	192.168.2.4	64.202.125.18
Feb 25, 2021 21:49:22.973431110 CET	49711	443	192.168.2.4	64.202.125.18
Feb 25, 2021 21:49:22.973722935 CET	49712	443	192.168.2.4	64.202.125.18
Feb 25, 2021 21:49:23.107963085 CET	443	49712	64.202.125.18	192.168.2.4
Feb 25, 2021 21:49:23.108000040 CET	443	49711	64.202.125.18	192.168.2.4
Feb 25, 2021 21:49:23.108568907 CET	443	49712	64.202.125.18	192.168.2.4
Feb 25, 2021 21:49:23.108634949 CET	443	49712	64.202.125.18	192.168.2.4
Feb 25, 2021 21:49:23.108668089 CET	443	49712	64.202.125.18	192.168.2.4
Feb 25, 2021 21:49:23.108692884 CET	49712	443	192.168.2.4	64.202.125.18
Feb 25, 2021 21:49:23.108752012 CET	49712	443	192.168.2.4	64.202.125.18
Feb 25, 2021 21:49:23.109663010 CET	443	49711	64.202.125.18	192.168.2.4
Feb 25, 2021 21:49:23.109704971 CET	443	49711	64.202.125.18	192.168.2.4
Feb 25, 2021 21:49:23.109755993 CET	443	49711	64.202.125.18	192.168.2.4
Feb 25, 2021 21:49:23.109771013 CET	49711	443	192.168.2.4	64.202.125.18
Feb 25, 2021 21:49:23.109848022 CET	49711	443	192.168.2.4	64.202.125.18
Feb 25, 2021 21:49:23.149491072 CET	49711	443	192.168.2.4	64.202.125.18
Feb 25, 2021 21:49:23.149601936 CET	49712	443	192.168.2.4	64.202.125.18
Feb 25, 2021 21:49:23.156445980 CET	49712	443	192.168.2.4	64.202.125.18
Feb 25, 2021 21:49:23.156610012 CET	49712	443	192.168.2.4	64.202.125.18
Feb 25, 2021 21:49:23.156675100 CET	49711	443	192.168.2.4	64.202.125.18
Feb 25, 2021 21:49:23.287883997 CET	443	49712	64.202.125.18	192.168.2.4
Feb 25, 2021 21:49:23.288366079 CET	443	49712	64.202.125.18	192.168.2.4
Feb 25, 2021 21:49:23.288405895 CET	443	49712	64.202.125.18	192.168.2.4
Feb 25, 2021 21:49:23.288465977 CET	49712	443	192.168.2.4	64.202.125.18
Feb 25, 2021 21:49:23.288511992 CET	49712	443	192.168.2.4	64.202.125.18
Feb 25, 2021 21:49:23.288676977 CET	443	49711	64.202.125.18	192.168.2.4
Feb 25, 2021 21:49:23.289413929 CET	443	49711	64.202.125.18	192.168.2.4
Feb 25, 2021 21:49:23.289514065 CET	49711	443	192.168.2.4	64.202.125.18
Feb 25, 2021 21:49:23.289536953 CET	443	49711	64.202.125.18	192.168.2.4
Feb 25, 2021 21:49:23.289608002 CET	49711	443	192.168.2.4	64.202.125.18
Feb 25, 2021 21:49:23.289896011 CET	49712	443	192.168.2.4	64.202.125.18
Feb 25, 2021 21:49:23.290882111 CET	49711	443	192.168.2.4	64.202.125.18
Feb 25, 2021 21:49:23.293862104 CET	443	49712	64.202.125.18	192.168.2.4
Feb 25, 2021 21:49:23.293884039 CET	443	49712	64.202.125.18	192.168.2.4
Feb 25, 2021 21:49:23.294039965 CET	49712	443	192.168.2.4	64.202.125.18
Feb 25, 2021 21:49:23.294079065 CET	443	49711	64.202.125.18	192.168.2.4
Feb 25, 2021 21:49:23.294125080 CET	443	49711	64.202.125.18	192.168.2.4
Feb 25, 2021 21:49:23.294243097 CET	49711	443	192.168.2.4	64.202.125.18
Feb 25, 2021 21:49:23.339942932 CET	443	49712	64.202.125.18	192.168.2.4
Feb 25, 2021 21:49:23.340027094 CET	49712	443	192.168.2.4	64.202.125.18
Feb 25, 2021 21:49:23.340879917 CET	443	49712	64.202.125.18	192.168.2.4
Feb 25, 2021 21:49:23.340914011 CET	443	49712	64.202.125.18	192.168.2.4
Feb 25, 2021 21:49:23.340941906 CET	443	49712	64.202.125.18	192.168.2.4
Feb 25, 2021 21:49:23.340955973 CET	49712	443	192.168.2.4	64.202.125.18
Feb 25, 2021 21:49:23.341001987 CET	49712	443	192.168.2.4	64.202.125.18
Feb 25, 2021 21:49:23.427119970 CET	443	49712	64.202.125.18	192.168.2.4
Feb 25, 2021 21:49:23.428889990 CET	443	49711	64.202.125.18	192.168.2.4
Feb 25, 2021 21:49:23.509481907 CET	49714	443	192.168.2.4	13.224.94.82
Feb 25, 2021 21:49:23.509680033 CET	49717	443	192.168.2.4	13.224.94.82
Feb 25, 2021 21:49:23.509684086 CET	49715	443	192.168.2.4	13.224.94.82
Feb 25, 2021 21:49:23.509685993 CET	49716	443	192.168.2.4	13.224.94.82
Feb 25, 2021 21:49:23.555432081 CET	443	49714	13.224.94.82	192.168.2.4
Feb 25, 2021 21:49:23.555572987 CET	443	49717	13.224.94.82	192.168.2.4
Feb 25, 2021 21:49:23.555577993 CET	49714	443	192.168.2.4	13.224.94.82
Feb 25, 2021 21:49:23.555604935 CET	443	49715	13.224.94.82	192.168.2.4
Feb 25, 2021 21:49:23.555633068 CET	443	49716	13.224.94.82	192.168.2.4
Feb 25, 2021 21:49:23.555681944 CET	49717	443	192.168.2.4	13.224.94.82

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:49:23.555742025 CET	49715	443	192.168.2.4	13.224.94.82
Feb 25, 2021 21:49:23.556611061 CET	49716	443	192.168.2.4	13.224.94.82
Feb 25, 2021 21:49:23.557168007 CET	49714	443	192.168.2.4	13.224.94.82
Feb 25, 2021 21:49:23.557297945 CET	49716	443	192.168.2.4	13.224.94.82
Feb 25, 2021 21:49:23.557410002 CET	49715	443	192.168.2.4	13.224.94.82
Feb 25, 2021 21:49:23.557746887 CET	49717	443	192.168.2.4	13.224.94.82
Feb 25, 2021 21:49:23.603039026 CET	443	49714	13.224.94.82	192.168.2.4
Feb 25, 2021 21:49:23.603221893 CET	443	49716	13.224.94.82	192.168.2.4
Feb 25, 2021 21:49:23.603415966 CET	443	49715	13.224.94.82	192.168.2.4
Feb 25, 2021 21:49:23.603686094 CET	443	49715	13.224.94.82	192.168.2.4
Feb 25, 2021 21:49:23.603725910 CET	443	49715	13.224.94.82	192.168.2.4
Feb 25, 2021 21:49:23.603755951 CET	443	49717	13.224.94.82	192.168.2.4
Feb 25, 2021 21:49:23.603785038 CET	49715	443	192.168.2.4	13.224.94.82
Feb 25, 2021 21:49:23.603794098 CET	443	49715	13.224.94.82	192.168.2.4
Feb 25, 2021 21:49:23.603827953 CET	49715	443	192.168.2.4	13.224.94.82
Feb 25, 2021 21:49:23.603861094 CET	49715	443	192.168.2.4	13.224.94.82
Feb 25, 2021 21:49:23.605529070 CET	443	49716	13.224.94.82	192.168.2.4
Feb 25, 2021 21:49:23.605573893 CET	443	49716	13.224.94.82	192.168.2.4
Feb 25, 2021 21:49:23.605612040 CET	443	49715	13.224.94.82	192.168.2.4
Feb 25, 2021 21:49:23.605650902 CET	443	49716	13.224.94.82	192.168.2.4
Feb 25, 2021 21:49:23.605658054 CET	49716	443	192.168.2.4	13.224.94.82
Feb 25, 2021 21:49:23.605711937 CET	49716	443	192.168.2.4	13.224.94.82
Feb 25, 2021 21:49:23.605781078 CET	49715	443	192.168.2.4	13.224.94.82
Feb 25, 2021 21:49:23.605786085 CET	49716	443	192.168.2.4	13.224.94.82
Feb 25, 2021 21:49:23.609174013 CET	443	49716	13.224.94.82	192.168.2.4
Feb 25, 2021 21:49:23.609267950 CET	443	49714	13.224.94.82	192.168.2.4
Feb 25, 2021 21:49:23.609297037 CET	49716	443	192.168.2.4	13.224.94.82
Feb 25, 2021 21:49:23.609311104 CET	443	49714	13.224.94.82	192.168.2.4
Feb 25, 2021 21:49:23.609338999 CET	49714	443	192.168.2.4	13.224.94.82
Feb 25, 2021 21:49:23.609352112 CET	443	49714	13.224.94.82	192.168.2.4
Feb 25, 2021 21:49:23.609378099 CET	49714	443	192.168.2.4	13.224.94.82
Feb 25, 2021 21:49:23.609426022 CET	49714	443	192.168.2.4	13.224.94.82
Feb 25, 2021 21:49:23.610555887 CET	443	49717	13.224.94.82	192.168.2.4
Feb 25, 2021 21:49:23.610598087 CET	443	49717	13.224.94.82	192.168.2.4
Feb 25, 2021 21:49:23.610634089 CET	443	49717	13.224.94.82	192.168.2.4
Feb 25, 2021 21:49:23.610658884 CET	49717	443	192.168.2.4	13.224.94.82
Feb 25, 2021 21:49:23.610740900 CET	49717	443	192.168.2.4	13.224.94.82
Feb 25, 2021 21:49:23.612086058 CET	443	49714	13.224.94.82	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:49:14.407222986 CET	53	51025	8.8.8.8	192.168.2.4
Feb 25, 2021 21:49:15.367268085 CET	61516	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:49:15.416750908 CET	53	61516	8.8.8.8	192.168.2.4
Feb 25, 2021 21:49:16.485523939 CET	49182	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:49:16.538923025 CET	53	49182	8.8.8.8	192.168.2.4
Feb 25, 2021 21:49:17.429836035 CET	59920	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:49:17.481463909 CET	53	59920	8.8.8.8	192.168.2.4
Feb 25, 2021 21:49:18.204673052 CET	57458	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:49:18.256663084 CET	53	57458	8.8.8.8	192.168.2.4
Feb 25, 2021 21:49:19.373246908 CET	50579	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:49:19.426578045 CET	53	50579	8.8.8.8	192.168.2.4
Feb 25, 2021 21:49:20.539603949 CET	51703	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:49:20.592570066 CET	53	51703	8.8.8.8	192.168.2.4
Feb 25, 2021 21:49:21.503369093 CET	65248	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:49:21.556062937 CET	53	65248	8.8.8.8	192.168.2.4
Feb 25, 2021 21:49:21.757666111 CET	53723	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:49:21.820346117 CET	53	53723	8.8.8.8	192.168.2.4
Feb 25, 2021 21:49:22.761984110 CET	64646	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:49:22.821523905 CET	53	64646	8.8.8.8	192.168.2.4
Feb 25, 2021 21:49:22.894510984 CET	65298	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:49:22.944829941 CET	53	65298	8.8.8.8	192.168.2.4
Feb 25, 2021 21:49:23.390244007 CET	59123	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:49:23.400770903 CET	54531	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:49:23.459878922 CET	53	59123	8.8.8.8	192.168.2.4
Feb 25, 2021 21:49:23.474745035 CET	53	54531	8.8.8.8	192.168.2.4
Feb 25, 2021 21:49:24.899801970 CET	49714	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:49:24.948277950 CET	53	49714	8.8.8.8	192.168.2.4
Feb 25, 2021 21:49:25.232553959 CET	58028	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:49:25.289808989 CET	53	58028	8.8.8.8	192.168.2.4
Feb 25, 2021 21:49:25.461447954 CET	53097	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:49:25.511614084 CET	53	53097	8.8.8.8	192.168.2.4
Feb 25, 2021 21:49:26.602405071 CET	49257	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:49:26.651021004 CET	53	49257	8.8.8.8	192.168.2.4
Feb 25, 2021 21:49:27.558491945 CET	62389	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:49:27.609946012 CET	53	62389	8.8.8.8	192.168.2.4
Feb 25, 2021 21:49:28.544265985 CET	49910	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:49:28.598001957 CET	53	49910	8.8.8.8	192.168.2.4
Feb 25, 2021 21:49:29.425713062 CET	55854	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:49:29.477586985 CET	53	55854	8.8.8.8	192.168.2.4
Feb 25, 2021 21:49:30.656040907 CET	64549	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:49:30.704886913 CET	53	64549	8.8.8.8	192.168.2.4
Feb 25, 2021 21:49:31.794320107 CET	63153	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:49:31.845982075 CET	53	63153	8.8.8.8	192.168.2.4
Feb 25, 2021 21:49:32.787489891 CET	52991	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:49:32.836251020 CET	53	52991	8.8.8.8	192.168.2.4
Feb 25, 2021 21:49:33.985794067 CET	53700	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:49:34.037585020 CET	53	53700	8.8.8.8	192.168.2.4
Feb 25, 2021 21:49:40.229692936 CET	51726	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:49:41.215920925 CET	51726	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:49:41.273334980 CET	53	51726	8.8.8.8	192.168.2.4
Feb 25, 2021 21:49:41.882498026 CET	56794	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:49:41.939737082 CET	53	56794	8.8.8.8	192.168.2.4
Feb 25, 2021 21:49:44.186899900 CET	56534	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:49:44.238667011 CET	53	56534	8.8.8.8	192.168.2.4
Feb 25, 2021 21:49:44.928365946 CET	56627	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:49:44.981012106 CET	53	56627	8.8.8.8	192.168.2.4
Feb 25, 2021 21:49:45.171308041 CET	56621	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:49:45.229485035 CET	53	56621	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 21:49:22.761984110 CET	192.168.2.4	8.8.8.8	0x148	Standard query (0)	public.3.basecamp.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:23.390244007 CET	192.168.2.4	8.8.8.8	0xa544	Standard query (0)	bc3-production-assets-cdn.basecamp-static.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:23.400770903 CET	192.168.2.4	8.8.8.8	0x3590	Standard query (0)	bc3-production-assets-cdn.basecamp-static.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:24.899801970 CET	192.168.2.4	8.8.8.8	0x7209	Standard query (0)	3.basecamp.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:25.232553959 CET	192.168.2.4	8.8.8.8	0xe99f	Standard query (0)	beanstalk.37signals.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:40.229692936 CET	192.168.2.4	8.8.8.8	0xb105	Standard query (0)	public.3.basecamp.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:41.215920925 CET	192.168.2.4	8.8.8.8	0xb105	Standard query (0)	public.3.basecamp.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:41.882498026 CET	192.168.2.4	8.8.8.8	0xd44f	Standard query (0)	3.basecamp.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:44.186899900 CET	192.168.2.4	8.8.8.8	0x76f8	Standard query (0)	mibghgh.weebly.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:44.928365946 CET	192.168.2.4	8.8.8.8	0x5817	Standard query (0)	cdn1.editmysite.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:45.171308041 CET	192.168.2.4	8.8.8.8	0xc908	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 21:49:22.821523905 CET	8.8.8.8	192.168.2.4	0x148	No error (0)	public.3.basecamp.com		64.202.125.18	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:23.459878922 CET	8.8.8.8	192.168.2.4	0xa544	No error (0)	bc3-production-assets-cdn.basecamp-static.com	d30fxesrqrvb2r.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:49:23.459878922 CET	8.8.8.8	192.168.2.4	0xa544	No error (0)	d30fxesrqrvb2r.cloudfront.net		13.224.94.73	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:23.459878922 CET	8.8.8.8	192.168.2.4	0xa544	No error (0)	d30fxesrqrvb2r.cloudfront.net		13.224.94.67	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:23.459878922 CET	8.8.8.8	192.168.2.4	0xa544	No error (0)	d30fxesrqrvb2r.cloudfront.net		13.224.94.30	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:23.459878922 CET	8.8.8.8	192.168.2.4	0xa544	No error (0)	d30fxesrqrvb2r.cloudfront.net		13.224.94.82	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:23.474745035 CET	8.8.8.8	192.168.2.4	0x3590	No error (0)	bc3-production-assets-cdn.basecamp-static.com	d30fxesrqrvb2r.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:49:23.474745035 CET	8.8.8.8	192.168.2.4	0x3590	No error (0)	d30fxesrqrvb2r.cloudfront.net		13.224.94.82	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:23.474745035 CET	8.8.8.8	192.168.2.4	0x3590	No error (0)	d30fxesrqrvb2r.cloudfront.net		13.224.94.73	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:23.474745035 CET	8.8.8.8	192.168.2.4	0x3590	No error (0)	d30fxesrqrvb2r.cloudfront.net		13.224.94.67	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:23.474745035 CET	8.8.8.8	192.168.2.4	0x3590	No error (0)	d30fxesrqrvb2r.cloudfront.net		13.224.94.30	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:24.948277950 CET	8.8.8.8	192.168.2.4	0x7209	No error (0)	3.basecamp.com		64.202.125.15	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:25.289808989 CET	8.8.8.8	192.168.2.4	0xe99f	No error (0)	beanstalk.37signals.com		130.211.11.159	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:41.273334980 CET	8.8.8.8	192.168.2.4	0xb105	No error (0)	public.3.basecamp.com		64.202.125.18	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:41.939737082 CET	8.8.8.8	192.168.2.4	0xd44f	No error (0)	3.basecamp.com		64.202.125.15	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:44.238667011 CET	8.8.8.8	192.168.2.4	0x76f8	No error (0)	mibghgh.weebly.com	pages-wildcard.weebly.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:49:44.238667011 CET	8.8.8.8	192.168.2.4	0x76f8	No error (0)	pages-wildcard.weebly.com		199.34.228.53	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:44.238667011 CET	8.8.8.8	192.168.2.4	0x76f8	No error (0)	pages-wildcard.weebly.com		199.34.228.54	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:44.981012106 CET	8.8.8.8	192.168.2.4	0x5817	No error (0)	cdn1.editmysite.com	weebly.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:49:44.981012106 CET	8.8.8.8	192.168.2.4	0x5817	No error (0)	weebly.map.fastly.net		151.101.1.46	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:44.981012106 CET	8.8.8.8	192.168.2.4	0x5817	No error (0)	weebly.map.fastly.net		151.101.65.46	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:44.981012106 CET	8.8.8.8	192.168.2.4	0x5817	No error (0)	weebly.map.fastly.net		151.101.129.46	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:44.981012106 CET	8.8.8.8	192.168.2.4	0x5817	No error (0)	weebly.map.fastly.net		151.101.193.46	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:45.229485035 CET	8.8.8.8	192.168.2.4	0xc908	No error (0)	cdn2.editmysite.com	weebly.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:49:45.229485035 CET	8.8.8.8	192.168.2.4	0xc908	No error (0)	weebly.map.fastly.net		151.101.1.46	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:45.229485035 CET	8.8.8.8	192.168.2.4	0xc908	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 21:49:45.229485035 CET	8.8.8.8	192.168.2.4	0xc908	No error (0)	weebly.map .fastly.net		151.101.129.46	A (IP address)	IN (0x0001)
Feb 25, 2021 21:49:45.229485035 CET	8.8.8.8	192.168.2.4	0xc908	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 21:49:23.108668089 CET	64.202.125.18	443	192.168.2.4	49712	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	Tue Oct 12 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=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 21:49:23.109755993 CET	64.202.125.18	443	192.168.2.4	49711	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	Tue Oct 12 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=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 21:49:23.605612040 CET	13.224.94.82	443	192.168.2.4	49715	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	Sat Jun 12 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=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 21:49:23.609174013 CET	13.224.94.82	443	192.168.2.4	49716	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 21:49:23.612086058 CET	13.224.94.82	443	192.168.2.4	49714	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 21:49:23.614859104 CET	13.224.94.82	443	192.168.2.4	49717	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 21:49:25.397043943 CET	130.211.11.159	443	192.168.2.4	49720	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
					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 21:49:25.433609962 CET	64.202.125.15	443	192.168.2.4	49718	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		

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 21:49:25.434670925 CET	64.202.125.15	443	192.168.2.4	49719	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	Mon Feb 15 01:00:00 CET 2021	Sat Mar 19 00:59:59 CET 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=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 21:49:41.551229954 CET	64.202.125.18	443	192.168.2.4	49730	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	Tue Oct 12 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	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		
Feb 25, 2021 21:49:42.210942984 CET	64.202.125.15	443	192.168.2.4	49731	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	Mon Feb 15 01:00:00 CET 2021	Sat Mar 19 00:59:59 CET 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	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 21:49:44.644933939 CET	199.34.228.53	443	192.168.2.4	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	Thu Dec 02 13:00:00 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=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 21:49:44.646378994 CET	199.34.228.53	443	192.168.2.4	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		
Feb 25, 2021 21:49:45.073743105 CET	151.101.1.46	443	192.168.2.4	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 21:49:45.074157000 CET	151.101.1.46	443	192.168.2.4	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
					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 21:49:45.326427937 CET	151.101.1.46	443	192.168.2.4	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 21:49:45.326689005 CET	151.101.1.46	443	192.168.2.4	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		

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 21:49:45.327378988 CET	151.101.1.46	443	192.168.2.4	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		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6136 Parent PID: 800

General

Start time:	21:49:21
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:	0x7ff661a10000
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	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: 5888 Parent PID: 6136

General

Start time:	21:49:21
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:6136 CREDAT:17410 /prefetch:2
Imagebase:	0x1110000
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

Disassembly