ID: 404066
Sample Name:
BCJOphish040520219700.html
Cookbook: default.jbs
Time: 17:16:40
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

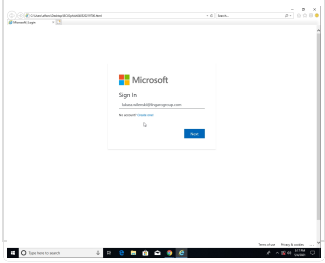
Analysis Report BCJOphish040520219700.html

Overview

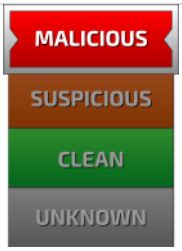
General Information

Sample Name:	BCJOphish040520219700.html
Analysis ID:	404066
MD5:	724cbfa451d94bd.
SHA1:	d39571159adc5d..
SHA256:	713e7b41006aea..
Infos:	

Most interesting Screenshot:



Detection



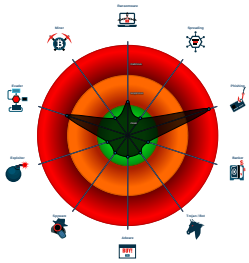
HTMLPhisher

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Phishing site detected (based on fav…
- Yara detected HtmlPhish10
- Yara detected HtmlPhish44
- Yara detected obfuscated html page
- Obfuscated HTML file found
- HTML body contains low number of …
- HTML title does not match URL
- IP address seen in connection with o…
- Invalid T&C link found
- JA3 SSL client fingerprint seen in co…
- None HTTPS page querying sensitiv…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6424 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6480 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6424 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

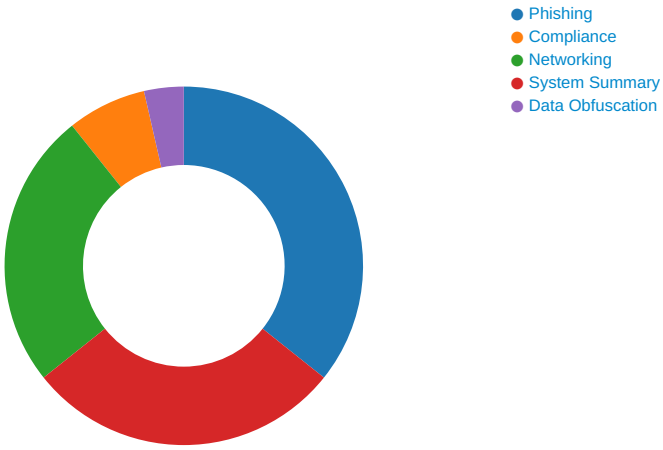
Initial Sample

Source	Rule	Description	Author	Strings
BCJOphish040520219700.html	JoeSecurity_Obshtml	Yara detected obfuscated html page	Joe Security	
BCJOphish040520219700.html	JoeSecurity_HtmlPhish_44	Yara detected HtmlPhish_44	Joe Security	

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 HtmlPhish10

Yara detected HtmlPhish44

Yara detected obfuscated html page

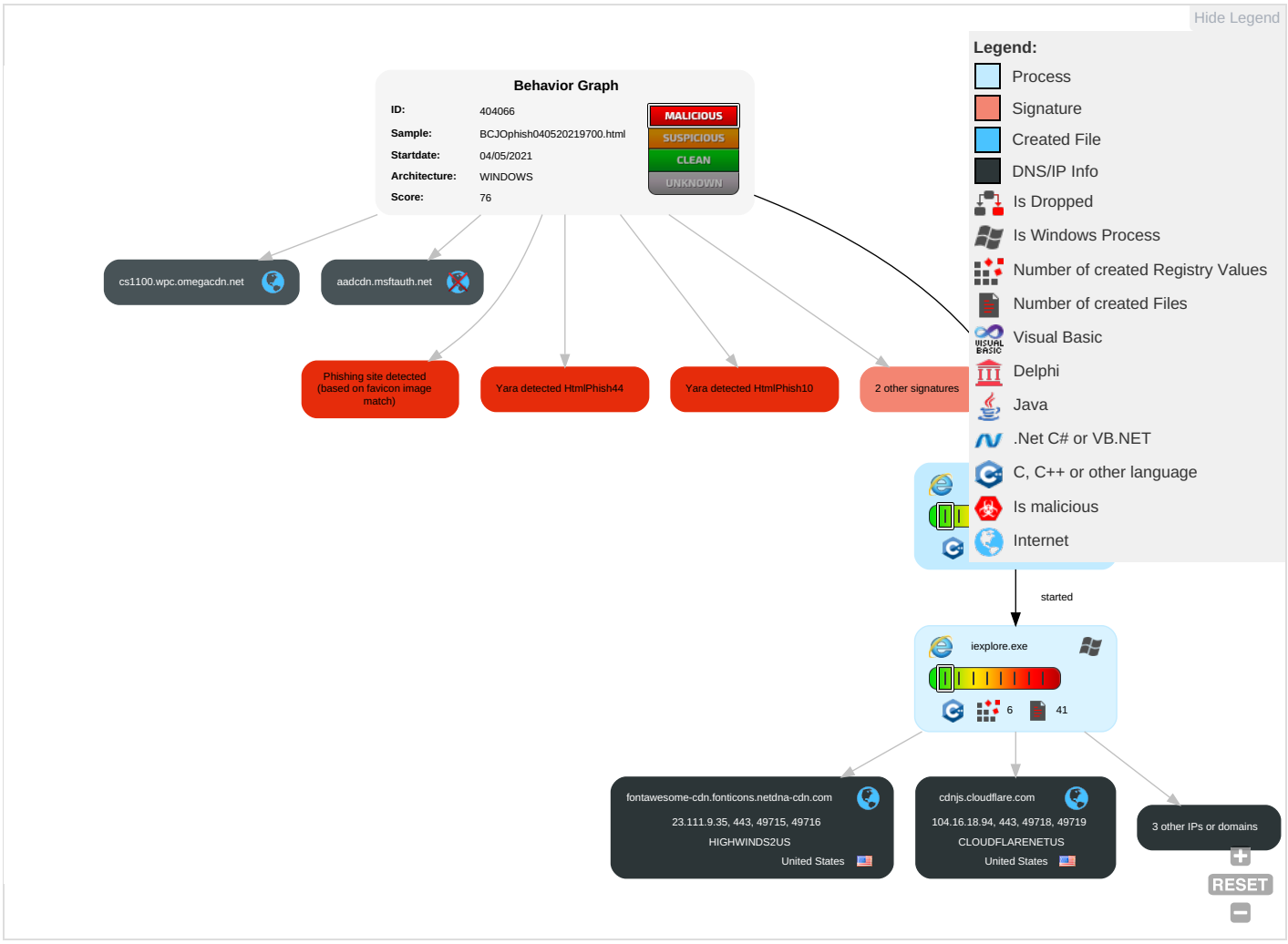
Data Obfuscation:

Obfuscated HTML file found

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	Impact
Valid Accounts	Scripting 1	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	Modify System Partition
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	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 1	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	Delete Device Data

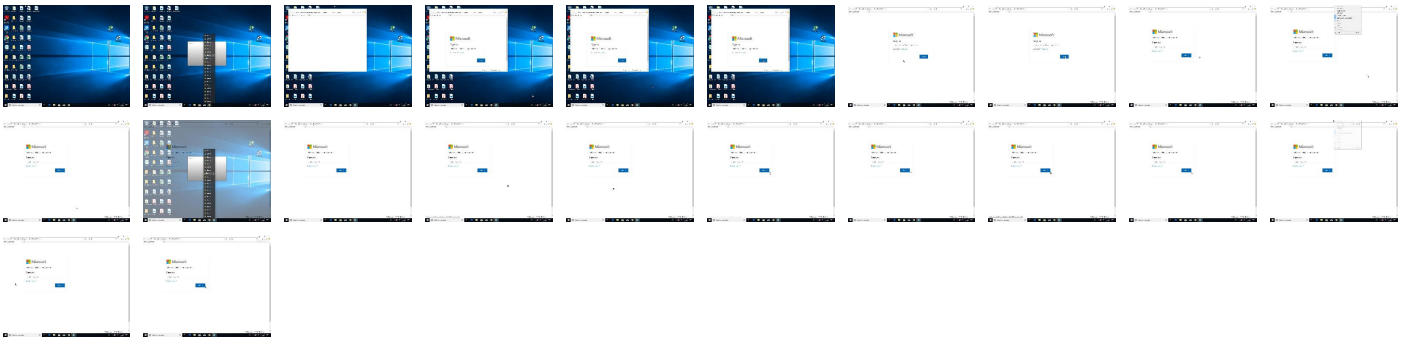
Behavior Graph

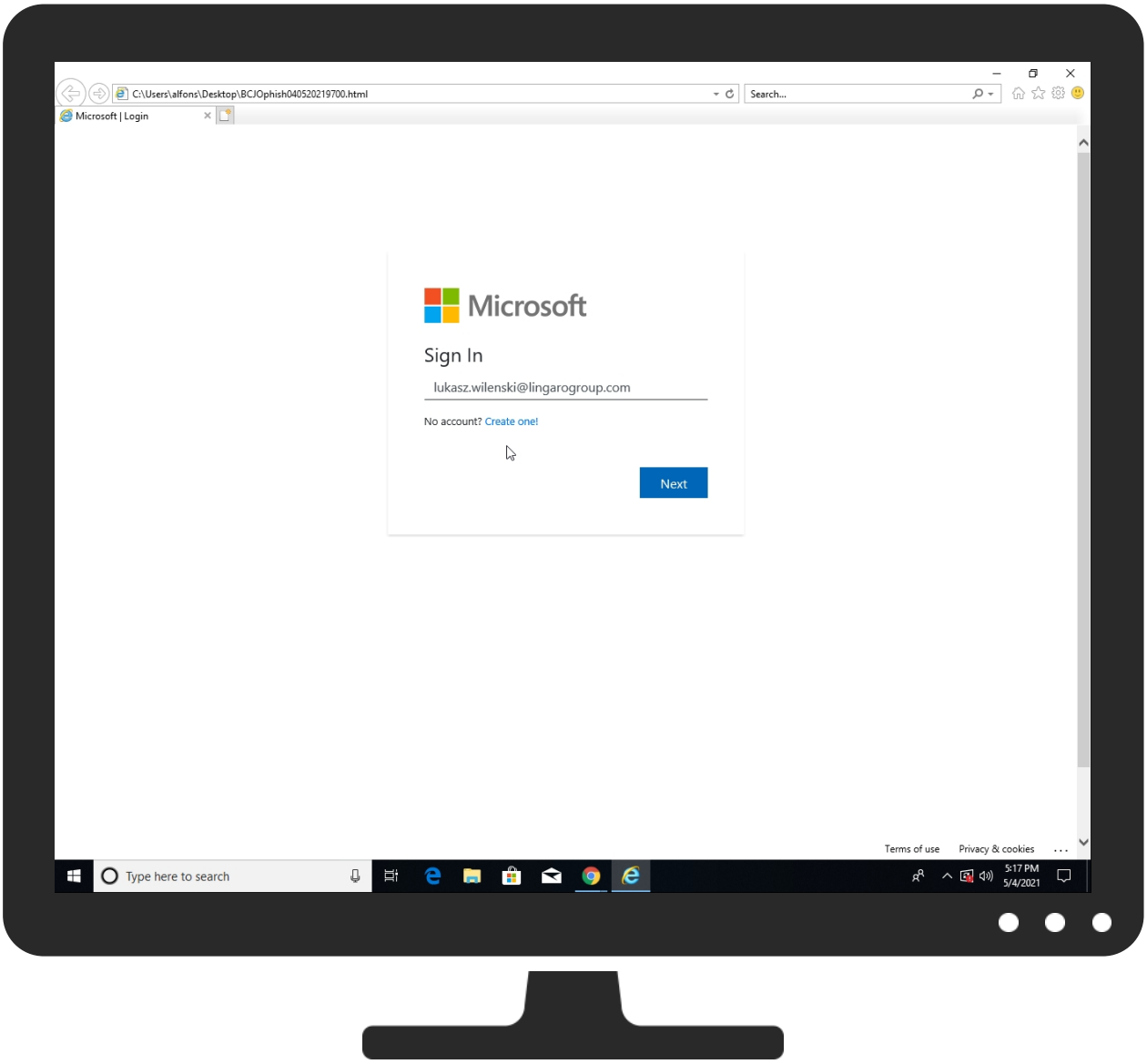


Screenshots

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
BCJOphish040520219700.html	3%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cs1100.wpc.omegacdn.net	0%	Virustotal		Browse
aadcdn.msftauth.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://promisesaplus.com/#point-75	0%	URL Reputation	safe	
http://https://promisesaplus.com/#point-75	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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-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-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://promisesaplus.com/#point-61	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-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-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://promisesaplus.com/#point-54	0%	URL Reputation	safe	
http://https://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	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	
http://https://promisesaplus.com/#point-48	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cs1100.wpc.omegacdn.net	152.199.23.37	true	false	• 0%, Virustotal, Browse	unknown
cdnjs.cloudflare.com	104.16.18.94	true	false		high
maxcdn.bootstrapcdn.com	104.18.11.207	true	false		high
fontawesome-cdn.fonticons.netdna-cdn.com	23.111.9.35	true	false		high
use.fontawesome.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
aadcdn.msftauth.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/BCJOphish040520219700.html	true		low

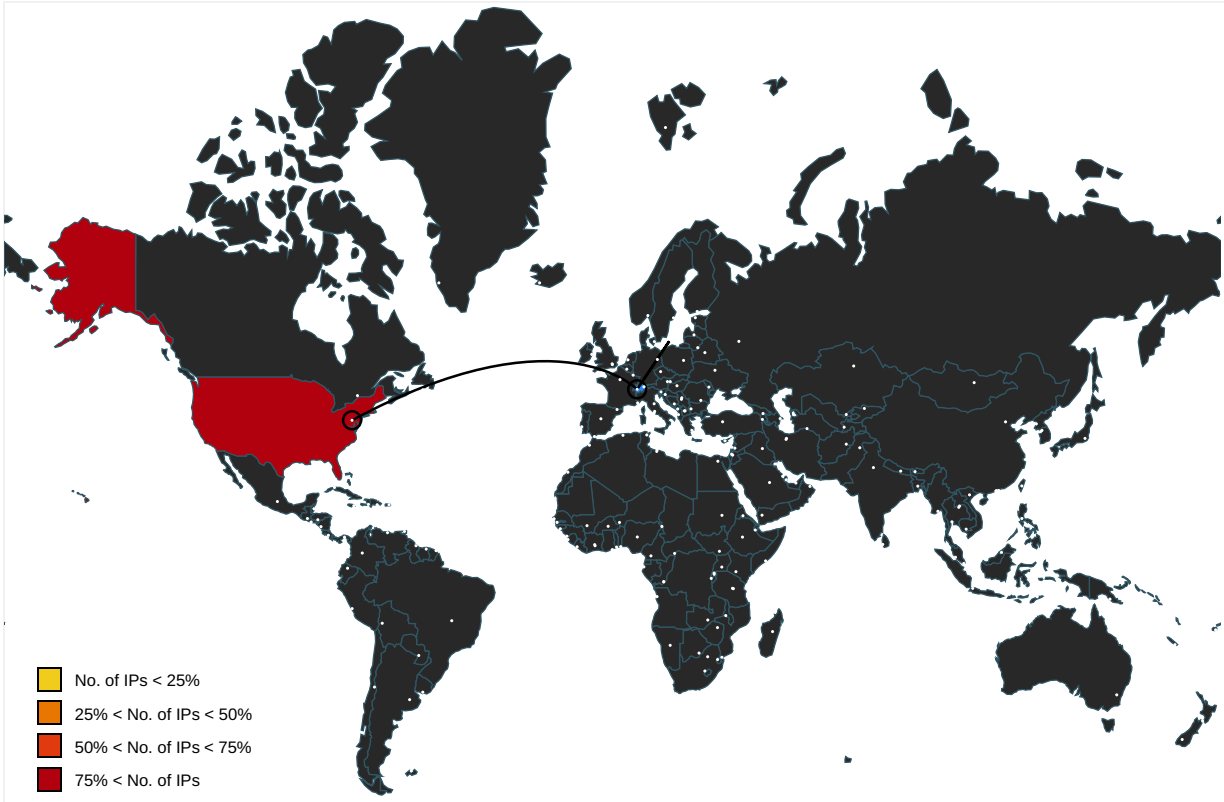
URLs from Memory and Binaries

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://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://web.archive.org/web/20100324014747/blindsignals.com/index.php/2009/07/jquery-delay/	jquery-3.3.1[1].js.2.dr	false		high
http://www.amazon.com/	msapplication.xml.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
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 • 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://www.twitter.com/	msapplication.xml5.1.dr	false		high
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	all[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	all[1].css.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://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 • URL Reputation: safe	unknown
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://https://promisesaplus.com/#point-61	jquery-3.3.1[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.nytimes.com/	msapplication.xml3.1.dr	false		high
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://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 • URL Reputation: safe	unknown
http://https://jsperf.com/getall-vs-sizzle/2	jquery-3.3.1[1].js.2.dr	false		high
http://https://promisesaplus.com/#point-57	jquery-3.3.1[1].js.2.dr	false	• URL Reputation: safe • 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 • 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://jquery.com/	jquery-3.3.1[1].js.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://getbootstrap.com)	bootstrap.min[1].js.2.dr, bootstrap.min[1].css.2.dr	false	• Avira URL Cloud: safe	low
http://www.youtube.com/	msapplication.xml7.1.dr	false		high
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://www.wikipedia.com/	msapplication.xml6.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://promisesaplus.com/#point-48	jquery-3.3.1[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.live.com/	msapplication.xml2.1.dr	false		high
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
104.18.11.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
23.111.9.35	fontawesome-cdn.fonticons.netdna-cdn.com	United States		33438	HIGHWINDS2US	false
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404066
Start date:	04.05.2021
Start time:	17:16:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	BCJOphish040520219700.html
Cookbook file name:	default.jbs
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:	23
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.phis.evad.winHTML@3/24@5/3
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .html
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 104.42.151.234, 131.253.33.200, 13.107.22.200, 93.184.220.29, 204.79.197.200, 13.107.21.200, 20.50.102.62, 52.147.198.201, 92.122.145.220, 88.221.62.148, 216.58.212.138, 69.16.175.42, 69.16.175.10, 142.250.184.234, 23.57.80.111, 152.199.19.161, 2.20.142.209, 2.20.142.210, 92.122.213.247, 92.122.213.194, 20.54.26.129 • TCP Packets have been reduced to 100 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, cds.s5x3j6q5.hwcdn.net, cs9.wac.phicdn.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.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, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, fonts.googleapis.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ajax.googleapis.com, ie9comview.vo.msecnd.net, ris-prod.trafficmanager.net, aadcdnoriginneu.azureedge.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, aadcdnoriginneu.ec.azureedge.net, dual-a-0001.dc-msedge.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.18.11.207	VM_04_28_22.HTM	Get hash	malicious	Browse	
	ATT50279.html	Get hash	malicious	Browse	
	afafd.htm	Get hash	malicious	Browse	
	agnesng@hanglung.comOnedrive.html	Get hash	malicious	Browse	
	FAXNIV0MSWBUP.htm	Get hash	malicious	Browse	
	VM_04_28_22.HTM	Get hash	malicious	Browse	
	Telex_Copy.html	Get hash	malicious	Browse	
	VM_04_28_22.HTM	Get hash	malicious	Browse	
	sean.adair@redwirespace.com1__redwirespace.com.htm	Get hash	malicious	Browse	
	#Ud83d#UdcccSusitarimas 43023pdf.html	Get hash	malicious	Browse	
	This computer is BLOCKED.html	Get hash	malicious	Browse	
	quote_Jroof166.htm	Get hash	malicious	Browse	
	Four.exe	Get hash	malicious	Browse	
	nicoleta.fagaras-DHL_TRACKING_1394942.html	Get hash	malicious	Browse	
	FARASIS.xlsx	Get hash	malicious	Browse	
	Friday, April 2nd, 2021, 20210402062906.8CE1B73ADE2A192C@compassionarmy.com.htm	Get hash	malicious	Browse	
	#U260f8284.HTML	Get hash	malicious	Browse	
	SOC_0#7198, INV#512 Via GoogleDocs gracechung.html	Get hash	malicious	Browse	
	vm583573758.htm	Get hash	malicious	Browse	
	vm583573758.htm	Get hash	malicious	Browse	
23.111.9.35	http://1minutemarketing.net/	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://www.visioncraftng.com/wp-admin/paclm/aTOOClFPHUo66z	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://giftbuying411.com/wp-includes/64358352543832/1xd5izerfl-00002/	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://www.00rcasey.sebelt.com/?VGH=cmNhc2V5QGNnc2luYy5jb20=	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://www.00dhoy.sebelt.com/?VGH=ZGhveUBjZ3NpbmMuY2E=	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://casehunter.com.br	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://alaksir.com/Scripts/TW6LJpx/	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://azetta.org/Manage-AbsaOnlineBanking-httpsib.absa.co.zaabsa-onlinelogin.jsp-Logon-AbsaExpress/~AbsaOnline%206-1.htm	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://bluetechprism.com/css/9zWF1bV_EzUmPytyJH5nFH6_sector/individual_n8i69k9xbanwxg_cnav2o/549242_o6OPbP/	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://magecart.net	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://https://protect-us.mimecast.com/s/uOyvC4xWr5FzL0Zyux-GUS?domain=t.yesware.com	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://https://telegra.ph/Notification-Checkpoin2020-07-12-2?fbclid=IwAR3CW1pVoB2bo4DBxz90-mn4s4lYZcDve12Q_Z31J30jf9ZtOUBqmdx9ZjE	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://bespokemerchandises.com	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://https://v.ht/5DsS	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://lavicentelopezcaferesto.com.ar/aquawestdubbo/prop/normal/	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://earningtipsbd.com/pn/Buy-Sell_Agreement_0786719_04272020.zip	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://https://onedrive.live.com/view.aspx?resid=1A4116533EC50398!1032&authkey=!AEhxS1cHS1VlwMY	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://www.8888scents.com/js/	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://sakshampharmaceuticals.com/wp-includes/wglyons.php?t=VHVlLCAxNCBBcHIgMjAyMCAyMjowMTMwMA==	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://rjsimmonscpa.com/colopeaks	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdnjs.cloudflare.com	ATT51630.htm	Get hash	malicious	Browse	• 104.16.18.94
	ATT50279.html	Get hash	malicious	Browse	• 104.16.19.94
	efax637637637.htm	Get hash	malicious	Browse	• 104.16.19.94
	Minebest686.html	Get hash	malicious	Browse	• 104.16.19.94
	afafd.htm	Get hash	malicious	Browse	• 104.16.18.94
	agnesng@hanglung.comOnedrive.html	Get hash	malicious	Browse	• 104.16.18.94
	FAXNIV0MSWBUP.htm	Get hash	malicious	Browse	• 104.16.18.94
	Telex_Copy.html	Get hash	malicious	Browse	• 104.16.18.94
	.htm	Get hash	malicious	Browse	• 104.16.19.94
	sean.adair@redwirespace.com1__redwirespace.com.htm	Get hash	malicious	Browse	• 104.16.19.94
	FAXQKJEZPA42S.htm	Get hash	malicious	Browse	• 104.16.18.94
	#Ud83d#Udcde.htm	Get hash	malicious	Browse	• 104.16.18.94
	ATT50064.html	Get hash	malicious	Browse	• 104.16.18.94
	Remittance_Advice_-7889x_pdf.HTml	Get hash	malicious	Browse	• 104.16.19.94
	Hanglung872.html	Get hash	malicious	Browse	• 104.16.18.94
	Final_report_202110.htm	Get hash	malicious	Browse	• 104.16.19.94
	775.htm	Get hash	malicious	Browse	• 104.16.18.94
	file.htm	Get hash	malicious	Browse	• 104.16.18.94
	file.htm	Get hash	malicious	Browse	• 104.16.18.94
	VoicePlayback (0129) for nerlyn.cama ibo .html	Get hash	malicious	Browse	• 104.16.18.94
maxcdn.bootstrapcdn.com	FAX_fake@fake.com_file.htm	Get hash	malicious	Browse	• 104.18.10.207
	ATT50279.html	Get hash	malicious	Browse	• 104.18.11.207
	Minebest686.html	Get hash	malicious	Browse	• 104.18.10.207
	afafd.htm	Get hash	malicious	Browse	• 104.18.11.207
	agnesng@hanglung.comOnedrive.html	Get hash	malicious	Browse	• 104.18.10.207
	FAXNIV0MSWBUP.htm	Get hash	malicious	Browse	• 104.18.11.207
	Telex_Copy.html	Get hash	malicious	Browse	• 104.18.11.207
	sean.adair@redwirespace.com1__redwirespace.com.htm	Get hash	malicious	Browse	• 104.18.11.207
	FAXQKJEZPA42S.htm	Get hash	malicious	Browse	• 104.18.10.207
	ATT50064.html	Get hash	malicious	Browse	• 104.18.10.207
	Hanglung872.html	Get hash	malicious	Browse	• 104.18.10.207
	Final_report_202110.htm	Get hash	malicious	Browse	• 104.18.10.207
	ATT55873.html	Get hash	malicious	Browse	• 104.18.10.207
	Notification_test.htm	Get hash	malicious	Browse	• 104.18.10.207
	This computer is BLOCKED.html	Get hash	malicious	Browse	• 104.18.11.207
	quote_Jroof166.htm	Get hash	malicious	Browse	• 104.18.11.207
	Voicemail sound attachment.HTM	Get hash	malicious	Browse	• 104.18.10.207
	Four.exe	Get hash	malicious	Browse	• 104.18.11.207
	nicoleta.fagaras-DHL_TRACKING_1394942.html	Get hash	malicious	Browse	• 104.18.11.207
	FARASIS.xlsx	Get hash	malicious	Browse	• 104.18.11.207
cs1100.wpc.omegacdn.net	Master Fund Distributions.pdf.html	Get hash	malicious	Browse	• 152.199.23.37
	efax637637637.htm	Get hash	malicious	Browse	• 152.199.23.37
	Minebest686.html	Get hash	malicious	Browse	• 152.199.23.37
	afafd.htm	Get hash	malicious	Browse	• 152.199.23.37
	efax663663663.htm	Get hash	malicious	Browse	• 152.199.23.37
	sean.adair@redwirespace.com1__redwirespace.com.htm	Get hash	malicious	Browse	• 152.199.23.37
	New%20order%20contract.html	Get hash	malicious	Browse	• 152.199.23.37
	Hanglung872.html	Get hash	malicious	Browse	• 152.199.23.37
	775.htm	Get hash	malicious	Browse	• 152.199.23.37
	VoicePlayback (0129) for nerlyn.cama ibo .html	Get hash	malicious	Browse	• 152.199.23.37
	VoicePlayback (0151) for norgaardr sacda .html	Get hash	malicious	Browse	• 152.199.23.37
	VoicePlayback (0151) for norgaardr sacda .html	Get hash	malicious	Browse	• 152.199.23.37
	E3761 80251728_03312021.html	Get hash	malicious	Browse	• 152.199.23.37
	AttachementHtm.html	Get hash	malicious	Browse	• 152.199.23.37
	VoicePlayback (0155) for umclune myumanitoba .html	Get hash	malicious	Browse	• 152.199.23.37

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	1-page-fax-from-+33822822.htm	Get hash	malicious	Browse	• 152.199.23.37
	VoicePlayback (0195) for turnerrd pellamw .html	Get hash	malicious	Browse	• 152.199.23.37
	VoicePlayback (0162) for jonathan.siberry wyg .html	Get hash	malicious	Browse	• 152.199.23.37
	VoicePlayback (0129) for paul.mathias brewin .html	Get hash	malicious	Browse	• 152.199.23.37
	VoicePlayback (01_70) for t .html	Get hash	malicious	Browse	• 152.199.23.37

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HIGHWINDS2US	Pro-Forma invoicve.html	Get hash	malicious	Browse	• 23.111.9.35
	Minebest686.html	Get hash	malicious	Browse	• 23.111.9.35
	afafd.htm	Get hash	malicious	Browse	• 23.111.9.35
	sean.adair@redwirespace.com1__redwirespace.com.htm	Get hash	malicious	Browse	• 23.111.9.35
	Hanglung872.html	Get hash	malicious	Browse	• 23.111.9.35
	wyg.com Leave Policy Thursday, April 15th, 2021.htm	Get hash	malicious	Browse	• 23.111.9.35
	6BympvyPAv.exe	Get hash	malicious	Browse	• 23.111.8.154
	Three.exe	Get hash	malicious	Browse	• 23.111.8.154
	Four.exe	Get hash	malicious	Browse	• 23.111.8.154
	Six.exe	Get hash	malicious	Browse	• 23.111.8.154
	One.exe	Get hash	malicious	Browse	• 23.111.8.154
	Five.exe	Get hash	malicious	Browse	• 23.111.8.154
	Two.exe	Get hash	malicious	Browse	• 23.111.8.154
	FARASIS.xlsx	Get hash	malicious	Browse	• 23.111.9.35
	FARASIS.xlsx	Get hash	malicious	Browse	• 23.111.9.35
	Friday, April 2nd, 2021, 20210402062906.8CE1B73ADE2A192C@compassionarmy.com.htm	Get hash	malicious	Browse	• 23.111.9.35
	covid.exe	Get hash	malicious	Browse	• 23.111.9.35
	scan-100218.docm	Get hash	malicious	Browse	• 108.161.187.71
	SOC_0#7198, INV#512 Via GoogleDocs gracechung.html	Get hash	malicious	Browse	• 23.111.9.35
	SecuriteInfo.com.Variant.Bulz.385171.11582.exe	Get hash	malicious	Browse	• 23.111.8.154
CLOUDFLARENETUS	5.exe	Get hash	malicious	Browse	• 104.17.62.50
	Payment.xlsx	Get hash	malicious	Browse	• 66.235.200.147
	pasteBorder.dll	Get hash	malicious	Browse	• 104.20.184.68
	Indeed_Update_File.html	Get hash	malicious	Browse	• 104.16.169.131
	AgTxGlXxu9.exe	Get hash	malicious	Browse	• 104.22.18.188
	08917506_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.227.38.74
	f97e137e_by_Libranalysis.exe	Get hash	malicious	Browse	• 162.159.134.233
	heUGqZXAJv.exe	Get hash	malicious	Browse	• 104.21.33.129
	6ccd0000.bilper.dll	Get hash	malicious	Browse	• 104.20.184.68
	6bae0000.bilper.dll	Get hash	malicious	Browse	• 104.20.184.68
	6c130000.da.dll	Get hash	malicious	Browse	• 104.20.184.68
	gNRclqPGkE.exe	Get hash	malicious	Browse	• 104.21.21.140
	Halkbank_Ekstre_20210504_080203_744632.exe	Get hash	malicious	Browse	• 104.21.19.200
	3QHQELjQ1s.exe	Get hash	malicious	Browse	• 104.21.21.140
	EXPEDIENTE CSJVAA 20-43.js	Get hash	malicious	Browse	• 104.26.5.223
	valuePasteList.dll	Get hash	malicious	Browse	• 104.20.184.68
	Payment Invoice.pdf.exe	Get hash	malicious	Browse	• 104.23.98.190
	oiY37pLlj7.exe	Get hash	malicious	Browse	• 172.67.208.174
	MV RED SEA.docx	Get hash	malicious	Browse	• 172.67.8.238
	MV RED SEA.docx	Get hash	malicious	Browse	• 104.22.0.232

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	pasteBorder.dll	Get hash	malicious	Browse	• 104.18.11.207 • 23.111.9.35 • 104.16.18.94
	Indeed_Update_File.html	Get hash	malicious	Browse	• 104.18.11.207 • 23.111.9.35 • 104.16.18.94
	#U266b VM-Tunes-Playback.htm	Get hash	malicious	Browse	• 104.18.11.207 • 23.111.9.35 • 104.16.18.94
	presentation.jar	Get hash	malicious	Browse	• 104.18.11.207 • 23.111.9.35 • 104.16.18.94

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	presentation.jar	Get hash	malicious	Browse	• 104.18.11.207 • 23.111.9.35 • 104.16.18.94
	ausgangsrechnung@condor.com_ProjectDocument.HTML	Get hash	malicious	Browse	• 104.18.11.207 • 23.111.9.35 • 104.16.18.94
	6ccd0000.bilper.dll	Get hash	malicious	Browse	• 104.18.11.207 • 23.111.9.35 • 104.16.18.94
	6bae0000.bilper.dll	Get hash	malicious	Browse	• 104.18.11.207 • 23.111.9.35 • 104.16.18.94
	6c130000.da.dll	Get hash	malicious	Browse	• 104.18.11.207 • 23.111.9.35 • 104.16.18.94
	609110f2d14a6.dll	Get hash	malicious	Browse	• 104.18.11.207 • 23.111.9.35 • 104.16.18.94
	valuePasteList.dll	Get hash	malicious	Browse	• 104.18.11.207 • 23.111.9.35 • 104.16.18.94
	3ZtdRsbjxo.exe	Get hash	malicious	Browse	• 104.18.11.207 • 23.111.9.35 • 104.16.18.94
	Pro-Forma invoicve.html	Get hash	malicious	Browse	• 104.18.11.207 • 23.111.9.35 • 104.16.18.94
	#U260e#Ufe0fAUDIO-2020-05-26-18-51-m4a_MP4messages_2202-434.htm	Get hash	malicious	Browse	• 104.18.11.207 • 23.111.9.35 • 104.16.18.94
	6a9b0000.da.dll	Get hash	malicious	Browse	• 104.18.11.207 • 23.111.9.35 • 104.16.18.94
	6ba90000.da.dll	Get hash	malicious	Browse	• 104.18.11.207 • 23.111.9.35 • 104.16.18.94
	s.dll	Get hash	malicious	Browse	• 104.18.11.207 • 23.111.9.35 • 104.16.18.94
	setup-lightshot.exe	Get hash	malicious	Browse	• 104.18.11.207 • 23.111.9.35 • 104.16.18.94
	s.dll	Get hash	malicious	Browse	• 104.18.11.207 • 23.111.9.35 • 104.16.18.94
	EAGLE.dll	Get hash	malicious	Browse	• 104.18.11.207 • 23.111.9.35 • 104.16.18.94

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{46CC5D3F-AD37-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	36440
Entropy (8bit):	1.8975785966894385
Encrypted:	false
SSDEEP:	96:rlZKZ42wLWbtdbfnmNKM4VFqq/Qyxf9ml6r0A62HK:rlZKZ42EWbtBfnFM7rsf98rGD
MD5:	8DFED0CE7C083C2CEB4C5E662253D564
SHA1:	123D405404A24BCAAF8F4E3D3947ECF190104636
SHA-256:	2EF90EF5E969FDC4DF39585AF8813E8AF713E543B472768A7C355BBC3F36E7E7
SHA-512:	93337E1BCD19481D046C49CBD8189EE57011226891011907ABC1ABF983703ED7D5633BAC9B2C8927311F4D4A37EF201DFA0F9356D9400A8C4E25E1D139E58DA
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{46CC5D3F-AD37-11EB-90E5-ECF4BB570DC9}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{46CC5D41-AD37-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30636
Entropy (8bit):	1.967050071720412
Encrypted:	false
SSDEEP:	96:r7ZIQI6CBSrzjE852EemqWEpME0+XqNaD8qNFqbcqNirfFr4G7tEFEh:r7ZIQI6CkXjF2NWSMWXx8jcfCFEh
MD5:	7355EF013ED548BA167FDD0AD39CFA5E
SHA1:	4998A4E1C25FDB996A905D56D81E0C2A85EB9625
SHA-256:	78294C9B262E6A5FF4B9B980C51D7DAE744CD86FB85FD1A6C6FB87EE4DF4EBB8
SHA-512:	11443CE66966F243464068B1C7F4C963542F814DB74F6149F318E20CBDA31B860CDB638FDE2C0A5FBE3E727E95174AFCF2EDB7D970F6C87096AF25C721D2014
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\{4D6DE73B-AD37-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5663913909098688
Encrypted:	false
SSDEEP:	48:IwUGcprRGwpaGG4pQCGrapbSQZGQpKaG7HpRYaTGIpG:rIZLQ26EBSQzA1TYeA
MD5:	057FE73D363D2859B0A7C111D33BEF43
SHA1:	DF79F622926CD8699E746B4876F3F09E0BCE627D
SHA-256:	9BF19F57D05B73EBC14B51CE1A5859FF5B949EA6FA8240AA3A05DA47E3631C38
SHA-512:	E7338A263B82EFCD90D2FA2CB501437AD6BABF72F0A85603FB21F89C17939EFFCC3E3C104AE29DF5F5CE227E17980D75ABDC152F52A73F40646A3DE83486AB 0
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	657
Entropy (8bit):	5.103165301730317
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEQhphQnWimI002EtM3MHdNMNxOEQhphQnWimI00ONVbkEtMb:2d6NxOeSZHKd6NxOeSZ7Qb
MD5:	8C49D43D6DA504D17110C79B022F6A85
SHA1:	C306D3D7B79C3CD29FEDC361A76049CF9BAB6C4B
SHA-256:	2EADF8848D25022F3E91D934CE66A2AFCF42B52521CFB2FD8211026BF67F440B
SHA-512:	C31FCAC1D7E40C7046F1DBF754A115F17C6DD5F2B80841174E0E12EC9527BA495F6A3BC1C1CEF03347FF0025907D39CDBFFF5EB09D2F8540424C2188D6323C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x1e6b26e8,0x01d74144</date><accdate>0x1e6b26e8,0x01d74144</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x1e6b26e8,0x01d74144</date><accdate>0x1e6b26e8,0x01d74144</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	654
Entropy (8bit):	5.084076439075371
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2klxfnWimI002EtM3MHdNMNxe2klxfnWimI00ONkak6EtMb:2d6NxrYxfSZHKd6NxrYxfSZ72a7b
MD5:	5999C08D81197A39BE0775983D28B435
SHA1:	5879231458378695F75004A40B5623CF7716E039
SHA-256:	DC86D0EAAA514E24BEB194A660E42E7B89309B3088D38231897B2800270FEB7A
SHA-512:	348EB0FCA122AC343453F04D8ECFF3DA50C2F01225F8F5EC02212ABC85CB20FE0179A7B85C983FE94F0EB11D235DBEFCEDC603C6685645301DE778E5029177
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x1e5f3b0a,0x01d74144</date><accdate>0x1e5f3b0a,0x01d74144</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x1e5f3b0a,0x01d74144</date><accdate>0x1e5f3b0a,0x01d74144</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.12315900980938
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLQhphQnWimI002EtM3MHdNMNxvLQhphQnWimI00ONmZEtMb:2d6Nxv3SZHKd6Nxv3SZ7Ub
MD5:	1AD1E39E1035E28BD008B79F867A75CF
SHA1:	D448984FF83F70E0EA9CE29653A4E3775B122468
SHA-256:	A264FC89B3257331BEFFC300BE51D5FC1AC0FEE5B8FAC1CBF1B1A2424D13B27F
SHA-512:	8AEDFAB1C2C48D29244A1948666C5671A7019F90EFBBC5DFF790FE55CFDD866F942505D0A556089EA8EB6F2B75864AA33ECC667CCC8BE14A470FAD9759CFA864
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x1e6b26e8,0x01d74144</date><accdate>0x1e6b26e8,0x01d74144</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x1e6b26e8,0x01d74144</date><accdate>0x1e6b26e8,0x01d74144</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	648
Entropy (8bit):	5.128223958234596
Encrypted:	false
SSDEEP:	12:TMHdNMNxiQTkTfnWimI002EtM3MHdNMNxiQTkTfnWimI00ONd5EtMb:2d6NxlefSZHKd6NxlefSZ7njb
MD5:	798081775820D445EFB8BF62F9E3EB79
SHA1:	0FF74E9F4935CFA5EDDD5AF88D0DA6D145DD7316
SHA-256:	CB78A391B1A6F80DD7E5A3B26636C6C6FD61317E8941895B7B1FAE3DE4FBD853
SHA-512:	187C2DD00FF4222857BDF43CB86694C04465BB0C025BB0C03CC9DCEED480866DD08C4E617701DD5810DF5C4E812DD2B972F0D513022D628CAE23A849F0F0C1D
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x1e666235,0x01d74144</date><accdate>0x1e666235,0x01d74144</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x1e666235,0x01d74144</date><accdate>0x1e666235,0x01d74144</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	657
Entropy (8bit):	5.12814929942092

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwQ0PnWimI002EtM3MHdNMNxhGwQ0PnWimI00ON8K075EtMb:2d6NxQ4SZHKd6NxQ4SZ7uKajb
MD5:	BC17F081D88E97F39947F57E63A244A0
SHA1:	87D24F4CFE29680732EDA28872C1CE91E7187B39
SHA-256:	F3488CAC77524144E5BF11DD4E51E1821BEC6A6F59E50C9C1B9BD2844C1317ED
SHA-512:	95D3E2136EE2A68E22C2880C152581AB4D5ECAE37DBE79E1BF57DFDEE82A20C16D5E158B0504B770ECE7BE1E75980CD1249C8415E49AC4389124729C86A381 3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x1e6d8903,0x01d74144</date> accdate>0x1e6d8903,0x01d74144</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x1e6d8903,0x01d74144</date><accdate>0 x1e6d8903,0x01d74144</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	654
Entropy (8bit):	5.088115186843123
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nQNEnWimI002EtM3MHdNMNx0nQNEnWimI00ONxEtMb:2d6Nx0LSZHKd6Nx0LSZ7Vb
MD5:	FE9117D6678047E9A08B9F73D2F677DD
SHA1:	40AC03156CDF1C5026C5BD0CBA5CD37E649DCD14
SHA-256:	2F0D4341A6C46B934B6F53F2DA891081B3AE2E35D514E1EEE5154BC801626734
SHA-512:	1663A7A5D2230587C7AB68F15AD78F9B08EB283F235BAD0EC78101B669AB236DB5A2B527B9C07DF8FAC2B6230FB820E596C84E335F5300ABF0977D6B542BB7A 1
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x1e68c49a,0x01d74144</date><a ccdate>0x1e68c49a,0x01d74144</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x1e68c49a,0x01d74144</date><accdate>0x1 e68c49a,0x01d74144</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	657
Entropy (8bit):	5.154419854557322
Encrypted:	false
SSDEEP:	12:TMHdNMNxxQTkTfnWimI002EtM3MHdNMNxxQTkEnWimI00ON6Kq5EtMb:2d6NxIefSZHKd6NxIDSZ7ub
MD5:	B086A85EB6991733BA5A250FD169F7E5
SHA1:	B15531F0C2AFACF0FBB5A4C73E8F36F1D54034EF
SHA-256:	07AA052ED06942D68F4E83FE141DDE8ABD003AD8BE3389F480EB8980205BE8E9
SHA-512:	4F98A6D684B5CAE7A0A1344325AF811480F13FE3399FD8793B9280F8B1094ADBA5593CB1EF9FD6EA2B9445E302FCEFB3D85DD694EAFEB5C2DB9BDFBD5C672(E5
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x1e666235,0x01d74144</date> accdate>0x1e666235,0x01d74144</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x1e666235,0x01d74144</date><accdate>0 x1e68c49a,0x01d74144</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	660
Entropy (8bit):	5.0999508137014695
Encrypted:	false
SSDEEP:	12:TMHdNMNxcQSNnWimI002EtM3MHdNMNxcQSNnWimI00ONVEtMb:2d6NxgSZHKd6NxgSZ71b
MD5:	E6CBC064E2C69E9ED9F56B4FB7610ADE

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
SHA1:	6F673337A709F0337A5B9E425EE29D2F47B817DB
SHA-256:	7E26C0ECA76B725F9674717D2190FC96BB60FA5B415B04EB76345A2425939970
SHA-512:	A75D46692E9F00A594AF8E9A371BE01710BF7ADC120C4B86183BE2CE7B1FCEEB7B32445A50346814D7E17A0A05EBF1C0E308032C94A4AFCC092507FCC5E4F4 6
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x1e63ffc2,0x01d74144</date> <accdate>0x1e63ffc2,0x01d74144</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x1e63ffc2,0x01d74144</date><accdate >0x1e63ffc2,0x01d74144</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	654
Entropy (8bit):	5.094061998262943
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnQSNnWimI002EtM3MHdNMNxfnQSTfnWimI00ONe5EtMb:2d6NxRSZHKd6NxffSZ7Ejb
MD5:	AFA63780BB64123E71B86088B2EB6B1D
SHA1:	C4B690938BBC914F762EBC1DAA7C5EF7A104F688
SHA-256:	89375232A8EA1A8A4566AC2745A3D56FCCC4831BFCEB0AF9003D10D87A1C3F47
SHA-512:	0B4A7E5BFBF724BE4B00F8E17B35AEA1B8B4B7F5C55B525B73C36DE0B14CB27E343E6BC8AA8357E7AD1E3F6C75BAB184CBA2E8E6BE4DE4DA24BFAF01BAC F58D5
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x1e63ffc2,0x01d74144</date><a ccdate>0x1e63ffc2,0x01d74144</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x1e63ffc2,0x01d74144</date><accdate>0x1 e666235,0x01d74144</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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:	moderate, very likely benign file
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).pare ntNode.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\4PB7FJMT\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\jquery-3.3.1[1].js	
SHA-512:	E525248B09A6FB4022244682892E67BBF64A3E875EB889DB43B0A24AB4A75077B5D5D26943CA382750D4FEBC3883193F3BE581A4660065B6FC7B5EC20C4A044B
Malicious:	false
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\B87Z87FM\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
Malicious:	false
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"),require("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.prototype.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\B87Z87FM\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:	9EA12CC277C9858524083FEBBE1A3E61FDECE5268F63B14C9FFAFE29396C7CCDB3B07BE10E829936BCCD8F3B9E39DCFA6BC4316F189E4CEA914F1D06916DB66B
Malicious:	false
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/tss0ApVBdCYD5Q7hcxTE1ArZ0bbwiXo.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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:	0D40BCCAA59FEDECF7243D63B33C42592541D0330FEFC78EC81A4C6B9689922D5B211011CA4BE23AE22621CCE4C658F52A1552C92D7AC3615241EB640F8514B
Malicious:	false
IE Cache URL:	http://https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\jquery.min[1].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\Microsoft\Windows\INetCache\IE\NUEPGTR9\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
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.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}html{font-family:sans

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.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\PEJLKQA8\all[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	54641
Entropy (8bit):	4.712564291864468
Encrypted:	false
SSDEEP:	768:SuV31Uz1RPq4NvvU63HJYkQCZ/WMQyjJKp7CzsGnQzU:SuczrC4NnzHSBCkgu7cs1w
MD5:	251D28BD755F5269A4531DF8A81D5664
SHA1:	C0F035B41B23C6E8FAB735F618AA3CFF0897B4F9
SHA-256:	AFDC6BF2DE981FFD7D370B76F44E7580572F197EFBE214B9CFA4005D189D8EAE
SHA-512:	8111F411C21C6011644139DBA4EF24D1696C0F6D31E55CE384E0353A0F3E65402170C502BDDF803C3DF9149C371B31C03F77BE98FDBC61C0C9C55AFBE399681
Malicious:	false
IE Cache URL:	http://https://use.fontawesome.com/releases/v5.7.0/css/all.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\all[1].css	
Preview:	/*!. * Font Awesome Free 5.7.0 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,.fal,.far,.fas{-moz-osx-font-smoothing:grayscale;-webkit-font-smoothing:antialiased;display:inline-block;font-style:normal;font-variant: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;position:absolute;text-align:center;width:2em;line-height:inherit}.fa-border{border:.08em solid #eee;border-radius:.1em;padding:.2em .25em .15em}.fa-pull-lef

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\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:	53A2B560B20551672FBB0E6E72632D4FD1C7E2DD2ECF7337EBAAAB179CB8BE7C87E9D803CE7765706BC7FCBCF993C34587CD1237DE5A279AEA19911D69067E65
Malicious:	false
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\Temp\~DF5CF08E3835D7EFC4.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40305
Entropy (8bit):	0.6100586821911878
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+EeEYESEbEIE7qNpqN6rfFr4G7tE:kBqoxKAuqR+fBjKRmMLC
MD5:	1D468CB80A84EDD163B63257875A29EB
SHA1:	20DE86E41A47BC5DDECB5599AB49A025E83E4D0C
SHA-256:	F694496BB1C3E8B2849602F8B910D435BEFE6A3864A8B1080D2BBF59305AB908
SHA-512:	9E1A0A376DF7AB6DC4EA83580EBE9FC061DC1EAE9A79A779C4D0B0680031850E7F456910DD7D0AE93426F140E32518D89072FA8ACF558892395061EA8FF6671A
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFDB291DF1B61879C7.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13125
Entropy (8bit):	0.5446838522127703
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loC9loy9lWqKomD:kBqoItrqjE
MD5:	5CD43DE47E60E33406BEC0A35E04CAD3
SHA1:	F6D331B84895CFD8F9AD6478CF39B46F22E123AE
SHA-256:	B5EF1887054EF72C5036248D75DB1A10084A9F35E6F6B20E6CBDEA04AB3EFA55
SHA-512:	22D688D0CF072D6A37A15776A4892DC23D0149C3B3FFBB8F9CFA556D3D766209A04D3B96CF02C5BC6DD44F036D09B85BBD24C6E98E0C0EA245B533FEF46CB29
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFFAFD318CFED77F8E.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.3121039228538688
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAgg:kBqoxxJhHWSVSEab
MD5:	6ABBB10EDEAE22AF7D21BDE1A825CE94
SHA1:	D34032A00F89F4204EF6B60DDE85F82E1AAD8CE1
SHA-256:	CEC9F79860727C551FA55C82A7CF233645FC903A5CA7F7E2EBD07FB383C091AA
SHA-512:	982CB539FDA70A6E5D0806F0209C69A7178FBD693D065D38A593D3AD081022569616B979D9510D05E96497C8C3230D45C10954FF9DACC53E0CE7D54776D6DDD
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

General

File type:	HTML document, ASCII text, with very long lines
Entropy (8bit):	3.355721431904543
TrID:	
File name:	BCJOphish040520219700.html
File size:	70638
MD5:	724cbfa451d94bd57998a09c9956fcab
SHA1:	d39571159adc5da02c99350b21a843a80b57233b
SHA256:	713e7b41006aea09ddf4786a43d386b8e6338555d47e97 b4a2726af59956e167
SHA512:	1a5a220f6dcaf7470bf8a8e66feb647eea8ff550d1b75f04c 5137dc5763e16721e38a0a941a89b8d45d6ec00a98bbcf c5eaec1541986eb69f556b7ee8e625997
SSDEEP:	768:GU4RQXCfYberLbJGdUPt7pCfYberLbJGdUPt7iiB D/T6a:fglg5
File Content Preview:	<script language="javascript">........document.write(unescape('%0a%3c%21%64%6f%63%74%79%70%65%20%68%74%6d%6c%3e%0a%3c%68%74%6d%6c%20%6c%61%6e%67%3d%22%69%74%22%3e%0a%3c%68%65%61%64%3e%0a%3c%73%63%72%69%70%74%20%74%79%70%65%3d%22%74%65%78%74%2f%6a%61%76%61

File Icon

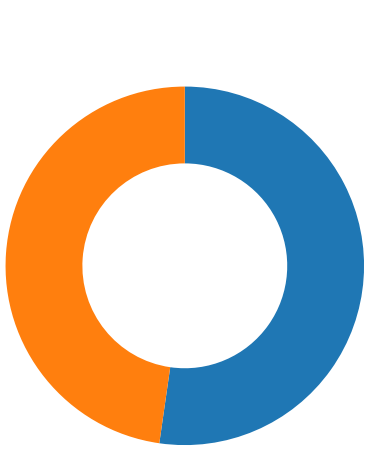
Icon Hash:	f8c89c9a9a998cb8

Network Behavior

Network Port Distribution

Total Packets: 88

- 53 (DNS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 17:17:33.888235092 CEST	49711	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:33.889281034 CEST	49712	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:33.940841913 CEST	443	49711	104.18.11.207	192.168.2.5
May 4, 2021 17:17:33.941003084 CEST	49711	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:33.941920996 CEST	49711	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:33.942097902 CEST	443	49712	104.18.11.207	192.168.2.5
May 4, 2021 17:17:33.942229033 CEST	49712	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:33.942946911 CEST	49712	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:33.993510962 CEST	443	49711	104.18.11.207	192.168.2.5
May 4, 2021 17:17:33.994561911 CEST	443	49712	104.18.11.207	192.168.2.5
May 4, 2021 17:17:33.994738102 CEST	443	49712	104.18.11.207	192.168.2.5
May 4, 2021 17:17:33.994791031 CEST	443	49712	104.18.11.207	192.168.2.5
May 4, 2021 17:17:33.994844913 CEST	49712	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:33.994885921 CEST	49712	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:34.002806902 CEST	443	49711	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.002868891 CEST	443	49711	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.002939939 CEST	49711	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:34.002990007 CEST	49711	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:34.016500950 CEST	49711	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:34.017101049 CEST	49711	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:34.017301083 CEST	49711	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:34.019836903 CEST	49712	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:34.020648003 CEST	49712	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:34.068322897 CEST	443	49711	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.068409920 CEST	443	49711	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.068914890 CEST	443	49711	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.069767952 CEST	443	49711	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.069868088 CEST	49711	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:34.070436001 CEST	443	49711	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.070514917 CEST	49711	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:34.070880890 CEST	443	49712	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.070947886 CEST	49711	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:34.071046114 CEST	443	49712	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.071118116 CEST	49712	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:34.071295023 CEST	443	49712	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.071355104 CEST	49712	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:34.071773052 CEST	443	49712	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.071793079 CEST	443	49712	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.071867943 CEST	49712	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:34.072132111 CEST	49712	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:34.124732971 CEST	443	49711	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.124756098 CEST	443	49712	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.128181934 CEST	443	49711	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.128206968 CEST	443	49711	104.18.11.207	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 17:17:34.128218889 CEST	443	49711	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.128226995 CEST	443	49711	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.128242016 CEST	443	49711	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.128254890 CEST	443	49711	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.128365040 CEST	49711	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:34.128427029 CEST	49711	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:34.129410982 CEST	443	49711	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.129442930 CEST	443	49711	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.129550934 CEST	49711	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:34.130587101 CEST	443	49711	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.130613089 CEST	443	49711	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.130712032 CEST	49711	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:34.131824017 CEST	443	49711	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.131848097 CEST	443	49711	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.131934881 CEST	49711	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:34.132983923 CEST	443	49711	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.133007050 CEST	443	49711	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.133106947 CEST	49711	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:34.134180069 CEST	443	49711	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.134205103 CEST	443	49711	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.134336948 CEST	49711	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:34.135376930 CEST	443	49711	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.135402918 CEST	443	49711	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.135468006 CEST	49711	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:34.135524035 CEST	49711	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:34.136621952 CEST	443	49711	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.136641979 CEST	443	49711	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.136734009 CEST	49711	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:34.137851000 CEST	443	49711	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.137871027 CEST	443	49711	104.18.11.207	192.168.2.5
May 4, 2021 17:17:34.137968063 CEST	49711	443	192.168.2.5	104.18.11.207
May 4, 2021 17:17:34.725748062 CEST	49715	443	192.168.2.5	23.111.9.35
May 4, 2021 17:17:34.726716995 CEST	49716	443	192.168.2.5	23.111.9.35
May 4, 2021 17:17:34.772289038 CEST	443	49715	23.111.9.35	192.168.2.5
May 4, 2021 17:17:34.772407055 CEST	49715	443	192.168.2.5	23.111.9.35
May 4, 2021 17:17:34.773026943 CEST	443	49716	23.111.9.35	192.168.2.5
May 4, 2021 17:17:34.773111105 CEST	49716	443	192.168.2.5	23.111.9.35
May 4, 2021 17:17:35.137341022 CEST	49715	443	192.168.2.5	23.111.9.35
May 4, 2021 17:17:35.169694901 CEST	49716	443	192.168.2.5	23.111.9.35
May 4, 2021 17:17:35.185164928 CEST	443	49715	23.111.9.35	192.168.2.5
May 4, 2021 17:17:35.187714100 CEST	443	49715	23.111.9.35	192.168.2.5
May 4, 2021 17:17:35.187750101 CEST	443	49715	23.111.9.35	192.168.2.5
May 4, 2021 17:17:35.187772989 CEST	443	49715	23.111.9.35	192.168.2.5
May 4, 2021 17:17:35.187793016 CEST	443	49715	23.111.9.35	192.168.2.5
May 4, 2021 17:17:35.187865019 CEST	49715	443	192.168.2.5	23.111.9.35
May 4, 2021 17:17:35.188555002 CEST	49715	443	192.168.2.5	23.111.9.35
May 4, 2021 17:17:35.204070091 CEST	49715	443	192.168.2.5	23.111.9.35
May 4, 2021 17:17:35.204134941 CEST	49715	443	192.168.2.5	23.111.9.35
May 4, 2021 17:17:35.205528021 CEST	49715	443	192.168.2.5	23.111.9.35
May 4, 2021 17:17:35.216139078 CEST	443	49716	23.111.9.35	192.168.2.5
May 4, 2021 17:17:35.217027903 CEST	443	49716	23.111.9.35	192.168.2.5
May 4, 2021 17:17:35.217078924 CEST	443	49716	23.111.9.35	192.168.2.5
May 4, 2021 17:17:35.217097998 CEST	443	49716	23.111.9.35	192.168.2.5
May 4, 2021 17:17:35.217112064 CEST	49716	443	192.168.2.5	23.111.9.35
May 4, 2021 17:17:35.217116117 CEST	443	49716	23.111.9.35	192.168.2.5
May 4, 2021 17:17:35.217135906 CEST	49716	443	192.168.2.5	23.111.9.35

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 17:17:22.081626892 CEST	52212	53	192.168.2.5	8.8.8.8
May 4, 2021 17:17:22.140546083 CEST	53	52212	8.8.8.8	192.168.2.5
May 4, 2021 17:17:22.327716112 CEST	54302	53	192.168.2.5	8.8.8.8
May 4, 2021 17:17:22.388881922 CEST	53	54302	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 17:17:22.604229927 CEST	53784	53	192.168.2.5	8.8.8.8
May 4, 2021 17:17:22.654594898 CEST	53	53784	8.8.8.8	192.168.2.5
May 4, 2021 17:17:23.071007013 CEST	65307	53	192.168.2.5	8.8.8.8
May 4, 2021 17:17:23.112180948 CEST	64344	53	192.168.2.5	8.8.8.8
May 4, 2021 17:17:23.130151987 CEST	53	65307	8.8.8.8	192.168.2.5
May 4, 2021 17:17:23.163559914 CEST	53	64344	8.8.8.8	192.168.2.5
May 4, 2021 17:17:23.443809032 CEST	62060	53	192.168.2.5	8.8.8.8
May 4, 2021 17:17:23.492634058 CEST	53	62060	8.8.8.8	192.168.2.5
May 4, 2021 17:17:24.642558098 CEST	61805	53	192.168.2.5	8.8.8.8
May 4, 2021 17:17:24.694297075 CEST	53	61805	8.8.8.8	192.168.2.5
May 4, 2021 17:17:25.790116072 CEST	54795	53	192.168.2.5	8.8.8.8
May 4, 2021 17:17:25.838814974 CEST	53	54795	8.8.8.8	192.168.2.5
May 4, 2021 17:17:25.886300087 CEST	49557	53	192.168.2.5	8.8.8.8
May 4, 2021 17:17:25.943465948 CEST	53	49557	8.8.8.8	192.168.2.5
May 4, 2021 17:17:26.905867100 CEST	61733	53	192.168.2.5	8.8.8.8
May 4, 2021 17:17:26.960458040 CEST	53	61733	8.8.8.8	192.168.2.5
May 4, 2021 17:17:29.008280993 CEST	65447	53	192.168.2.5	8.8.8.8
May 4, 2021 17:17:29.070107937 CEST	53	65447	8.8.8.8	192.168.2.5
May 4, 2021 17:17:30.253631115 CEST	52441	53	192.168.2.5	8.8.8.8
May 4, 2021 17:17:30.305485964 CEST	53	52441	8.8.8.8	192.168.2.5
May 4, 2021 17:17:30.577924013 CEST	62176	53	192.168.2.5	8.8.8.8
May 4, 2021 17:17:30.631161928 CEST	53	62176	8.8.8.8	192.168.2.5
May 4, 2021 17:17:32.587939024 CEST	59596	53	192.168.2.5	8.8.8.8
May 4, 2021 17:17:32.656425953 CEST	53	59596	8.8.8.8	192.168.2.5
May 4, 2021 17:17:33.013144016 CEST	65296	53	192.168.2.5	8.8.8.8
May 4, 2021 17:17:33.064724922 CEST	53	65296	8.8.8.8	192.168.2.5
May 4, 2021 17:17:33.825314045 CEST	63183	53	192.168.2.5	8.8.8.8
May 4, 2021 17:17:33.886040926 CEST	53	63183	8.8.8.8	192.168.2.5
May 4, 2021 17:17:34.351999044 CEST	60151	53	192.168.2.5	8.8.8.8
May 4, 2021 17:17:34.417228937 CEST	53	60151	8.8.8.8	192.168.2.5
May 4, 2021 17:17:34.672514915 CEST	56969	53	192.168.2.5	8.8.8.8
May 4, 2021 17:17:34.723994970 CEST	53	56969	8.8.8.8	192.168.2.5
May 4, 2021 17:17:35.321125984 CEST	55161	53	192.168.2.5	8.8.8.8
May 4, 2021 17:17:35.369767904 CEST	53	55161	8.8.8.8	192.168.2.5
May 4, 2021 17:17:35.453356028 CEST	54757	53	192.168.2.5	8.8.8.8
May 4, 2021 17:17:35.515465021 CEST	53	54757	8.8.8.8	192.168.2.5
May 4, 2021 17:17:36.512840033 CEST	49992	53	192.168.2.5	8.8.8.8
May 4, 2021 17:17:36.573519945 CEST	53	49992	8.8.8.8	192.168.2.5
May 4, 2021 17:17:37.336000919 CEST	60075	53	192.168.2.5	8.8.8.8
May 4, 2021 17:17:37.388040066 CEST	53	60075	8.8.8.8	192.168.2.5
May 4, 2021 17:17:40.294874907 CEST	55016	53	192.168.2.5	8.8.8.8
May 4, 2021 17:17:40.343532085 CEST	53	55016	8.8.8.8	192.168.2.5
May 4, 2021 17:17:41.413710117 CEST	64345	53	192.168.2.5	8.8.8.8
May 4, 2021 17:17:41.465807915 CEST	53	64345	8.8.8.8	192.168.2.5
May 4, 2021 17:17:48.750657082 CEST	57128	53	192.168.2.5	8.8.8.8
May 4, 2021 17:17:48.809895992 CEST	53	57128	8.8.8.8	192.168.2.5
May 4, 2021 17:17:50.923748016 CEST	54791	53	192.168.2.5	8.8.8.8
May 4, 2021 17:17:50.998872042 CEST	53	54791	8.8.8.8	192.168.2.5
May 4, 2021 17:18:00.567071915 CEST	50463	53	192.168.2.5	8.8.8.8
May 4, 2021 17:18:00.620613098 CEST	53	50463	8.8.8.8	192.168.2.5
May 4, 2021 17:18:01.572004080 CEST	50463	53	192.168.2.5	8.8.8.8
May 4, 2021 17:18:01.625463009 CEST	53	50463	8.8.8.8	192.168.2.5
May 4, 2021 17:18:01.874799967 CEST	50394	53	192.168.2.5	8.8.8.8
May 4, 2021 17:18:01.933238029 CEST	53	50394	8.8.8.8	192.168.2.5
May 4, 2021 17:18:02.590485096 CEST	50463	53	192.168.2.5	8.8.8.8
May 4, 2021 17:18:02.624840021 CEST	58530	53	192.168.2.5	8.8.8.8
May 4, 2021 17:18:02.642205954 CEST	53	50463	8.8.8.8	192.168.2.5
May 4, 2021 17:18:02.673909903 CEST	53	58530	8.8.8.8	192.168.2.5
May 4, 2021 17:18:02.865133047 CEST	50394	53	192.168.2.5	8.8.8.8
May 4, 2021 17:18:02.913945913 CEST	53	50394	8.8.8.8	192.168.2.5
May 4, 2021 17:18:03.879930019 CEST	50394	53	192.168.2.5	8.8.8.8
May 4, 2021 17:18:03.928689003 CEST	53	50394	8.8.8.8	192.168.2.5
May 4, 2021 17:18:04.826987982 CEST	50463	53	192.168.2.5	8.8.8.8
May 4, 2021 17:18:04.879061937 CEST	53	50463	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 17:18:05.895569086 CEST	50394	53	192.168.2.5	8.8.8.8
May 4, 2021 17:18:05.944274902 CEST	53	50394	8.8.8.8	192.168.2.5
May 4, 2021 17:18:08.834618092 CEST	50463	53	192.168.2.5	8.8.8.8
May 4, 2021 17:18:08.886136055 CEST	53	50463	8.8.8.8	192.168.2.5
May 4, 2021 17:18:09.895793915 CEST	50394	53	192.168.2.5	8.8.8.8
May 4, 2021 17:18:09.945930958 CEST	53	50394	8.8.8.8	192.168.2.5
May 4, 2021 17:18:18.517640114 CEST	53813	53	192.168.2.5	8.8.8.8
May 4, 2021 17:18:18.574867964 CEST	53	53813	8.8.8.8	192.168.2.5
May 4, 2021 17:18:54.927655935 CEST	63732	53	192.168.2.5	8.8.8.8
May 4, 2021 17:18:54.990108967 CEST	53	63732	8.8.8.8	192.168.2.5
May 4, 2021 17:19:18.991050959 CEST	57344	53	192.168.2.5	8.8.8.8
May 4, 2021 17:19:19.043968916 CEST	53	57344	8.8.8.8	192.168.2.5
May 4, 2021 17:19:44.496299982 CEST	54450	53	192.168.2.5	8.8.8.8
May 4, 2021 17:19:44.570121050 CEST	53	54450	8.8.8.8	192.168.2.5
May 4, 2021 17:19:54.716213942 CEST	59261	53	192.168.2.5	8.8.8.8
May 4, 2021 17:19:54.779120922 CEST	53	59261	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 17:17:33.013144016 CEST	192.168.2.5	8.8.8.8	0xc483	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
May 4, 2021 17:17:33.825314045 CEST	192.168.2.5	8.8.8.8	0x1cfb	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
May 4, 2021 17:17:34.672514915 CEST	192.168.2.5	8.8.8.8	0x5fad	Standard query (0)	use.fontawesome.com	A (IP address)	IN (0x0001)
May 4, 2021 17:17:35.453356028 CEST	192.168.2.5	8.8.8.8	0x5dce	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
May 4, 2021 17:17:48.750657082 CEST	192.168.2.5	8.8.8.8	0xf997	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 17:17:33.064724922 CEST	8.8.8.8	192.168.2.5	0xc483	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 17:17:33.886040926 CEST	8.8.8.8	192.168.2.5	0x1cfb	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
May 4, 2021 17:17:33.886040926 CEST	8.8.8.8	192.168.2.5	0x1cfb	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
May 4, 2021 17:17:34.723994970 CEST	8.8.8.8	192.168.2.5	0x5fad	No error (0)	use.fontawesome.com	fontawesome-cdn.fonticons.netdna-cdn.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 17:17:34.723994970 CEST	8.8.8.8	192.168.2.5	0x5fad	No error (0)	fontawesome-cdn.fonticons.netdna-cdn.com		23.111.9.35	A (IP address)	IN (0x0001)
May 4, 2021 17:17:35.515465021 CEST	8.8.8.8	192.168.2.5	0x5dce	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
May 4, 2021 17:17:35.515465021 CEST	8.8.8.8	192.168.2.5	0x5dce	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
May 4, 2021 17:17:48.809895992 CEST	8.8.8.8	192.168.2.5	0xf997	No error (0)	aadcdn.msftauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 17:17:48.809895992 CEST	8.8.8.8	192.168.2.5	0xf997	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 17:17:33.994791031 CEST	104.18.11.207	443	192.168.2.5	49712	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, 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	Mon Mar 01 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Tue Mar 01 00:59:59 CET 2022 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		
May 4, 2021 17:17:34.002868891 CEST	104.18.11.207	443	192.168.2.5	49711	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, 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	Mon Mar 01 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Tue Mar 01 00:59:59 CET 2022 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		
May 4, 2021 17:17:35.187772989 CEST	23.111.9.35	443	192.168.2.5	49715	CN=*.fontawesome.com, O=Fonticons Inc, L=Bentonville, ST=Arkansas, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, 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	Fri Nov 13 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Wed Dec 15 00:59:59 CET 2021 Tue Sep 24 01:59:59 CEST 2030 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 TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					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		
May 4, 2021 17:17:35.217097998 CEST	23.111.9.35	443	192.168.2.5	49716	CN=*.fontawesome.com, O=Fonticons Inc, L=Bentonville, ST=Arkansas, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, 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	Fri Nov 13 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Wed Dec 15 00:59:59 CET 2021 Tue Sep 24 01:59:59 CEST 2030 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 TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					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
May 4, 2021 17:17:35.622600079 CEST	104.16.18.94	443	192.168.2.5	49718	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		
May 4, 2021 17:17:35.622662067 CEST	104.16.18.94	443	192.168.2.5	49719	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		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6424 Parent PID: 792

General

Start time:	17:17:29
Start date:	04/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6462e0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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: 6480 Parent PID: 6424

General

Start time:	17:17:30
Start date:	04/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6424 CREDAT:17410 /prefetch:2
Imagebase:	0x930000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly