ID: 358587
Cookbook: browseurl.jbs
Time: 21:53:00
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

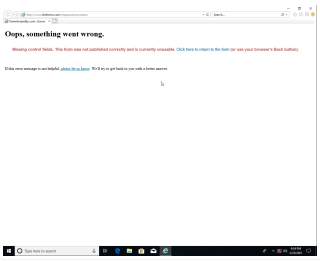
Analysis Report http://www.tfaforms.com/responses/pro…

Overview

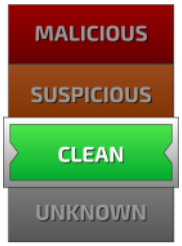
General Information

Sample URL:	http://www.tfaforms.com/responses/processor
Analysis ID:	358587
Infos:	

Most interesting Screenshot:



Detection

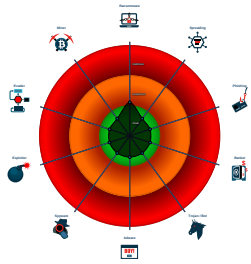


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

No high impact signatures.

Classification



Analysis Advice

Some HTTP requests failed (404). It is likely the sample will exhibit less behavior

Uses HTTPS for network communication, use the 'Proxy HTTPS (port 443) to read its encrypted data' cookbook for further analysis

Startup

- **System is w10x64**
- iexplore.exe (PID: 4616 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4588 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4616 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

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

Compliance:

Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Mitre Att&ck Matrix

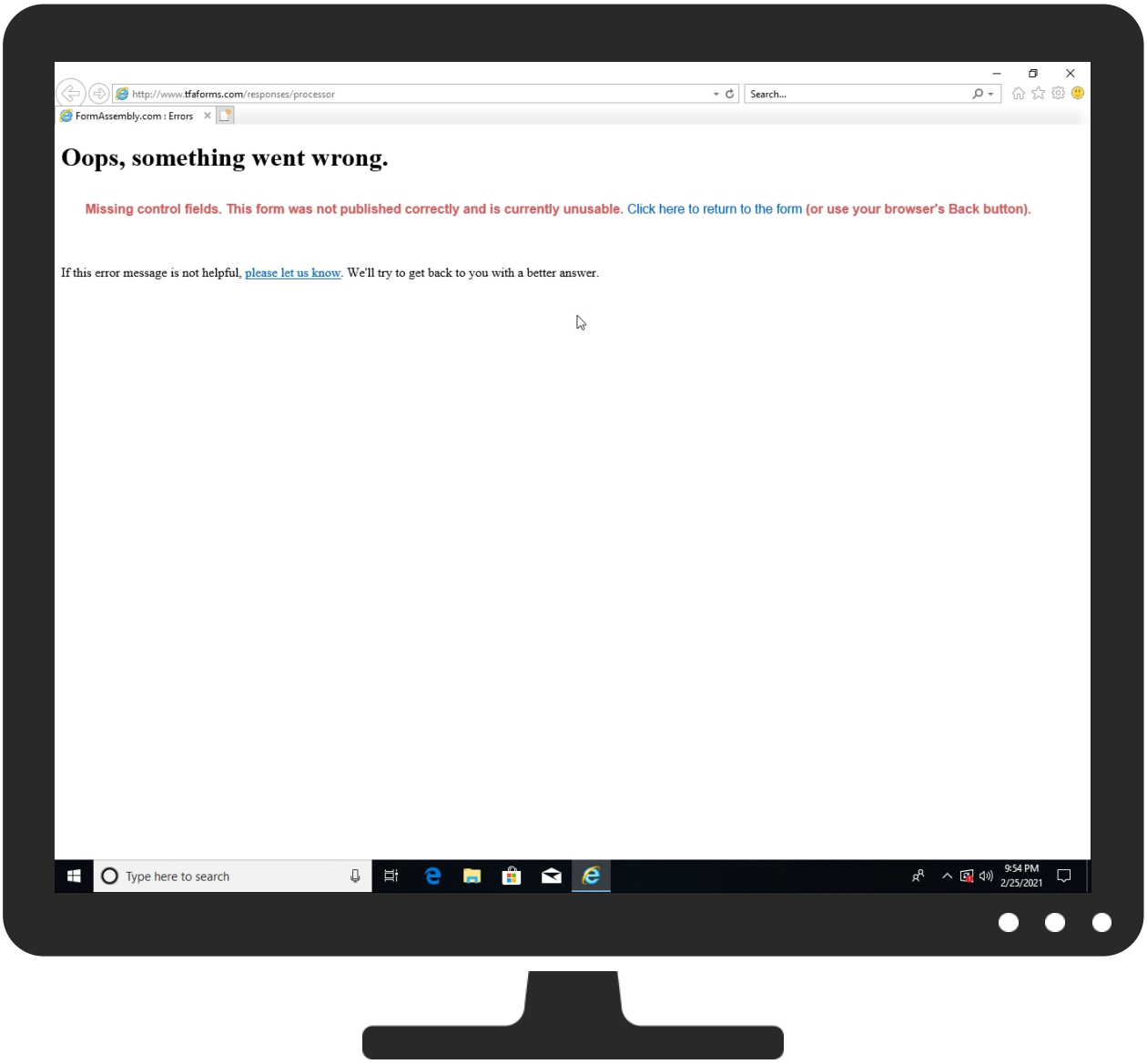
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partit
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 4	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 3	SIM Card Swap		Carri Billin Fraud

Behavior Graph

Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://www.tfaforms.com/responses/processor	0%	Virustotal		Browse
http://www.tfaforms.com/responses/processor	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
bam-cell.nr-data.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://fontawesome.iohttp://fontawesome.iohttp://fontawesome.io/license/http://fontawesome.io/licens	0%	Avira URL Cloud	safe	
http://https://help.formassemm/responses/processorbly.com/helpocessorRoot	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://designmodo.comAttribution-NonCommercial-NoDerivs	0%	Avira URL Cloud	safe	
http://designmodo.github.io/Flat-UI/)	0%	Avira URL Cloud	safe	
http://https://help.formassem	0%	Avira URL Cloud	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://getbootstrap.com)	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
formassembly.knowledgeowl.com	54.152.202.195	true	false		high
app-elbapp-a6b1wbowxm9e-391051627.us-east-1.elb.amazonaws.com	3.226.66.230	true	false		high
app.knowledgeowl.com	54.152.202.195	true	false		high
dyzz9obi78pm5.cloudfront.net	13.224.89.142	true	false		high
pi-ue1-lba3.pardot.com	35.174.150.168	true	false		high
formassembly.com	104.196.12.68	true	false		high
www.tfaforms.com	unknown	unknown	false		high
js-agent.newrelic.com	unknown	unknown	false		high
help.formassembly.com	unknown	unknown	false		high
bam-cell.nr-data.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
www.formassembly.com	unknown	unknown	false		high
pi.pardot.com	unknown	unknown	false		high

Contacted URLs

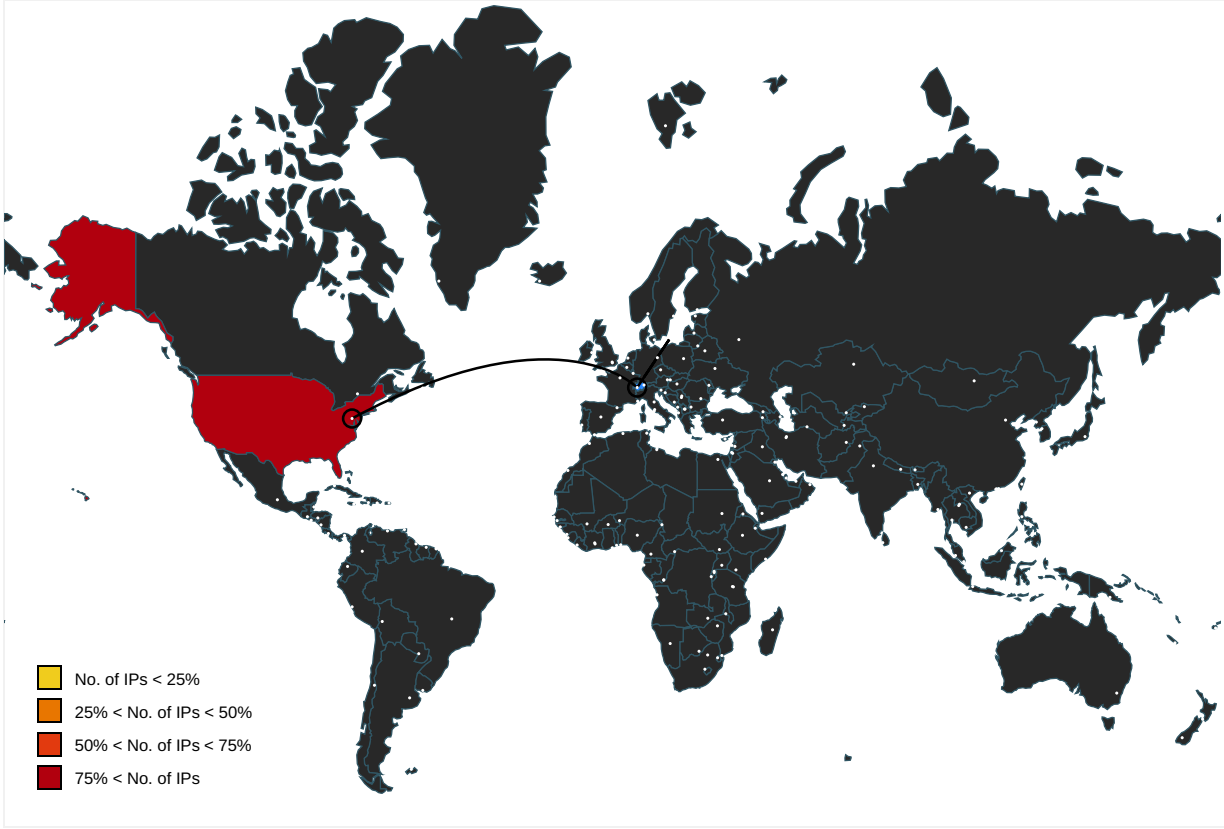
Name	Malicious	Antivirus Detection	Reputation
http://www.tfaforms.com/responses/processor	false		high
http://www.tfaforms.com/wForms/3.11/js/wforms.js?v=6b1109ac309299ec751af6a3c690f678773e405f	false		high
http://www.tfaforms.com/js/iframe_message_helper_internal.js?v=2	false		high
http://www.tfaforms.com/support/	false		high
http://https://help.formassembly.com/help	false		high
http://www.tfaforms.com/responses/favicon.ico	false		high
http://www.tfaforms.com/dist/form-builder/5.0.0/wforms-jsonly.css?v=6b1109ac309299ec751af6a3c690f678773e405f	false		high
http://www.tfaforms.com/pages/support	false		high
http://www.tfaforms.com/dist/form-builder/5.0.0/wforms-layout.css?v=6b1109ac309299ec751af6a3c690f678773e405f	false		high
http://www.tfaforms.com/responses/processor	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tfaforms.com/responses/processorRoot	{FD194317-77F6-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false		high
http://https://github.com/andris9/simpleStorage	iframe_message_helper_internal[1].js.2.dr	false		high
http://https://help.formassembly.com/app/image/id/5eac6dd7ad121cde5ddf2202/n/avenir-heavy.woff2	help[1].htm.2.dr	false		high
http://fontawesome.io	g=koFontawesome[1].css.2.dr, fontawesome-webfont[1].eot.2.dr	false		high
http://www.apache.org/licenses/LICENSE-2.0	g=publicJsFooter[1].js.2.dr	false		high
http://https://help.formassembly.com/help/form-tags-and-descriptions	help[1].htm.2.dr	false		high
http://stackoverflow.com/questions/20524815/ie-11-bug-image-inside-label-inside-form	wforms-layout[1].css.2.dr	false		high
http://fontawesome.iohttp://fontawesome.iohttp://fontawesome.io/license/http://fontawesome.io/licens	fontawesome-webfont[1].eot.2.dr	false	• Avira URL Cloud: safe	unknown
http://www3.formassembly.com/blog/wp-content/uploads/2014/03/play.png);	help[1].htm.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tfaforms.com/responses/processor2FormAssembly.com	~DF48068F2185627C41.TMP.1.dr	false		high
http://https://help.formassemm/responses/processorbly.com/helpocessorRoot	{FD194317-77F6-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://help.formassembly.com/knowledgebase/articles/340359-publish-with-an-iframe	iframe_message_helper_internal[1].js.2.dr	false		high
http://www3.formassembly.com/blog/wp-content/uploads/2014/03/play_orange.png);	help[1].htm.2.dr	false		high
http://designmodo.comAttribution-NonCommercial-NoDerivs	flat-ui-icons-regular[1].eot.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.tfaforms.com/responses/processor2Fbly.com/helpocessorRoot	{FD194317-77F6-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false		high
http://designmodo.github.io/Flat-UI/)	g=koCss[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://help.formassem	{FD194317-77F6-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://creativecommons.org/licenses/by-nc-nd/3.0/Version	flat-ui-icons-regular[1].eot.2.dr	false		high
http://www.tfaforms.com/responses/processor2FRoot	{FD194317-77F6-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false		high
http://https://formassembly.workable.com	help[1].htm.2.dr	false		high
http://fontawesome.io/license	g=koFontawesome[1].css.2.dr	false		high
http://designmodo.com/flatSergey	flat-ui-icons-regular[1].eot.2.dr	false		high
http://fontawesome.io/license/	fontawesome-webfont[1].eot.2.dr	false		high
http://https://www.formassembly.com/content/uploads/2017/05/Favicon.png	imagestore.dat.2.dr	false		high
http://https://www.google.%/ads/ga-audiences	analytics[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://help.formassembly.com/helpocessorx	{FD194317-77F6-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false		high
http://getbootstrap.com)	g=koCss[1].css.2.dr	false	• Avira URL Cloud: safe	low
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	g=koCss[1].css.2.dr	false		high
http://https://help.formassembly.com/helpocessor	~DF48068F2185627C41.TMP.1.dr	false		high
http://https://stats.g.doubleclick.net/j/collect	analytics[1].js.2.dr	false		high
http://https://help.formassembly.com/helpocessorf	~DF48068F2185627C41.TMP.1.dr	false		high
http://https://help.formassembly.com/help	~DF48068F2185627C41.TMP.1.dr, help[1].htm.2.dr	false		high
http://https://www.formassembly.com/terms-of-service.php	help[1].htm.2.dr	false		high
http://https://help.formassembly.com/helpVFormAssembly	~DF48068F2185627C41.TMP.1.dr	false		high
http://https://www.formassembly.com/privacy-policy.php	help[1].htm.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.224.89.142	unknown	United States		16509	AMAZON-02US	false
35.174.150.168	unknown	United States		14618	AMAZON-AESUS	false
104.196.12.68	unknown	United States		15169	GOOGLEUS	false
3.226.66.230	unknown	United States		14618	AMAZON-AESUS	false
54.152.202.195	unknown	United States		14618	AMAZON-AESUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358587
Start date:	25.02.2021
Start time:	21:53:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://www.tfaforms.com/responses/processor
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:	14
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	CLEAN
Classification:	clean0.win@3/41@9/5
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: http://www.tfaforms.com/support/
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, HxTsr.exe, backgroundTaskHost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 204.79.197.200, 13.107.21.200, 51.104.139.180, 93.184.220.29, 13.88.21.125, 52.147.198.201, 23.54.113.53, 104.43.139.144, 88.221.62.148, 151.101.2.110, 151.101.66.110, 151.101.130.110, 151.101.194.110, 162.247.243.146, 162.247.243.147, 184.30.20.56, 216.58.208.170, 216.58.206.36, 142.250.184.110, 172.217.18.99, 216.58.208.163, 152.199.19.161, 51.104.144.132 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, arc.msn.com.nsatc.net, cs9.wac.phicdn.net, tls12.newrelic.com.cdn.cloudflare.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, go.microsoft.com, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, www.google.com, watson.telemetry.microsoft.com, www.gstatic.com, prod.fs.microsoft.com.akadns.net, www.google-analytics.com, www.bing.com, fonts.googleapis.com, fs.microsoft.com, www-google-analytics.l.google.com, dual-a-0001.a-msedge.net, fonts.gstatic.com, ie9comview.vo.msecnd.net, f4.shared.global.fastly.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus15.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\DURNCK2N\www.tfaforms[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aK1r0aKb:JFK1rFKb
MD5:	132294CA22370B52822C17DCB5BE3AF6
SHA1:	DD26B82638AD38AD471F7621A9EB79FED448A71C
SHA-256:	451ABBE0AEFC000F49967DABF8D42344D146429F03C8C8D4AE5E33FF9963CF77
SHA-512:	6D5808CAD199A785C82763C68F0AE1F4938C304B46B70529EA26B3D300EF9430AD496C688D95D01588576B3A577001D62245D98137FD5CD825AD62E17D36F15C
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{FD194315-77F6-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8572343199844275
Encrypted:	false
SSDEEP:	96:r7ZcTZj2JWgtWbfUUzKMvrq+RQAxfVUi6X:r7ZcTZj2JWgtWfURMWlOfVsX
MD5:	B8D5EF430AD0B9D97F8BAE1E542BB308
SHA1:	3DF93C92E05464EDB0262CD61974A73D4EDD83E2
SHA-256:	7ACB3E5EBC810FA75570D1602EFB1B83875371AB712439273F2827B34AB54C1C
SHA-512:	6BD4EE7995C189E8C81374BCD2AA9647DDF879A08ADC334ED7EC74FAF978AAD09EE20AA6A149DB5E9BCCB894B25306DFBA54D3EA5DF386E3CCF81F2A8615F68
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\{FD194317-77F6-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	38376
Entropy (8bit):	1.9503309874860666
Encrypted:	false
SSDEEP:	192:r/Z4TQl6bkij12dWmM+Y0Y7Vjbn49OSc3CoaVSXlxDiqWx3ms:rhdQgcs0PD0CV3n49OSc3XaIX3iqgt
MD5:	BD959427FE90F6C2B29CE1C96155D59C
SHA1:	0515D0EBEAEF4EBEA8C1A3AD70DDC67ED933BB93
SHA-256:	D002A0654B0543EC8F1AA735EF8E55C79893409652AD1102F09CA5DF2FDE7F3F
SHA-512:	8F9840A4B25335096642313277A26F797297017AD10A9396C98FC0496B48EFC216776C5243B156267AFC057F8C3ADCAE41BDFD3B1EAD18AB9409B5E98E17A386
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{FD194317-77F6-11EB-90E5-ECF4BB570DC9}.dat	
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{FD194318-77F6-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5635650915055552
Encrypted:	false
SSDEEP:	48:IwJGcpreZGwpaDG4pQrGrapbSQGQpKjG7HpRcTGIpG:rPZeTQ16fBSYAyTIA
MD5:	A9960B910D188984CE9830D587FCF3E8
SHA1:	0897D1B55DE3B26045BBB7987A063A28A35FB504
SHA-256:	A8E23AD72DA2DAB97C61F7C0397F77D4F17DCA1F191FCE9EB4A8DC4828FC356F
SHA-512:	66EE4CEE60EA69B4C4A4061E437CF90313ADA35D7113CC12A250FA20E5C379215BB2B36C4CABCE36B3D57200D6D486106F03A87AF32502E3E10FC3BE4D9623 9
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\dikxvqf\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	1028
Entropy (8bit):	7.356921251969959
Encrypted:	false
SSDEEP:	24:D9BAGj1l8DLudUSQrYw+6yi8PXJcsNKJwq4:D9BAGj1CDLud5Qx3yi+XJTPT
MD5:	A7ABA22AB5FE3A8403F0052EAF1FA3F7
SHA1:	C14ADDC997BC88B346D6505BBD341800F59ECB43
SHA-256:	306D7634E159C01D65DF65B57EC8E3EE9E56869792C8B210A42553CC506EF764
SHA-512:	31292B55D2AC3C6C059E92F960EB1CFDD7D60435C25FD05AB76B97630287114DC50AD11CF5FDB5AB2F774EDD4E717B76D02E148EE6244F7F7E0012834B54AC 2
Malicious:	false
Reputation:	low
Preview:	@.h.t.t.p.s.:././.w.w.w...f.o.r.m.a.s.s.e.m.b.l.y...c.o.m./.c.o.n.t.e.n.t./.u.p.l.o.a.d.s./.2.0.1.7./.0.5./.F.a.v.i.c.o.n...p.n.g.^....PNG.....IHDR...(...(.....m...%IDATx..9h.Q...I$.W. .&."..bk%bc....AH.dsy..`."..S..2K..@E..hvM..n6q..`5....>?.....w....{3.[.y^U%..G....T.q...*0.....q5V`mA.W.....+Ep.g.....r..Wr.'.T..F0E.0.....r..30.R..g..=%....4...=.s.F."H..... ..1...\m.....3.....D.r..n.r...Ho.m...h..uy.....k..4.'.|$WA'..(7,{...v.....x.y. ..f+. r.5.E|.c/....e!7.....(..o.v.....}.L..PA.1...RdT.d%pS.^.....T.....H9.....o..=.i.y.Ij.:N.}.\0.BP....Q....X"...r'... .7. 8....j...../..q.nLr.v....<.....`6d..j.....1...ZS...?nM.M.%.)u.kF....~./..}cM..$R2.....#.-".....>.Q..#pN-...W....K!r_Y...A.(.X...5.....r..5..W....2...rk..Ip. .@.....[..J.,..rk. ..#.U.lu1!7.. .....o&@...{p.[.....35..1_.AG..H9%rP....K.?...\A..d.<.=RN.WI.r.....j5..!..V...XlA.?dx...%....5.r(. o.....4j6.....z..$..YWVAG'.)..@..U....b.A+cy.V.W.a.....(:....IEND.B`.(...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\Favicon[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	162
Entropy (8bit):	4.43530643106624
Encrypted:	false
SSDEEP:	3:qVoB3tUROGclXqyvXboAcMBXqWSZUXqXlIVLLP61IwcWWGu:q43tISl6kXiMIWSU6Xll5LP8IpfGu
MD5:	4F8E702CC244EC5D4DE32740C0ECBD97
SHA1:	3ADB1F02D5B6054DE0046E367C1D687B6CDF7AFF
SHA-256:	9E17CB15DD75BBBD5DBB984EDA674863C3B10AB72613CF8A39A00C3E11A8492A
SHA-512:	21047FEA5269FEE75A2A187AA09316519E35068CB2F2F76CFAF371E5224445E9D5C98497BD76FB9608D2B73E9DAC1A3F5BFADFDC4623C479D53ECF93D81D3C F
Malicious:	false
Reputation:	low
Preview:	<html>..<head><title>301 Moved Permanently</title></head>..<body>.. 301 Moved Permanently ..<hr> nginx ..</body>.. </html>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\analytics[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	47332
Entropy (8bit):	5.518633523108405
Encrypted:	false
SSDEEP:	768:UyC36rcBLbfsl5XqYoyPndHTkoWY3SoavVVy2WiCgYUD0FEw0stZb:UyDAZfY5hVdHTwY3Soljw0sD
MD5:	6A10EB2BB5C90414980729F4F96FFBDA
SHA1:	8BBBD5948255549E4B691B614AA3177DEA9AF1B7
SHA-256:	0F3BE44690AE9914AE3E47B7752E1BDEA316F09938E9094F99E0DE19CCD8987A
SHA-512:	5A505CBAAEEAB8961AA0DE94767F76A09B6F03E60EB0C72954B85EC0392EE1CE383D2088939A314D3175AB24B7A69390C841CFE0237C1D1C40966B43F22AE92 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google-analytics.com/analytics.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var n=this||self,p=function(a,b){a=a.split(".");var c=n;a[0]in c||"undefin ed"==typeof c.execScript||c.execScript("var "+a[0]);for(var d;a.length&&(d=a.shift());)a.length||void 0===b?c=c[d]&&c[d]!==Object.prototype[d]?c[d]:c[d]={}:c[d]=b};var q= function(a,b){for(var c in b)b.hasOwnProperty(c)&&(a[c]=b[c])},r=function(a){for(var b in a)if(a.hasOwnProperty(b))return!0;return!1};var t=/^(?:(?:https?|mailto|ftp):|[^:/?#]*(?: [/?#]|$))/i;var v=window,x=document,y=function(a,b){x.addEventListener?x.addEventListener(a,b,!1):x.attachEvent&&x.attachEvent("on"+a,b)};var z={},A=function(){z .TAGGING=z.TAGGING\|\|[];z.TAGGING[1]=!0};var B=/:[0-9]+$/,C=function(a,b,c){a=a.split("&");for(var d=0;d<a.length;d++){var e=a[d].split("=");if(decodeURIComponen t(e[0]).replace(/\+/g," ")===b)return b=e.slice(1).join("="),c?b:decodeURIComponent(b).replace(/\+/g," ")}},F=function(a,b){b&&(b=String(b).toLowerCase());if("p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\flat-ui-icons-regular[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), flat-ui-pro-icons family
Category:	downloaded
Size (bytes):	25912
Entropy (8bit):	6.106742023542436
Encrypted:	false
SSDEEP:	384:MoJYNb9fSYaiaAwjHg8dX0JQpop4BuEPgCW+b/pcNCi1TgmLj+veAsbLgmKR:BYNZ+Hg8dX0Jui4fPb3/Cn1LCvdK9
MD5:	F1D025E1D5DC1B25678397FCF6AE70D7
SHA1:	ACA0199880BA1945FEB4AE85DFDF7436D4AFFEC2
SHA-256:	DD97A7F8D8B4B790804C55C6C7FE10CBF0D6DC7CA4782201774A4DE1196E290F
SHA-512:	3C1FB7BA70650CBC9D584507B382BF9A7140125AB50C6E58D1952090A1A956AB058DB86B5748DFBCAD920E8AB095559A3ED7AA2DB5250578DEB88F785301C8C 5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://app.knowledgeowl.com/flatui/fonts/glyphicons/flat-ui-icons-regular.eot?
Preview:	8e..ld.....LP.....u.....".f.l.a.t.-.u.i.-.p.r.o.-.i.c.o.n.s.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .1...1...".f.l.a.t.-.u.i.-.p.r.o.-.i.c.o.n.s.....0OS/2..... .`cmap.U.....Lgasp.....h....glyf...N...p..\.head..P..^,...6hhea... ..^d...$hmtx.....^.....loca./...`.....maxp.o....`.... name;.....a....Cpost.....dL... .....3..... .....@...`.....@..... .....8..... .`..... .....79.....79.....79.....%..!.....!..... .....!.....!.....%.....@.@..... .....A..A..... .....'..7...a..A.....A...A.>..A.=... .....4...!....+ ."..5.!"..=.4>.3!.4>.;.2....!2.....#.....@.....@....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\fontawesome-webfont[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), FontAwesome family
Category:	downloaded
Size (bytes):	165742
Entropy (8bit):	6.705073372195656
Encrypted:	false
SSDEEP:	3072:qbhEnD+IzsU9z9QJ6/P3Xe2iEiEPGFCMW1JVJG6wVTDsk6BmG6S1yKshojskO+b2:qenD+IzsU9z9QJ6/PO2FiEP2C/DVJG6I
MD5:	674F50D287A8C48DC19BA404D20FE713
SHA1:	D980C2CE873DC43AF460D4D572D441304499F400
SHA-256:	7BFCAB6DB99D5CFBF1705CA0536DDC78585432CC5FA41BBD7AD0F009033B2979
SHA-512:	C160D3D77E67EFF986043461693B2A831E1175F579490D7F0B411005EA81BD4F5850FF534F6721B727C002973F3F9027EA960FAC4317D37DB1D4CB53EC9D343A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dyzz9obi78pm5.cloudfront.net/css/font-awesome-4.7.0/fonts/fontawesome-webfont.eot?
Preview:	n.....LP.....Yx.....F.o.n.t.A.w.e.s.o.m.e.....R.e.g.u.l.a.r...$.V.e.r.s.i.o.n. .4...7...0. .2.0.1.6.....F.o.n.t.A.w.e.s.o.m.e.....PFFTMk .G.....GDEF.....p... OS/2.z@...X...`cmap..:.....gasp.....h....glyf...M.....L.head...-.....6hhea.....$hmtxEy.....loca...\.....maxp.,.....8... name....gh....post.....k.... u.....xY_.<.....3.2.....3.2.....'.....@.....i.....3.....3...s.....pyrs.@. ....p.....U..... .....].....y...n.....2.....@..... .....z.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\g=koCss[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	284796
Entropy (8bit):	5.101704501368992
Encrypted:	false
SSDEEP:	1536:VwldERdvGNIkabbRk3ch9OW5pK38FfFVyl2+285/sIjRV42:QhBshT5k285/so
MD5:	94A9B8F202B7E5F82FA1D9D1D3782DF1
SHA1:	AC5D534A5964FCB8DAF843168F19A6C559E316F8
SHA-256:	870425DFBB1EBF55058A7C67FF5C86A28B7900555D0D9BB54557CED4E498120E
SHA-512:	565B922BA712F2A9FB27DB81FFCDB9BCC18AE6774B68BBD5B6A642C5FFDB53294ADA89C49F2F110C8ED77688C74E95D06CCF245779AD59BFB21D7D7066980 2A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dyzz9obi78pm5.cloudfront.net/2021022501/min/g=koCss
Preview:	/*!. * Bootstrap v3.2.0 (http://getbootstrap.com). * Copyright 2011-2014 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). *//*! normalize.css v3.0.1 | MIT License | git.io/normalize */html{font-family:sans-serif;-webkit-text-size-adjust:100%;-ms-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:0 0}a:active,a:hover{outline:0}abbr[title]{border-bottom:1px dotted}b,strong{font-weight:700} dfn{font-style:italic}h1{margin:.67em 0;font-size:2em}mark{color:#000;background:#ff0}small{font-size:80%}sub,sup{position:relative;font-size:75%;line-height:0;vertical-a lign:baseline}sup{top:-.5em}sub{bottom:-.25em}img{border:0}svg:not(:root){overflow:hidden}figure{margin:1em 40px}hr{height:0;-webkit-box-sizing:conten

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\help[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	116645
Entropy (8bit):	5.121804763790916
Encrypted:	false
SSDEEP:	1536:zco5S3dzGyKUVcRN+gOLmCvIUxumR5NHjkgx:0dmTRNxCvIw
MD5:	92742A0BE374285C597B3D43C7C19A2B
SHA1:	75CFCEEF32E42E124E6EDB7746646C5BD17A19E9
SHA-256:	AAE0D2C03A00C3C87C027DBDA79F55CCE98CFE4B1145CCE3B1114BB99396178E
SHA-512:	5F227F17FAF71850BEC043A97F8135561B01E6A6134160A437B606378E4CA25716DF87A366F37E26A13EA188E4448C73A53466FFFF8641B92F2BA27161A2B5AF
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html>..<head>...<meta http-equiv="X-UA-Compatible" content="IE=edge" />...<title>FormAssembly | FormAssembly Resource Center</title>...<meta charset="UTF-8" />...<meta name="viewport" content="width=device-width, initial-scale=1.0">...<meta name="description" content="FormAssembly Resource Center can help you find new ways to make your forms better!">...<link rel="stylesheet" href="//dyzz9obi78pm5.cloudfront.net/min/g=koFontawesome" type="text/css">..... [if IE 7]>. .....<link rel="stylesheet" type="text/css" href="2021022501/css/ie7.css">.....<![endif]-->.....<link rel="stylesheet" href="//dyzz9obi78pm5.cloudfront.net/20210225 01/min/g=koCss" type="text/css">...<link href="https://help.formassembly.com/app/image/id/5eac6dd7ad121cde5ddf2202/n/avenir-heavy.woff2" rel="stylesheet" type=" text/css"><link href="https://fonts.googleapis.com/css?family=Lato" rel="stylesheet" type="text/css">...<style type="text/css">.documentation-body{background-color:#fffff f}.hg-cl

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\rainbow-custom.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	28512
Entropy (8bit):	5.329815063874166
Encrypted:	false
SSDEEP:	768:mSBHOmiydMJOicfY9tqz8vriHnd6L5Ggxt6x7mAjD:NHOmixsEtqz8jOd6V7i93
MD5:	83B8621ACC08A9921D10DAD68E6CB234
SHA1:	BFD1BAC2B6EA455B05076E3DA688B71BA4DC9C78
SHA-256:	7D396FB0806284C2D164F205B2D2251339F3A30E91D0935E1D3EB9B76112BA45
SHA-512:	CA99447639D4F83084982C7DA2D9D9352D7402D652E2B6638351ABBB942B39C3994EACF88D6819AE2D226E66DD407073284DBC730CF48116FA27528C16623A7D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://help.formassembly.com/js/rainbow/rainbow-custom.min.js
Preview:	/* Rainbow v1.2 rainbowco.de | included languages: c, shell, java, d, coffeescript, generic, scheme, javascript, r, haskell, python, html, smalltalk, csharp, go, php, ruby, lua, css */.var k=!0;.window.Rainbow=function(){function B(a){var b=a.getAttribute("data-language")||a.parentNode.getAttribute("data-language");if(!b){var c=/\blang(?:uage)?-(\w+)/;(a=a.className.match(c)||a.parentNode.className.match(c))&&(b=a[1])}return b}function C(a,b){for(var c in f[d]){c=parseInt(c,10);if(a==c&&b==f[d][c]?0:a<=c& &b>=f[d][c])delete f[d][c],delete j[d][c];if(a>=c&&a<f[d][c]||b>c&&b<f[d][c])return k}return!1}function r(a,b){return'<span class="'+a.replace(/\./g," ")+(m?" "+m:"")+'">'+b+" "}function s(a,.b,c,i){if("undefined"===typeof a||null===a)i();else{var e=a.exec(c);if(e){++t;!b.name&&"string"==typeof b.matches[0]&&(b.name=b.matches[0],delete b.matches[0]);var l=e[0],g=e.index,u=e[0].length+g,h=function(){function e(){s(a,b,c,i)}t%100>0?e():setTimeout(e,0)};if(C(g,u))h();else{var n=v(b.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\wforms-jsonly[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	755
Entropy (8bit):	4.764598419421799
Encrypted:	false
SSDEEP:	12:zSmmdOdWGQqfTTLxdXLXETvTTPdXCCni/rTvjCPdXMVjCRQW/TTHRA1W/jC3C+Tr:zSmASWYTHHjEbThpi/rbCsCjTTmcN+Tr
MD5:	7115B3A93075ECB5E36335002FCAFF7E
SHA1:	F655788CAA361AA3F2A6A3A1AAD1FCA871450743
SHA-256:	2C3626D21F1D22DC053238489A0AC7B58C451C95B516C1A13BD8BCF08E555C1A
SHA-512:	3CD1DCE5E5A4EADFCA07D48F60684916F028D15E8621B12DBC1011D6AA62B8F4672401B4BDDA75104264A1B58EBAAE58DB8FDD99522E84734BE9E27AA637310B
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.tfaforms.com/dist/form-builder/5.0.0/wforms-jsonly.css?v=6b1109ac309299ec751af6a3c690f678773e405f
Preview:	../* Accessiblity Related Rules */./* These are the rules that should *not* apply if javascript is disabled. */....offstate {. display: none !important;.}..html .wForm form .wfPage, html .wForm form .wfHideSubmit {. display: none !important;.}.html .wForm form .saveAndResume .actions .wfHideSubmit {. display: block !important;.}.html .wForm form .wfCurrentPage {. display: block !important;.}...offstate-resumelater {. display: none !important;.}..onstate-resumelater {. display: block !important;.} ..#saveAndResumeFieldset {. display: none;.}../* Handle page visibility */.html .wForm form .wfPage, html .wForm form .wfHideSubmit {. display: none !important;.}.html .wForm form .wfCurrentPage {. display: block !important;.}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\Favicon[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 40 x 40, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	862
Entropy (8bit):	7.653640922797821
Encrypted:	false
SSDEEP:	12:6v/7Qh1QGw9Yj1l2ZgwLudBSSQGeYwPUiSw6nFV/n6y2FuFPPJfVnJhG28WNKJwg:xj1l8DLudUSQrYw+6yi8PXJcsNKJwqz
MD5:	9BC284924A839F4CCDEB5167E28804B7
SHA1:	6CC3350B72D727F596BE53C1891D101C844F7D66
SHA-256:	E7650F78F6405F203399B6A590BC2A884AF74616E89A63E0E0078CA94EC8165C
SHA-512:	D4552D94C7708A3A793E489B3EDB374A7126A5A2128F14C4FE22245099B45DECD8D8B37564604CA41C8FC0511566F36D3556F3B7D18BAB61B8BDF2F18D4A2B3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.formassembly.com/wp-content/uploads/2017/05/Favicon.png
Preview:	.PNG.....IHDR...(...(.....m...%IDATx..9h.Q...l$.W..&."..bk%bc....AH.dsy..`."..S..2K..@E..hvM..n6q..`5....>?.....w....{3.[.y^U%..G....T.q...*0.....q5V`mA.W.....+Ep.g.....r..Wr.'.T..F0E.0.....r..30.R..g..=%....4...=.s.F."H.....1...\m.....3.....D.r..n.r...Ho.m...h..uy....k..4.'.\|$WA'..(7,{...v.....x.y. ..f+. r.5.E|.c/....e!7.....(..o.v.....}.L..PA.1...RdT.d%pS.^.....T.....H9.....o..=.i.y.Ij.:N.}.\0.BP....Q....X"...r'....7. 8.....j...../..q.nLr.v....<.....`6d..j.....1...ZS...?nM.M.%.)u.kF....~./..}cM..$R2.....#.-".....>.Q..#pN-...W....K!r_Y...A.(.X...5.....r..5..W....2...rk..Ip. .@.....[..J.,..rk. ..#.U.lu1!7.....o&@...{p.[.....35..1_.AG..H9%rP....K.?...\A..d.<.=RN.WI.r.....j5..!..V...XlA.?dx...%....5.r(. o.....4j6.....z..$..YWVAG'.)..@..U....b.A+cy.V.W.a.....(:....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\api[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	850
Entropy (8bit):	5.527084929213002
Encrypted:	false
SSDEEP:	24:2jkm94/zKPccAv+KVCetQ1IeqsLqo40RWUnYN:VKEctKoe61IoLrwUnG
MD5:	F265186D221473A895D2373E5666BC80
SHA1:	1B167F3E67EA18FD54FA21AFB265156B4AEAF7E6
SHA-256:	7BE93782718B63BDF0478467DBAE39879064F603EB44D42A90A6C6FEE1EE81A3
SHA-512:	F677A3F22F324555AAAF6249EA0569F68F35BCB1B567956BF517026646E4B88275EBCCDFBFDB32B06FA067767AD0B966379C53BE4D19071408A99EAC867F1987
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/recaptcha/api.js
Preview:	/* PLEASE DO NOT COPY AND PASTE THIS CODE. */(function(){var w=window,C='___grecaptcha_cfg',cfg=w[C]=w[C]||{},N='grecaptcha';var gr=w[N]=w[N]||{};gr.ready=gr.ready||function(f){(cfg['fns']=cfg['fns']||[]).push(f);};w['__recaptcha_api']='https://www.google.com/recaptcha/api2/';(cfg['render']=cfg['render']||[]).push('onload');w['__google_recaptcha_client']=true;var d=document,po=d.createElement('script');po.type='text/javascript';po.async=true;po.src='https://www.gstatic.com/recaptcha/releases/jxFQ7RQ9s9HTGKeWcoa6UQdD/recaptcha__en.js';po.crossOrigin='anonymous';po.integrity='sha384-M9863pj8VTkCmdbfuuaGvQUaNXo72mc4KbfOtDfVBjv+zjrQy0vx5uzX9BsGSepE';var e=d.querySelector('script[nonce]'),n=e&&(e['nonce']||e.getAttribute('nonce'));if(n){po.setAttribute('nonce',n);}var s=d.getElementsByTagName('script')[0];s.parentNode.insertBefore(po, s);})();

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\css[1].css	
File Type:	ASCII text
Category:	downloaded
Size (bytes):	169
Entropy (8bit):	5.07579670704692
Encrypted:	false
SSDEEP:	3:0SYWFFWIIYCZZ5RI5XwDKLRIHDfFRWdFTfqzrZqcdjK/mRtBsYARNin:0IFFN+56ZRWHTizlpdgmRtBaNin
MD5:	21293E4BE383F939F010DEEFB93A12DC
SHA1:	63B5D1E607AC77495ABCC9450717EFC4DD39B35B
SHA-256:	A026EF5D961447E008A0E17E2D1B5076A09D1AD83C1FE38C6954E66B420A8484
SHA-512:	EF6E376333D67B4354C185484F3DE1AC5E7C79B2B6A193FDCC0385CA0F62643A96C60DF8BB384BC5AC7B352993A14E7D4A2BBE201D6DE796513371D6D57C2F3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Lato
Preview:	@font-face {. font-family: 'Lato';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/lato/v17/S6uyw4BMUTPHjx4wWA.woff) format('woff');.}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\css[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1184
Entropy (8bit):	5.300645554985999
Encrypted:	false
SSDEEP:	24:5MOYNFMOYsiMOYN7q/EOYNNxlwTg/EOYsNxlwTN+/EOYN7NxlwTHa:SOWGOLpOCVOWNITHOLNITNZOCNIT6
MD5:	44CB14977FC77909F0C8EA26B9A22094
SHA1:	236BB248452AD13193C37AE0A040C8C68420C7DA
SHA-256:	4696FA8BF1CF824217DDF70DF758460696FFF45DE941540F52C5E17DB3D40800
SHA-512:	36C4AC520FB04F9554327044413DD9A07FA7A5DF61A0C2A1A3D814FD4D10E529366586358A81AC19BE025D2353D212BFBF80F505BB87D02C2BE4043EE5B30CE
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UN_r8OUuhv.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/opensans/v18/mem8YaGs126MiZpBA-UFVZ0d.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UN7rgOUuhv.woff) format('woff');.}.@font-face {. font-family: 'Roboto Slab';. font-style: normal;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/robotoslab/v13/BngbUXZYTXPIvIBgJJSb6s3BzlRRfKOFbvjo0oSmb2Rl.woff) format('woff');.}.@font-face {. font-family: 'Roboto Slab';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/robotoslab/v13/BngbUXZYTXPIvIBgJJSb6s3BzlRRfKOFbvjojISmb2Rl.woff) format('woff');.}.@font-face {. font-fami

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\g=publicJsFooter[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	285373
Entropy (8bit):	5.235397507665197
Encrypted:	false
SSDEEP:	3072:l6LMBJUExACDqZbMNIeCN0HS/vq5vZBMIfESco7XEUXCEZnF0Mhev:l6LMiZbYHS/vq5ZEazZnF0MUv
MD5:	7BF4A2C91F6A22CA2A39FE11830F431B
SHA1:	3E2A5DE28278B18AF1A15089AA066A154BB6E50F
SHA-256:	2FD1FFA5DD8AED0B247F54A5FA28EF1EEDBECD3D7DF803D4B1664FB3FCD2147B
SHA-512:	CCE2C04A6CB8CF0B396F2D95E8572C36DAF214B4D69FAAED7CF13F59DDFB5CC6F00D0C0BD50306A951323FD7E7236E4D2DBCD708517627943EC279215E115A4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dyzz9obi78pm5.cloudfront.net/2021022501/min/g=publicJsFooter
Preview:	!function(a){"function"==typeof define&&define.amd?define(["jquery"],a):a(jQuery)}(function(a){function b(b,d){var e,f,g,h=b.nodeName.toLowerCase();return"area"===h?(e=b.parentNode,f=e.name,!(!b.href||!f||"map"!==e.nodeName.toLowerCase())&&(g=a("img[usemap='#"+f+"']")[0],!!g&&c(g))):(/input|select|textarea|button|object/.test(h)?!b.disabled:"a"===h?b.href||d:d)&&c(b)}function c(b){return a.expr.filters.visible(b)&&!a(b).parents().addBack().filter(function(){return"hidden"===a.css(this,"visibility")}).length}function y(a){for(var b,c;a.length&&a[0]!==document;){if(b=a.css("position"),("absolute"===b||"relative"===b||"fixed"===b)&&(c=parseInt(a.css("zIndex"),10),!isNaN(c)&&0!==c))return c;a=a.parent()}return 0}function z(){this._curInst=null,this._keyEvent=!1,this._disabledInputs=[],this._datepickerShowing=!1,this._inDialog=!1,this._mainDivId="ui-datepicker-div",this._inlineClass="ui-datepicker-inline",this._appendClass="ui-datepicker-append",this._triggerClass="ui-datepicker-trigger",th

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\pd[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	5186
Entropy (8bit):	5.177511759121435

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\pd[1].js	
Encrypted:	false
SSDEEP:	96:SZ6XcSJpDSMe+8gGVHRwE9gib6Ymv4/q1ykQ7KJcBWXDylZP25A/F4tT5yqUg8:SZMcSK/PgdQYBQ7KGBW2lZ25A9mT5f8
MD5:	4801DAC64526FE7AE9A2B34F19E7943F
SHA1:	4DF465117F396C248B6A3EFC4E897D496C1D2041
SHA-256:	925BE107869153B6120DE872C1AE333977BFAEE69A0F7C6271F32D4A8348BCA8
SHA-512:	4E911ABB2A57BE6491AD3AD0E7E82AF31674B83E20B3017D544015AC269BD9A84FC5D7ABF0BF055779EAED7D1084BDE5C6E7B4D8118BE8B6902733FF45A16AF8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pi.pardot.com/pd.js
Preview:	/*! 2020-03-12 10:41:10 */.function checkNamespace(e){for(var t=e.split("."),r=window,i=0;i<t.length;i++){var a=t[i];r[a]||(r[a]={}),r=r[a]}}function getPardotUrl(){var e="pi.pardot.com";return"string"==typeof piHostname&&(e=piHostname),("https:"==document.location.protocol?"https://":"http://")+e}function piTracker(e){if(checkNamespace("pi.tracker"),pi.tracker.visitor_id=piGetCookie("visitor_id"+(piAId-1e3)),pi.tracker.visitor_id_sign=piGetCookie("visitor_id"+(piAId-1e3)+"-hash"),pi.tracker.pi_opt_in=piGetCookie("pi_opt_in"+(piAId-1e3)),"false"!=pi.tracker.pi_opt_in||void 0!==pi.tracker.title&&pi.tracker.notify_pi){var t=piGetParameter(document.URL,"pi_campaign_id");null!=t?pi.tracker.campaign_id=t:"undefined"!=typeof piCId&&""!=piCId&&null!=piCId?pi.tracker.campaign_id=piCId:pi.tracker.campaign_id=null,pi.tracker.account_id=piAId,pi.tracker.title=document.title,"undefined"!=typeof piPoints&&(pi.tracker.pi_points=piPoints),pi.tracker.url=void 0!==e?e:document.URL,pi.tracker.referrer=d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\wforms-layout[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	30044
Entropy (8bit):	5.085412382641297
Encrypted:	false
SSDEEP:	384:v4oDbxnuXCx+xn3DxNSlbEfsnlDrpsJvLe40z3YzecUUlMDR7igWKVNyW+VHZxpf:goPaBxBwzYfw+xhCLUEEKW/K/vG
MD5:	468114E6FD705DA883A1EC1182EA0513
SHA1:	196C780923CCB37B90C395086F3274FDC19D90CC
SHA-256:	7DAD717CD3BBABC16A91B8404874EDA70C68F023A66DDEEA1D26579C0C774215
SHA-512:	CEA8AE0120FF73620152E0F2122FB19A8AF070C5154547DA5B68EBAC449DAC005E86C846F2E3A03F7905265FE39D1EA04391866E1128C676114D54051BAEF9F0
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.tfaforms.com/dist/form-builder/5.0.0/wforms-layout.css?v=6b1109ac309299ec751af6a3c690f678773e405f
Preview:	* {..-webkit-font-smoothing: antialiased;.}../* Reset CSS - scope limited to .wForm - based on YUI reset. * ----------. */..wForm dl, .wForm dt, .wForm dd, .wForm ul, .wForm ol, .wForm li, .wForm div, .wForm th,..wForm h1, .wForm h2, .wForm h3, .wForm h4, .wForm h5, .wForm h6, .wForm pre, .wForm td,..wForm form, .wForm fieldset, .wForm input, .wForm textarea, .wForm p, .wForm blockquote {..margin:0; padding:0; }..wForm table { border-collapse:collapse; border-spacing:0; }..wForm fieldset, .wForm img { border:0; }..wForm address, .wForm caption, .wForm cite, .wForm code, .wForm dfn,.wForm em, .wForm strong, .wForm th, .wForm var {..font-style:normal; font-weight:normal; }..wForm ol, .wForm ul { list-style:none; }..wForm caption, .wForm th { text-align:left; }..wForm h1, .wForm h2, .wForm h3:not(.wFormTitle), .wForm h4, .wForm h5, .wForm h6 { font-size:100%; font-weight:normal; }..wForm q:before, .wForm q:after { content:''; }..wForm abbr, .w

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\wforms[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	243215
Entropy (8bit):	5.430619101104077
Encrypted:	false
SSDEEP:	3072:gsEQV0+H4O8ebj1cHcmcrCWEPIc+7/dTXmPYlNCH:rsO8en6l+7/dTX2
MD5:	14E383468CFC2E8356E5007F5946F85E
SHA1:	97124AC35550A0FA6165EFD184E4D1D92E7F06D8
SHA-256:	900D2CBF35F85BDB03AFBD715CF013E206C87C932134D4D966399ABE5BFC1F39
SHA-512:	F8D272E7BF216A61128CEA3D2C9674CA34A7722221FB1D29EEFA87677521A8EA0532D98E54FEBE4A86B46E2F43FAA50DCEDB0D6232CAF999AD9907E4874C20E
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.tfaforms.com/wForms/3.11/js/wforms.js?v=6b1109ac309299ec751af6a3c690f678773e405f
Preview:	var base2={name:"base2",version:"1.0",exports:"Base,Package,Abstract,Module,Enumerable,Map,Collection,RegGrp,Undefined,Null,This,True,False,assignID,detect,global",namespace:""};new function(_no_shrink_){var Undefined=K(),Null=K(null),True=K(true),False=K(false),This=function(){return this};var global=This();var base2=global.base2;var _FORMAT=/%([1-9])/g;var _LTRIM=/^\s\s*/;var _RTRIM=/\s\s*$/;var _RESCAPE=/([\/()[\]{}\|*+-.,^$?\\])/g;var _BASE=/try/.test(detect)?/\bbase\b/:/.*/;var _HIDDEN=["constructor","toString","valueOf"];var _MSIE_NATIVE_FUNCTION=detect("(jscript)")?new RegExp("^"+rescape(isNaN).replace(/isNaN/,"\\w+")+"$"):{test:False};var _counter=1;var _slice=Array.prototype.slice;_Function_forEach();function assignID(object){if(!object.base2ID){object.base2ID="b2_"+_counter++}return object.base2ID}var _subclass=function(_instance,_static){base2.__prototyping=this.prototype;var _prototype=new this;if(_instance){extend(_prototype,_instance)}delete base2.__prototyping;var _constr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\c33294f5df[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\c33294f5df[1].gif	
Size (bytes):	24
Entropy (8bit):	2.459147917027245
Encrypted:	false
SSDEEP:	3:CUXJ/lH:Dl
MD5:	BC32ED98D624ACB4008F986349A20D26
SHA1:	2D3DF8C11D2168CE2C27E0937421D11D85016361
SHA-256:	0C9CF152A0AD00D4F102C93C613C104914BE5517AC8F8E0831727F8BFBE8B300
SHA-512:	71ACC6DA78D5D5BF0EEA30E2EE0AC5C992B00EFEC959077DFE0AB769F1DBBD9AF12D5C5C155046283D5416BEB606A9EF323FB410E903768B1569B69F37075B4E
Malicious:	false
Reputation:	low
Preview:	GIF89a.....,.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\g=koFontawesome[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	31317
Entropy (8bit):	4.759435559291011
Encrypted:	false
SSDEEP:	384:u3Y5yWeTUKW+KlkJ5de2UYDyVfwYUas2l8yQ/8dwmaUX:umlr+Klk3Yi+fwYUf2l8yQ/e9vX
MD5:	4405176548FEF6B438C79BA353FDFFB5
SHA1:	E3679C8CD9EE81EB23D782A8B6FB996C9102ACD7
SHA-256:	A9F4746243E00C74C7CAE7F9BE3E0A6B588C8513711E80FD7D8B887251C2834E
SHA-512:	2B44F92DAB327E09899267DC719A568E7AAB00CC26AAFA55C9C5075E1036C58E2A81268BC597F706ABC1F69D2093E48440A12F1C3FC000F1B9423EE5CCFC9C3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dyzz9obi78pm5.cloudfront.net/min/g=koFontawesome
Preview:	./*!. * Font Awesome 4.7.0 by @davegandy - http://fontawesome.io - @fontawesome. * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License). */.@font-face{font-family:'FontAwesome';src:url('//dyzz9obi78pm5.cloudfront.net/css/font-awesome-4.7.0/fonts/fontawesome-webfont.eot?v=4.7.0');src:url('//dyzz9obi78pm5.cloudfront.net/css/font-awesome-4.7.0/fonts/fontawesome-webfont.eot?#iefix&v=4.7.0') format('embedded-opentype'), url('//dyzz9obi78pm5.cloudfront.net/css/font-awesome-4.7.0/fonts/fontawesome-webfont.woff2?v=4.7.0') format('woff2'), url('//dyzz9obi78pm5.cloudfront.net/css/font-awesome-4.7.0/fonts/fontawesome-webfont.woff?v=4.7.0') format('woff'), url('//dyzz9obi78pm5.cloudfront.net/css/font-awesome-4.7.0/fonts/fontawesome-webfont.ttf?v=4.7.0') format('truetype'), url('//dyzz9obi78pm5.cloudfront.net/css/font-awesome-4.7.0/fonts/fontawesome-webfont.svg?v=4.7.0#fontawesomeregular') format('svg');font-weight:normal;font-style:normal}.fa{display:inline-block;font:no

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\jquery.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	92996
Entropy (8bit):	5.367795820022782
Encrypted:	false
SSDEEP:	1536:dT4r9sfd4PtunP/C1nGzg8d82pDos2JvrdXLvxj7z0tjNeGvHucaRsfcQaqOdVIS:1kGzg8ylGHkjr
MD5:	D72D040960D0CD6ABDF28AE022F1DE3D
SHA1:	D5339F5085091C053614137F81390BB5CBB3EB41
SHA-256:	54BC986C1297FEDA871DEFF1E37DBA0FD6545EA40491C1FAB05E28BBD7309322
SHA-512:	7D56B6064693853656EE5E5FF870F5907E6FDD3D9DCF26AB0FD42B4ED99588E96FCF6B360780E4A85E70BD17889C43A590E42C0CC1FEF98B21E32B12CCF6555
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dyzz9obi78pm5.cloudfront.net/js/libraries/jquery.min.js
Preview:	!function(a,b){function h(a){var c,d,b=g[a]={};for(a=a.split(/\s+/),c=0,d=a.length;c<d;c++)b[a[c]]=!0;return b}function l(a,c,d){if(d===b&&1===a.nodeType){var e="data-"+c.replace(k,"-$1").toLowerCase();if(d=a.getAttribute(e),"string"==typeof d){try{d="true"===d||"false"!==d&&("null"===d?null:f.isNumeric(d)?parseFloat(d):j.test(d)?f.parseJSON(d):d)}catch(a){}f.data(a,c,d)}else d=b}return d}function m(a){for(var b in a)if(("data"!==b||!f.isEmptyObject(a[b]))&&"toJSON"!==b)return!1;return!0}function n(a,b,c){var d=b+"defer",e=b+"queue",g=b+"mark",h=f._data(a,d);!h||"queue"!==c&&f._data(a,e)||"mark"!==c&&f._data(a,g)||setTimeout(function(){f._data(a,e)||f._data(a,g)||(f.removeData(a,d,!0),h.fire())},0)}function J(){return!1}function K(){return!0}function S(a){return!a||!a.parentNode||11===a.parentNode.nodeType}function T(a,b,c){if(b=b||0,f.isFunction(b))return f.grep(a,function(a,d){var e=!!b.call(a,d,a);return e===c});if(b.nodeType)return f.grep(a,function(a,d){return a===b===c});if("stri

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\lato-black[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Lato Black family
Category:	downloaded
Size (bytes):	30838
Entropy (8bit):	7.975436222063131
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\lato-black[1].eot	
SSDEEP:	768:JI+ICM2LqTTGQfKnsgmz1DUh73Y/VgYQm3q/qjB:JGB2k49mz1DUh7OgYQmcQB
MD5:	5407DE996A439DD4470D0A1E98ECD396
SHA1:	4C4F74BFD9C499AE6FF7E5BA3CC13A9C3F2C22DD
SHA-256:	D572501EFAA6AFF46941C17D10C9A8B2F8A2ECA3E33E7EF0C4C49D73E41FD206
SHA-512:	1B9136638AE5A9236E6C807A81DB08B0B7ACC7D97A7FDAC5A67712D4AD4090BD47E07F4EF449922F974C9FBC31E2808C2D05DB8E31287E06F5901BF6C90CA8A2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://app.knowledgeowl.com/flatui/fonts/lato/lato-black.eot?
Preview:	vx..hw.....LP....K`.P..... ....\.\.....L.a.t.o. .B.l.a.c.k.....R.e.g.u.l.a.r...P.V.e.r.s.i.o.n. .1...1.0.4.;. .W.e.s.t.e.r.n.+.P.o.l.i.s.h. .o.p.e.n.s.o.u.r.c.e...$. L.a.t.o. .B.l.a.c.k. .R.e.g.u.l.a.r.....BSGP.....(.N..N..J.....xZg.icyR..&c..4o4F..w....[.yM...R.Y.._.Y.ulb.&*...O.....%(...I.:[*i.b/g...2.4....F3..q..T.\.....<g.!.|....92C2$....`..tj...P.....8:t.....X?<...t@d...`))....lT.Ct..dX.u-..$..C....NXj..Y..%Jk\l.. .....]...~B.`.....q6...5Qsr..^.:....~..Q...~3..5..3.0.$.*th*...hDI%vF.*....'...;.0...H.9.....Z+(.l.$X.q..~d$.(q:/u...H.....&oA..Ef....u..".c.a...9.....bi.O...KN.y.(.v.7b.)(.....M.Y(=_...V.P.....d.hP.SV@{x.....[...../.%.A..ry....I.<.a@....G9..=...p{P.....a...Vg.d.$N..!T..!..H.y..dl..W.oI....Q]3-..Y.{ .bD4..X..A;.R..E.....31..$.5..4i.n...B.O.gO.....uE.=Rj.T..(.U..).8.-.....kl.A.A..M..a..#....{...(..K.n.PE"..C..z .@.oc...4.u'i;..i.@W.....tzGi..+..+.*3.....6.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\lato-bold[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Lato family
Category:	downloaded
Size (bytes):	32056
Entropy (8bit):	7.970959360968234
Encrypted:	false
SSDEEP:	768:KRC8eq4QSKzT7UhLsdI/40JS+CB4m+Yonj1PZsamBZk:csq4yT7sLgM4cmbonYbBZk
MD5:	2D4919CE2E98D98674657605CEEF758B
SHA1:	3A74EA081B6A622B43164D4C43AF7D78FAA1C52B
SHA-256:	3A18A112543C04AD0AD5C0365F4B535A5D6CEAD1C720D88595729A33FAAA12C1
SHA-512:	197AB63EFB512161B915AAA0F703439F78082A6009C0BA7B509CAFAD8DAE29DC27B6501889385AD28C46A4CA6FA75690C2AE67F6D0B09DF1F667304F821264E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://app.knowledgeowl.com/flatui/fonts/lato/lato-bold.eot?
Preview:	8}..N|.....LP....K`.P..... ....L.a.t.o.....B.o.l.d...P.V.e.r.s.i.o.n. .1...1.0.4.;. .W.e.s.t.e.r.n.+.P.o.l.i.s.h. .o.p.e.n.s.o.u.r.c.e.....L.a.t.o. .B.o.l.d. ....BSGP.....d.Q..Q..L2....xZg.icyR..&c..4o4F..w....[.yM...R.Y.P..1.V.0...'..@..9j.J8..T.fN..y...q.3-.&.L...&3..q..F.Q.E...j...&.\.(-.;o...G..P.X..]Ow..!.....v..K.$"....@x.=.d. 7..S..2D..M;..f.r..x..X.^../BP.c..L+.O-....T.x...k....'t.....8.....W....NQ.E..K..V1...M...,?....14#.<y....x>0B>.....g^.....S....X[X6Y....N...oQ..'.. .....~.q..:3N.n[|.#.3.. #.T.....|...-.in^..-T. .a.....F.t..da.....d:...~...d.RT.d>7....\b.%.~.:.....2,c$.....L4w.;.....s...k.Nd.6..n-(....]...$..1./.F..>^....%a3`..F...Z.....2.rm$..0...s..6.n.yP.Sh..<m.CQCmCQ@.%6Jl.. n@/@. .ap..../.K.....f.....v..K>..J\.....-~.O...s....W.....I._Sz..X....i..M._[z..=...v.L;b;.j...R6.e@3."v0.{.%..E..9L.g./..DN/z./`..."uSL.....:.+RH...*.WX...o.....o.}D..%.._.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\lato-bolditalic[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Lato family
Category:	downloaded
Size (bytes):	30340
Entropy (8bit):	7.974632118478816
Encrypted:	false
SSDEEP:	768:GbJCUSQ4+z/6/H1wfjT/EjqlvMyuCKQauBYSzV:aJpzS/C/skACKQVBtzV
MD5:	8A6AF3182A48E9E713931C04E6C656E8
SHA1:	1D7EF4A285A6B3E4D942E25FB05718357D26B532
SHA-256:	F63842BB377D0345DA11E322928CB4D363F138AFAEF944BBCB31439A32E255EE
SHA-512:	64A0D9947E52ABF71AC71A092335370A533F6D180E524875EDFAAFDE64CE1D0639A8BB0BB7CE6B9DE2624F2A67D1BC142BC01FC5DDE69BAD46A93F897A8ECB7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://app.knowledgeowl.com/flatui/fonts/lato/lato-bolditalic.eot?
Preview:	.v..~u.....LP....K`.P..... .....W.....L.a.t.o.....B.o.l.d. .l.t.a.l.i.c...P.V.e.r.s.i.o.n. .1...1.0.4.;. .W.e.s.t.e.r.n.+.P.o.l.i.s.h. .o.p.e.n.s.o.u.r.c.e... .L.a.t.o. .B.o.l.d. .l.t.a.l.i.c.....BSGP.....V..e..D.....xZg.icyR..&c..4o4F..w....[.....H..Z...[.....V...,.....%(.6z.12t.T...o..j.o96.%.6..{n;>.o..z.l....nz..V..{.'U8e...7B..".{....Z.....f..J.$(g ..v..kC..Bh...h[X....2w..'.3H....-y%.J..}.m9c..d.E.O.c.....).P.8.....Y..8J.It.."7...1.9D.).\..c..]...y.."..?.?t...g5.0..Y/..%.....:=.N3N.p....]&t..Q...../.ja.p.....1..!.*.0&]....N.{?...H...@.... ..+..&N..&..;.....&.L.wc.FQ....cRm./+..9.fq9..... .?.(82s..h.....K...5.B..$....u7#\.R.I..=.A..~.Hu....S..y.....!...E.z...%...@...A.5.3.. ..?.o(.Sl..Ar.....N...c...m.I.|L_..0T.T?....:.*..\. ?....f..\qy..|g...Y.7..=....x.G..J..>....ST..e.K.mS.U;3..U..d..*..X<..)..A.4..IPi....Qh2%}+.YCl.-...[.D...t5.....%y....=.W..k.2fF9.f.....}6D=.l.e.5.^

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\lato-italic[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Lato family
Category:	downloaded
Size (bytes):	29887
Entropy (8bit):	7.9706763780696415
Encrypted:	false
SSDEEP:	768:XKpZhP5zYzEOjLJKDjpa7sz+s7dLViGWPDMKbvMr:aJhzhKL+a7ij1ViGWPDMKDMr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\lato-italic[1].eot	
MD5:	CCE53FC2EB9E68832563771801E3B84B
SHA1:	68DA735AB36101777F8C0F03AB257A5AF4EB3A32
SHA-256:	642B31507C814CEC165C55FFC37F06AF12502BAB0BD4377EA1D8FA67CA6DAC7B
SHA-512:	D34B207EC5104EE0C8CA58A69DD4426AD0C42931CF7B4A0E0F4732A9DE1E80CEC20D60C164D474275612539C9B5A85B101978B15D4D77048010D5E6BE238E86
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://app.knowledgeowl.com/flatui/fonts/lato/lato-italic.eot?
Preview:	.t...s.....LP....K`.P..... ....q(.R.....L.a.t.o.....l.t.a.l.i.c...P.V.e.r.s.i.o.n. .1...1.0.4.;. .W.e.s.t.e.r.n.+.P.o.l.i.s.h. .o.p.e.n.s.o.u.r.c.e.....L.a.t.o. .l.t.a.l.i.c... ..BSGP.....V/.e..D.....xZg.icyR..&c..4o4F..w....[.....H..Z...[.....V...,.....%(.6z.12t.T...o....o96.%.....'.9&.z..{9..Z....^!..T.....{....X1.1.`qy.....;.v.N...\^yi`.....k.... m.....XL.".%....C...,....c..Y.C.....*.g?y%.?1b.hI..Y...`..<..1.9B....D....m.3.....6.ax=..K.t...6e`R.....1../V.r.....{.....4t .D...2ep..U.....;.f.B].j@L...a.}..S^,..1..@....9..&.....Z. H.>.1.6=.J..@.....5&..y...8..3....j1j.R...@9.u....!.4i%;K...).....cy...uc..].3.gd,.8r.....q.8.n.>.5.....7.....d..L.....7..3T.).PD.F..%_..%...x=...i..,s...G...3..3.bf....,9....u.}..~.. [..W....o.....7-..Fj7Q.....HjGRZ...jWR.%..N..f"jW.=Xi=.Q.O.$..?.ZY[...,f.\....e|.I...zIN,..|.....9.O!V$.....y....m....@gZ..}.....}.,.GM$.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\lato-light[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Lato Light family
Category:	downloaded
Size (bytes):	30116
Entropy (8bit):	7.968862266911759
Encrypted:	false
SSDEEP:	768:vPnXD+nR1D2r6swU/U3poNB4ExlKBcF/UcEe/kxsV:HnXDYN2rq5W4vWVRd
MD5:	1B75C6E45BFC6D5659B119723A95FB0C
SHA1:	DE33FE3EDF02B9A283840D832DBD7CA6EC751746
SHA-256:	6EABBF263F4E5F08EC1046F174EA06598B573D807320C2B833987F84F3047518
SHA-512:	BA0FF395E982154CA3C477B2947AD4B018961E6EBE427C459C04058CBF636EBEC62FCB78216AAC59A2685F63B5215A299FC41AB491D42CEAFC504134FE45922
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://app.knowledgeowl.com/flatui/fonts/lato/lato-light.eot?
Preview:	.u...t.....,.....LP....K`.P..... .....R.....L.a.t.o. .L.i.g.h.t.....R.e.g.u.l.a.r...P.V.e.r.s.i.o.n. .1...1.0.4.;. .W.e.s.t.e.r.n.+.P.o.l.i.s.h. .o.p.e.n.s.o.u.r.c.e...$.L.a.t.o. .L.i.g.h.t. .R.e.g.u.l.a.r.....BSGP.....Mh.Mn.I.....xZg.icyR..&c..4o4F..w....[.yM...R.Y.._.Y.ulb.&*...O.....%(...I.:[*i.b/g..d.o.m.^.....*b.K.{...e.3.+..3$.H..l.[".8a..i. ...P.....8:.|d...=...y.h+.)q.Ab.....+[$p..).....>...|T..V.....G.....t.....'.(A.!p.H.).1XG..(...v..v..y.Daxh.....hn(.....+R.R..A.[..dc.....D..+.8...^..\...e.....AC...../8..0T...,Z?.P0 .&R....k|.....;..fh3n...!E.....p.....x*3....[..}.\..#..9t..M_..x..U I...69D..+...-I.p.")9..Y~I.....r2D.....%.'....i.'.03.%1Zc.p.r.K6..=....f...`..0.....<....9.6..#...".M.X.*0U..*VW,.^.a.C...R..g]Il...X...I'.....b..a..)..yV.....[....D...&_3y..2(...&...._..g_.....}As@.C./Q.T...>.5S..Xc..5sv...../.K...q...G...,..ia.#..6=pU^.<Z.H..=aA.....}[i.;.....Q...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\lato-regular[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Lato family
Category:	downloaded
Size (bytes):	30978
Entropy (8bit):	7.973346592876513
Encrypted:	false
SSDEEP:	768:9PzdPeTK3cKyn6o9nrnEN1Bobqk2tdxOxei8vug1:9bdPeTK3cvn99TE2ItdaeTv3
MD5:	77F286E48A458105B9DEB4433D0844D9
SHA1:	7CC6733853B2A7F917824B68FDDBED2A735E0828
SHA-256:	DFE79473D1A937DFDEE1EF16C453B7C52FDE7E35ECC37798EFE80710A091D6F0
SHA-512:	4D653943CA53D734BFD36B27CE5E3D6A75453D91DBB346711D30148D576A6FB850FAD11D87E9A3BC1FF23AD244E33E4CC68B1671AEDFA7F458B18AB7EBC1D 49
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://app.knowledgeowl.com/flatui/fonts/lato/lato-regular.eot?
Preview:	.y...x.....LP....K`.P..... .....K.6.....L.a.t.o.....R.e.g.u.l.a.r...P.V.e.r.s.i.o.n. .1...1.0.4.;. .W.e.s.t.e.r.n.+.P.o.l.i.s.h. .o.p.e.n.s.o.u.r.c.e.....L.a.t.o. .R. e.g.u.l.a.r.....BSGP.....N:.N@.I.....xZg.icyR..&c..4o4F..w....[.yM...R.Y.._.Y.ulb.&*...O.....%(...I.:[*i.b/g..O2.4...sF3..q..T.....!.Pr7..wbG..3b=I..`..r...t..P.....8.....{q:.. M...>.Q.c.&..-[..bJ...Tx...R!R..%..=.z..r.P.2.|..[.f.?.....y.....91Bm...`$....;.P...d.Z...')C.`.YE.....U....7%p4{.3..h\Y%.../#..../.....1..&].A.....(.\.h.....n..'.Y,.(D..yq&k.....`.Vn H1)..a..2H.~H.....zKH.....i./"E.....="..Z..g&$...;,.=BS8.2_.....9.0.k..p.....l.&.T.$`H#.-..>.U..g...v.X;....7l].`/.D.....s....4.....z.9..e...X.e.KT.$SD..7.A$.HZ.q .A..$.V...g.mjax..WO..#. q.....q...:s...Z...,.4.q0|.....Y....?..Zq..:i....O.Z...?.T:....5K.mS...]._+.u.....i>..K.. .s%.sd....)1.#..RU2s.+.F!...%...c.j...h9.f..K<...N....4....+.....($....+.8.4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\nr-1198.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	28120
Entropy (8bit):	5.31469238173269
Encrypted:	false
SSDEEP:	384:yZevj5awnX8RfzD7WdPs8tzmwUyAH77jx+zJTREUi2bikgHIvYboLLAJ1fFKohtJ:yZUQKi8tzA76AFIAbo/M1jtnWE5
MD5:	59C98195BA35E0B45CBE2E5BEEBD1AC8
SHA1:	BB1DD82667456B0B608750BBF8D2871A018535B0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\nr-1198.min[1].js	
SHA-256:	39893061747F88B837A34D0395D05FCA83E7CD5BBF2D582D181A73C5C9A174C6
SHA-512:	9CCE07757B9475D6A3C20CAD19A4775422EED4AE018F27521D4EF29FB89C5B5CEFB3991A6CDD3E422B532C32D43699A5EE86F61FD7FEA9FCDB90F2670A40E762
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://js-agent.newrelic.com/nr-1198.min.js
Preview:	!function(n,e,t){function r(t,i){if(!e[t]){if(!n[t]){var a="function"==typeof __nr_require&&__nr_require;if(!i&&a)return a(t,!0);if(o)return o(t,!0);throw new Error("Cannot find module '"+t+"'")}var u=e[t]={exports:{}};n[t][0].call(u.exports,function(e){var o=n[t][1][e];return r(o||e)},u,u.exports)}return e[t].exports}for(var o="function"==typeof __nr_require&&__nr_require,i=0;i<t.length;i++)r(t[i]);return r}({1:[function(n,e,t){e.exports=function(n,e){return"addEventListener"in window?window.addEventListener(n,e,!1):"attachEvent"in window?window.attachEvent("on"+n,e):void 0}},{}],2:[function(n,e,t){function r(n,e,t,r,i){|[n]||(|[n]={});var a=|[n][e];return a||(a=|[n][e]={params:t||{}},i&&(a.custom=i),a.metrics=o(r,a.metrics),a}function o(n,e){return e||(e={count:0}),e.count+=1,f(n,function(n,t){e[n]=i(t,e[n])}),e}function i(n,e){return e?(e&&!e.c&&(e={t:e.t,min:e.t,max:e.t,sos:e.t*e.t,c:1}),e.c+=1,e.t+=n,e.sos+=n*n,n>e.max&&(e.max=n),n<e.min&&(e.min=n),e):{t:n}}function a(n,e){return

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\S6uyw4BMUTPHjx4wWA[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 28660, version 1.1
Category:	downloaded
Size (bytes):	28660
Entropy (8bit):	7.986798426962959
Encrypted:	false
SSDEEP:	768:Rr8uuUMtVCqVsUnrZAT9vaxw9pi95vSVc+Dfpy:R9uZV9VnndAJvaCGPvwDhy
MD5:	B8EE546ACD6CC0C49F42AD3D48EF244F
SHA1:	7D8BFF4143A36AA9CC1C2801F60FA0E99969E3F6
SHA-256:	04050BAE4CC3B9CCD20D3C7F57F5B1BA249D4A54D6EFF75A1E4DF504362E8C00
SHA-512:	700D04F4CAF24A20919C2136DD3700BBE07F509F5BD0045084063B78EA8B6FD72BFEA6BBF2A94A5865A75CD6C7197DAB500B809122AA5A3910F46E1D9816D00
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/lato/v17/S6uyw4BMUTPHjx4wWA.woff
Preview:	wOFF.....o.....l.....GPOS...l.....z....GSUB...<...S...p.:.|OS/2.....Z...`y$aycmap.....cvt ...x...+.....fpgm.....rZr@gasp...$.....glyf...0..YY...H@ ...head..h....6...6...#hhea..h.....$...whmtx..h.....v}.O7loca..j.....9maxp..l.... ... ....name..l....8....:.TApost..n.....EW..xprep..o....K...K....x.T..l Q.EO....m.m.m;X...Fl..? us..p.$z3.....G.f.N...`Yv...p.a.N.*."b.3...]p..`...l,.5...]=.%U..D...]v?.xX.w...;.w>.....mt?....+.....]..G.>]:(.JO.+.J.R.=.k.....@9.+.....:(.UP.k.bZ...B..a....U....6\..Q.10....H'...../.....1. !.e....HF1..Lf...l.0.y,`.KY.rV....b7{....p...,.8...r.+..>.x.#....%.x.[...|.....7.._.....$.H..&.X.'.D.I!.^xX...=.....{XC.hySQy....p...n)..h..M.(..f)"..)..j...L.qw..R`).E..8..1*.X..7...\..9(q(. .32.PJ)K).....#)|(.X...{.....7.g..\s.:..7dL...K.>..0H.!.Y.v.U.Xg...m.-..a.=.:...<!..c.9~....?B...w...-..|(.>..TQM...X..5...G.J..P.\..=4.H31Z....q.j.6.....v.#..z.G..e.q

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\analytics[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with no line terminators
Category:	downloaded
Size (bytes):	72
Entropy (8bit):	4.098434282903269
Encrypted:	false
SSDEEP:	3:hGQRALjCjETEIuJ9QREi2KNVKVMmRcn:hCvTGWl2KNVKHKn
MD5:	5090AC56E33ACAFB87EF9885B07AD758
SHA1:	3323A659231A1C5E6D0E2B7D94443C8393CC91D7
SHA-256:	D5ED0D3BB98AE16AD90BE29DB3BECF6153A1390B922506A19CCCF2400BBDB1C1
SHA-512:	9D2DB73DC3A5332832942FADB5F4B5BFEE57CB6BC9B62E9D2C177E2CB398C71D0F39A67DD869DF731B17E15D771AC0675F6C083DCDDE077B5E6BF1F893138AA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pi.pardot.com/analytics?ver=3&visitor_id=&visitor_id_sign=&pi_opt_in=&campaign_id=39444&account_id=78672&title=FormAssembly%20%7C%20FormAssembly%20Resource%20Center&url=https%3A%2F%2Fhelp.formassembly.com%2Fhelp&referrer=
Preview:	This content isn.t available. Contact the owner of this site for help.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\c33294f5df[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	24
Entropy (8bit):	2.459147917027245
Encrypted:	false
SSDEEP:	3:CUXJ/lH:Dl
MD5:	BC32ED98D624ACB4008F986349A20D26
SHA1:	2D3DF8C11D2168CE2C27E0937421D11D85016361
SHA-256:	0C9CF152A0AD00D4F102C93C613C104914BE5517AC8F8E0831727F8BFBE8B300

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\c33294f5df[1].gif	
SHA-512:	71ACC6DA78D5D5BF0EEA30E2EE0AC5C992B00EFEC959077DFE0AB769F1DBBD9AF12D5C5C155046283D5416BEB606A9EF323FB410E903768B1569B69F37075B4E
Malicious:	false
Reputation:	low
Preview:	GIF89a.....,.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\c33294f5df[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.340020120659463
Encrypted:	false
SSDEEP:	3:U3KTDW3MiqVkMWVrfUh:H6NukMWVr8h
MD5:	06DD80AEB628C60DC680BC7A4BEE6651
SHA1:	8C86EB7DDFF5E1E5D527BD7A41C9D3F6767E23E0
SHA-256:	5E864C2E3F674C60970513411EAEEEAFD2D615D842E65EC01D09CCFCB4A7B38D
SHA-512:	C6EE8252743A760AD7BEE017FF7A804B6E34236764BC5630289D5E4C7C15E38CB971F161821586F0235882FD581630F1531FD6396761BF1284581CD8C2CAC4C6
Malicious:	false
Reputation:	low
Preview:	NREUM.setToken({'stn':0,'err':1,'ins':1,'cap':0,'spa':1})

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\iframe_message_helper_internal[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	19914
Entropy (8bit):	4.836036794825976
Encrypted:	false
SSDEEP:	384:CsZ97WRJzbfbjm/7jSWlrfgNhjI5LD05fdpiOXfcvrnhAs:CsZ9IJPfbEro7IJgV/0vrnhAs
MD5:	2487F6102C216F30BAE1C6F30719AA4E
SHA1:	219F04E9D52126BAF4019155A37704A2506A106D
SHA-256:	3F43A10CC040E064D28E2200C192C162A48C22ECB10BA69EFAE5F628DD0EFDE4
SHA-512:	739327B161811EFD18ED0AA9A693770E0C788B8307F75BAD728BCE63D4FA43D7FE2614F893ED40EC196683AA63F2D3CEB7EB66AD646D95C76FBB57E788E63FD
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.tfaforms.com/js/iframe_message_helper_internal.js?v=2
Preview:	/**. * This script must be included in a FormAssembly form.. * When loaded in an IFRAME, it will continuously send its updated. * height so that the container can adjust IFRAME height to match. * it content's height.. *. * The posting is done through a cross-domain message mechanism.. * simpleStorage js library is also used (included mini fied below) -. * it is needed to store data between page reloads in the IFRAME.. *. * The message sent in the following format:. * h,iframeID,targetUrl. *. * - h: either new height in pixels or a command like "submitted";. * the message receiver in the parent window will handle it accordingly.. * - iframeID: the unique iframe ID for which the message must be applied,. * in other words it is the IFRAME running this script;. * - targetURL: the fallback solution if no iframeID is available;. * indicates the value of IFRAME's "src" attribute to identify. * the IFRAME. Identifying IFRAME by targetURL will not work after. * form resubmission as the

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\recaptcha__en[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	339250
Entropy (8bit):	5.72235648390319
Encrypted:	false
SSDEEP:	6144:2LgyvcysILY+3SqzE30QvvbuzLRp/epQx2g9tlxGdPLy:2LQ6HWEAbyRopQx9IC+
MD5:	32C49DC5F9FA12F530A84CD51D5E274A
SHA1:	89C75509FB3E3807679E55B57A4C0569A4B8EDD8
SHA-256:	46C97699759B3239F2306F7D09DF96131FB1044315B07CFDD62B66C2E4C0125B
SHA-512:	7388DB3DF5DDC98C633E0037020672366D5DD0F078206EE9A2412A90C9EBC9806CB43131A0C947A71E97FAD1F3EF6460FD1AC28991797E1EA2665B576500168
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/recaptcha/releases/jxFQ7RQ9s9HTGKeWcoa6UQdD/recaptcha__en.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\recaptcha__en[1].js

Preview:

```
(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var F=function(){return[function(B,G,Z,I,W,l,d,N){if(!(B+(N=[2,11,13],N)[0
]&N[2]))a:{for(I=(Z=L[32](N[1],!1,G(),g[N[0]].bind(null,32)),0);I<Z.length;I++)if(Z[I].src&&M[16](N[0]).test(Z[I].src)){d=I;break a}d=-1}return(B^644)%((B<<1&((B-6)%5||Z.Y||
(Z.Y=new IA,Z.Z=0,Z.S&&L[3](3,null,1,"&","=",function(S,x){Z.add(decodeURIComponent(S.replace(/\+/g,G)),x)},Z.S)),15))==N[0]&&(G.Y=I,d={value:Z}),9)||(k.call(this),thi
s.C=l8[Z]||l8[1],this.o=I,this.S=I,this.W=G,this.Y=W),d},function(B,G,Z,I,W,l){return(B|.((B-9)%2||(l=dR(Z.W,function(d){return"function"===typeof d[G]})),8))&7||(I==G?Z.
I.call(Z.S,W):Z.Z&&Z.Z.call(Z.S,W)),l},function(B,G,Z,I,W,l,d,N,S){if(!((B^(N=[19,3,10],349))%N[0])){if(I==Z)throw Error("Unable to set parent component");if(l=Z&&I.I&&I.
uZ)W=I.I,d=I.uZ,l=W.K&&d?w[47](N[1],d,W.K)||G:null;if(l&&I.I!=Z)throw Error("Unable to set parent component");(I.I=Z,k.O).Hm.call(I,Z)}if(!((B>>2)%11)
```

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\slideout.min[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	7498
Entropy (8bit):	5.0622345652577
Encrypted:	false
SSDEEP:	192:d0Nfp4xKoXGJzb3mj3jWMxjcMjwx9nTZIdl3EOvY0zGr:mNfpIXGZ3S8x9TZI7Ex0K
MD5:	5EAA0D1BEFD974B5B2188B52A9E5318C
SHA1:	A89CB7085989D9D127F12748721E03D2C4CE5D56
SHA-256:	D42CCAA3D862E908AD8059D0504F077FB9313F3A7FDAAB6930EF382A71D73422
SHA-512:	2C8F2582FB51BE07E7B739BA8A0F86344F5525738F7EF523D853277AA44E6565B6FD453A1FDFF6B1261DA9A71E2A2BC475E054E280A3843EEA2BB5E79B711494
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dyzz9obi78pm5.cloudfront.net/js/slideout.min.js

Preview:

```
!function(t){if("object"==typeof exports&&"undefined"!=typeof module)module.exports=t();else if("function"==typeof define&&define.amd)define([],t);else{var e;"undefined"!
=typeof window?e=window:"undefined"!=typeof global?e=global:"undefined"!=typeof self&&(e=self),e.Slideout=t()}}(function(){return function s(r,a,l){function u(n,t){if(!a[n])
{if(!r[n]){var e="function"==typeof require&&require;if(!t&&e)return e(n,!0);if(h)return h(n,!0);var i=new Error("Cannot find module '"+n+"'");throw i.code="MODULE_NOT
_FOUND",i}var o=a[n]={exports:{}};r[n][0].call(o.exports,function(t){var e=r[n][1][t];return u(e||t)},o,o.exports,s,r,a,l)}return a[n].exports}for(var h="function"==typeof require&
&require,t=0;t<l.length;t++)u(l[t]);return u}({1:[function(t,e,n){"use strict";var i,o,s,r=t("decouple"),a=t("emitter"),l=!1,u=window.document,h=u.documentElement,c=windo
w.navigator.msPointerEnabled,p={start:c?"MSPointerDown":"touchstart",move:c?"MSPointerMove":"touchmove",end:c?"MSPointerUp":"touchend"},d=fu
```

C:\Users\user\AppData\Local\Temp\~DF049D6DF724C2332B.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4805429850200503
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lol9loF9lWyl5DiO:kBqoIOwy3Dj
MD5:	BE9BAAB6F57ACB9443FF68E274A2CF0D
SHA1:	636915D391C71B692A1B9764D3BE0D0D30B925C0
SHA-256:	EA0AE2F045E532FF6970148AE95608F9A40E4A61E2082850C016C8EA3C085542
SHA-512:	0DB2B85DE2056ACECC0CF455C369B2AB2515F26B4ACA88DBD64058FC2D9B8B707CF5F554AC389399BF4E8FE271CD84E41D66464C73CE5661B6C7B7C511085E 30
Malicious:	false
Reputation:	low

Preview:

```
............................*%..H..M..{y..+.0...(.................. ..............................................*%..H..M..{y..+.0...(.................. ..........................................................................................
.........................................................................................................................................................................................................................
.........................................................................................................................................................................................................................
.................................................................................................................................................................................
```

C:\Users\user\AppData\Local\Temp\~DF48068F2185627C41.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	44777
Entropy (8bit):	0.5727327886556867
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+V75or/0RD49OSc3jrRqj:kBqoxKAuqR+V75or/0RD49OSc3HRq
MD5:	C3BF47D12E2DC3DDBFA316093C3E426C
SHA1:	D86257D1D0B253C0D1369397378EAECDFB304E7A
SHA-256:	C53375DB680FD405C18F823C3411D47BC6BF24AE86B48ACB15B949C3AEEB4831
SHA-512:	D494C08532165CF96F9E5C492145A9FC8E13D7AC22F8E9300C76D0275DFF37E4B2209F7E41792659CABFF966E67387BCFA21E58460064C8574A4F148C03A19B7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DF48068F2185627C41.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF6DEBFC0F3597EB51.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.4356386577583772
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAvj:kBqoxxJhHWSVSEabv
MD5:	5957EC2EA352A8C408047A47D41A938E
SHA1:	B77922F75DA7E383C3F74421B0A1073638505B24
SHA-256:	55D4A902DC89B0C8E380E57796B6D00103BF0419F0535CA894FDF087E27252AF
SHA-512:	50DE7D48EAF0F6A49303F75679B2E08B46F874D830FA6AB041A000D579D5441174C2322CF5F2A05DB35201CB0AD4FC5D79E764ABB4AF9968DC68FE49A93822B
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: 91

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:53:48.135471106 CET	49715	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.136902094 CET	49714	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.265638113 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.265775919 CET	49715	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.266498089 CET	49715	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.267066002 CET	80	49714	3.226.66.230	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:53:48.267165899 CET	49714	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.393596888 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.552665949 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.552726030 CET	49715	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.552741051 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.552773952 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.552783966 CET	49715	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.552808046 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.552818060 CET	49715	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.552846909 CET	49715	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.552846909 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.552861929 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.552882910 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.552908897 CET	49715	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.552912951 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.552941084 CET	49715	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.552967072 CET	49715	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.552974939 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.553011894 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.553014040 CET	49715	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.553047895 CET	49715	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.680006981 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.680032969 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.680049896 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.680066109 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.680082083 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.680099964 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.680118084 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.680134058 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.680150986 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.680167913 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.680170059 CET	49715	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.680183887 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.680196047 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.680198908 CET	49715	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.680264950 CET	49715	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.697365046 CET	49715	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.698326111 CET	49714	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.698908091 CET	49717	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.825715065 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.826980114 CET	80	49714	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.827569962 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.827616930 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.827656984 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.827662945 CET	49715	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.827693939 CET	49715	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.827694893 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.827699900 CET	49715	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.827733040 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.827743053 CET	49715	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.827771902 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.827785969 CET	49715	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.827811956 CET	80	49717	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.827821016 CET	49715	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.827882051 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.827893019 CET	49717	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.827917099 CET	80	49715	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.827934027 CET	49715	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.827965975 CET	49715	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.828516960 CET	49717	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.829545021 CET	80	49714	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.829587936 CET	80	49714	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.829634905 CET	80	49714	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.829654932 CET	49714	80	192.168.2.5	3.226.66.230

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:53:48.829678059 CET	80	49714	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.829689026 CET	49714	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.829694986 CET	49714	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.829715967 CET	80	49714	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.829732895 CET	49714	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.829755068 CET	80	49714	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.829794884 CET	80	49714	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.829813004 CET	49714	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.829819918 CET	49714	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.829834938 CET	80	49714	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.829874039 CET	80	49714	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.829895973 CET	49714	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.829901934 CET	49714	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.829911947 CET	80	49714	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.829971075 CET	49714	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.829982996 CET	49714	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.846951008 CET	49715	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.955929995 CET	80	49717	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.957109928 CET	80	49714	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.957153082 CET	80	49714	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.957200050 CET	80	49714	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.957231045 CET	49714	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.957242966 CET	80	49714	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.957257032 CET	49714	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.957262993 CET	49714	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.957283020 CET	80	49714	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.957315922 CET	49714	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.957321882 CET	80	49714	3.226.66.230	192.168.2.5
Feb 25, 2021 21:53:48.957331896 CET	49714	80	192.168.2.5	3.226.66.230
Feb 25, 2021 21:53:48.957360983 CET	80	49714	3.226.66.230	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:53:39.699780941 CET	54302	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:53:39.748326063 CET	53	54302	8.8.8.8	192.168.2.5
Feb 25, 2021 21:53:40.098433018 CET	53784	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:53:40.128937960 CET	65307	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:53:40.148503065 CET	53	53784	8.8.8.8	192.168.2.5
Feb 25, 2021 21:53:40.180955887 CET	53	65307	8.8.8.8	192.168.2.5
Feb 25, 2021 21:53:40.259001017 CET	64344	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:53:40.266726017 CET	62060	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:53:40.309478045 CET	53	64344	8.8.8.8	192.168.2.5
Feb 25, 2021 21:53:40.318841934 CET	53	62060	8.8.8.8	192.168.2.5
Feb 25, 2021 21:53:40.434493065 CET	61805	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:53:40.482974052 CET	53	61805	8.8.8.8	192.168.2.5
Feb 25, 2021 21:53:40.635515928 CET	54795	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:53:40.684750080 CET	53	54795	8.8.8.8	192.168.2.5
Feb 25, 2021 21:53:42.072879076 CET	49557	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:53:42.130569935 CET	53	49557	8.8.8.8	192.168.2.5
Feb 25, 2021 21:53:42.860096931 CET	61733	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:53:42.910979033 CET	53	61733	8.8.8.8	192.168.2.5
Feb 25, 2021 21:53:43.167395115 CET	65447	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:53:43.911930084 CET	52441	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:53:43.966656923 CET	53	52441	8.8.8.8	192.168.2.5
Feb 25, 2021 21:53:44.169456959 CET	65447	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:53:44.229216099 CET	53	65447	8.8.8.8	192.168.2.5
Feb 25, 2021 21:53:44.813282013 CET	62176	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:53:44.866594076 CET	53	62176	8.8.8.8	192.168.2.5
Feb 25, 2021 21:53:45.859076023 CET	59596	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:53:45.907787085 CET	53	59596	8.8.8.8	192.168.2.5
Feb 25, 2021 21:53:46.905576944 CET	65296	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:53:46.964546919 CET	53	65296	8.8.8.8	192.168.2.5
Feb 25, 2021 21:53:47.187109947 CET	63183	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:53:47.245925903 CET	53	63183	8.8.8.8	192.168.2.5
Feb 25, 2021 21:53:48.063653946 CET	60151	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:53:48.126220942 CET	53	60151	8.8.8.8	192.168.2.5
Feb 25, 2021 21:53:48.370547056 CET	56969	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:53:48.419287920 CET	53	56969	8.8.8.8	192.168.2.5
Feb 25, 2021 21:53:49.332905054 CET	55161	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:53:49.381422043 CET	53	55161	8.8.8.8	192.168.2.5
Feb 25, 2021 21:53:49.764834881 CET	54757	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:53:49.813411951 CET	53	54757	8.8.8.8	192.168.2.5
Feb 25, 2021 21:53:50.351694107 CET	49992	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:53:50.401343107 CET	53	49992	8.8.8.8	192.168.2.5
Feb 25, 2021 21:53:51.560137987 CET	60075	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:53:51.610153913 CET	53	60075	8.8.8.8	192.168.2.5
Feb 25, 2021 21:54:04.577862024 CET	55016	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:54:04.637146950 CET	53	55016	8.8.8.8	192.168.2.5
Feb 25, 2021 21:54:08.276302099 CET	64345	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:54:08.349158049 CET	53	64345	8.8.8.8	192.168.2.5
Feb 25, 2021 21:54:08.482579947 CET	57128	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:54:08.542680025 CET	53	57128	8.8.8.8	192.168.2.5
Feb 25, 2021 21:54:09.128279924 CET	54791	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:54:09.135535002 CET	50463	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:54:09.148871899 CET	50394	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:54:09.185343027 CET	53	54791	8.8.8.8	192.168.2.5
Feb 25, 2021 21:54:09.200495005 CET	53	50463	8.8.8.8	192.168.2.5
Feb 25, 2021 21:54:09.210706949 CET	53	50394	8.8.8.8	192.168.2.5
Feb 25, 2021 21:54:10.070586920 CET	58530	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:54:10.079468012 CET	53813	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:54:10.087682962 CET	63732	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:54:10.106203079 CET	57344	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:54:10.127825022 CET	53	58530	8.8.8.8	192.168.2.5
Feb 25, 2021 21:54:10.138173103 CET	53	53813	8.8.8.8	192.168.2.5
Feb 25, 2021 21:54:10.138961077 CET	53	63732	8.8.8.8	192.168.2.5
Feb 25, 2021 21:54:10.171334028 CET	53	57344	8.8.8.8	192.168.2.5
Feb 25, 2021 21:54:11.320425987 CET	54450	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:54:11.326370001 CET	59261	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:54:11.375371933 CET	53	54450	8.8.8.8	192.168.2.5
Feb 25, 2021 21:54:11.377552032 CET	53	59261	8.8.8.8	192.168.2.5
Feb 25, 2021 21:54:17.039442062 CET	57151	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:54:17.092674017 CET	53	57151	8.8.8.8	192.168.2.5
Feb 25, 2021 21:54:17.634516954 CET	59413	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:54:17.687428951 CET	53	59413	8.8.8.8	192.168.2.5
Feb 25, 2021 21:54:18.326524019 CET	57151	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:54:18.381495953 CET	53	57151	8.8.8.8	192.168.2.5
Feb 25, 2021 21:54:18.639045954 CET	59413	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:54:18.699165106 CET	53	59413	8.8.8.8	192.168.2.5
Feb 25, 2021 21:54:20.119844913 CET	59413	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:54:20.140557051 CET	57151	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:54:20.174002886 CET	53	59413	8.8.8.8	192.168.2.5
Feb 25, 2021 21:54:20.192372084 CET	53	57151	8.8.8.8	192.168.2.5
Feb 25, 2021 21:54:22.132635117 CET	59413	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:54:22.148195982 CET	57151	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:54:22.186842918 CET	53	59413	8.8.8.8	192.168.2.5
Feb 25, 2021 21:54:22.196691036 CET	53	57151	8.8.8.8	192.168.2.5
Feb 25, 2021 21:54:26.148108006 CET	59413	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:54:26.148438931 CET	57151	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:54:26.197433949 CET	53	57151	8.8.8.8	192.168.2.5
Feb 25, 2021 21:54:26.199886084 CET	53	59413	8.8.8.8	192.168.2.5
Feb 25, 2021 21:54:27.197058916 CET	60516	53	192.168.2.5	8.8.8.8
Feb 25, 2021 21:54:27.248581886 CET	53	60516	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 21:53:48.063653946 CET	192.168.2.5	8.8.8.8	0xbc4c	Standard query (0)	www.tfaformms.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:53:49.332905054 CET	192.168.2.5	8.8.8.8	0x33da	Standard query (0)	js-agent.newrelic.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:53:49.764834881 CET	192.168.2.5	8.8.8.8	0xf117	Standard query (0)	bam-cell.nr-data.net	A (IP address)	IN (0x0001)
Feb 25, 2021 21:54:04.577862024 CET	192.168.2.5	8.8.8.8	0x3321	Standard query (0)	www.tfaformms.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:54:08.276302099 CET	192.168.2.5	8.8.8.8	0x3000	Standard query (0)	help.formassembly.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:54:09.128279924 CET	192.168.2.5	8.8.8.8	0x2b3a	Standard query (0)	dyzz9obi78pm5.cloudfront.net	A (IP address)	IN (0x0001)
Feb 25, 2021 21:54:10.079468012 CET	192.168.2.5	8.8.8.8	0x8e08	Standard query (0)	app.knowledgeowl.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:54:11.320425987 CET	192.168.2.5	8.8.8.8	0x9b96	Standard query (0)	www.formassembly.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:54:11.326370001 CET	192.168.2.5	8.8.8.8	0x51da	Standard query (0)	pi.pardot.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 21:53:48.126220942 CET	8.8.8.8	192.168.2.5	0xbc4c	No error (0)	www.tfaformms.com	app-elbapp-a6b1wbowxm9e-391051627.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:53:48.126220942 CET	8.8.8.8	192.168.2.5	0xbc4c	No error (0)	app-elbapp-a6b1wbowxm9e-391051627.us-east-1.elb.amazonaws.com		3.226.66.230	A (IP address)	IN (0x0001)
Feb 25, 2021 21:53:48.126220942 CET	8.8.8.8	192.168.2.5	0xbc4c	No error (0)	app-elbapp-a6b1wbowxm9e-391051627.us-east-1.elb.amazonaws.com		34.233.52.23	A (IP address)	IN (0x0001)
Feb 25, 2021 21:53:48.126220942 CET	8.8.8.8	192.168.2.5	0xbc4c	No error (0)	app-elbapp-a6b1wbowxm9e-391051627.us-east-1.elb.amazonaws.com		52.86.83.232	A (IP address)	IN (0x0001)
Feb 25, 2021 21:53:49.381422043 CET	8.8.8.8	192.168.2.5	0x33da	No error (0)	js-agent.newrelic.com	f4.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:53:49.813411951 CET	8.8.8.8	192.168.2.5	0xf117	No error (0)	bam-cell.nr-data.net	tls12.newrelic.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:54:04.637146950 CET	8.8.8.8	192.168.2.5	0x3321	No error (0)	www.tfaformms.com	app-elbapp-a6b1wbowxm9e-391051627.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:54:04.637146950 CET	8.8.8.8	192.168.2.5	0x3321	No error (0)	app-elbapp-a6b1wbowxm9e-391051627.us-east-1.elb.amazonaws.com		3.226.66.230	A (IP address)	IN (0x0001)
Feb 25, 2021 21:54:04.637146950 CET	8.8.8.8	192.168.2.5	0x3321	No error (0)	app-elbapp-a6b1wbowxm9e-391051627.us-east-1.elb.amazonaws.com		34.233.52.23	A (IP address)	IN (0x0001)
Feb 25, 2021 21:54:04.637146950 CET	8.8.8.8	192.168.2.5	0x3321	No error (0)	app-elbapp-a6b1wbowxm9e-391051627.us-east-1.elb.amazonaws.com		52.86.83.232	A (IP address)	IN (0x0001)
Feb 25, 2021 21:54:08.349158049 CET	8.8.8.8	192.168.2.5	0x3000	No error (0)	help.formassembly.com	formassembly.knowledgeowl.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:54:08.349158049 CET	8.8.8.8	192.168.2.5	0x3000	No error (0)	formassembly.knowledgeowl.com		54.152.202.195	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 21:54:09.185343027 CET	8.8.8.8	192.168.2.5	0x2b3a	No error (0)	dyzz9obi78pm5.cloudfront.net		13.224.89.142	A (IP address)	IN (0x0001)
Feb 25, 2021 21:54:09.185343027 CET	8.8.8.8	192.168.2.5	0x2b3a	No error (0)	dyzz9obi78pm5.cloudfront.net		13.224.89.117	A (IP address)	IN (0x0001)
Feb 25, 2021 21:54:09.185343027 CET	8.8.8.8	192.168.2.5	0x2b3a	No error (0)	dyzz9obi78pm5.cloudfront.net		13.224.89.211	A (IP address)	IN (0x0001)
Feb 25, 2021 21:54:09.185343027 CET	8.8.8.8	192.168.2.5	0x2b3a	No error (0)	dyzz9obi78pm5.cloudfront.net		13.224.89.143	A (IP address)	IN (0x0001)
Feb 25, 2021 21:54:10.138173103 CET	8.8.8.8	192.168.2.5	0x8e08	No error (0)	app.knowledgeowl.com		54.152.202.195	A (IP address)	IN (0x0001)
Feb 25, 2021 21:54:11.375371933 CET	8.8.8.8	192.168.2.5	0x9b96	No error (0)	www.formassembly.com	formassembly.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:54:11.375371933 CET	8.8.8.8	192.168.2.5	0x9b96	No error (0)	formassembly.com		104.196.12.68	A (IP address)	IN (0x0001)
Feb 25, 2021 21:54:11.377552032 CET	8.8.8.8	192.168.2.5	0x51da	No error (0)	pi.pardot.com	pi-ue1.pardot.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:54:11.377552032 CET	8.8.8.8	192.168.2.5	0x51da	No error (0)	pi-ue1.pardot.com	pi.t.pardot.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:54:11.377552032 CET	8.8.8.8	192.168.2.5	0x51da	No error (0)	pi.t.pardot.com	pi-ue1-lba3.pardot.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:54:11.377552032 CET	8.8.8.8	192.168.2.5	0x51da	No error (0)	pi-ue1-lba3.pardot.com		35.174.150.168	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.tfaforms.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49715	3.226.66.230	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 21:53:48.266498089 CET	888	OUT	GET /responses/processor HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www.tfaforms.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 21:53:48.552665949 CET	1084	IN	HTTP/1.1 400 Bad Request Date: Thu, 25 Feb 2021 20:53:48 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: AWSALB=G5teNT+mPnhY4FafeUdFCQ4qpE7NMCAv52/lB6FGm+nJ8CQskggT5uw7fUU2YPyZOopJ7hJ YfXTgmfwYtSLXzHuGXQFLqebmYZrsaIQDgKX/t5WSb1nhVUqL3YxL; Expires=Thu, 04 Mar 2021 20:53:48 GMT; Path=/ Set-Cookie: AWSALBCORS=G5teNT+mPnhY4FafeUdFCQ4qpE7NMCAv52/lB6FGm+nJ8CQskggT5uw7fUU2YPyZOop J7hJYfXTgmfwYtSLXzHuGXQFLqebmYZrsaIQDgKX/t5WSb1nhVUqL3YxL; Expires=Thu, 04 Mar 2021 20:53:48 GMT; Pa th=/; SameSite=None Server: nginx P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM" Set-Cookie: FORMASSEMBLY=5bc75b683de75add4a7696e2f018028f; HttpOnly=1; Path=/; SameSite=None; Secure Data Raw: 35 64 38 36 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 6d 41 73 73 65 6d 62 6c 79 2e 63 6f 6d 20 20 3a 20 45 72 72 6f 72 73 3c 2f 74 69 74 6c 65 3e 0a 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 20 2f 3e 0a 0a 20 20 20 20 0a 20 20 20 20 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2 f 6a 61 76 61 73 63 72 69 70 74 22 3e 28 77 69 6e 64 6f 77 2e 4e 52 45 55 4d 7c 7c 28 4e 52 45 55 4d 3d 7b 7d 29 29 2e 69 6e 69 74 3d 7b 70 72 69 76 61 63 79 3a 7b 63 6f 6f 6b 69 65 73 5f 65 6e 61 62 6c 65 64 3a 66 61 6c 73 65 7d 7d 3b 28 77 69 6e 64 6f 77 2e 4e 52 45 55 4d 7c 7c 28 4e 52 45 55 4d 3d 7b 7d 29 29 2e 6c 6f 61 64 65 72 5f 63 6f 6e 66 69 67 3d 7b 78 70 69 64 3a 22 56 51 41 4f 55 56 42 54 43 78 41 4a 56 46 46 55 44 67 63 46 56 41 3d 3d 22 2c 6c 69 63 65 6e 73 65 4b 65 79 3a 22 63 33 33 32 39 34 66 35 64 66 22 2c 61 70 70 6c 69 63 61 74 69 6f 6e 49 44 3a 22 39 30 30 36 39 36 32 32 22 7d 3b 77 69 6e 64 6f 77 2e 4e 52 45 55 4d 7c 7c 28 4e 52 45 55 4d 3d 7b 7d 29 2c 5f 5f 6e 72 5f 72 65 71 75 69 72 65 3d 66 75 6e 63 74 69 6f 6e 28 74 2c 65 2c 6e 29 7b 66 75 6e 63 74 69 6f 6e 20 72 28 6e 29 7b 69 66 28 21 65 5b 6e 5d 29 7b 76 61 72 20 69 3d 65 5b 6e 5d 3d 7b 65 78 70 6f 72 74 73 3a 7b 7d 7d 3b 74 5b 6e 5d 5b 30 5d 2e 63 61 6c 6c 28 69 2e 65 78 70 6f 72 74 73 2c 66 75 6e Data Ascii: 5d86<!DOCTYPE HTML><html lang="en"><head> <title>FormAssembly.com : Errors</title> <meta na me="viewport" content="width=device-width, initial-scale=1.0" /> <meta http-equiv="Content-Type" content="tex t/html; charset=utf-8" /><script type="text/javascript">(window.NREUM||(NREUM={})).init={privacy:{cookies_enabled:false} };(window.NREUM||(NREUM={})).loader_config={xpid:"VQAOUVBTCxAJVFFUDgcFVA==",licenseKey:"c33294f5df", applicationID:"90069622"};window.NREUM||(NREUM={}),__nr_require=function(t,e,n){function r(n){if(!e[n]){var i=e[n]= {exports:{}};t[n][0].call(i.exports,fun
Feb 25, 2021 21:53:48.697365046 CET	1117	OUT	GET /dist/form-builder/5.0.0/wforms-layout.css?v=6b1109ac309299ec751af6a3c690f678773e405f HTTP/1.1 Accept: text/css, */* Referer: http://www.tfaforms.com/responses/processor Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www.tfaforms.com Connection: Keep-Alive Cookie: AWSALB=G5teNT+mPnhY4FafeUdFCQ4qpE7NMCAv52/lB6FGm+nJ8CQskggT5uw7fUU2YPyZOopJ7hJYfXT gmfwYtSLXzHuGXQFLqebmYZrsaIQDgKX/t5WSb1nhVUqL3YxL; AWSALBCORS=G5teNT+mPnhY4FafeUdFCQ4qpE7N MCAv52/lB6FGm+nJ8CQskggT5uw7fUU2YPyZOopJ7hJYfXTgmfwYtSLXzHuGXQFLqebmYZrsaIQDgKX/t5WSb1nhVU qL3YxL
Feb 25, 2021 21:53:48.827569962 CET	1121	IN	HTTP/1.1 200 OK Date: Thu, 25 Feb 2021 20:53:48 GMT Content-Type: text/css Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: AWSALB=CvNn7KFgppI/g1URhWAIcbq3D4e8IKs1CIWTJY0NO6OC2wHSTtHqB7/vj296KINXjw93e1C ju1D9T1dluajHUSCqZKYFAElluDh1dYUOFi7DgG1GvyMPml51yHas; Expires=Thu, 04 Mar 2021 20:53:48 GMT; Path=/ Set-Cookie: AWSALBCORS=CvNn7KFgppI/g1URhWAIcbq3D4e8IKs1CIWTJY0NO6OC2wHSTtHqB7/vj296KINXjw9 3e1Cju1D9T1dluajHUSCqZKYFAElluDh1dYUOFi7DgG1GvyMPml51yHas; Expires=Thu, 04 Mar 2021 20:53:48 GMT; Pa th=/; SameSite=None Server: nginx Last-Modified: Thu, 25 Feb 2021 17:42:29 GMT ETag: W/"6037e185-755c" X-FA-app: 10-107 Content-Encoding: gzip Data Raw: 32 33 31 31 0d 0a 1f 8b 08 00 00 00 00 00 04 03 d5 5d 6b 73 1b c7 72 fd 4c fe 8a 89 55 37 a2 64 61 f9 90 28 c9 50 ae eb 52 94 68 2b a1 24 47 94 93 72 dd 72 a5 16 c0 82 58 13 c0 c2 bb 0b 92 b2 e2 ff 9e 73 ba 67 66 67 5f 24 24 26 95 44 7e 88 5c ec 4c f7 f4 bb 7b 7a 06 0f cd e7 ed ad c1 55 32 ba 48 cb c1 34 5b 96 83 62 91 65 e5 2c 5d 9e 0f 4d bc 2c d3 78 9e c6 45 32 79 b1 fd e7 f6 f6 ee 43 f3 21 29 92 d2 1c 9f 9d 99 81 29 c6 d9 2a 31 f3 74 91 96 c9 c4 94 99 89 ae 4e b2 7c 81 4f 46 1c 62 b2 a5 f9 e5 e7 37 26 e7 90 6d f3 d0 0c be f2 0f c6 ee 6e db b9 27 f3 47 0e cc a4 ac 7e 9c f8 1f d7 d5 0b 59 f5 e3 3c f5 2f 4c d2 4b ff 73 39 7b e4 26 9e ed fb a7 b3 83 ea c7 c7 d5 8f 4f aa 1f 0f ab 1f 9f fa 1f 57 79 e2 7f 2e 27 7e e2 29 48 e2 9f 4f d3 64 3e 01 39 fc 83 74 b9 5a 57 bf 95 c9 75 19 e7 49 ec 3f 5e f9 9f 46 f3 6c 7c f1 fb 3a 2b 13 72 6c 11 e7 e7 e9 72 b8 f7 c2 ac e2 c9 84 cc c2 8f 7f ba b5 94 f1 68 8e d7 cc 28 cb 27 49 3e 18 67 f3 79 bc 2a 92 a1 fb e1 85 fb a4 58 c5 e3 e6 e0 36 8a 8b 73 3f 57 0d 0c 20 83 b7 85 47 71 1c af ca 34 5b 56 bf 43 2e aa 5f b2 49 f5 cb 64 ba 7c 64 19 9a 54 c 4 29 ca 3c 5b 9e fb 11 60 8e 63 f5 65 9c 73 d5 2a 9f e5 a7 79 32 5c 82 aa f1 fc 85 91 47 57 49 7a 3e 2b fd 33 4f 87 40 00 d6 73 ac 61 9e 16 90 6f 3b 7e 99 04 14 6b a2 5e ce f0 3a b9 31 80 fc 9f 2f 87 f3 64 5a 06 af f7 09 0b 50 28 77 74 61 1f d3 72 9e 3c f0 2b 98 f5 48 0f c0 e8 aa d2 3f 92 e1 fe de de 5f 6e 59 d2 ef c3 51 02 89 aa 48 f9 fb 30 9e 96 09 c8 63 c6 d0 de 64 59 0e ef df 0f 30 8d 47 a3 dc 23 11 8f 41 e0 4f 0b bc ab 92 a1 dc 14 bd 7e 09 8d ad a9 ed fd 42 b4 fc 24 5b 2f 27 31 d9 da af f0 77 d1 6d 31 09 a1 82 9b d9 3e 59 bd fb 70 ff f9 ea da 5c a6 b1 d8 90 13 ac 4d 11 9a 7a 84 60 14 ac 44 08 ed 1e 3f 8f 0e ff 42 33 65 05 cb cc 0e ec 44 4f bf 6c a2 83 c7 d1 7e 7d a2 c7 2d be da 99 9f 7c d9 cc 7b cf c3 79 fb 84 48 e7 86 3d 5d 99 7f 04 a3 ca 32 5b 18 d5 f7 8a 41 94 19 53 60 dd 34 8d ce 1a ec 27 0b b3 17 50 a0 0f 80 97 87 3e a1 f4 2f a8 46 2a 42 a3 1c 96 02 ff 02 a5 f9 64 09 bd 07 36 e3 0b 9a fd 59 12 c3 cc 14 70 17 f0 Data Ascii: 2311]ksrLU7da(PRh+$GrrXsgfg_$$&D~\L{zU2H4[be,]M,xE2yC!))*1tN|OFb7&mn'G~Y</LKs9{&OWy.'~)H Od>9tZWuI?^Fl|:+rlrh('I>gy*X6s?W Gq4[VC._Id|dT)<[`ces*y2\GWIz>+3O@sao;~k^:1/dZP(wtar<+H?_nYQH0cdY0G# AO~B$[/'1wm1>Yp\Mz`D?B3eDOl~}-|{yH=]2[AS`4'P>/F*Bd6Yp

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 21:53:48.846951008 CET	1145	OUT	GET /dist/form-builder/5.0.0/wforms-jsonly.css?v=6b1109ac309299ec751af6a3c690f678773e405f HTTP/1.1 Accept: text/css, */* Referer: http://www.tfaforms.com/responses/processor Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www.tfaforms.com Connection: Keep-Alive Cookie: AWSALB=KCbRl27TtolgZdt9YzzzEVXZShIHcErTPtr3hJOL7l8pRtWwPgaR+axy8lVtC9EdUQZFe9KlOpF VmtCxnGesMOb1TBg7xk0/jGmMcdW5a093IRzUAJECn4roAuCZ; AWSALBCORS=KCbRl27TtolgZdt9YzzzEVXZShIH cErTPtr3hJOL7l8pRtWwPgaR+axy8lVtC9EdUQZFe9KlOpFVmtCxnGesMOb1TBg7xk0/jGmMcdW5a093IRzUAJECn4 roAuCZ
Feb 25, 2021 21:53:48.975475073 CET	1188	IN	HTTP/1.1 200 OK Date: Thu, 25 Feb 2021 20:53:48 GMT Content-Type: text/css Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: AWSALB=rX+ntaeAJCEkzztTjGj94kJTM2s7FB1FnMDrpmrd32zmMXoTesGf8ZLBQdoUumC0EQIhtCi m8tUb7TVUDZ+ZTwG+x22XOR6IjUEs2Y16AidM6w3hGoDIn5hX8FSZ; Expires=Thu, 04 Mar 2021 20:53:48 GMT; Path=/ Set-Cookie: AWSALBCORS=rX+ntaeAJCEkzztTjGj94kJTM2s7FB1FnMDrpmrd32zmMXoTesGf8ZLBQdoUumC0EQI htCim8tUb7TVUDZ+ZTwG+x22XOR6IjUEs2Y16AidM6w3hGoDIn5hX8FSZ; Expires=Thu, 04 Mar 2021 20:53:48 GMT; Pa th=/; SameSite=None Server: nginx Last-Modified: Thu, 25 Feb 2021 17:42:29 GMT ETag: W/"6037e185-2f3" X-FA-app: 10-107 Content-Encoding: gzip Data Raw: 31 32 30 0d 0a 1f 8b 08 00 00 00 00 00 04 03 b5 52 b1 4e c4 30 0c dd f3 15 46 6c 15 f4 76 98 4e 48 a7 1b 4f 85 1f 70 1b 97 1a d2 a4 8a dd 56 15 e2 df 49 ba 20 ee 0a 82 81 0c 59 6c 3f 3f bf f7 8c d9 15 b0 6f 1a 12 e1 da b1 2e 50 91 43 25 0b d5 e8 48 a0 d8 e5 86 a7 8e 84 00 23 81 76 04 71 ad 68 87 0a d2 85 d1 59 28 7c d0 02 70 18 dc 02 dc c2 0b 4e 28 4d e4 41 81 05 2c 0b d6 8e 6c 99 c1 8c 29 43 db 8a a6 15 f0 66 20 bd 54 1e 1c 2e 77 e0 83 27 b8 e2 7e 08 51 d1 eb bd 79 37 a6 d3 de 41 39 1f 42 ec a1 cd 5f 39 b7 27 7c a6 1b d8 aa 1c d9 d2 e3 58 f7 ac bf c0 be 04 10 9c 68 ef 6d 45 32 f6 04 25 36 ca c1 0b e4 9d df 23 d7 2e 34 af 67 b4 2f a1 e7 f6 61 8c 91 bc 66 f2 e7 e4 b6 20 3e 65 ba 8d 2b 9f 6c 4a 3c 9f dc 90 ac 4c 94 b3 ba 3f 8d 6d 2e bc fe 72 fe 81 c9 59 a1 4d 21 57 67 52 2a 8e e8 ad 23 18 f2 49 13 a7 fc f0 1a a0 e4 f2 96 00 ff 66 db 5f b5 fd 00 08 fc da 09 f3 02 00 00 0d 0a Data Ascii: 120RN0FlvNHOpVl Yl??o.PC%H#vqhY(|pN(MA,l)Cf T.w'~Qy7A9B_9'|XhmE2%6#.4g/af >e+lJ<L?m.rYM! WgR*#lf_

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49714	3.226.66.230	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 21:53:48.698326111 CET	1118	OUT	GET /wForms/3.11/js/wforms.js?v=6b1109ac309299ec751af6a3c690f678773e405f HTTP/1.1 Accept: application/javascript, */*;q=0.8 Referer: http://www.tfaforms.com/responses/processor Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www.tfaforms.com Connection: Keep-Alive Cookie: AWSALB=G5teNT+mPnhY4FafeUdFCQ4qpE7NMCAv52/lB6FGm+nJ8CQskggT5uw7fUU2YPyZOopJ7hJYfXT gmfwYtSLXzHuGXQFLqebmYZrsaIQDgKX/t5WSb1nhVUqL3YxL; AWSALBCORS=G5teNT+mPnhY4FafeUdFCQ4qpE7N MCAv52/lB6FGm+nJ8CQskggT5uw7fUU2YPyZOopJ7hJYfXTgmfwYtSLXzHuGXQFLqebmYZrsaIQDgKX/t5WSb1nhVU qL3YxL

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 21:53:48.829545021 CET	1132	IN	HTTP/1.1 200 OK Date: Thu, 25 Feb 2021 20:53:48 GMT Content-Type: application/javascript; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: AWSALB=KCbRl27TtolgZdt9YzzzEVXZShIHcErTPtr3hJOL7l8pRtWwPgaR+axy8lVtC9EdUQZFe9K lOpFVmtCxnGesMOb1TBg7xk0/jGmMcdW5a093IRzUAJECn4roAuCZ; Expires=Thu, 04 Mar 2021 20:53:48 GMT; Path=/ Set-Cookie: AWSALBCORS=KCbRl27TtolgZdt9YzzzEVXZShIHcErTPtr3hJOL7l8pRtWwPgaR+axy8lVtC9EdUQZ Fe9KlOpFVmtCxnGesMOb1TBg7xk0/jGmMcdW5a093IRzUAJECn4roAuCZ; Expires=Thu, 04 Mar 2021 20:53:48 GMT; Path=/; SameSite=None Server: nginx Last-Modified: Thu, 25 Feb 2021 17:57:20 GMT ETag: W/"6037e500-3b60f" X-FA-app: 10-107 Content-Encoding: gzip Data Raw: 36 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 04 03 ec bd e9 76 5b 47 92 2e fa bb cf 53 80 bb 24 0a 10 36 c1 c1 43 55 81 de a6 39 c9 66 5b 53 8b b4 bb 4f 83 30 16 48 80 22 2c 12 e0 01 40 cb 2a 82 fd ec e7 fb 62 c8 cc 0d 80 92 ec ea 5e f7 ae bb 6e 77 59 c4 ce 39 23 23 23 63 ca c8 df ba e3 ca 59 77 d2 df 2a ee 86 dd eb 7e 33 93 8f 2c ff ad 3f 9e 0c 46 c3 66 b6 d9 d8 c8 f2 fe ef 37 a3 f1 74 d2 cc f6 50 34 7f dd 3d 7f d7 7d db cf 77 cf 26 d3 71 f7 7c 9a bf 18 f5 6e af fa f9 e1 f0 f6 ba 3f ee 9e e1 e7 8b ee 4d be 3f ba ba ea 9f 4f d1 4a fe a6 ff f6 fb f1 4d fe d3 b0 d7 bf 18 0c fb bd fc e5 ed d5 55 7e 72 39 98 e4 27 e3 db 7e fe ac 7b 85 76 bb 93 c9 e0 ed f0 e8 20 ef f5 a7 a8 98 bf bd 1a 9d 75 af b2 9c 03 9b dc 74 cf 31 ba ec 7e 7b d8 7f 5f b9 b8 1d 4a c3 d5 ce 70 d4 99 5c 8e 07 c3 77 9d da dd 6f 98 4b e8 a2 f8 b1 5a 93 6e f0 63 88 de 6a d2 13 3e a 6 e8 b0 a6 3d e2 eb 82 3d 23 0f 43 29 42 ab b5 bb 71 7f 7a 3b 1e 56 a6 48 be df 66 bb 3a 96 82 e5 aa 35 49 51 a8 69 7a 43 3e 24 b9 f3 ec d5 9b 17 bb 27 c5 fa e3 6a 6b 73 ed ef ed da fa 5b 4d 7f 7e f2 e6 e8 45 b1 fe cb e9 e4 74 f2 74 5d d3 de 68 9a 24 3d f2 b4 c3 e3 fd dd d7 87 c5 7a b5 75 ba 5e ad b5 4e db 77 f7 b3 a7 f5 b5 46 fe cb a3 9d d3 d3 d8 e0 de ee 31 4a 4d c7 1f d6 1b d3 fe 64 5a 55 a8 d5 76 d6 4f cf 38 9c d3 b3 f5 e6 7a c3 7b fa e1 e8 e0 e0 f0 65 d1 ca ce 47 43 ac da ed f9 74 34 ce f2 6c 3a 3a 9e 02 7a 6f f1 f3 b7 ee d5 6d ff d5 45 d6 d6 a1 bd 38 3e 3a ec bc dc 3d 39 fa f9 b0 f3 ec a7 97 fb 27 47 af 5e 16 da 45 35 ab fe 3a 39 1f 0f 6e a6 b5 ac b6 c3 f5 c0 fa 1e fe 7e 53 cd 7e c9 ea e3 fe e4 bc 7b d3 af 0e 26 2f bb 2f 6b 8d 71 ff e6 0a 2b 57 5d 97 ef f5 3c 3b 3d 7d 5f cf 6a f5 ec 51 56 6b de 71 dc 4d 59 7c 85 72 e7 7c 74 3b 9c f6 c7 c5 a6 0e 62 72 35 38 ef 17 bb e3 71 f7 43 e3 66 3c 9a 8e a6 1f 6e fa 0d 49 dd ee 3c 33 24 e8 5c 8c c6 87 dd f3 4b ac 8b af 60 c5 51 a9 3a 3a fb 15 a8 54 bb 1b 5c 54 57 f4 b7 ae d5 d1 41 ed ae fc 5d 64 67 5b 9d ac ee 43 a8 d7 ef 0d Data Ascii: 6000v[G.S$6CU9f[SO0H",@*b^nwY9###cYw*~3,?Ff7tP4=}w&q\|n?M?OJMU~r9'~{v ut1~{_Jp\woKZncj>== #C)Bqz;VHf:5IQizC>$'jks[M~Ett]h$=zu^NwF1JMdZUvO8z{eGCt4l::zomE8>:=9'G^E5:9n~S~{&//kq+W]<;=}_jQVkqMY\| r\|t;br58qCf<nI<3$\K`Q::T\TWA]dg[C
Feb 25, 2021 21:54:07.655030966 CET	1653	OUT	GET /support/ HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www.tfaforms.com Connection: Keep-Alive Cookie: AWSALB=Jr1KpBU0IiY2xw54lW1Dmf0+Y1qJzsbrtbg4DyaV5cWmuitGVUmQvVYJhx9Bccjkyqn1DwY/lWD eTSADlti3m4300rktFVFipBuOGSfwKq+wQcNmzRqe/UV6ql2D; AWSALBCORS=Jr1KpBU0IiY2xw54lW1Dmf0+Y1qJ zsbrtbg4DyaV5cWmuitGVUmQvVYJhx9Bccjkyqn1DwY/lWDeTSADlti3m4300rktFVFipBuOGSfwKq+wQcNmzRqe/U V6ql2D
Feb 25, 2021 21:54:08.008790970 CET	1653	IN	HTTP/1.1 302 Found Date: Thu, 25 Feb 2021 20:54:07 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: AWSALB=w2xsCRk8PDwyPr2U7uUX039HzmHDtqkU4eBp/O2BRjf+Jny08ehMgk4sD2wTwPyNOmZN2UA az6WF+V27xF0v0RPZjE1nQN4BrUwpRSJEq5UGNZxx90wDnvw9BcSh; Expires=Thu, 04 Mar 2021 20:54:07 GMT; Path=/ Set-Cookie: AWSALBCORS=w2xsCRk8PDwyPr2U7uUX039HzmHDtqkU4eBp/O2BRjf+Jny08ehMgk4sD2wTwPyNOmZ N2UAaz6WF+V27xF0v0RPZjE1nQN4BrUwpRSJEq5UGNZxx90wDnvw9BcSh; Expires=Thu, 04 Mar 2021 20:54:07 GMT; Path=/; SameSite=None Server: nginx P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM" Set-Cookie: CAKEPHP=caa58e0fa02091d8517d35b02c8892bb; HttpOnly=1; Path=/; SameSite=None; Secure Location: http://www.tfaforms.com/pages/support X-FA-app: 10-107 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Feb 25, 2021 21:54:08.014332056 CET	1654	OUT	GET /pages/support HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www.tfaforms.com Connection: Keep-Alive Cookie: AWSALB=w2xsCRk8PDwyPr2U7uUX039HzmHDtqkU4eBp/O2BRjf+Jny08ehMgk4sD2wTwPyNOmZN2UAaz6W F+V27xF0v0RPZjE1nQN4BrUwpRSJEq5UGNZxx90wDnvw9BcSh; AWSALBCORS=w2xsCRk8PDwyPr2U7u UX039HzmHDtqkU4eBp/O2BRjf+Jny08ehMgk4sD2wTwPyNOmZN2UAaz6WF+V27xF0v0RPZjE1nQN4BrUwpRSJEq5UG NZxx90wDnvw9BcSh

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 21:54:08.260314941 CET	1655	IN	HTTP/1.1 302 Found Date: Thu, 25 Feb 2021 20:54:08 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: AWSALB=Q32h0UgGiAOSXfZRntdY3Ds23kDJARxefYd/AN3GfasjgFiEkSRIp6TVXZgtwERqE0AWEvt KxhTkhdmzdhprSbdeoCSzE0ELv96dzcdwZNB6UvJeXVo7jxRh6PnP; Expires=Thu, 04 Mar 2021 20:54:08 GMT; Path=/ Set-Cookie: AWSALBCORS=Q32h0UgGiAOSXfZRntdY3Ds23kDJARxefYd/AN3GfasjgFiEkSRIp6TVXZgtwERqE0A WEvtKxhTkhdmzdhprSbdeoCSzE0ELv96dzcdwZNB6UvJeXVo7jxRh6PnP; Expires=Thu, 04 Mar 2021 20:54:08 GMT; Pa th=/; SameSite=None Server: nginx P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM" Set-Cookie: CAKEPHP=9337805f66c5e8fd50a05c0629e96888; HttpOnly=1; Path=/; SameSite=None; Secure Location: https://help.formassembly.com X-FA-app: 10-107 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49717	3.226.66.230	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 21:53:48.828516960 CET	1131	OUT	GET /js/iframe_message_helper_internal.js?v=2 HTTP/1.1 Accept: application/javascript, */*;q=0.8 Referer: http://www.tfaforms.com/responses/processor Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www.tfaforms.com Connection: Keep-Alive Cookie: AWSALB=G5teNT+mPnhY4FafeUdFCQ4qpE7NMCAv52/lB6FGm+nJ8CQskggT5uw7fUU2YPyZOopJ7hJYfXT gmfwYtSLXzHuGXQFLqebmYZrsaIQDgKX/t5WSb1nhVUqL3YxL; AWSALBCORS=G5teNT+mPnhY4FafeUdFCQ4qpE7N MCAv52/lB6FGm+nJ8CQskggT5uw7fUU2YPyZOopJ7hJYfXTgmfwYtSLXzHuGXQFLqebmYZrsaIQDgKX/t5WSb1nhVU qL3YxL
Feb 25, 2021 21:53:48.957947969 CET	1176	IN	HTTP/1.1 200 OK Date: Thu, 25 Feb 2021 20:53:48 GMT Content-Type: application/javascript; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: AWSALB=u+nSfl7Ae5PVrHQevIhhLhE+NJa8dvdDqC0lhr/2RIEgvo+O8ZWusO6Um5lD2NQo3dYZF3+ cPB0SZmp7FFavhWzfoAntrs7gGGWpgpTJKv/Bw3kIrfdQ6X9im14G; Expires=Thu, 04 Mar 2021 20:53:48 GMT; Path=/ Set-Cookie: AWSALBCORS=u+nSfl7Ae5PVrHQevIhhLhE+NJa8dvdDqC0lhr/2RIEgvo+O8ZWusO6Um5lD2NQo3dY ZF3+cPB0SZmp7FFavhWzfoAntrs7gGGWpgpTJKv/Bw3kIrfdQ6X9im14G; Expires=Thu, 04 Mar 2021 20:53:48 GMT; Pa th=/; SameSite=None Server: nginx Last-Modified: Thu, 25 Feb 2021 17:32:37 GMT ETag: W/"6037df35-4dca" X-FA-app: 10-107 Content-Encoding: gzip Data Raw: 31 61 36 39 0d 0a 1f 8b 08 00 00 00 00 00 04 03 c5 5c 6d 57 db d6 b2 fe de 5f b1 71 cf 32 72 10 c2 24 69 9a 9a ba dc b4 49 4f b8 27 81 de 40 7a ba 16 e5 64 c9 96 8c 95 c8 92 2b c9 10 0e f8 bf df e7 99 bd b7 de 6c 68 48 db 55 fa 02 96 b6 66 cf fb cc 9e 19 79 e7 c1 83 2f d4 03 75 32 8d 72 95 8f b3 68 5e a8 d9 22 2f d4 28 54 51 32 8e 17 41 18 e0 0f e5 ab 1f d3 6c f6 2c cf c3 d9 28 be 52 13 7c f0 f8 dc bf a7 61 a2 e2 d4 b7 cb 12 75 f0 e3 9b 67 af 5f b8 2a 2a d4 65 14 c7 6a 9c 26 45 94 2c d2 45 8e e7 f2 30 01 b8 22 57 8b 79 e0 17 61 40 10 d3 30 3a 9f 16 2a 4f 55 31 f5 0b fc 2f 94 67 fc 28 09 33 35 f6 b1 77 f0 9e 18 69 c0 76 79 91 aa 99 5f 8c a7 84 80 ad b8 4b 98 14 9b b9 b9 4f e4 78 eb 04 d0 e6 69 0e 0c ce 15 28 0c d2 24 c4 0e 59 ba 38 9f 82 a6 71 96 e6 f9 76 90 ce b0 99 9a 85 79 ee 9f 87 f8 3d 9e fa 49 94 6b 02 f3 68 36 8f c3 e3 22 cd 78 ef 7d ae e2 68 94 f9 d9 15 a1 f9 31 90 5e e4 e0 90 53 f2 6a 16 25 d1 24 c2 a5 51 18 a7 97 3d b5 6d 10 c4 f2 24 0c c9 26 60 9e 03 5c a8 c0 01 1f cb 8a cb 10 3c 9c 13 7c 86 67 fc 20 27 c3 c9 06 4d 71 9d 14 8b 23 f8 58 d8 55 93 34 c6 4e 24 90 52 f1 8b 01 77 9c ba d1 24 f3 67 e1 c1 73 b7 f0 b3 f3 b0 78 9b c5 86 25 db 6a 3a 50 61 84 0d 32 a0 74 69 19 8a 3d e7 d1 c7 30 ce 55 9a 91 35 e9 6c e6 43 58 71 f4 21 54 9d 7c 31 9a 45 05 04 d6 d9 23 74 25 e8 59 64 b2 70 1c 46 17 80 66 d0 9e fb 19 d1 03 4a 41 7a a9 95 00 0c 0d 62 68 54 a1 fc f1 38 cd 02 60 1b 5f 89 02 6d 2b 8b e8 40 80 2e 92 e8 b7 05 56 0a f6 ea e0 39 89 52 97 d3 68 3c 6d ec 69 75 d4 9f cf 63 70 db d5 58 01 81 54 e8 ba c4 1e 60 23 78 94 d7 38 a9 b2 45 92 90 51 45 a5 ed 42 cf b6 32 4c 7a f3 4a 63 31 f1 e3 78 e4 8f 3f 40 2b e3 45 11 a5 09 10 52 49 5a e2 2a d2 bf f0 a3 d8 1f c5 a1 61 09 c8 8d c6 50 6a bd e3 85 1f 83 8c 74 62 84 08 c5 ec e4 d9 b8 a3 fc a2 c8 a2 d1 a2 80 1a 02 5c 00 46 45 93 ab 8a a7 46 e4 ea c0 dc 21 b6 46 f1 47 57 15 96 9a ab 49 0a 2e a7 d9 07 e5 4f 8a 30 d3 40 a8 03 d0 23 11 58 9e 13 73 bf ce 82 35 78 88 95 66 Data Ascii: 1a69\mW_q2r$iIO'@zd+lhHUfy/u2rh^"/(TQ2Al,(R\|aug_**ej&E,E0"Wya@0:*OU1/g(35wivy_KOxi($Y8qv y=Ikh6"x}h1^Sj%$Q=m$&`\<|g 'Mq#XU4N$Rw$gsx%j:Pa2ti=0U5lCXq!T|1E#t%YdpFfJAzbhT8`_m+@.V9Rh<miucpXT`#x8 EQEB2LzJc1x?@+ERIZ*aPjtb\FEF!FGWI.O0@#Xs5xf

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49724	3.226.66.230	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 21:54:04.768224001 CET	1621	OUT	GET /responses/favicon.ico HTTP/1.1 User-Agent: AutoIt Host: www.tfaforms.com Cookie: AWSALB=rX+ntaeAJCEkzztTjGj94kJTM2s7FB1FnMDrpmrd32zmMXoTesGf8ZLBQdoUumC0EQlhtCim8tUb7TVUDZ+ZTwG+x22XOR6ljUEs2Y16AidM6w3hGoDIn5hX8FSZ; AWSALBCORS=rX+ntaeAJCEkzztTjGj94kJTM2s7FB1FnMDrpmrd32zmMXoTesGf8ZLBQdoUumC0EQlhtCim8tUb7TVUDZ+ZTwG+x22XOR6ljUEs2Y16AidM6w3hGoDIn5hX8FSZ
Feb 25, 2021 21:54:05.075164080 CET	1623	IN	HTTP/1.1 404 Not Found Date: Thu, 25 Feb 2021 20:54:05 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: AWSALB=Jr1KpBU0liY2xw54lW1Dmf0+Y1qJzsbrtbg4DyaV5cWmuitGVUmQvVYJhx9Bccjkyqn1DwY/lWDeTSADlti3m4300rktFVFipBuOGSfwKq+wQcNmzRqe/UV6ql2D; Expires=Thu, 04 Mar 2021 20:54:04 GMT; Path=/ Set-Cookie: AWSALBCORS=Jr1KpBU0liY2xw54lW1Dmf0+Y1qJzsbrtbg4DyaV5cWmuitGVUmQvVYJhx9Bccjkyqn1DwY/lWDeTSADlti3m4300rktFVFipBuOGSfwKq+wQcNmzRqe/UV6ql2D; Expires=Thu, 04 Mar 2021 20:54:04 GMT; Path=/; SameSite=None Server: nginx P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM" Set-Cookie: CAKEPHP=08f519fdfa456469e460b5af44981a9f; HttpOnly=1; Path=/; SameSite=None; Secure Data Raw: 36 63 62 30 0d 0a 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 2f 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 28 77 69 6e 64 6f 77 2e 4e 52 45 55 4d 7c 7c 28 4e 52 45 55 4d 3d 7b 7d 29 29 2e 69 6e 69 74 3d 7b 70 72 69 76 61 63 79 3a 7b 63 6f 6f 6b 69 65 73 5f 65 6e 61 62 6c 65 64 3a 66 61 6c 73 65 7d 7d 3b 28 77 69 6e 64 6f 77 2e 4e 52 45 55 4d 7c 7c 28 4e 52 45 55 4d 3d 7b 7d 29 29 2e 6c 6f 61 64 65 72 5f 63 6f 6e 66 69 67 3d 7b 78 70 69 64 3a 22 56 51 41 4f 55 56 42 54 43 78 41 4a 56 46 46 55 44 67 63 46 56 41 3d 3d 22 2c 6c 69 63 65 6e 73 65 4b 65 79 3a 22 63 33 33 32 39 34 66 35 64 66 22 2c 61 70 70 6c 69 63 61 74 69 6f 6e 49 44 3a 22 39 30 30 36 39 36 32 32 22 7d 3b 77 69 6e 64 6f 77 2e 4e 52 45 55 4d 7c 7c 28 4e 52 45 55 4d 3d 7b 7d 29 2c 5f 5f 6e 72 5f 72 65 71 75 69 72 65 3d 66 75 6e 63 74 69 6f 6e 28 74 2c 65 2c 6e 29 7b 66 75 6e 63 74 69 6f 6e 20 72 28 6e 29 7b 69 66 28 21 65 5b 6e 5d 29 7b 76 61 72 20 69 3d 65 5b 6e 5d 3d 7b 65 78 70 6f 72 74 73 3a 7b 7d 7d 3b 74 5b 6e 5d 5b 30 5d 2e 63 61 6c 6c 28 69 2e 65 78 70 6f 72 74 73 2c 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 69 3d 74 5b 6e 5d 5b 31 5d 5b 65 5d 3b 72 65 74 75 72 6e 20 72 28 69 7c 7c 65 29 7d 2c 69 2c 69 2e 65 78 70 6f 72 74 73 29 7d 72 65 74 75 72 6e 20 65 5b 6e 5d 2e 65 78 70 6f 72 74 73 7d 69 66 28 22 66 75 6e 63 74 69 6f 6e 22 3d 3d 74 79 70 65 6f 66 20 5f 5f 6e 72 5f 72 65 71 75 69 72 65 29 72 65 74 75 72 6e 20 5f 5f 6e 72 5f 72 65 71 75 69 72 65 3b 66 6f 72 28 76 61 72 20 69 3d 30 3b 69 3c 6e 2e 6c 65 6e 67 74 68 3b Data Ascii: 6cb0<!DOCTYPE html><html><head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8"/> <script type="text/javascript">(window.NREUM||(NREUM={})).init={privacy:{cookies_enabled:false}};(window.NREUM||(NREUM={})).loader_config={xpid:"VQAOUVBTCxAJVFFUDgcFVA==",licenseKey:"c33294f5df",applicationID:"90069622"};window.NREUM||(NREUM={}),__nr_require=function(t,e,n){function r(n){if(!e[n]){var i=e[n]={exports:{}};t[n][0].call(i.exports,function(e){var i=t[n][1][e];return r(i||e)},i,i.exports)}return e[n].exports}if("function"==typeof __nr_require)return __nr_require;for(var i=0;i<n.length;

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 21:54:08.611567020 CET	54.152.202.195	443	192.168.2.5	49727	CN=help.formassembly.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Jan 31 17:22:30 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Sat May 01 18:22:30 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Feb 25, 2021 21:54:08.614350080 CET	54.152.202.195	443	192.168.2.5	49728	CN=help.formassembly.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Jan 31 17:22:30 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Sat May 01 18:22:30 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

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 21:54:09.286130905 CET	13.224.89.142	443	192.168.2.5	49733	CN=*.cloudfront.net, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Tue May 26 02:00:00 CEST 2020 Thu Aug 01 14:00:00 CEST 2013 Mon Nov 06 01:00:00 CET 2017	Wed Apr 21 14:00:00 CEST 2021 Tue Aug 01 14:00:00 CEST 2028 Sun Nov 06 00:59:59 CET 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert Global CA G2, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		
Feb 25, 2021 21:54:09.286622047 CET	13.224.89.142	443	192.168.2.5	49731	CN=*.cloudfront.net, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Tue May 26 02:00:00 CEST 2020 Thu Aug 01 14:00:00 CEST 2013 Mon Nov 06 01:00:00 CET 2017	Wed Apr 21 14:00:00 CEST 2021 Tue Aug 01 14:00:00 CEST 2028 Sun Nov 06 00:59:59 CET 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert Global CA G2, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		
Feb 25, 2021 21:54:09.286655903 CET	13.224.89.142	443	192.168.2.5	49732	CN=*.cloudfront.net, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Tue May 26 02:00:00 CEST 2020 Thu Aug 01 14:00:00 CEST 2013 Mon Nov 06 01:00:00 CET 2017	Wed Apr 21 14:00:00 CEST 2021 Tue Aug 01 14:00:00 CEST 2028 Sun Nov 06 00:59:59 CET 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert Global CA G2, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		
Feb 25, 2021 21:54:09.286887884 CET	13.224.89.142	443	192.168.2.5	49734	CN=*.cloudfront.net, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Tue May 26 02:00:00 CEST 2020	Wed Apr 21 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
							Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		
							Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		
					CN=DigiCert Global CA G2, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		
Feb 25, 2021 21:54:09.335412979 CET	13.224.89.142	443	192.168.2.5	49739	CN=*.cloudfront.net, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Tue May 26 02:00:00 CEST 2020	Wed Apr 21 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
							Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		
							Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		
					CN=DigiCert Global CA G2, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		
Feb 25, 2021 21:54:09.349229097 CET	13.224.89.142	443	192.168.2.5	49740	CN=*.cloudfront.net, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Tue May 26 02:00:00 CEST 2020	Wed Apr 21 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
							Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		
							Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert Global CA G2, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		
Feb 25, 2021 21:54:10.427422047 CET	54.152.202.195	443	192.168.2.5	49748	CN=*.knowledgeowl.com, OU=PremiumSSL Wildcard, OU=IT, O=Silly Moose LLC, STREET=2552 W 133rd Circle, L=Broomfield, ST=Colorado, OID.2.5.4.17=80020, C=US CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Jul 19 02:00:00 CEST 2019 Fri Nov 02 01:00:00 CET 2018 Mon Feb 01 01:00:00 CET 2010	Tue Jul 27 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2031 Tue Jan 19 00:59:59 CET 2038	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Mon Feb 01 01:00:00 CET 2010	Tue Jan 19 00:59:59 CET 2038		
Feb 25, 2021 21:54:10.430417061 CET	54.152.202.195	443	192.168.2.5	49744	CN=*.knowledgeowl.com, OU=PremiumSSL Wildcard, OU=IT, O=Silly Moose LLC, STREET=2552 W 133rd Circle, L=Broomfield, ST=Colorado, OID.2.5.4.17=80020, C=US CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Jul 19 02:00:00 CEST 2019 Fri Nov 02 01:00:00 CET 2018 Mon Feb 01 01:00:00 CET 2010	Tue Jul 27 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2031 Tue Jan 19 00:59:59 CET 2038	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Mon Feb 01 01:00:00 CET 2010	Tue Jan 19 00:59:59 CET 2038		

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 21:54:10.433835030 CET	54.152.202.195	443	192.168.2.5	49749	CN=*.knowledgeowl.com, OU=PremiumSSL Wildcard, OU=IT, O=Silly Moose LLC, STREET=2552 W 133rd Circle, L=Broomfield, ST=Colorado, OID.2.5.4.17=80020, C=US	CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	Fri Jul 19 02:00:00 CEST 2019	Tue Jul 27 01:59:59 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=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Mon Feb 01 01:00:00 CET 2010	Tue Jan 19 00:59:59 CET 2038		
Feb 25, 2021 21:54:10.436851025 CET	54.152.202.195	443	192.168.2.5	49747	CN=*.knowledgeowl.com, OU=PremiumSSL Wildcard, OU=IT, O=Silly Moose LLC, STREET=2552 W 133rd Circle, L=Broomfield, ST=Colorado, OID.2.5.4.17=80020, C=US	CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	Fri Jul 19 02:00:00 CEST 2019	Tue Jul 27 01:59:59 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=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Mon Feb 01 01:00:00 CET 2010	Tue Jan 19 00:59:59 CET 2038		
Feb 25, 2021 21:54:10.452405930 CET	54.152.202.195	443	192.168.2.5	49746	CN=*.knowledgeowl.com, OU=PremiumSSL Wildcard, OU=IT, O=Silly Moose LLC, STREET=2552 W 133rd Circle, L=Broomfield, ST=Colorado, OID.2.5.4.17=80020, C=US	CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	Fri Jul 19 02:00:00 CEST 2019	Tue Jul 27 01:59:59 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=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Mon Feb 01 01:00:00 CET 2010	Tue Jan 19 00:59:59 CET 2038		

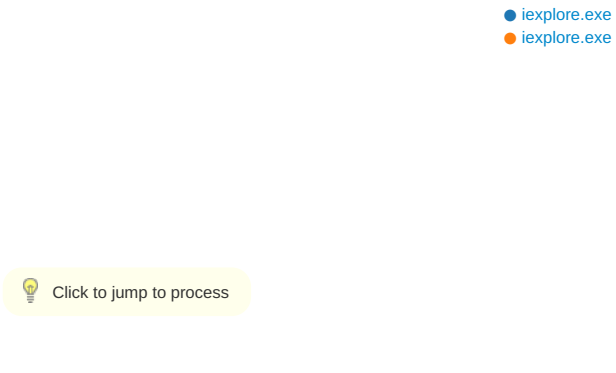
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Mon Feb 01 01:00:00 CET 2010	Tue Jan 19 00:59:59 CET 2038		
Feb 25, 2021 21:54:10.457192898 CET	54.152.202.195	443	192.168.2.5	49750	CN=*.knowledgeowl.com, OU=PremiumSSL Wildcard, OU=IT, O=Silly Moose LLC, STREET=2552 W 133rd Circle, L=Broomfield, ST=Colorado, OID.2.5.4.17=80020, C=US CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Jul 19 02:00:00 CEST 2019 Fri Nov 02 01:00:00 CET 2018 Mon Feb 01 01:00:00 CET 2010	Tue Jul 27 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2031 Tue Jan 19 00:59:59 CET 2038	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Mon Feb 01 01:00:00 CET 2010	Tue Jan 19 00:59:59 CET 2038		
Feb 25, 2021 21:54:11.637028933 CET	35.174.150.168	443	192.168.2.5	49756	CN=pi.pardot.com, O="salesforce.com, inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sat Dec 05 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Sun Dec 05 00:59:59 CET 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Feb 25, 2021 21:54:11.637166023 CET	35.174.150.168	443	192.168.2.5	49757	CN=pi.pardot.com, O="salesforce.com, inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sat Dec 05 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Sun Dec 05 00:59:59 CET 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Feb 25, 2021 21:54:11.652435064 CET	104.196.12.68	443	192.168.2.5	49754	CN=www.formassembly.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 13 14:25:04 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Tue Apr 13 15:25:04 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

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 21:54:11.654108047 CET	104.196.12.68	443	192.168.2.5	49755	CN=www.formassembly.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 13 14:25:04 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Tue Apr 13 15:25:04 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 4616 Parent PID: 792

General

Start time:	21:53:46
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:	0x7ff7395b0000
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: 4588 Parent PID: 4616

General

Start time:	21:53:46
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:4616 CREDAT:17410 /prefetch:2
Imagebase:	0x950000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly